Acronis

acronis.com

Cyber Protection

24.03

Manuale dell'utente

REVISIONE: 11/04/2024

Sommario

Introduzione a Cyber Protection **19**
Attivazione dell'account 19
Requisiti per la password 19
Autenticazione a due fattori 19
Impostazioni di privacy 21
Accesso al servizio Cyber Protection 22
Requisiti software 23
Browser Web supportati 23
Sistemi operativi e ambienti supportati 23
Versioni supportate di Microsoft SQL Server 30
Versioni supportate di Microsoft Exchange Server 30
Versioni di Microsoft SharePoint supportate 31
Versioni di Oracle Database supportate 31
Versioni di SAP HANA supportate 31
Versioni di MySQL supportate 32
Versioni di MariaDB supportate 32
Piattaforme di virtualizzazione supportate 32
Compatibilità con il software di crittografia 42
Compatibilità con gli storage Dell EMC Data Domain 43
Funzionalità di protezione supportate in base al sistema operativo 44
Sistemi operativi e versioni supportati 45
File system supportati 54
Operazioni supportate con i volumi logici 57
Backup 57
Ripristino 57
Installazione e deployment di agenti Cyber Protection **59**
Preparazione 59
Passaggio 1 59
Passaggio 2 59
Passaggio 3 59
Passaggio 4 59
Passaggio 5 60
Passaggio 6 61
Di quale agente occorre disporre? 62
Backup con agente e agentless 66

© Acronis International GmbH, 2003-2024

Quale tipo di backup scegliere? 66
Requisiti di sistema per agenti 66
Pacchetti di Linux 69
I pacchetti richiesti sono già installati? 69
Installazione di pacchetti dal repository 70
Installazione manuale dei pacchetti 71
Configurazione delle impostazioni del server proxy 72
Installazione degli agenti di protezione 76
Download degli agenti di protezione 77
Installazione degli agenti di protezione in Windows 77
Installazione degli agenti di protezione in Linux 80
Installazione degli agenti di protezione in macOS 82
Concedere le autorizzazioni di sistema richieste a Connect Agent 84
Modifica dell'account di accesso su sistemi Windows 85
Installazione e disinstallazione dinamica di componenti 87
Installazione o disinstallazione automatica 88
Installazione o disinstallazione automatica in Windows 88
Esempi 89
Esempio 90
Esempi 90
Esempi 98
Esempio 100
Esempi 100
Installazione o disinstallazione automatica in Linux 106
Installazione e disinstallazione automatica in macOS 112
Registrazione e annullamento della registrazione di workload in modalità manuale 122
Password con caratteri speciali o spazi 126
Modifica della registrazione di un workload 126
Individuazione automatica dei sistemi 127
Prerequisiti 127
Funzionamento dell'individuazione automatica 128
Funzionamento dell'installazione remota di agenti 130
Esecuzione dell'individuazione automatica e dell'individuazione manuale 130
Gestione dei sistemi individuati 136
Risoluzione dei problemi 137
Distribuzione dell'Agente per VMware (Virtual Appliance) 138
Prima di iniziare 138

© Acronis International GmbH, 2003-2024

Distribuzione del modello OVF ... 139
Configurazione dell'appliance virtuale ... 139
Distribuzione dell'Agente per Scale Computing HC3 (appliance virtuale) ... 142
Prima di iniziare ... 142
Distribuzione del modello QCOW2 ... 143
Configurazione dell'appliance virtuale ... 144
Agente per Scale Computing HC3 - ruoli necessari ... 147
Distribuzione dell'Agente per Virtuozzo Hybrid Infrastructure (appliance virtuale) ... 148
Prima di iniziare ... 148
Configurazione delle reti in Virtuozzo Hybrid Infrastructure ... 149
Configurazione degli account utente in Virtuozzo Hybrid Infrastructure ... 149
Distribuzione del modello QCOW2 ... 152
Configurazione dell'appliance virtuale ... 153
Distribuzione dell'Agente per oVirt (Virtual Appliance) ... 156
Prima di iniziare ... 156
Distribuzione del modello OVA ... 158
Configurazione dell'appliance virtuale ... 159
Agente per oVirt – ruoli e porte richiesti ... 162
Distribuzione dell'Agente per Synology ... 163
Prima di iniziare ... 163
Download del programma di installazione ... 164
Installazione dell'Agente per Synology ... 164
Aggiornamento di Agente per Synology ... 169
Distribuzione di agenti tramite i Criteri di gruppo ... 171
Prerequisiti ... 171
Generazione del token di registrazione ... 172
Creazione del file di trasformazione ed estrazione dei pacchetti di installazione ... 175
Impostazione dell'oggetto Criteri di gruppo ... 176
Connessioni SSH a un'appliance virtuale ... 177
Avvio del daemon Secure Shell ... 177
Impostazione della password radice su un'appliance virtuale ... 177
Accesso a un'appliance virtuale tramite un client SSH ... 178
Aggiornamento di agenti ... 178
Aggiornamento manuale degli agenti ... 179
Aggiornamento automatico degli agenti ... 181
Aggiornamento degli agenti sui workload protetti da BitLocker ... 183
Impedire la disinstallazione o la modifica non autorizzate degli agenti ... 183

© Acronis International GmbH, 2003-2024

Disinstallazione di agenti ... 185
Impostazioni di protezione ... 186
Aggiornamenti automatici dei componenti ... 187
Aggiornamento delle definizioni di Cyber Protection in base alla pianificazione ... 188
Aggiornamento delle definizioni di Cyber Protection su richiesta ... 188
Archiviazione cache ... 188
Modifica della quota di servizio dei sistemi ... 189
Servizi di Cyber Protection installati nell'ambiente ... 190
Servizi installati in Windows ... 191
Servizi installati in macOS ... 191
Salvataggio di un file del registro agente ... 191
Open VPN site-to-site - Informazioni aggiuntive ... 192
Gestione delle licenze per i management server in locale ... 198
Definizione degli elementi da proteggere e delle modalità di protezione ... 199
Scheda Gestione ... 199
Stati del piano ... 199
Piani di protezione ... 200
Piani di backup per applicazioni cloud ... 200
Piani di scansione del backup ... 200
Elaborazione dei dati al di fuori dell'host ... 201
Heartbeat MV ... 209
Convalida screenshot ... 210
Snapshot intermedi ... 217
Piani e moduli di protezione ... 217
Creazione di un piano di protezione ... 218
Azioni eseguibili con i piani di protezione ... 220
Risoluzione dei conflitti tra piani ... 224
Piani di protezione predefiniti ... 225
Piani di protezione individuali per le integrazioni con pannelli di controllo per l'hosting ... 232
#CyberFit Score dei sistemi ... 233
Come funziona ... 233
Esecuzione di una scansione #CyberFit Score ... 237
Cyber Scripting ... 239
Prerequisiti ... 239
Limitazioni ... 239
Piattaforme supportate ... 239
Ruoli utente e diritti di Cyber Scripting ... 240

© Acronis International GmbH, 2003-2024

Script ... 242
Repository di script ... 252
Piani di scripting ... 253
Esecuzione rapida dello script ... 262
Protezione di applicazioni di collaborazione e comunicazione ... 263
Comprensione del livello attuale di protezione ... 265
Monitoraggio ... 265
Pannello di controllo Panoramica ... 265
Dashboard Attività ... 266
Dashboard Avvisi ... 267
Tipi di avviso ... 268
Widget di avviso ... 289
Cyber Protection ... 290
Stato protezione ... 290
Widget di Endpoint Detection and Response (EDR) ... 291
#CyberFit Score per sistema ... 295
Monitoraggio integrità del disco ... 296
Mappa di protezione dati ... 300
Widget di valutazione delle vulnerabilità ... 301
Widget di installazione patch ... 303
Informazioni sulla scansione del backup ... 304
Recentemente interessato ... 305
Applicazioni cloud ... 305
Widget Inventario software ... 306
Widget Inventario hardware ... 307
Widget sessioni remote ... 308
Protezione intelligente ... 309
Scheda Attività ... 316
Cyber Protect Monitor ... 317
Configurazione delle impostazioni del server proxy in Cyber Protect Monitor ... 318
Report ... 319
Azioni con i report ... 320
Dati inseriti nel report in base al tipo di widget ... 322
Gestione di workload nella console di Cyber Protect ... 325
La console di Cyber Protect ... 325
Novità della console di Cyber Protect ... 326
Utilizzo della console di Cyber Protect come amministratore di partner ... 327

© Acronis International GmbH, 2003-2024

Prerequisiti ... 331
Workload ... 335
Aggiunta di workload alla console di Cyber Protect ... 336
Eliminazione di workload dalla console di Cyber Protect ... 341
Gruppi dispositivi ... 345
Gruppi integrati e gruppi personalizzati ... 346
Gruppi statici e gruppi dinamici ... 346
Gruppi cloud-to-cloud e gruppi non cloud-to-cloud ... 347
Creazione di un gruppo statico ... 348
Aggiunta di workload a un gruppo statico ... 349
Creazione di un gruppo dinamico ... 350
Modifica di un gruppo dinamico ... 368
Eliminare un gruppo ... 369
Applicazione di un piano a gruppo ... 369
Revocare un piano da un gruppo ... 370
Lavorare con il modulo Controllo dispositivo ... 371
Utilizzo del modulo Controllo dispositivo ... 374
Impostazioni di accesso ... 381
Lista di tipi di dispositivo consentiti ... 386
Lista di dispositivi USB consentiti ... 387
Esclusione di processi dal controllo dell'accesso ... 392
Avvisi di Controllo dispositivo ... 394
Cancellazione dei dati da un workload gestito ... 398
Visualizzazione di workload gestiti dalle integrazioni RMM ... 399
Workload CyberApp ... 400
Workload aggregati ... 400
Lavorare con workload CyberApp ... 400
Lavorare con workload aggregati ... 401
Collegare workload a utenti specifici ... 402
Trovare l'ultimo utente connesso ... 403
Gestione del backup e del ripristino di workload e file ... 404
Backup ... 404
Panoramica del piano di protezione ... 406
Selezione dei dati del backup ... 409
Selezione di un intero sistema ... 409
Selezione di dischi o volumi ... 409
Selezione di file e cartelle ... 412

© Acronis International GmbH, 2003-2024

Selezione dello stato di sistema ... 415
Selezione della configurazione ESXi ... 415
Protezione continua dei dati (CDP) ... 416
Come funziona ... 417
Origini dati supportate ... 418
Destinazioni supportate ... 419
Configurazione di un backup CDP ... 419
Selezione di una destinazione ... 420
Opzione di archiviazione avanzata ... 421
Informazioni su Secure Zone ... 422
Pianificazione del backup ... 425
Schemi di backup ... 425
Tipi di backup ... 427
Esecuzione di un backup da una pianificazione ... 428
Esecuzione manuale di un backup ... 442
Regole di conservazione ... 443
Suggerimenti importanti ... 443
Regole di conservazione in base allo schema di backup ... 444
Configurazione delle regole di conservazione ... 446
Replica ... 447
Esempi di utilizzo ... 447
Posizioni supportate ... 448
Crittografia ... 449
Configurazione della crittografia nel piano di protezione ... 449
Configurazione della crittografia come proprietà del sistema ... 450
Autenticazione ... 452
Come utilizzare l'autenticazione ... 452
Come funziona ... 452
Opzioni di backup predefinite ... 453
Opzioni di backup ... 453
Disponibilità delle opzioni di backup ... 453
Avvisi ... 456
Consolidamento backup ... 456
Nome file di backup ... 457
Formato backup ... 462
Convalida del backup ... 463
Changed block tracking (CBT) ... 464

© Acronis International GmbH, 2003-2024

Modalità backup cluster ... 464
Livello di compressione ... 466
Gestione degli errori ... 466
Backup incrementale/differenziale veloce ... 467
Filtri file (Inclusioni/Esclusioni) ... 468
Istantanea di backup a livello di file ... 470
Dati forensi ... 470
Troncamento registro ... 479
Creazione snapshot LVM ... 480
Punti di montaggio ... 480
Snapshot multivolume ... 481
One-click Recovery ... 482
Prestazioni e finestra di backup ... 486
Consegna fisica dei dati ... 490
Comandi pre/post ... 491
Comandi prima/dopo la cattura dei dati ... 493
Programmazione ... 496
Backup settore per settore ... 497
Suddivisione ... 497
Gestione fallimento dell'attività ... 498
Condizioni di avvio dell'attività ... 498
Servizio Copia Shadow del volume (VSS) ... 499
Servizio Copia Shadow del volume per macchine virtuali ... 501
Backup settimanale ... 503
Registro eventi di Windows ... 503
Ripristino ... 503
Panoramica del ripristino ... 503
Ripristino sicuro ... 506
Ripristino di una macchina ... 507
Preparazione delle unità ... 517
Verificare l'accesso ai driver nell'ambiente di avvio ... 517
Ricerca automatica dei driver ... 517
Driver di archiviazione di massa da installare in ogni caso ... 518
Ripristino di file ... 519
Ripristino dello stato del sistema ... 526
Ripristino della configurazione ESXi ... 527
Opzioni di ripristino ... 528

© Acronis International GmbH, 2003-2024

Operazioni con backup ... 536
La scheda Archivio di backup ... 536
Montaggio di volumi da un backup ... 538
Convalida di backup ... 540
Esportazione di backup ... 541
Eliminazione di backup ... 542
Analisi del rilevamento dei colli di bottiglia ... 544
Backup di workload su cloud pubblici ... 548
Definizione di una posizione di backup in Microsoft Azure ... 548
Definizione di una posizione di backup in Amazon S3 ... 551
Definizione di una posizione di backup in Wasabi ... 553
Visualizzazione e aggiornamento delle posizioni di backup nel cloud pubblico ... 555
Gestione dell'accesso agli account di cloud pubblico ... 556
Protezione delle applicazioni Microsoft ... 567
Protezione di Microsoft SQL Server e Microsoft Exchange Server ... 567
Protezione di Microsoft SharePoint ... 567
Protezione di un controller di dominio ... 568
Ripristino delle applicazioni ... 568
Prerequisiti ... 569
Backup di database ... 571
Backup compatibile con l’applicazione ... 577
Backup caselle di posta ... 579
Ripristino di database SQL ... 581
Ripristino dei database di Exchange ... 590
Ripristino di caselle di posta di Exchange e relativi elementi ... 592
Modificare le credenziali di accesso a SQL Server o al server di Exchange ... 599
Protezione dei dispositivi mobili ... 600
Dispositivi mobili supportati ... 600
Elementi di cui è possibile eseguire il backup ... 600
Informazioni fondamentali ... 600
Per scaricare l'app Cyber Protect ... 601
Per avviare il backup dei dati ... 602
Per ripristinare i dati in un dispositivo mobile ... 602
Come rivedere i dati tramite la console di Cyber Protect ... 603
Protezione dei dati per Exchange ospitato ... 604
Di quali elementi è possibile eseguire il backup? ... 604
Quali elementi è possibile ripristinare? ... 604

© Acronis International GmbH, 2003-2024

Selezione delle caselle di posta di Exchange Online ... 605
Ripristino di caselle postali e di elementi delle caselle postali ... 605
Protezione dei dati di Microsoft 365 ... 608
Perché eseguire il backup dei dati di Microsoft 365? ... 608
Agente cloud e agente locale ... 608
Diritti utente necessari ... 611
Limitazioni ... 612
Report sul licensing delle utenze di Microsoft 365 ... 613
Registrazione ... 613
Utilizzo dell'Agente installato in locale per Office 365 ... 613
Utilizzo dell'Agente cloud per Microsoft 365 ... 618
Protezione dei dati di Google Workspace ... 654
Cosa si intende con protezione dei dati di Google Workspace? ... 654
Diritti utente necessari ... 654
Informazioni sulla pianificazione dei backup ... 655
Limitazioni ... 655
Registrazione ... 656
Aggiunta di un'organizzazione Google Workspace ... 656
Creazione di un progetto personale Google Cloud ... 657
Individuazione delle risorse di Google Workspace ... 660
Impostazione della frequenza dei backup di Google Workspace ... 661
Protezione dei dati di Gmail ... 662
Protezione di file di Google Drive ... 666
Protezione di file di unità condivise ... 671
Autenticazione ... 675
Ricerca nei backup cloud-to-cloud ... 676
Ricerca testo completo ... 677
Indici di ricerca ... 678
Verifica della dimensione di un indice di ricerca ... 678
Aggiornare, ricompilare o eliminare gli indici ... 678
Abilitazione della ricerca avanzata nei backup crittografati ... 680
Abilitazione o disabilitazione della ricerca avanzata nei piani esistenti ... 680
Disabilitazione della ricerca a tutto testo per i backup di Gmail ... 681
Protezione per Oracle Database ... 681
Protezione di SAP HANA ... 681
Protezione dei dati di MySQL e MariaDB ... 682
Configurare un backup application-aware ... 683

© Acronis International GmbH, 2003-2024

Ripristino dei dati da un backup application-aware ... 684
Protezione di siti Web e di server di hosting ... 689
Protezione di siti Web ... 689
Protezione di server di hosting su Web ... 692
Operazioni speciali con le macchine virtuali ... 693
Esecuzione di una macchina virtuale da un backup (Ripristino istantaneo) ... 693
Lavorare in VMware vSphere ... 697
Backup di sistemi Hyper-V in cluster ... 717
Limitare il numero totale di macchine virtuali di cui viene eseguito il backup simultaneo ... 718
Migrazione della macchina ... 719
Backup di virtual machine Microsoft Azure e Amazon EC2 ... 723
Creazione di un supporto di avvio per recuperare i sistemi operativi ... 724
Qual è la differenza tra un supporto di avvio personalizzato e uno pronto all'uso? ... 724
Qual è la differenza tra un supporto di avvio basato su Linux o uno basato su WinPE? ... 725
Creazione di un supporto di avvio fisico ... 725
Generatore di supporti riavviabili ... 726
Ripristino dall'archiviazione cloud ... 730
Ripristino da una condivisione di rete ... 730
File di uno script ... 731
Struttura di autostart.json ... 732
Oggetto di livello superiore ... 732
Oggetto variabile ... 732
Tipo di Controllo ... 733
Connessione a un sistema avviato da un supporto di avvio ... 740
Operazioni locali con un supporto di avvio ... 741
Operazioni remoto con un supporto di avvio ... 743
Startup Recovery Manager ... 746
Implementazione del disaster recovery ... 749
Informazioni su Cyber Disaster Recovery Cloud ... 749
Funzionalità principali ... 749
Requisiti software ... 750
Sistemi operativi supportati ... 750
Piattaforme di virtualizzazione supportate ... 750
Limitazioni ... 751
Versione in trial di Cyber Disaster Recovery Cloud ... 752
Limitazioni durante l'utilizzo di Geo-redundant Cloud Storage ... 753
Compatibilità di Disaster Recovery con il software di crittografia ... 753

© Acronis International GmbH, 2003-2024

Punti di calcolo ... 753
Configurazione della funzionalità di disaster recovery ... 755
Creare un piano di protezione di disaster recovery ... 755
Modifica dei parametri predefiniti del server di ripristino ... 757
Infrastruttura di rete cloud ... 758
Configurazione della connessione ... 759
Concetti sulla rete ... 759
Configurazione della connessione iniziale ... 770
Prerequisiti ... 773
Gestione della rete ... 779
Prerequisiti ... 795
Configurazione dei server di ripristino ... 796
Creazione di un server di ripristino ... 796
Funzionamento del processo di failover ... 799
Funzionamento del processo di failback ... 807
Prerequisiti ... 810
Prerequisiti ... 814
Operare con backup crittografati ... 818
Operazioni con virtual machine di Microsoft Azure ... 819
Configurazione dei server primari ... 819
Creazione di un server primario ... 819
Operazioni con un server primario ... 822
Gestione dei server cloud ... 822
Regole del firewall per i server cloud ... 823
Impostazione delle regole del firewall per server cloud ... 824
Controllo delle attività del firewall cloud ... 827
Backup dei server cloud ... 827
Orchestrazione (runbook) ... 828
Perché utilizzare i runbook? ... 828
Creazione di runbook ... 829
Operazioni con i runbook ... 832
Configurazione della protezione antivirus e anti-malware ... 835
Piattaforme supportate ... 835
Funzionalità supportate per piattaforma ... 836
Protezione antivirus e anti-malware ... 839
Funzionalità anti-malware ... 839
Tipi di scansione ... 839

© Acronis International GmbH, 2003-2024

Impostazioni di Protezione antivirus e anti-malware ... 840
Active Protection nell'edizione Cyber Backup Standard ... 857
Impostazioni di Active Protection in Cyber Backup Standard ... 857
Filtro URL ... 865
Come funziona ... 865
Flusso di lavoro di configurazione del filtro URL ... 867
Impostazioni Filtro URL ... 867
Descrizione ... 874
Microsoft Defender Antivirus e Microsoft Security Essentials ... 874
Pianifica scansione ... 874
Azioni predefinite ... 875
Protezione in tempo reale ... 875
Avanzato ... 876
Esclusioni ... 877
Gestione firewall ... 877
Quarantena ... 878
Come vengono spostati i file nella cartella Quarantena? ... 878
Gestione dei file in quarantena ... 879
Posizione della cartella Quarantena nei sistemi ... 879
Cartella personalizzata self-service su richiesta ... 880
Elenco degli elementi consentiti aziendale ... 880
Aggiunta automatica all'elenco degli elementi consentiti ... 880
Aggiunta manuale all'elenco degli elementi consentiti ... 881
Aggiunta di file in quarantena all'elenco degli elementi consentiti ... 881
Impostazioni dell'elenco degli elementi consentiti ... 881
Visualizzare informazioni sugli elementi dell'elenco degli elementi consentiti ... 881
Scansione anti-malware dei backup ... 882
Limitazioni ... 883
Lavorare con le funzionalità di protezione avanzata ... 884
Advanced Data Loss Prevention ... 886
Creazione della policy di flusso dei dati e delle regole della policy ... 886
Abilitazione di Advanced Data Loss Prevention nei piani di protezione ... 896
Rilevamento automatico della destinazione ... 900
Definizioni di dati sensibili ... 900
Eventi di prevenzione della perdita di dati ... 907
Widget di Advanced Data Loss Prevention nella dashboard Panoramica ... 908
Categorie di riservatezza personalizzate ... 909

© Acronis International GmbH, 2003-2024

Mappa dell'organizzazione ... 911
Problemi noti e limitazioni ... 914
Endpoint Detection and Response (EDR) ... 915
Perché Endpoint Detection and Response (EDR) è una soluzione necessaria ... 915
Abilitare la funzionalità Endpoint Detection and Response (EDR) ... 918
Come utilizzare la funzionalità Endpoint Detection and Response (EDR) ... 920
Visualizzazione dei problemi attualmente non risolti ... 924
Comprensione dell'ambito e dell'impatto dei problemi ... 925
Come orientarsi nelle fasi di attacco ... 934
Abilitazione della modalità di monitoraggio per Endpoint Detection and Response (EDR) ... 970
Come verificare il corretto funzionamento della funzionalità Endpoint Detection and Response (EDR) ... 972
Valutazione delle vulnerabilità e gestione delle patch ... 974
Valutazione delle vulnerabilità ... 974
Prodotti Microsoft e prodotti di terze parti supportati ... 975
Prodotti Apple e prodotti di terze parti supportati ... 976
Prodotti Linux supportati ... 977
Impostazioni di Valutazione delle vulnerabilità ... 977
Valutazione delle vulnerabilità per sistemi Windows ... 980
Valutazione delle vulnerabilità per sistemi Linux ... 980
Valutazione della vulnerabilità per dispositivi macOS ... 981
Gestione delle vulnerabilità individuate ... 981
Gestione patch ... 983
Flusso di lavoro di gestione delle patch ... 984
Impostazioni di gestione delle patch nel piano di protezione ... 985
Visualizzazione dell'elenco delle patch disponibili ... 990
Approvazione automatica della patch ... 992
Approvazione manuale delle patch ... 997
Installazione delle patch su richiesta ... 997
Gestione dell'inventario software e hardware ... 999
Inventario software ... 999
Abilitazione della scansione dell'inventario software ... 999
Esecuzione manuale di una scansione dell'inventario software ... 1000
Navigazione nell'inventario software ... 1000
Visualizzazione dell'inventario software di un singolo dispositivo ... 1002
Inventario hardware ... 1003
Abilitazione della scansione dell'inventario hardware ... 1004

© Acronis International GmbH, 2003-2024

Esecuzione manuale di una scansione dell'inventario hardware 1004
Navigazione nell'inventario hardware 1005
Visualizzazione dell'hardware di un singolo dispositivo 1008
Connessione a workload per attività di desktop remoto o assistenza remota 1010
Funzionalità di desktop remoto e assistenza remota supportate 1012
Piattaforme supportate 1014
Protocolli di connessione remota 1015
NEAR 1015
RDP 1016
Condivisione schermo di Apple 1016
Reindirizzamento audio remoto 1017
Connessioni a workload remoti per desktop remoto o assistenza remota 1018
Piani di gestione remota 1019
Creazione di un piano di gestione remota 1019
Aggiunta di un workload a un piano di gestione remota 1027
Rimozione di workload da un piano di gestione remota 1028
Ulteriori operazioni con i piani di gestione remota esistenti 1028
Problemi di compatibilità con i piani di gestione remota 1031
Risoluzione dei problemi di compatibilità con i piani di gestione remota 1031
Credenziali del workload 1032
Aggiunta di credenziali 1033
Assegnazione di credenziali a un workload 1034
Eliminazione delle credenziali 1034
Annullamento dell'assegnazione di credenziali da un workload 1034
Operare con workload gestiti 1035
Configurazione delle impostazioni RDP 1035
Connessione a workload gestiti per desktop remoto o assistenza remota 1036
Connetti a un workload gestito tramite client web 1039
Trasferimento di file 1039
Esecuzione di azioni di controllo sui workload gestiti 1040
Monitoraggio dei workload tramite la trasmissione di screenshot 1042
Osservazione di più workload gestiti simultaneamente 1043
Operare con workload non gestiti 1044
Connessione a workload non gestiti tramite Acronis Quick Assist 1044
Connessione a workload non gestiti tramite indirizzo IP 1045
Trasferimento di file tramite Acronis Quick Assist 1046
Utilizzo della barra degli strumenti nella finestra del visualizzatore 1047

© Acronis International GmbH, 2003-2024

Registrazione e riproduzione di sessioni remote ... 1049
Configurazione delle impostazioni di Connect Client ... 1050
Notifier del desktop remoto ... 1051
Monitoraggio dell'integrità e delle prestazioni dei workload ... 1053
Piani di monitoraggio ... 1053
Tipi di monitoraggio ... 1053
Monitoraggio basato sulle anomalie ... 1054
Piattaforme supportate per il monitoraggio ... 1054
Monitor configurabili ... 1054
Impostazioni del monitor Spazio su disco ... 1059
Impostazioni del monitor Temperatura CPU ... 1061
Impostazioni del monitor Temperatura GPU ... 1063
Impostazioni del monitor Modifiche hardware ... 1064
Impostazioni del monitor Utilizzo della CPU ... 1065
Impostazioni del monitor Utilizzo della memoria ... 1067
Impostazioni del monitor Velocità di trasferimento disco ... 1069
Impostazioni del monitor Utilizzo della rete ... 1072
Impostazioni del monitor Utilizzo della CPU per processo ... 1074
Impostazioni del monitor Utilizzo della memoria per processo ... 1075
Impostazioni del monitor Velocità di trasferimento disco per processo ... 1076
Impostazioni del monitor Utilizzo della rete per processo ... 1077
Impostazioni del monitor Stato dei servizi Windows ... 1079
Impostazioni del monitor Stato del processo ... 1079
Impostazioni del monitor Software installato ... 1080
Impostazioni del monitor Ultimo riavvio del sistema ... 1080
Impostazioni del monitor Registro eventi di Windows ... 1081
Impostazioni del monitor Dimensione file e cartelle ... 1082
Impostazioni del monitor Stato di Windows Update ... 1083
Impostazioni del monitor Stato del firewall ... 1083
Impostazioni del monitor Accessi non riusciti ... 1084
Impostazioni del monitor Stato del software anti-malware ... 1084
Impostazioni del monitor Stato della funzionalità di esecuzione automatica ... 1086
Impostazioni del monitor personalizzato ... 1086
Piani di monitoraggio ... 1088
Creazione di un piano di monitoraggio ... 1088
Aggiunta di workload ai piani di monitoraggio ... 1090
Revoca di piani di monitoraggio ... 1091

© Acronis International GmbH, 2003-2024

Configurazione delle azioni di risposta automatica ... 1091
Ulteriori operazioni con i piani monitoraggio ... 1094
Problemi di compatibilità con i piani monitoraggio ... 1096
Risoluzione dei problemi di compatibilità con i piani monitoraggio ... 1097
Reimpostazione dei modelli di machine learning ... 1098
Monitoraggio avvisi ... 1098
Configurazione degli avvisi di monitoraggio ... 1099
Variabili del monitoraggio avvisi ... 1100
Azioni di risposta manuali ... 1102
Visualizzazione degli avvisi di monitoraggio di un workload ... 1105
Visualizzazione del registro degli avvisi di monitoraggio ... 1106
Configurazione delle policy di notifica e-mail ... 1106
Visualizzazione dei dati di monitoraggio ... 1107
Widget dei monitor ... 1108
Strumenti Cyber Protection aggiuntivi ... 1110
Modalità Conformità ... 1110
Limitazioni ... 1110
Funzionalità non supportate ... 1110
Impostare la password di crittografia ... 1111
Modifica della password di crittografia ... 1111
Ripristino dei backup per i tenant in modalità Conformità ... 1112
Archivio immutabile ... 1112
Modalità dell'archivio immutabile ... 1112
Storage e agenti supportati ... 1113
Abilitazione dell'archivio immutabile ... 1113
Disabilitazione dell'archivio immutabile ... 1114
Accesso ai backup eliminati nell'archivio immutabile ... 1114
Storage con geo-ridondanza ... 1115
Abilitazione e disabilitazione dello storage con geo-ridondanza ... 1115
Stato della geo-replica ... 1116
Limitazioni ... 1116
Glossario ... 1117
Indice ... 1121

© Acronis International GmbH, 2003-2024

Introduzione a Cyber Protection

Attivazione dell'account

Quando un amministratore crea un account per l'utente, quest'ultimo riceve un messaggio al proprio indirizzo e-mail. Il messaggio contiene le seguenti informazioni:

- **Dati di login.** Il nome utente utilizzato per accedere. I dati di login vengono visualizzati anche nella pagina di attivazione dell'account.
- Pulsante **Attiva account**. Fare clic sul pulsante e impostare la password per l'account. Verificare che la password sia lunga almeno nove caratteri. Per ulteriori informazioni sulla password, fare riferimento a "Requisiti per la password" (pag. 19).

Se l'amministratore ha attivato l'autenticazione a due fattori, verrà richiesto di configurarla per l'account utente. Per ulteriori informazioni, fare riferimento a "Autenticazione a due fattori" (pag. 19).

Requisiti per la password

La password di un account utente deve essere lunga almeno 9 caratteri. Viene inoltre effettuato un controllo sulla complessità delle password, dopo il quale le password vengono collocate in una delle seguenti categorie:

- Vulnerabile
- Medio
- Complessa

Non è possibile salvare una password vulnerabile, anche se contiene 9 caratteri o più. Le password che ripetono il nome utente, il login, l'e-mail dell'utente o il nome del tenant al quale appartiene l'account utente sono considerate vulnerabili. Anche le password più comuni sono considerate vulnerabili.

Per rafforzare una password, aggiungere più caratteri. L'uso di più caratteri, come numeri, lettere maiuscole e minuscole e caratteri speciali non è obbligatorio, ma consente di creare password più complesse e anche più corte.

Autenticazione a due fattori

L'autenticazione a due fattori (2FA) fornisce una protezione aggiuntiva contro l'accesso non autorizzato all'account. Se è stata configurata l'autenticazione 2FA, per accedere alla console di Cyber Protect è necessario inserire la password (il primo fattore) e un codice temporaneo (il secondo fattore). Il codice temporaneo è generato da un'applicazione specifica che deve essere installata sullo smartphone o su un altro dispositivo dell'utente. Anche nel caso in cui qualcuno individui il login e la password dell'utente, non potrà accedere all'account senza utilizzare il dispositivo di secondo fattore.

© Acronis International GmbH, 2003-2024

Per configurare l'autenticazione a due fattori per l'account utente

È necessario configurare l'autenticazione a due fattori per l'account dell'utente se l'amministratore ha abilitato tale autenticazione per l'organizzazione. Se l'amministratore ha abilitato l'autenticazione a due fattori mentre l'utente è collegato alla console di Cyber Protect, l'utente dovrà configurarla alla scadenza della sessione corrente.

Prerequisiti

- L'autenticazione a due fattori è abilitata per l'organizzazione da un amministratore.

Per configurare l'autenticazione a due fattori per l'account utente

1. Installare un'app di autenticazione sul dispositivo mobile.
   Sono esempi di app di autenticazione:
   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
2. Scansionare il codice QR utilizzando l'app di autenticazione, quindi inserire il codice a 6 cifre visualizzato nell'app di autenticazione nella finestra **Configurare l'autenticazione a due fattori**.
3. Fare clic su **Avanti**.
   Vengono visualizzate le istruzioni su come ripristinare l'accesso all'account se si smarrisce il dispositivo di secondo fattore o si disinstalla l'app di autenticazione.
4. Salvare o stampare il file PDF.

   Nota
   Accertarsi di salvare il file PDF in un luogo sicuro o stamparlo per riferimento futuro. Questa procedura è il modo migliore per ripristinare l'accesso.

5. Tornare alla pagina di login della console di Cyber Protect e inserire il codice generato.
   Il codice temporaneo resta valido per 30 secondi. Se trascorrono più di 30 secondi, utilizzare il codice successivo.

Al successivo accesso è possibile selezionare la casella di controllo per **Considerare il browser attendibile**. In questo modo, non è necessario inserire il codice quando si accede utilizzando il browser definito su questo sistema.

Nota
Si consiglia di non selezionare questa casella di controllo. Altrimenti, si perde l'accesso con l'autenticazione a due fattori per l'account.

Per ripristinare l'autenticazione a due fattori (2FA) su un nuovo dispositivo

Se è possibile accedere all'app di autenticazione mobile precedentemente installata

© Acronis International GmbH, 2003-2024

1. Installare un'app di autenticazione sul nuovo dispositivo.
2. Utilizzare il file PDF salvato al momento della configurazione dell'autenticazione 2FA nel dispositivo. Questo file contiene il codice a 32 cifre che deve essere inserito nell'app di autenticazione per collegarla di nuovo all'account Acronis.

   Importante
   Se il codice non funziona, accertarsi di aver sincronizzato l'orario nell'app di autenticazione mobile con quello del dispositivo.

   Se al momento della configurazione non è stato salvato il file PDF:

a. Fare clic su **Reimposta l'autenticazione 2FA** e inserire la password temporanea mostrata nell'app di autenticazione mobile.
b. Seguire le istruzioni a video.

Se non è possibile accedere all'app di autenticazione mobile precedentemente installata

1. Prendere un nuovo dispositivo mobile.
2. Utilizzare il file PDF archiviato per collegare un nuovo dispositivo (il nome predefinito del file è `cyberprotect-2fa-backupcode.pdf`).
3. Ripristinare l'accesso all'account dal backup. Verificare che l'app mobile supporti i backup.
4. Aprire l'app con lo stesso account da un altro dispositivo mobile se è supportato dall'app.

Impostazioni di privacy

Le impostazioni di privacy aiutano a indicare se si è fornito o meno il consenso alla raccolta, all'uso e alla diffusione delle proprie informazioni personali.

A seconda del paese in cui si utilizza Cyber Protect Cloud e il data center Cyber Protect Cloud che fornisce servizi all'utente, all'avvio iniziale di Cyber Protect Cloud può essere chiesto di confermare se si accetta l'uso di Google Analytics in Cyber Protect Cloud.

Google Analytics ci aiuta a comprendere meglio i comportamenti degli utenti e a migliorare l'esperienza utente con Cyber Protect Cloud raccogliendo dati presentati con l'uso di pseudonimi.

Se Google Analytics è stato abilitato o rifiutato durante l'avvio iniziale di Cyber Protect Cloud, l'utente potrà modificare la decisione in un momento successivo.

Per abilitare o disabilitare Google Analytics

1. Nella console di Cyber Protect, fare clic su **Gestisci account**.
2. Fare clic sull'icona dell'account nell'angolo in alto a destra.
3. Selezionare **Impostazioni di privacy personali**. Viene visualizzata la finestra **Impostazioni di privacy personali**.
4. Nella sezione **Raccolta dati tramite Google Analytics** selezionare uno dei seguenti pulsanti:

© Acronis International GmbH, 2003-2024

- **On** per abilitare Google Analytics
- **Off** per disabilitare Google Analytics

Nella sezione **Come eliminare i cookie** è possibile controllare e gestire i cookie direttamente dal browser.

Nota
Se la sezione Google Analytics non è visibile, è probabile che il prodotto non sia utilizzato nel paese dell'utente.

Nella sezione **Onboarding e guida interattiva all'interno del prodotto**, mostrato all'inizio del periodo di prova, è possibile indicare se continuare o meno a ricevere informazioni sulle migliorie e le nuove funzionalità del programma. La funzionalità è abilitata per impostazione predefinita, ma è possibile disabilitarla spostando l'interruttore su **Off**.

Accesso al servizio Cyber Protection

Dopo aver attivato l'account, è possibile accedere al servizio Cyber Protection effettuando il login nella console di Cyber Protect o tramite il portale di gestione.

Per accedere alla console di Cyber Protect

1. Passare alla pagina di accesso al servizio Cyber Protection.
2. Digitare il login e quindi fare clic su **Avanti**.
3. Digitare la password e quindi fare clic su **Avanti**.
4. [Se si utilizza più di un servizio Cyber Protect Cloud] Fare clic su **Cyber Protection**.
   Gli utenti che hanno accesso solo al servizio Cyber Protection accedono direttamente alla console di Cyber Protect.
   Se il servizio **Cyber Protection** non è l'unico a cui si può accedere, è possibile passare da un servizio all'altro usando l'icona nell'angolo in alto a destra. Gli amministratori possono usare questa icona anche per passare al portale di gestione.

Il periodo di timeout per la console di Cyber Protect è di 24 ore per le sessioni attive e di un'ora per le sessioni inattive.

È possibile cambiare la lingua dell'interfaccia web facendo clic sull'icona dell’account nell'angolo in alto a destra.

Per accedere alla console di Cyber Protect dal portale di gestione

1. Nel portale di gestione passare a **Monitoraggio** > **Utilizzo**.
2. In **Cyber Protect**, selezionare **Protezione** quindi fare clic su **Gestisci servizio**.
   In alternativa, in **Clienti**, selezionare un cliente e quindi fare clic su **Gestisci servizio**.

L'utente viene reindirizzato alla console di Cyber Protect.

© Acronis International GmbH, 2003-2024

Importante
Se per il cliente è attiva la modalità di gestione **Self-service**, non sarà possibile gestire i servizi per suo conto. Solo gli amministratori del cliente possono modificare la modalità in **Gestito dal service provider** e a questo punto gestirne i servizi.

Per reimpostare la password

1. Passare alla pagina di accesso al servizio Cyber Protection.
2. Digitare il login e quindi fare clic su **Avanti**.
3. Fare clic su **Password dimenticata**
4. Confermare che si desidera ricevere ulteriori istruzioni facendo clic su **Invia**.
5. Seguire le istruzioni nell'e-mail ricevuta.
6. Impostare la nuova password.

Requisiti software

Browser Web supportati

La console di Cyber Protect utilizza il protocollo TLS 1.2 e supporta i browser web seguenti:

- Google Chrome 29 o versione successiva
- Mozilla Firefox 23 o versione successiva
- Opera 16 o versione successiva
- Microsoft Edge 25 o versioni successive
- Safari 8 o versioni successive in esecuzione nei sistemi operativi macOS e iOS

In altri browser Web (inclusi browser Safari eseguiti in altri sistemi operativi), l'interfaccia utente potrebbe essere visualizzata in modo non corretto o alcune funzioni potrebbero non essere disponibili.

Sistemi operativi e ambienti supportati

Agente per Windows

Questo agente include un componente per la Protezione antivirus e anti-malware e per il Filtro URL. Consultare "Funzionalità di protezione supportate in base al sistema operativo" (pag. 44) per informazioni sulle funzionalità supportate dai diversi sistemi operativi.

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows Server 2003 SP1/2003 R2 e versioni successive – Edizioni Standard ed Enterprise (x86, x64)

© Acronis International GmbH, 2003-2024

- Windows Small Business Server 2003/2003 R2
- Windows Server 2008, Windows Server 2008 SP2* – Edizioni Standard, Enterprise, Datacenter, Foundation e Web (x86, x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7 - tutte le edizioni

Nota
Per utilizzare Cyber Protection con Windows 7, è necessario installare i seguenti aggiornamenti Microsoft prima di installare l'agente di protezione:

- Windows 7 Extended Security Updates (ESU)
- KB4474419
- KB4490628

Per ulteriori informazioni sugli aggiornamenti richiesti, fare riferimento a questo articolo della Knowledge Base.

- Windows Server 2008 R2* – Edizioni Standard, Enterprise, Datacenter, Foundation e Web
- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011* – tutte le edizioni
- Windows 8/8.1 – tutte le edizioni (x86, x64), eccetto le edizioni Windows RT
- Windows Server 2012/2012 R2 - tutte le edizioni
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Edizioni Home, Pro, Education, Enterprise, IoT Enterprise e LTSC (in precedenza LTSB)
- Windows Server 2016 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2019 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows 11 - tutte le edizioni
- Windows Server 2022 - tutte le opzioni di installazione, ad eccezione di Nano Server

Nota
* Per utilizzare Cyber Protection con questa versione di Windows, è necessario installare l'aggiornamento del supporto per la firma del codice SHA2 da Microsoft (KB4474419) prima di installare l'agente di protezione.

Per informazioni sulle problematiche correlate all'aggiornamento del supporto per la firma del codice SHA2, fare riferimento a questo articolo della Knowledge Base.

© Acronis International GmbH, 2003-2024

Agente per SQL, Agente per Active Directory, Agente per Exchange (per il backup di database e il backup application-aware)

Ognuno di questi agenti può essere installato su una macchina con qualunque sistema operativo sopra elencato e una versione supportata della rispettiva applicazione.

Agente per la prevenzione della perdita di dati

Controllo dispositivo

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

Nota
L'Agente per la Prevenzione della perdita di dati per macOS supporta solo processori x64. I processori Apple Silicon ARM non sono supportati.

Prevenzione della perdita di dati

- Microsoft Windows 7 Service Pack 1 e versioni successive
- Microsoft Windows Server 2008 R2 e versioni successive

Nota
L'Agente per la Prevenzione della perdita di dati potrebbe essere installato su sistemi macOS non supportati in quanto parte integrante dell'Agente per Mac. In questo caso, la console di Cyber Protect mostra che l'Agente per la Prevenzione della perdita di dati è installato nel sistema, ma la funzionalità di controllo del dispositivo e di prevenzione della perdita dei dati è disattivata. Controllo dispositivo funziona infatti solo sui sistemi macOS supportati dall'Agente per la Prevenzione della perdita di dati.

Agente per Advanced Data Loss Prevention

- Microsoft Windows 7 Service Pack 1 e versioni successive
- Microsoft Windows Server 2008 R2 e versioni successive

Agente per File Sync & Share

Per un elenco dei sistemi operativi supportati, fare riferimento al Manuale utente di Cyber Files Cloud.

© Acronis International GmbH, 2003-2024

Agente per Exchange (per il backup delle caselle di posta)

- Windows Server 2008 - edizioni Standard, Enterprise, Datacenter, Foundation e Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 - tutte le edizioni
- Windows Server 2008 R2 - edizioni Standard, Enterprise, Datacenter, Foundation e Web
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 - tutte le edizioni
- Windows 8/8.1 – tutte le edizioni (x86, x64), eccetto le edizioni Windows RT
- Windows Server 2012/2012 R2 - tutte le edizioni
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 - edizioni Home, Pro, Education ed Enterprise
- Windows Server 2016 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2019 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows 11 - tutte le edizioni
- Windows Server 2022 - tutte le opzioni di installazione, ad eccezione di Nano Server

Agente per Microsoft 365

- Windows Server 2008 - edizioni Standard, Enterprise, Datacenter, Foundation e Web (solo x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2 - edizioni Standard, Enterprise, Datacenter, Foundation e Web
- Windows Home Server 2011
- Windows Small Business Server 2011 - tutte le edizioni
- Windows 8/8.1 - tutte le edizioni (solo x64), tranne le edizioni Windows RT
- Windows Server 2012/2012 R2 - tutte le edizioni
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (solo x64)
- Windows 10 - edizioni Home, Pro, Education ed Enterprise (solo x64)
- Windows Server 2016 – tutte le opzioni di installazione (solo x64), ad eccezione di Nano Server
- Windows Server 2019 – tutte le opzioni di installazione (solo x64), ad eccezione di Nano Server
- Windows 11 - tutte le edizioni
- Windows Server 2022 - tutte le opzioni di installazione, ad eccezione di Nano Server

© Acronis International GmbH, 2003-2024

Agente per Oracle

- Windows Server 2008 R2 - edizioni Standard, Enterprise, Datacenter e Web (x86, x64)
- Windows Server 2012 R2 - edizioni Standard, Enterprise, Datacenter e Web (x86, x64)
- Linux - qualsiasi kernel e distribuzione supportata dall'Agente per Linux (elencata di seguito)

Agente per MySQL/MariaDB

- Linux - qualsiasi kernel e distribuzione supportata dall'Agente per Linux (elencata di seguito)

Agente per Linux

Questo agente include un componente per la Protezione antivirus e anti-malware e per il Filtro URL. Consultare "Funzionalità di protezione supportate in base al sistema operativo" (pag. 44) per informazioni sulle funzionalità supportate dai diversi sistemi operativi.

Le seguenti distribuzioni e versioni del kernel Linux sono state testate in modo specifico. Tuttavia, anche se la distribuzione o la versione del kernel Linux in uso non è inclusa nell'elenco, è possibile lavorare correttamente in tutti gli scenari necessari, grazie alle specifiche dei sistemi operativi Linux.

Se si riscontrano problemi durante l'utilizzo di Cyber Protection con la combinazione della distribuzione e della versione del kernel Linux in uso, contattare il team di assistenza per ulteriori indagini.

Linux con kernel da 2.6.9 a 5.19 e glibc 2.3.4 o versione successiva, incluse le distribuzioni x86 e x86_64 seguenti:

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

  Importante
  Le configurazioni con Btrfs non sono supportate in SUSE Linux Enterprise Server 12 e SUSE Linux Enterprise Server 15.

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

© Acronis International GmbH, 2003-2024

Nota
L'installazione dell'agente di protezione su un sistema Oracle Linux 8.6 e versioni successive, sul quale è abilitato l'avvio sicuro, richiede la firma manuale dei moduli del kernel. Per ulteriori informazioni su come firmare un modulo del kernel, fare riferimento a questo articolo della Knowledge Base.

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

* A partire dalla versione 8.4, supportato solo con kernel da 4.18 a 5.19

Agente per Mac

Questo agente include un componente per la Protezione antivirus e anti-malware e per il Filtro URL. Consultare "Funzionalità di protezione supportate in base al sistema operativo" (pag. 44) per informazioni sulle funzionalità supportate dai diversi sistemi operativi.

Sono supportate le architetture x64 e ARM (utilizzate nei processori Apple Silicon come Apple M1 e M2).

Nota
Non è possibile ripristinare i backup del disco di sistemi Mac con processori Intel su Mac con processori Apple Silicon, e viceversa. È possibile ripristinare file e cartelle.

- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14

Importante
A partire dalla versione C23.07, Cyber Protect Cloud non supporta i sistemi operativi indicati di seguito: OS X Yosemite 10.10, OS X El Capitan 10.11 e macOS Sierra 10.12.

È consigliabile aggiornare il sistema operativo a una versione supportata per garantire la compatibilità e poter utilizzare tutte le funzionalità di Cyber Protect Cloud.

© Acronis International GmbH, 2003-2024

Agente per VMware (appliance virtuale)

Questo agente è fornito come appliance virtuale per l'esecuzione su un host ESXi.

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

Agente per VMware (Windows)

Questo agente è fornito come applicazione Windows per l'esecuzione in qualunque sistema operativo nell'elenco precedente per l'Agente per Windows, con le seguenti eccezioni:

- I sistemi operativi a 32 bit non sono supportati.
- Windows XP, Windows Server 2003/2003 R2 e Windows Small Business Server 2003/2003 R2 non sono supportati.

Agente per Hyper-V

- Windows Server 2008 (solo x64) con ruolo Hyper-V, inclusa la modalità di installazione Server Core
- Windows Server 2008 R2 con ruolo Hyper-V, inclusa la modalità di installazione Server Core
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 con ruolo Hyper-V, inclusa la modalità di installazione Server Core
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (solo x64) con Hyper-V
- Windows 10, edizioni Pro, Education ed Enterprise con Hyper-V
- Windows Server 2016 con ruolo Hyper-V - tutte le opzioni di installazione, ad eccezione di Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 con ruolo Hyper-V - tutte le opzioni di installazione, ad eccezione di Nano Server
- Microsoft Hyper-V Server 2019
- Windows Server 2022 - tutte le opzioni di installazione, ad eccezione di Nano Server

Agente per Virtuozzo

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

Agente per Virtuozzo Hybrid Infrastructure

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

© Acronis International GmbH, 2003-2024

Agente per Scale Computing HC3

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

Agente per oVirt

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agente per Synology

DiskStation Manager 6.2.x, 7.x

L'Agente per Synology supporta soltanto i dispositivi NAS con processori x86_64. I processori ARM non sono supportati.

Cyber Protect Monitor

- Windows 7 o versioni successive
- Windows Server 2008 R2 e versioni successive
- Tutte le versioni di macOS supportate dall'Agente per Mac

Versioni supportate di Microsoft SQL Server

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

Sono inoltre supportate le edizioni SQL Server Express delle versioni del server SQL indicate sopra.

Nota
Il backup di Microsoft SQL è supportato solo per i database eseguiti su file system NTFS, REFS e FAT32. ExFat non è supportato.

Versioni supportate di Microsoft Exchange Server

- Microsoft Exchange Server 2019: tutte le edizioni.
- Microsoft Exchange Server 2016: tutte le edizioni.

© Acronis International GmbH, 2003-2024

- Microsoft Exchange Server 2013: tutte le edizioni, l'Aggiornamento cumulativo 1 (CU1) e versioni successive.
- Microsoft Exchange Server 2010: tutte le edizioni, tutti i Service Pack. Il backup delle caselle di posta e il ripristino granulare dai backup dei database sono supportati a partire dal Service Pack 1 (SP1).
- Microsoft Exchange Server 2007: tutte le edizioni, tutti i Service Pack. Il backup delle caselle di posta e il ripristino granulare dai backup dei database non sono supportati.

Versioni di Microsoft SharePoint supportate

Cyber Protection supporta le seguenti versioni di Microsoft SharePoint:

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

*Per utilizzare SharePoint Explorer con queste versioni, è necessaria una farm di ripristino di SharePoint a cui collegare i database.

La versione in cui hanno avuto origine i backup o i database da cui si estraggono i dati deve corrispondere alla versione di SharePoint in cui è installato SharePoint Explorer.

Versioni di Oracle Database supportate

- Oracle Database versione 11g, tutte le edizioni
- Oracle Database versione 12c, tutte le edizioni
- Oracle Database versione 19c, tutte le edizioni
- Oracle Database versione 21c, tutte le edizioni

Sono supportate solo configurazioni a singola istanza.

Versioni di SAP HANA supportate

HANA 2.0 SPS 03 installato in RHEL 7.6 in esecuzione su una macchina fisica o macchina virtuale VMware ESXi.

Siccome SAP HANA non supporta il ripristino di contenitori di database multitenant tramite l'uso di snapshot di archiviazione, questa soluzione supporta solo contenitori di SAP HANA con database a singolo tenant.

© Acronis International GmbH, 2003-2024

Versioni di MySQL supportate

- 5.5.x − Edizioni Community Server, Enterprise, Standard e Classic
- 5.6.x − Edizioni Community Server, Enterprise, Standard e Classic
- 5.7.x − Edizioni Community Server, Enterprise, Standard e Classic
- 8.0.x − Edizioni Community Server, Enterprise, Standard e Classic

Versioni di MariaDB supportate

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

Piattaforme di virtualizzazione supportate

La seguente tabella contiene un riepilogo del supporto di varie piattaforme di virtualizzazione.

Per ulteriori informazioni sulle differenze tra il backup con agente e il backup agentless, consultare "Backup con agente e agentless" (pag. 66).

Nota
Se si utilizza una piattaforma di virtualizzazione o una versione non elencata di seguito, il metodo Backup con agente **(Backup da un sistema operativo guest (backup con agente)** può ancora funzionare correttamente in tutti gli scenari necessari. Se si riscontrano problemi con il backup con agente, contattare il supporto tecnico per approfondimenti.

VMware

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Versioni di VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 **Edizioni di VMware vSphere:**	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **VMware ESXi** > **Agente per**	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

© Acronis International GmbH, 2003-2024

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	**l'installazione in Windows** oppure **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **VMware ESXi** > **Appliance virtuale (OVF)**	
VMware vSphere Hypervisor (Free ESXi)**	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**
VMware Server (VMware Virtual Server) VMware Workstation VMware ACE VMware Player	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

* In queste edizioni, il trasporto HotAdd per i dischi virtuali è supportato su vSphere 5.0 e versioni successive. Nella versione 4.1, l'esecuzione dei backup potrebbe essere più lenta.

** Il backup a livello di hypervisor non è supportato per vSphere Hypervisor, poiché questo prodotto limita l'accesso a Remote Command Line Interface (RCLI) alla modalità sola lettura. L'agente funziona durante il periodo di valutazione di vSphere Hypervisor senza codice di serie inserito. Una volta inserito un codice di serie, l'agente smette di funzionare.

Nota
Cyber Protect Cloud supporta ufficialmente qualsiasi aggiornamento relativo alla versione principale di vSphere supportata.

Ad esempio, il supporto per vSphere 8.0 include il supporto per qualsiasi aggiornamento di questa versione, se non diversamente specificato. Ciò significa che anche vSphere 8.0 Update 1 è supportato insieme a vSphere 8.0, la versione rilasciata in origine.

Il supporto per una specifica versione di VMware vSphere significa che viene supportato anche il vSAN della versione corrispondente. Ad esempio, il supporto per vSphere 8.0 significa che anche il vSAN 8.0 viene supportato.

© Acronis International GmbH, 2003-2024

Limitazioni

- **Sistemi a tolleranza di errore**
  L'Agente per VMware esegue il backup di un sistema a tolleranza di errore solo se la tolleranza di errore è stata abilitata in VMware vSphere 6.0 e versioni successive. Se si è eseguito l'aggiornamento da una versione di vSphere precedente, è sufficiente disattivare e attivare la tolleranza di errore per ciascun sistema. Se si utilizza una versione di vSphere precedente, installare un agente nel sistema operativo guest.
- **Dischi e RDM indipendenti**
  L'Agente per VMware non esegue il backup di dischi RDM (Raw Device Mapping) in modalità di compatibilità fisica o di dischi indipendenti. L'agente ignora questi dischi e aggiunge avvisi al registro. È possibile evitare gli avvisi escludendo dischi indipendenti e RDM in modalità compatibilità fisica dal piano di protezione. Se si vuole eseguire il backup di tali dischi o dati, installare un agente nel sistema operativo guest.
- **Connessione del dispositivo iSCSI a un sistema guest**
  L'Agente per VMware non esegue il backup di volumi LUN connessi tramite un iniziatore iSCSI operante nel sistema operativo guest. Poiché l'hypervisor ESXi non è compatibile con tali volumi, questi ultimi non vengono inclusi negli snapshot a livello di hypervisor e sono omessi dal backup senza ulteriori avvisi. Se si vuole eseguire il backup di tali volumi o dei dati che essi contengono, installare un agente nel sistema operativo guest.
- **Macchine virtuali crittografate** (introdotte in VMware vSphere 6.5)
  - Le macchine virtuali crittografate sono incluse nel backup in uno stato coerente. Se la crittografia riveste un'importanza critica, abilitarla per i backup durante la creazione del piano di protezione.
  - Le macchine virtuali ripristinate sono sempre non crittografate. Una volta completato il ripristino, sarà possibile abilitare la crittografia manualmente.
  - Se si esegue il backup di macchine virtuali crittografate, è consigliabile crittografare anche le macchine in cui è eseguito l'Agente per VMware. In caso contrario, le operazioni con le macchine crittografate potrebbero risultare più lente del previsto. Applicare il **Criterio di crittografia delle macchine virtuali** alla macchina dell'agente mediante il client Web di vSphere.
  - Il backup delle macchine virtuali crittografate verrà eseguito via LAN, anche se per l'agente è stata configurata la modalità di trasporto SAN. L'agente eseguirà il fallback sul trasporto NBD poiché VMware non supporta il trasporto SAN per l'esecuzione di backup di dischi virtuali crittografati.
- **Secure Boot**
  - Macchine virtuali VMware: (introdotta in VMware vSphere 6.5) L'opzione **Secure Boot** è disabilitata dopo il ripristino di una macchina virtuale come nuova macchina virtuale. Una volta completato il ripristino, sarà possibile abilitare questa opzione manualmente. Questa limitazione si applica a VMware.
  - Macchine virtuali Hyper-V: Per tutte le macchine GEN2 VM, l'opzione Secure Boot è disabilitata dopo il ripristino di una macchina virtuale in una macchina virtuale nuova o esistente.

© Acronis International GmbH, 2003-2024

- **Backup configurazione ESXi** non supportato per VMware vSphere 7.0.
- **Operazioni supportate per sistemi con volumi logici**
  Il backup e il ripristino di workload con volumi logici, come LDM in Windows (dischi dinamici) e LVM in Linux, sono supportati con alcune limitazioni. Per ulteriori informazioni sulle limitazioni, consultare "Operazioni supportate con i volumi logici" (pag. 57).

Microsoft

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Windows Server 2008 (x64) con Hyper-V Windows Server 2008 R2 con Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 con Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) con Hyper-V Windows 10 con Hyper-V Windows Server 2016 con Hyper-V - tutte le opzioni di installazione, ad eccezione di Nano Server Microsoft Hyper-V Server 2016 Windows Server 2019 con Hyper-V – tutte le opzioni di installazione, ad eccezione di Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 con Hyper-V – tutte le opzioni di installazione, ad eccezione di Nano Server	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Hyper-V**	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

© Acronis International GmbH, 2003-2024

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Microsoft Virtual Server 2005	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

Nota
Sono supportate le virtual machine Hyper-V eseguite su cluster iperconvergente con Storage Spaces Direct (S2D). Storage Spaces Direct è supportato anche come storage di backup.

Limitazioni

- **Dischi pass-through**
  L'Agente per Hyper-V non esegue il backup dei dischi pass-through. Durante il backup, l'agente ignora questi dischi e aggiunge avvisi al registro. È possibile evitare gli avvisi escludendo i dischi pass-through dal piano di protezione. Se si vuole eseguire il backup di tali dischi o dati, installare un agente nel sistema operativo guest.
- **Cluster di guest Hyper-V**
  L'Agente per Hyper-V non supporta il backup delle macchine virtuali Hyper-V che sono nodi di un cluster di failover di Windows Server. Uno snapshot VSS a livello di host può disconnettere temporaneamente il disco quorum esterno dal cluster. Se si vuole eseguire il backup di queste macchine, installare l'agente nei sistemi operativi guest.
- **Connessione del dispositivo iSCSI a un sistema guest**
  L'Agente per Hyper-V non esegue il backup di volumi LUN connessi tramite un iniziatore iSCSI operante nel sistema operativo guest. Poiché l'hypervisor Hyper-V non è compatibile con tali volumi, questi ultimi non vengono inclusi negli snapshot a livello di hypervisor e sono omessi dal backup senza ulteriori avvisi. Se si vuole eseguire il backup di tali volumi o dei dati che essi contengono, installare un agente nel sistema operativo guest.
- **Secure Boot**
  Per tutte le macchine GEN2 VM, l'opzione Secure Boot è disabilitata dopo il ripristino di una macchina virtuale in una macchina virtuale nuova o esistente.
- **Operazioni supportate per sistemi con volumi logici**
  Il backup e il ripristino di workload con volumi logici, come LDM in Windows (dischi dinamici) e LVM in Linux, sono supportati con alcune limitazioni. Per ulteriori informazioni sulle limitazioni, consultare "Operazioni supportate con i volumi logici" (pag. 57).
- **Nomi di file VHD/VHDX con simboli di "E" commerciale**
  Negli host Hyper-V che eseguono Windows Server 2016 o versioni successive, non è possibile eseguire il backup di virtual machine esistenti (versione 5.0) originariamente create con Hyper-V 2012 R2 o versioni precedenti se il nome dei rispettivi file VHD/VHDX contiene il simbolo di "E" commerciale (&).

© Acronis International GmbH, 2003-2024

Per poter eseguire il backup di questi sistemi, in Hyper-V Manager scollegare il disco virtuale corrispondente dalla virtual machine, modificare il nome del file VHD/VHDX rimuovendo il simbolo di "E" commerciale, quindi ricollegare il disco alla virtual machine.

- **Dipendenze dal sottosistema Microsoft WMI**
  I backup agentless delle virtual machine Hyper-V dipendono dal sottosistema Microsoft WMI, e in particolare dalla classe `Msvm_VirtualSystemManagementService`. Se le query WMI non riescono, anche i backup non avranno esito positivo. Per ulteriori informazioni sulla classe `Msvm_VirtualSystemManagementService`, consultare la documentazione Microsoft.

Scale Computing

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Scale Computing HC3**	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

Limitazioni

Operazioni supportate per sistemi con volumi logici

Il backup e il ripristino di workload con volumi logici, come LDM in Windows (dischi dinamici) e LVM in Linux, sono supportati con alcune limitazioni. Per ulteriori informazioni sulle limitazioni, consultare "Operazioni supportate con i volumi logici" (pag. 57).

Citrix

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Citrix XenServer/Citrix Hypervisor 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 8.0, 8.1, 8.2	Non supportato	Supportato solo per guest completamente virtualizzati (noti come HVM). Non sono supportati i guest paravirtualizzati (noti come PV). **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Citrix XenServer** > **Windows** oppure **Linux**

© Acronis International GmbH, 2003-2024

Red Hat e Linux

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**
Red Hat Virtualization (gestito da oVirt) 4.2, 4.3, 4.4, 4.5	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Red Hat Virtualization (oVirt)**	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**
Macchine virtuali basate su Kernel (KVM)	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **KVM** > **Windows** oppure **Linux**
Virtual machine basate su Kernel (KVM) gestite da oVirt 4.3 in esecuzione su Red Hat Enterprise Linux 7.6, 7.7 o CentOS 7.6, 7.7	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Red Hat Virtualization (oVirt)**	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**
Virtual machine basate su Kernel (KVM) gestite da oVirt 4.4 in esecuzione su Red Hat Enterprise Linux 8.x o CentOS Stream 8.x	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Red Hat Virtualization (oVirt)**	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**
Virtual machine basate su Kernel (KVM) gestite da oVirt 4.5 in esecuzione su Red Hat Enterprise Linux 8.x o CentOS Stream 8.x	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Red Hat Virtualization (oVirt)**	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

Limitazioni

Operazioni supportate per sistemi con volumi logici

Il backup e il ripristino di workload con volumi logici, come LDM in Windows (dischi dinamici) e LVM in Linux, sono supportati con alcune limitazioni. Per ulteriori informazioni sulle limitazioni, consultare "Operazioni supportate con i volumi logici" (pag. 57).

© Acronis International GmbH, 2003-2024

Parallels

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Parallels Workstation	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**
Parallels Server 4 Bare Metal	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

Oracle

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Oracle Virtualization Manager (basato su oVirt)* 4.3	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Red Hat Virtualization (oVirt)**	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**
Oracle VM Server 3.0, 3.3, 3.4	Non supportato	Supportato solo per guest completamente virtualizzati (noti come HVM). Non sono supportati i guest paravirtualizzati (noti come PV). **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Oracle** > **Windows** oppure **Linux**
Oracle VM VirtualBox 4.x	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Oracle** > **Windows** oppure **Linux**

*Oracle Virtualization Manager è supportato dall'Agente per oVirt.

© Acronis International GmbH, 2003-2024

Limitazioni

Operazioni supportate per sistemi con volumi logici

Il backup e il ripristino di workload con volumi logici, come LDM in Windows (dischi dinamici) e LVM in Linux, sono supportati con alcune limitazioni. Per ulteriori informazioni sulle limitazioni, consultare "Operazioni supportate con i volumi logici" (pag. 57).

Nutanix

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Da Nutanix Acropolis Hypervisor (AHV) 20160925.x a 20180425.x	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Nutanix AHV** > **Windows** oppure **Linux**

Virtuozzo

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Virtuozzo**	Supportato solo per virtual machine. Non sono supportati i contenitori. **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**
Virtuozzo 7.0.13, 7.0.14	Supportato solo per container Ploop. Non sono supportate le macchine virtuali. **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Virtuozzo**	Supportato solo per virtual machine. Non sono supportati i contenitori. **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**
Virtuozzo Hybrid Server 7.5	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Virtuozzo**	Supportato solo per virtual machine. Non sono supportati i contenitori. **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

© Acronis International GmbH, 2003-2024

Limitazioni

Operazioni supportate per sistemi con volumi logici

Il backup e il ripristino di workload con volumi logici, come LDM in Windows (dischi dinamici) e LVM in Linux, sono supportati con alcune limitazioni. Per ulteriori informazioni sulle limitazioni, consultare "Operazioni supportate con i volumi logici" (pag. 57).

Virtuozzo Hybrid Infrastructure

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0	Supportato **Dispositivi** > **Aggiungi** > **Host di virtualizzazione** > **Virtuozzo Hybrid Infrastructure**	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

Limitazioni

- **Backup di virtual machine con dischi su uno storage iSCSI agentless**
  Non è possibile eseguire il backup di VM da Virtuozzo Hybrid Infrastructure, se i dischi delle VM sono posizionati su volumi iSCSI esterni (connessi al cluster VHI).
- **Operazioni supportate per sistemi con volumi logici**
  Il backup e il ripristino di workload con volumi logici, come LDM in Windows (dischi dinamici) e LVM in Linux, sono supportati con alcune limitazioni. Per ulteriori informazioni sulle limitazioni, consultare "Operazioni supportate con i volumi logici" (pag. 57).

Amazon

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Istanze di Amazon EC2	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

© Acronis International GmbH, 2003-2024

Microsoft Azure

Piattaforma	Backup agentless (Backup a livello di hypervisor)	Backup con agente (Backup da un sistema operativo guest)
Macchine virtuali Azure	Non supportato	Supportato **Dispositivi** > **Aggiungi** > **Workstation** oppure **Server** > **Windows** oppure **Linux**

Compatibilità con il software di crittografia

Non vi sono limiti relativi al backup e al ripristino dei dati crittografati mediante un software di crittografia a *livello di file*.

Il software di crittografia a *livello di disco* esegue la crittografia dei dati al volo. Per questo motivo i dati all'interno del backup non sono crittografati. Spesso il software di crittografia a livello di disco modifica le aree di sistema: i record di avvio, le tabelle di partizione o le tabelle di file system. Questi fattori incidono sul backup e ripristino del disco e sulla possibilità del sistema ripristinato di avviarsi e di accedere a Secure Zone.

È possibile eseguire il backup dei dati crittografati mediante il seguente software di crittografia a livello del disco.

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

Per assicurare un ripristino a livello del disco affidabile, seguire le regole comuni e le raccomandazioni specifiche per il software.

Regole di installazione comuni

Si consiglia fortemente l'installazione del software di crittografia prima di installare gli agenti di protezione.

Modalità di utilizzo di Secure Zone

Secure Zone non deve essere crittografata con la crittografia a livello del disco. Questo è l'unico modo per utilizzare Secure Zone:

1. Installare il software di crittografia; quindi installare l'agente.
2. Creare Secure Zone.
3. Escludere Secure Zone quando si esegue la crittografia del disco o dei suoi volumi.

© Acronis International GmbH, 2003-2024

Regole di backup comuni

È possibile creare un backup a livello del disco nel sistema operativo.

Procedure di ripristino specifiche per il software

Microsoft BitLocker Drive Encryption

Per ripristinare un sistema crittografato da BitLocker:

1. Avviare dal supporto di avvio.
2. Ripristinare il sistema. I dati ripristinati saranno non crittografati.
3. Riavviare il sistema ripristinato.
4. Attivare BitLocker.

Per ripristinare solo una partizione di un disco con più partizioni, eseguire questa operazione nel sistema operativo. Il ripristino dal supporto di avvio potrebbe rendere la partizione ripristinata non rilevata da Windows.

McAfee Endpoint Encryption e PGP Whole Disk Encryption

È possibile eseguire il ripristino della partizione di un sistema crittografato utilizzando solo il supporto di avvio.

Se il sistema ripristinato non è in grado di eseguire l'avvio, creare nuovamente il record di avvio principale (MBR) come descritto nel seguente articolo della Microsoft Knowledge Base: https://support.microsoft.com/kb/2622803

Compatibilità con gli storage Dell EMC Data Domain

È possibile utilizzare i dispositivi Dell EMC Data Domain come storage di backup.

Per questo storage si consiglia di utilizzare uno schema di backup che crea regolarmente backup completi, ad esempio **Sempre completo**. Per ulteriori informazioni sugli schemi di backup disponibili, consultare "Schemi di backup" (pag. 425).

È supportato il blocco della conservazione (Modalità Governance). Se è abilitato il blocco della conservazione, è necessario aggiungere la variabile di ambiente `AR_RETENTION_LOCK_SUPPORT` al sistema con l'agente di protezione che utilizza questo storage come destinazione di backup.

Nota
Agente per Mac non supporta i dispositivi di storage Dell EMC Data Domain per i quali è abilitato il blocco della conservazione.

Per aggiungere la variabile di ambiente `AR_RETENTION_LOCK_SUPPORT`

In Windows

© Acronis International GmbH, 2003-2024

1. Accedere come amministratore al sistema con l'agente di protezione installato.
2. Nel **Pannello di controllo**, passare a **Sistema e sicurezza** > **Sistema** > **Impostazioni di sistema avanzate**.
3. Nella scheda **Avanzate**, fare clic su **Variabili di ambiente**.
4. Nel riquadro **Variabili di sistema**, fare clic su **Nuova**.
5. Nella finestra **Nuova variabile di sistema**, aggiungere la nuova variabile come segue:
   - Nome della variabile: `AR_RETENTION_LOCK_SUPPORT`
   - Valore della variabile: `1`
6. Fare clic su **OK**.
7. Nella finestra **Variabili di ambiente**, fare clic su **OK**.
8. Riavviare la macchina.

In Linux

1. Accedere come amministratore al sistema con l'agente di protezione installato.
2. Passare alla directory `/sbin`, quindi aprire il file `acronis_mms` per la modifica.
3. Sopra alla riga `export LD_LIBRARY_PATH` aggiungere la riga seguente:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Salvare il file `acronis_mms`.
5. Riavviare la macchina.

In un'appliance virtuale

1. Accedere come amministratore all'appliance virtuale.
2. Passare alla directory `/bin`, quindi aprire il file `autostart` per la modifica.
3. Sotto alla riga `export LD_LIBRARY_PATH` aggiungere la riga seguente:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Salvare il file `autostart`.
5. Riavviare il sistema con l'appliance virtuale.

Funzionalità di protezione supportate in base al sistema operativo

Questo argomento contiene informazioni sulle funzionalità di protezione di Cyber Protect Cloud. Non è tuttavia un elenco delle funzionalità di backup e ripristino.

Le funzionalità di protezione sono supportate solo nei sistemi in cui è installato l'agente di protezione. Non sono disponibili per le virtual machine il cui backup è eseguito in modalità

© Acronis International GmbH, 2003-2024

agentless, ad esempio da Agente per Hyper-V, Agente per VMware, Agente per Virtuozzo Hybrid Infrastructure, Agente per Scale Computing o Agente per oVirt.

Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

Sistemi operativi e versioni supportati

Windows

Se non diversamente indicato per uno specifico insieme di caratteristiche, sono supportate le seguenti versioni di Windows:

- Windows 7 Service Pack 1 e versioni successive
- Windows Server 2008 R2 Service Pack 1 e versioni successive

Nota
Per Windows 7, è necessario installare i seguenti aggiornamenti Microsoft prima di installare l'agente di protezione.

- Windows 7 Extended Security Updates (ESU)
- KB4474419
- KB4490628

Per ulteriori informazioni sugli aggiornamenti richiesti, fare riferimento a questo articolo della Knowledge Base.

Linux

Le distribuzioni Linux supportate e le rispettive versioni dipendono dall'insieme di funzionalità, e sono indicate nella parte inferiore di ogni tabella.

macOS

Le versioni macOS supportate dipendono dall'insieme di funzionalità, e sono indicate nella parte inferiore di ogni tabella.

Caratteristiche	Windows	Linux	macOS
Piani di protezione predefiniti			
Lavoratori da remoto	Sì	No	No
Lavoratori in ufficio (antivirus di terze parti)	Sì	No	No
Lavoratori in ufficio (antivirus di Cyber Protect)	Sì	No	No
Cyber Protect Essentials (solo per l'edizione Cyber Protect Essentials)	Sì	No	No

© Acronis International GmbH, 2003-2024

Caratteristiche	Windows	Linux	macOS
Piani di protezione predefiniti			
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Backup con dati forensi			
Raccolta dump della memoria	Sì	No	No
Snapshot dei processi in esecuzione	Sì	No	No
Autenticazione del backup con dati forensi su immagine locale	Sì	No	No
Autenticazione del backup con dati forensi su immagine cloud	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Protezione continua dei dati (CDP)			
CDP per file e cartelle	Sì	No	No
CDP per file modificati tramite tracciamento delle applicazioni	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Individuazione automatica e installazione remota			
Individuazione basata su rete	Sì	No	No
Individuazione basata su Active Directory	Sì	No	No
Individuazione basata su modello (importazione di sistemi da file)	Sì	No	No
Aggiunta manuale dei dispositivi	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

© Acronis International GmbH, 2003-2024

Caratteristiche	Windows	Linux	macOS
Active Protection			
Individuazione dell'iniezione di processi	Sì	No	No
Ripristino automatico dei file interessati dalla cache locale	Sì	Sì	Sì
Autodifesa dei file di backup Acronis	Sì	No	No
Autodifesa del software Acronis	Sì	No	Sì (Solo componenti di Active Protection e Anti-malware)
Gestione dei processi affidabili/bloccati	Sì	No	Sì
Esclusione di processi/cartelle	Sì	Sì	Sì
Individuazione del ransomware basata sul comportamento di un processo (basata su IA)	Sì	Sì	Sì
Individuazione dei processi di mining delle criptovalute basata sul comportamento di un processo	Sì	No	No
Protezione di unità esterne (HDD, unità flash, schede SD)	Sì	No	Sì
Protezione delle cartelle di rete	Sì	Sì	Sì
Protezione lato server	Sì	No	No
Protezione per Zoom, Cisco Webex, Citrix Workspace e Microsoft Teams	Sì	No	No
Per ulteriori informazioni sui sistemi operativi supportati e sulle rispettive versioni, consultare "Piattaforme supportate" (pag. 835).			

Caratteristiche	Windows	Linux	macOS
Protezione antivirus e anti-malware			
Funzionalità Active Protection completamente integrata	Sì	No	No
Protezione antimalware in tempo reale	Sì	Sì, con il pacchetto Advanced	Sì, con il pacchetto Advanced

© Acronis International GmbH, 2003-2024

Caratteristiche	Windows	Linux	macOS
Protezione antivirus e anti-malware			
		Antimalware	Antimalware
Protezione antimalware Advanced in tempo reale con individuazione basata sulle firme in locale	Sì	Sì	Sì
Analisi statica per i file eseguibili con portabilità	Sì	No	Sì*
Scansione anti-malware su richiesta	Sì	Sì**	Sì
Protezione delle cartelle di rete	Sì	Sì	No
Protezione lato server	Sì	No	No
Scansione dei file archiviati	Sì	No	Sì
Scansione delle unità rimovibili	Sì	No	Sì
Scansione dei soli file nuovi e modificati	Sì	No	Sì
Esclusioni di cartelle/file	Sì	Sì	Sì***
Esclusioni di processi	Sì	No	Sì
Motore di analisi comportamentale	Sì	No	Sì
Prevenzione degli exploit	Sì	No	No
Quarantena	Sì	Sì	Sì
Pulizia automatica della cartella di quarantena	Sì	Sì	Sì
Filtro URL (http/https)	Sì	No	No
Elenco degli elementi consentiti aziendale	Sì	No	Sì
Gestione firewall****	Sì	No	No
Gestione di Microsoft Defender Antivirus*****	Sì	No	No
Gestione di Microsoft Security Essentials	Sì	No	No
Registrazione e gestione della protezione antivirus e anti-malware tramite il Centro sicurezza PC Windows	Sì	No	No
Per ulteriori informazioni sui sistemi operativi supportati e sulle rispettive versioni, consultare "Piattaforme supportate" (pag. 835).			

© Acronis International GmbH, 2003-2024

* L'analisi statica dei file eseguibili con portabilità è supportata solo per le scansioni pianificate su macOS.

** Le condizioni di avvio non sono supportate per la scansione su richiesta su Linux.

*** Le esclusioni di file/cartelle sono supportate solo nel caso in cui vengano specificati file e cartelle che non verranno scansionati dalla protezione in tempo reale o durante le scansioni pianificate su macOS.

**** La funzionalità di gestione del firewall è supportata in Windows 8 e versioni successive. Windows Server non è supportato.

***** La gestione di Windows Defender Antivirus è supportata in Windows 8.1 e versioni successive.

Caratteristiche	Windows	Linux	macOS
Valutazione delle vulnerabilità			
Valutazione delle vulnerabilità di un sistema operativo e delle relative applicazioni native	Sì	Sì******	Sì
Valutazione delle vulnerabilità per applicazioni di terze parti	Sì	No	Sì
Per ulteriori informazioni sui sistemi operativi supportati e sulle rispettive versioni, consultare "Prodotti Microsoft e prodotti di terze parti supportati" (pag. 975), "Prodotti Linux supportati" (pag. 977) e "Prodotti Apple e prodotti di terze parti supportati" (pag. 976).			

****** La vulnerability assessment dipende dalla disponibilità di avvisi di sicurezza ufficiali per la distribuzione specifica, ad esempio https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce e altri.

Caratteristiche	Windows	Linux	macOS
Gestione patch			
Approvazione automatica delle patch	Sì	No	No
Installazione automatica delle patch	Sì	No	No
Testing delle patch	Sì	No	No
Installazione manuale delle patch	Sì	No	No
Pianificazione delle patch	Sì	No	No
Applicazione delle patch provvisoria: esecuzione del backup del sistema prima dell'installazione delle patch come parte del piano di protezione	Sì	No	No
Annullamento del riavvio di un sistema se è in	Sì	No	No

© Acronis International GmbH, 2003-2024

Caratteristiche	Windows	Linux	macOS
Gestione patch			
esecuzione un backup			
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Mappa di protezione dati			
Definizione regolabile dei file importanti	Sì	No	No
Scansione dei sistemi per individuare file non protetti	Sì	No	No
Panoramica delle posizioni non protette	Sì	No	No
Possibilità di avviare le azioni di protezione dal widget Mappa di protezione dati (azione **Proteggi tutti i file**)	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Integrità del disco			
Controllo dell'integrità delle unità HDD e SSD basata su IA	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Piani di protezione intelligenti basati sugli avvisi derivanti dal centro operativo Acronis Cyber Protection			
Feed minacce	Sì	No	No
Procedura di correzione guidata	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Scansione del backup			
Scansione anti-malware delle immagini di backup inclusa nel piano di backup	Sì	No	No
Scansione dei backup dell'immagine alla ricerca del malware nel cloud	Sì	No	No

© Acronis International GmbH, 2003-2024

Caratteristiche	Windows	Linux	macOS
Scansione del backup			
Scansione del backup alla ricerca del malware nei backup crittografati	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Ripristino sicuro			
Scansione anti-malware con protezione antivirus e anti-malware durante il processo di ripristino	Sì	No	No
Ripristino sicuro dei backup crittografati	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Connessione al desktop remoto			
Connessione tramite NEAR	Sì	Sì	Sì
Connessione tramite RDP	Sì	No	No
Connessione tramite Condivisione schermo di Apple	No	No	Sì
Connessione tramite client web	Sì	No	No
Connessione tramite Quick Assist	Sì	Sì	Sì
Assistenza remota	Sì	Sì	Sì
Trasferimento di file	Sì	Sì	Sì
Trasmissione screenshot	Sì	Sì	Sì
Per ulteriori informazioni sui sistemi operativi supportati e sulle rispettive versioni, consultare "Piattaforme supportate" (pag. 1014).			

Caratteristiche	Windows	Linux	macOS
#CyberFit Score			
Stato del #CyberFit Score	Sì	No	No
Strumento autonomo #CyberFit Score	Sì	No	No

© Acronis International GmbH, 2003-2024

Caratteristiche	Windows	Linux	macOS
#CyberFit Score			
Raccomandazioni fornite da #CyberFit Score	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Prevenzione della perdita di dati			
Controllo dispositivo	Sì	No	Supportato su Mac con processori Intel che eseguono macOS 10.15 o versioni successive o macOS 11.2.3 o versioni successive. Non è supportato nei processori Apple Silicon basati su ARM, come ad esempio Apple M1/M2.
Advanced Data Loss Prevention	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45).			

Caratteristiche	Windows	Linux	macOS
Opzioni di gestione			
Scenari di upselling per promuovere le edizioni di Cyber Protect	Sì	Sì	Sì
Console web centralizzata e console di gestione remota	Sì	Sì	Sì
Sistemi operativi e versioni supportati: indipendente dalla piattaforma.			

© Acronis International GmbH, 2003-2024

Caratteristiche	Windows	Linux	macOS
Opzioni di protezione			
Cancellazione remota	Sì	No	No
Supportato in Windows 10 e versioni successive.			

Caratteristiche	Windows	Linux	macOS
Cyber Protect Monitor			
App Cyber Protect	Sì	No	Sì
Stato della protezione per Zoom	Sì	No	No
Stato della protezione per Cisco Webex	Sì	No	No
Stato della protezione per Citrix Workspace	Sì	No	No
Stato della protezione per Microsoft Teams	Sì	No	No
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45). Sui sistemi macOS, Cyber Protect Monitor è supportato da tutte le versioni nelle quali è possibile installare l'Agente per Mac. Per ulteriori informazioni, consultare "Agente per Mac" (pag. 28).			

Caratteristiche	Windows	Linux	macOS
Inventario software			
Scansione dell'inventario software	Sì	No	Sì
Monitoraggio dell'inventario software	Sì	No	Sì
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45). Nei sistemi macOS, Inventario software è supportato dalle versioni 10.13.x − 13.x.			

Caratteristiche	Windows	Linux	macOS
Inventario hardware			
Scansione dell'inventario hardware	Sì	No	Sì
Monitoraggio dell'inventario hardware	Sì	No	Sì
Vedere le versioni di Windows supportate in "Sistemi operativi e versioni supportati" (pag. 45). Nei sistemi macOS, Inventario hardware è supportato dalle versioni 10.13.x − 13.x.			

© Acronis International GmbH, 2003-2024

File system supportati

Un agente di protezione può eseguire il backup di qualsiasi file system accessibile dal sistema operativo in cui è installato l'agente. Ad esempio, l'Agente per Windows può eseguire il backup e il ripristino di un file system ext4 se in Windows è installato il relativo driver.

La seguente tabella contiene un riepilogo dei file system di cui è possibile eseguire il backup e il ripristino (i supporti di avvio supportano solo il ripristino). Le limitazioni si applicano sia agli agenti che ai supporti di avvio.

File system	Supportato da			Limitazioni
	Agenti	Supporto di avvio per Windows e Linux	Supporto di avvio per Mac	
FAT16/32	Tutti gli agenti	+	+	Nessun limite
NTFS	Tutti gli agenti	+	+	
Ext2/Ext3/Ext4	Tutti gli agenti	+	-	
HFS+	Agente per Mac	-	+	
APFS	Agente per Mac	-	+	• Supportato a partire da macOS High Sierra 10.13 • È necessario ricreare manualmente la configurazione del disco quando si effettua il ripristino su un sistema non originale o bare metal.
JFS	Agente per Linux	+	-	• I filtri file (Inclusioni/Esclusioni) non sono supportati • Non è possibile abilitare il backup incrementale/differenziale rapido
ReiserFS3	Agente per Linux	+	-	
ReiserFS4	Agente	+	-	• I filtri file (Inclusioni/Esclusioni)

© Acronis International GmbH, 2003-2024

File system	Supportato da			Limitazioni
	Agenti	**Supporto di avvio per Windows e Linux**	**Supporto di avvio per Mac**	
	per Linux			non sono supportati • Non è possibile abilitare il backup incrementale/differenziale rapido • Non è possibile ridimensionare il volumi nel corso di un ripristino
ReFS	Tutti gli agenti	+	+	• I filtri file (Inclusioni/Esclusioni) non sono supportati • Non è possibile abilitare il backup incrementale/differenziale rapido • Non è possibile ridimensionare il volumi nel corso di un ripristino • Il ripristino di un file da un backup ReFS prevede il ripristino del solo contenuto. Gli elenchi di controllo degli accessi e i flussi alternativi non vengono recuperati. I file sparse vengono ripristinati come file normali.
XFS	Tutti gli agenti	+	+	• I filtri file (Inclusioni/Esclusioni) non sono supportati • Non è possibile abilitare il backup incrementale/differenziale rapido • Non è possibile ridimensionare il volumi nel corso di un ripristino • La modalità di backup incrementale rapida non è

© Acronis International GmbH, 2003-2024

File system	Supportato da			Limitazioni
	Agenti	**Supporto di avvio per Windows e Linux**	**Supporto di avvio per Mac**	
				supportata dal file system XFS. I backup incrementali e differenziali dei volumi XFS nel cloud possono essere nettamente più lenti dei backup ext4 che utilizzano la modalità incrementale rapida.
Swap di Linux	Agente per Linux	+	-	Nessun limite
exFAT	Tutti gli agenti	+ Il supporto di avvio non è utilizzabile per il ripristino se il backup *è archiviato su* exFAT	+	• È supportato solo il backup del disco/del volume • I filtri file (Inclusioni/Esclusioni) non sono supportati • Non è possibile ripristinare file individuali da un backup

Il software passa automaticamente alla modalità settore per settore quando esegue il backup di unità con file system non riconosciuti o non supportati (ad esempio, Btrfs). Il backup settore per settore è possibile per qualsiasi file system che:

- è basato su blocco
- si estende su un disco singolo
- ha uno schema di partizione MBR/GPT standard

Se il file system non possiede questi requisiti, il backup non va a buon fine.

Deduplicazione dei dati

In Windows Server 2012 e versioni successive, è possibile abilitare la funzionalità Deduplicazione dati per un volume NTFS. La deduplicazione dei dati riduce lo spazio utilizzato sul volume archiviando solo una volta i frammenti duplicati dei file del volume.

È possibile eseguire il backup e il ripristino di un volume abilitato alla deduplicazione dei dati al livello del disco, senza limitazioni. Il backup a livello di file è supportato, tranne quando si utilizza

© Acronis International GmbH, 2003-2024

Acronis VSS Provider. Per ripristinare file da un backup di disco, è possibile eseguire una macchina virtuale dal backup oppure montare il backup su un sistema che esegue Windows Server 2012 o versioni successive, quindi copiare i file dal volume montato.

La funzionalità Deduplicazione dati di Windows Server non è correlata alla funzionalità Deduplicazione di Acronis Backup.

Operazioni supportate con i volumi logici

Il backup e il ripristino di workload con volumi logici, come LDM in Windows (dischi dinamici) e LVM in Linux, sono supportati con le limitazioni seguenti.

Backup

Il backup con agente è un backup creato da un agente di protezione installato nel workload o da un supporto di avvio.

Il backup agentless è disponibile solo per le virtual machine. Viene eseguito a livello di hypervisor da un agente che può eseguire il backup e il ripristino di tutte le virtual machine nell'ambiente. Nelle virtual machine protette non vengono installati singoli agenti.

Per ulteriori informazioni sulle differenze tra il backup con agente e il backup agentless, consultare "Backup con agente e agentless" (pag. 66).

Backup con agente	Backup agentless
• Il backup dei volumi logici viene eseguito per volume. • Sono supportati i filtri file (inclusioni/esclusioni).	• Quando viene rilevato un volume logico su un disco, il backup del disco viene eseguito in modalità RAW, settore per settore. La struttura della partizione del disco non viene analizzata e le immagini del volume non vengono memorizzate separatamente. • I singoli volumi LDM o LVM non possono essere selezionati come origine del backup, né tramite selezione diretta né utilizzando le regole delle policy. Nella sezione **Cosa includere nel backup** di un piano di protezione è disponibile soltanto l'opzione **Intera macchina**. • I filtri file (Inclusioni/Esclusioni) non sono supportati. Qualsiasi inclusione o esclusione configurata viene ignorata.

Ripristino

Il ripristino con agente è un ripristino eseguito da un agente installato nel workload o da un supporto di avvio.

© Acronis International GmbH, 2003-2024

Il ripristino agentless supporta come destinazioni solo le virtual machine. Viene eseguito a livello di hypervisor da un agente che può eseguire il backup e il ripristino di tutte le virtual machine dell'ambiente. Non è necessario creare manualmente un sistema di destinazione dove ripristinare il backup.

	Da backup con agente	Da backup agentless
Ripristino con agente	• È disponibile il ripristino per volume. • È disponibile il ripristino di file e cartelle.	• Non è disponibile il ripristino per volume. • È disponibile il ripristino di file e cartelle.
Ripristino agentless	• La migrazione del sistema (P2V, V2P e V2V) non è supportata. Per ripristinare i dati da un backup con agente, utilizzare un supporto di avvio. • L'operazione **Esegui come MV** non è supportata. • È disponibile il ripristino di file e cartelle.	• Non è disponibile il ripristino per volume. • È disponibile il ripristino completo del sistema. • È disponibile il ripristino di file e cartelle. • L'operazione **Esegui come MV** è supportata. Per rendere avviabile la virtual machine, potrebbe essere necessario modificare l'ordine di avvio. Per ulteriori informazioni, consultare questo articolo della Knowledge Base. • È supportata la conversione ai seguenti tipi di virtual machine: ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ Scale Computing HC3

© Acronis International GmbH, 2003-2024

Installazione e deployment di agenti Cyber Protection

Preparazione

Passaggio 1

Scegliere un agente a seconda degli elementi di cui si intende eseguire il backup. Per ulteriori informazioni sulle opzioni possibili, fare riferimento a Di quale agente occorre disporre?

Passaggio 2

Verificare che lo spazio disponibile sul disco rigido sia sufficiente per l'installazione di un agente. Per informazioni dettagliate sullo spazio necessario, fare riferimento a "Requisiti di sistema per agenti" (pag. 66).

Passaggio 3

Scaricare il programma di installazione. Per trovare i collegamenti per il download, fare clic su **Tutti i dispositivi** > **Aggiungi**.

La pagina **Aggiungi periferiche** fornisce installer Web per ciascun agente installato in Windows. L'installer è un piccolo file eseguibile che scarica il programma di installazione principale da Internet e lo salva come file temporaneo. Il file viene eliminato subito dopo l'installazione.

Per archiviare i programmi di installazione localmente, scaricare un pacchetto contenente tutti gli agenti per l'installazione in Windows utilizzando il collegamento che si trova in fondo alla pagina **Aggiungi periferiche**. Sono disponibili pacchetti per 32 e 64 bit. Tali pacchetti consentono di personalizzare l'elenco di componenti da installare. Tali pacchetti consentono inoltre di eseguire un'installazione automatica, ad esempio tramite Criterio di gruppo. Questo scenario avanzato è descritto in "Distribuzione di agenti tramite i Criteri di gruppo" (pag. 171).

Per scaricare il programma di installazione dell'Agente per Microsoft 365, fare clic sull'icona dell'account nell'angolo in alto a destra, quindi su **Download** > **Agente per Microsoft 365**.

L'installazione su Linux e macOS viene eseguita a partire da programmi di installazione normali.

Tutti i programmi di installazione richiedono una connessione Internet per registrare la macchina per il servizio Cyber Protection. In mancanza di una connessione Internet, l'installazione avrà esito negativo.

Passaggio 4

Le funzionalità di Cyber Protect richiedono Microsoft Visual C++ 2017 Redistributable. Verificare che sia già installato nel sistema o installarlo prima di procedere con l'installazione dell'agente. Dopo

© Acronis International GmbH, 2003-2024

l'installazione di Microsoft Visual C++, potrebbe essere necessario un riavvio. Il pacchetto Microsoft Visual C++ Redistributable è disponibile all'indirizzo https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Passaggio 5

Accertarsi che i firewall e gli altri componenti del sistema di sicurezza della rete (ad esempio il server proxy) consentano le connessioni in uscita attraverso le seguenti porte TCP:

- Porte **443** e **8443**

  Queste porte sono utilizzate per l'accesso alla console di Cyber Protect, la registrazione degli agenti, il download dei certificati, l'autorizzazione degli utenti e il download di file dal cloud storage.
- Porte nell'intervallo **7770** – **7800**

  Gli agenti utilizzano queste porte per comunicare con il management server.
- Porte **44445** e **55556**

  Gli agenti utilizzano queste porte per il trasferimento dei dati durante il backup e il ripristino.

Se nella rete è abilitato un server proxy, fare riferimento a "Configurazione delle impostazioni del server proxy" (pag. 72) per determinare se sia necessario configurare tali impostazioni su ciascun sistema che esegue un agente di protezione.

La velocità di connessione minima a Internet richiesta per gestire un agente dal cloud è di 1 Mbit/s (da non confondersi con la velocità di trasferimento dei dati accettabile per il backup nel cloud). Tenere presente questo aspetto se si usa una tecnologia di connessione a larghezza di banda ridotta come l'ADSL.

Porte TCP necessarie per il backup e la replica di macchine virtuali VMware

- Porta **443**

  L'Agente per VMware (sia Windows che appliance virtuale) si connette a questa porta sull'host ESXi/server vCenter per eseguire operazioni di gestione della VM quali creazione, aggiornamento ed eliminazione di VM su vSphere durante le attività di backup, ripristino e replica della VM.
- Porta **902**

  L'Agente per VMware (sia Windows che appliance virtuale) si connette a questa porta sull'host ESXi/ per stabilire connessioni NFC per scrivere/leggere dati sui dischi della VM durante le attività di backup, ripristino e replica della VM.
- Porta **3333**

  Se l'Agente per VMware (appliance virtuale) è in esecuzione sul cluster/host ESXi che serve come destinazione della replica della VM, il traffico della replica non viene indirizzato direttamente all'host ESXi sulla porta **902**. Il traffico verrà invece indirizzato dall'Agente per VMware di origine alla porta TCP **3333** dell'Agente per VMware (appliance virtuale) posizionata sul cluster/host ESXi.

  L'Agente per VMware di origine che legge i dati dai dischi della VM originale può trovarsi in qualsiasi altra posizione ed essere di qualsiasi tipo: appliance virtuale o Windows.

© Acronis International GmbH, 2003-2024

Il servizio responsabile dell'accettazione dei dati della replica della VM sull'Agente per VMware di destinazione (appliance virtuale) è chiamato "Server del disco di replica". Il servizio è responsabile delle tecniche di ottimizzazione della WAN, come la compressione del traffico e la deduplicazione durante la replica della VM, inclusa la raccolta dei dati di replica (vedere Raccolta dei dati di replica iniziali).Nel caso in cui non sia in esecuzione alcun Agente per VMware (appliance virtuale) nell'host ESXi di destinazione, il servizio non è disponibile e pertanto lo scenario della raccolta dei dati di replica non è supportato.

Porte necessarie per il componente Downloader

Il componente Downloader è responsabile della fornitura degli aggiornamenti a un computer e della loro distribuzione alle altre istanze di Downloader. Può essere eseguito in modalità agente, trasformando il relativo computer in un agente Downloader. Tale agente scarica gli aggiornamenti da Internet e funge da origine della distribuzione degli aggiornamenti agli altri computer. Per funzionare, il Downloader richiede le porte seguenti.

- Porta TCP e UDP (in entrata) **6888**
  Utilizzata dal protocollo BitTorrent per gli aggiornamenti peer-to-peer dei file torrent.
- Porta UDP **6771**
  Utilizzata come porta di rilevamento del peer locale. È utilizzata anche negli aggiornamenti peer-to-peer.
- Porta TCP **18018**
  Utilizzata per la comunicazione tra gli strumenti di aggiornamento che funzionano con modalità differenti: Updater e UpdaterAgent.
- Porta TCP **18019**
  Porta locale, utilizzata per la comunicazione tra l'Updater e l'agente di protezione.

Passaggio 6

Nel sistema in cui si pianifica di installare l'agente di protezione, verificare che le porte locali seguenti non siano utilizzate da altri processi.

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

Nota
Non è necessario aprirle nel firewall.

Modifica delle porte utilizzate dall'agente di protezione

Alcune delle porte necessarie all'agente di protezione possono essere utilizzate da altre applicazioni presenti nell'ambiente. Per evitare conflitti, è possibile modificare le porte predefinite utilizzate dall'agente di protezione modificando i file indicati di seguito.

© Acronis International GmbH, 2003-2024

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

Di quale agente occorre disporre?

La scelta di un agente è correlata agli elementi di cui si intende eseguire il backup. La seguente tabella presenta un riepilogo delle informazioni per agevolare la scelta.

In Windows, l'Agente per Exchange, l'Agente per SQL, l'Agente per Active Directory e l'Agente per Oracle richiedono che sia installato anche l'Agente per Windows. Pertanto, se si installa ad esempio l'Agente per SQL, si potrà eseguire anche il backup dell'intero sistema in cui è installato l'agente.

Si consiglia di installare anche l'Agente per Windows quando si installano l'Agente per VMware (Windows) e l'Agente per Hyper-V.

In Linux, Agente per Oracle, Agente per MySQL/MariaDB e Agente per Virtuozzo richiedono che sia installato anche Agent for Linux (64-bit). Questi agenti sono inclusi nel file di installazione dell'Agente per Linux (64-bit).

Quali elementi verranno inseriti nel backup?	Quale agente installare?	Dove è necessario eseguire l'installazione?
Macchine fisiche		
Macchine fisiche che eseguono Windows	Agente per Windows	Sul sistema di cui verrà eseguito il backup.
Macchine fisiche che eseguono Linux	Agente per Linux	
Macchine fisiche che eseguono macOS	Agente per Mac	
Database		
Database SQL	Agente per SQL	Sul sistema che esegue Microsoft SQL Server.
Database MySQL	Agente per MySQL/MariaDB (Incluso nel file di installazione dell'Agente per Linux (64-bit))	Sul sistema che esegue MySQL Server.
Database MariaDB	Agente per MySQL/MariaDB (Incluso nel file di	Sul sistema che esegue MariaDB Server.

© Acronis International GmbH, 2003-2024

	installazione dell'Agente per Linux (64-bit))	
Database Exchange	Agente per Exchange	Sul sistema che esegue il ruolo Cassette postali di Microsoft Exchange Server.*
Database Oracle	Agente per Oracle (In Linux, incluso nel file di installazione di Agente per Linux (64-bit))	Sul sistema che esegue Oracle Database.
Workload cloud-to-cloud		
Caselle di posta di Microsoft 365 (Agente cloud o agente locale)	Agente cloud (Non è richiesta l'installazione)	Questa funzionalità è disponibile con un agente cloud distribuito nel data center. Per ulteriori informazioni, consultare "Utilizzo dell'Agente cloud per Microsoft 365" (pag. 618).
	Agente per Office 365	Su una macchina Windows connessa a Internet. Per ulteriori informazioni, consultare "Utilizzo dell'Agente installato in locale per Office 365" (pag. 613).
File di Microsoft 365 OneDrive e siti di SharePoint Online	Agente cloud (Non è richiesta l'installazione)	Questa funzionalità è disponibile con un agente cloud distribuito nel data center. Per ulteriori informazioni, consultare "Utilizzo dell'Agente cloud per Microsoft 365" (pag.

© Acronis International GmbH, 2003-2024

		618).
Caselle di posta Gmail di Google Workspace, file di Google Drive e file di unità condivise	Agente cloud (Non è richiesta l'installazione)	Questa funzionalità è disponibile con un agente cloud distribuito nel data center. Per ulteriori informazioni, consultare "Protezione dei dati di Google Workspace" (pag. 654).
Active Directory		
Sistemi che eseguono i Servizi di dominio di Active Directory	Agente per Active Directory	Sul controller di dominio.
Macchine virtuali		
Macchine virtuali VMware ESXi	Agente per VMware (Windows)	Su un sistema Windows che dispone dell'accesso di rete a vCenter Server e all'archivio della macchina virtuale.**
	Agente per VMware (appliance virtuale)	Sull'host ESXi.
Macchine virtuali Hyper-V	Agente per Hyper-V	Sull'host Hyper-V.
Virtual machine Scale Computing HC3	Agente per Scale Computing HC3 (appliance virtuale)	Sull'host Scale Computing HC3.
Virtual machine Red Hat Virtualization (gestita da oVirt)	Agente per oVirt (Virtual Appliance)	Nell'host Red Hat Virtualization.
Macchine virtuali e contenitori Virtuozzo***	Agente per Virtuozzo (Incluso nel file di installazione dell'Agente per Linux (64-bit))	Sull'host Virtuozzo.
Macchine virtuali Virtuozzo Hybrid Infrastructure	Agente per Virtuozzo Hybrid	Nell'host Virtuozzo Hybrid Infrastructure.

© Acronis International GmbH, 2003-2024

	Infrastructure (appliance virtuale)	
Macchine virtuali ospitate su Amazon EC2	Analogamente alla macchine fisiche****	Sul sistema di cui verrà eseguito il backup.
Macchine virtuali ospitate su Windows Azure		
Macchine virtuali Citrix XenServer		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
Virtual machine basate su Kernel (KVM), non gestite da oVirt		
Virtual machine Oracle, non gestite da oVirt		
Macchine virtuali Nutanix AHV		
Red Hat Virtualization (RHV/RHEV), gestite da oVirt	Agente per oVirt (Virtual Appliance)	Sull'host di virtualizzazione.
Virtual machine basate su Kernel (KVM), gestite da oVirt		
Virtual machine Oracle, gestite da oVirt		
Dispositivi mobili		
Dispositivi mobili che eseguono Android	App mobile per Android	Sul dispositivo mobile di cui verrà eseguito il backup.
Dispositivi mobili che eseguono iOS	App mobile per iOS	

*Durante l'installazione, l'Agente per Exchange controlla la presenza dello spazio libero necessario nel sistema in cui verrà eseguito. Durante un ripristino granulare è temporaneamente necessario uno spazio disponibile equivalente al 15% del database di Exchange di maggiori dimensioni.

**Se ESXi utilizza un SAN attached storage, installare l'agente su una macchina connessa alla stessa SAN. L'agente eseguirà il backup delle macchine virtuali direttamente dall'archivio, anziché tramite l'host ESXi e la LAN. Per le istruzioni dettagliate, consultare "Agente per VMware - Backup senza LAN" (pag. 704).

***Virtuozzo 7 supporta solo i contenitori Ploop. Non sono supportate le macchine virtuali.

****Una macchina virtuale è considerata tale se il relativo backup viene eseguito da un agente esterno. Se un agente è installato nel sistema guest, le operazioni di backup e ripristino sono le stesse utilizzate per le macchine fisiche. Ciononostante, se Cyber Protection può identificare una virtual machine utilizzando l'istruzione CPUID, assegnerà ad essa una quota del servizio virtual machine. Se si utilizza il passthrough diretto o un'altra opzione che maschera l'ID del produttore della CPU, potranno essere assegnate solo quote per sistemi fisici.

© Acronis International GmbH, 2003-2024

Backup con agente e agentless

Per il backup con agente è necessario che in ogni sistema protetto sia installato un agente di protezione. Il backup con agente è supportato su tutti i sistemi fisici e le virtual machine. Per ulteriori informazioni sull'agente più adatto e sulla modalità di installazione, consultare "Di quale agente occorre disporre?" (pag. 62)

Il backup agentless è supportato da alcune piattaforme di virtualizzazione e non è disponibile per i sistemi fisici. Richiede un solo agente di protezione, che è installato in un sistema dedicato nell'ambiente virtuale. Questo agente esegue il backup di tutte le altre virtual machine dell'ambiente. Per ulteriori informazioni sui tipi di backup supportati dalle varie piattaforme di virtualizzazione, consultare "Piattaforme di virtualizzazione supportate" (pag. 32).

Per alcune piattaforme di virtualizzazione sono disponibili appliance virtuali. Un'appliance virtuale è una virtual machine già predisposta che contiene un agente di protezione. Le appliance virtuali sono disponibili nei formati specifici dell'hypervisor quali .ovf, .ova o .qcow.

Quale tipo di backup scegliere?

Il backup con agente è consigliabile se è richiesto quanto segue:

- Funzionalità di protezione aggiuntiva, ad esempio antivirus e anti-malware, patch management o connessione desktop remoto. Per ulteriori informazioni su queste funzionalità, consultare "Funzionalità di protezione supportate in base al sistema operativo" (pag. 44).
- Virtual machine separate a livello del tenant, ad esempio per far sì che gli utenti del tenant di accedere unicamente ai propri backup.
- Backup a livello di file da ripristinare sui sistemi operativi guest.

Il backup agentless è consigliabile se è richiesto quanto segue:

- Solo il backup, senza alcuna funzionalità di protezione aggiuntive.
- Gestione semplificata: è possibile eseguire il backup di più virtual machine installando e configurando un solo agente.
- Ridurre al minimo l'utilizzo delle risorse: un agente dedicato utilizza meno CPU e RAM rispetto a più agenti installati su ogni virtual machine dell'ambiente.
- Configurazioni di backup specifiche, come il backup senza LAN. Per ulteriori informazioni su questa funzionalità, consultare "Agente per VMware - Backup senza LAN" (pag. 704).
- Riduzione del lavoro di gestione delle configurazioni. L'agente dedicato esegue il backup delle virtual machine a livello di hypervisor, indipendentemente dai sistemi operativi guest.

Requisiti di sistema per agenti

Agente	Spazio su disco richiesto per l'installazione

© Acronis International GmbH, 2003-2024

Agente per Windows	1,2 GB
Agente per Linux	2 GB
Agente per Mac	1 GB
Agente per SQL e Agente per Windows	1,2 GB
Agente per Exchange e Agente per Windows	1,3 GB
Agente per la prevenzione della perdita di dati	500 MB
Agente per Microsoft 365	500 MB
Agente per Active Directory e Agente per Windows	2 GB
Agente per VMware e Agente per Windows	1,5 GB
Agente per Hyper-V e Agente per Windows	1,5 GB
Agente per Virtuozzo e Agente per Linux	1 GB
Agente per Virtuozzo Hybrid Infrastructure	700 MB
Agente per Oracle e Agente per Windows	2,2 GB
Agente per Oracle e Agente per Linux	2 GB
Agente per MySQL/MariaDB e Agente per Linux	2 GB

Le operazioni di backup, inclusa l'eliminazione dei backup, richiedono circa 1 GB di RAM per 1 TB di dimensione del backup. Il consumo di memoria può variare, a seconda della quantità e del tipo di dati elaborati dagli agenti.

Nota
Il consumo di RAM può aumentare quando si esegue il backup su set di backup di dimensioni molto grandi (4 TB e oltre).

Sui sistemi x64, le operazioni con supporto di avvio e ripristino di un disco con un riavvio richiedono almeno 2 GB di memoria.

Nei workload con processori moderni, come Intel Core generazione 11 o AMD Ryzen 7, che supportano la tecnologia CET, alcune funzionalità dell'Agente per la prevenzione della perdita di dati sono disabilitate, per evitare conflitti. Nella tabella seguente è indicata la disponibilità delle funzionalità Controllo dispositivo e Advanced DLP nei sistemi con CPU di questo tipo.

Caratteristiche	Controllo dispositivo	Advanced DLP

© Acronis International GmbH, 2003-2024

Canali locali		
Archivio rimovibile	n/d	Sì
Storage rimovibile crittografato	Sì	n/d
Stampanti	n/d	No
Unità mappate reindirizzate	n/d	Sì
Appunti reindirizzati	n/d	No
Comunicazioni di rete		
E-mail SMTP	n/d	Sì
Microsoft Outlook (MAPI)	n/d	Sì
Note IBM	n/d	No
Webmail	n/d	Sì
Messaggistica istantanea (ICQ)	n/d	No
Messaggistica istantanea (Viber)	n/d	No
Messaggistica istantanea (IRC, Jabber, Skype, Viber)	n/d	Sì
Servizi di condivisione file	n/d	Sì
Social network	n/d	Sì
Condivisione file di rete locale (SMB)	n/d	Sì
Accesso web (HTTP/HTTPS)	n/d	Sì
Trasferimenti di file (FTP/FTPS)	n/d	Sì
Elenco degli elementi consentiti per il trasferimento dei dati		
Elenco degli elementi consentiti per tipo di dispositivi	n/d	Sì
Elenco degli elementi consentiti per comunicazioni di rete	n/d	Sì
Elenco degli elementi consentiti per host remoti	n/d	Sì
Elenco degli elementi consentiti per applicazioni	n/d	Sì
Dispositivi periferici		
Archivio rimovibile	Sì	Sì
Storage rimovibile crittografato	Sì	Sì
Stampanti	No	No
Dispositivi mobile connessi tramite MTP	No	No

© Acronis International GmbH, 2003-2024

Schede Bluetooth	Sì	Sì
Unità ottiche	Sì	Sì
Unità floppy	Sì	Sì
Appunti di Windows	No	No
Acquisisci screenshot	No	No
Unità mappate reindirizzate	Sì	Sì
Appunti reindirizzati	No	No
Auto-protezione con agente di Cyber Protect		
Protezione da utenti finali standard	Sì	Sì
Protezione da amministratori di sistema locali	Sì	Sì

Pacchetti di Linux

Per aggiungere i moduli necessari al kernel Linux, il programma di installazione richiede i seguenti pacchetti Linux:

- Il pacchetto con le sorgenti o intestazioni del kernel. La versione del pacchetto deve corrispondere alla versione del kernel.
- Il sistema del compilatore GNU Compiler Collection (GCC). La versione di GCC deve essere quella con cui è stato compilato il kernel.
- Lo strumento Make.
- L'interprete Perl.
- Le librerie `libelf-dev`, `libelf-devel` o `elfutils-libelf-devel` per creare kernel che iniziano con 4.15 e sono configurati con CONFIG_UNWINDER_ORC=y. Per alcune distribuzioni, come Fedora 28, devono essere separate in modo distinto dalle intestazioni del kernel.

I nomi di questi pacchetti variano a seconda della distribuzione di Linux.

In Red Hat Enterprise Linux, CentOS e Fedora, i pacchetti normalmente saranno installati dal programma di installazione. In altre distribuzioni, è necessario installare i pacchetti se non sono installati o se non hanno la versione richiesta.

I pacchetti richiesti sono già installati?

Per controllare se i pacchetti sono già installati, eseguire questi passaggi:

1. Eseguire il seguente comando per rilevare la versione del kernel e la versione di GCC richiesta:

   ```
   cat /proc/version
   ```


© Acronis International GmbH, 2003-2024

Questo comando restituisce righe simili alla seguente: `Linux version 2.6.35.6` e `gcc version 4.5.1`

2. Eseguire il seguente comando per controllare se lo strumento Make e il compilatore GCC sono installati:

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

Per **gcc**, verificare che la versione restituita dal comando sia la stessa restituita da `gcc version` nel passaggio 1. Per **make**, verificare che il comando sia eseguito.

3. Controllare se la versione appropriata dei pacchetti per la creazione dei moduli del kernel è installata:
   - In Red Hat Enterprise Linux, CentOS e Fedora, eseguire il seguente comando:

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

   - In Ubuntu, eseguire i seguenti comandi:

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

In entrambi i casi, assicurarsi che le versioni del pacchetto siano le stesse della `Linux version` nel passaggio 1.

4. Eseguire il seguente comando per verificare che l'interprete Perl sia installato:

```
perl --version
```

Se vengono visualizzate le informazioni relative alla versione di Perl, l'interprete è installato.

5. In Red Hat Enterprise Linux, CentOS e Fedora, eseguire il seguente comando per verificare che `elfutils-libelf-devel` sia installata:

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

Se vengono visualizzate le informazioni relative alla versione della libreria, questa è installata.

Installazione di pacchetti dal repository

La seguente tabella elenca le modalità di installazione dei pacchetti richiesti in diverse distribuzioni Linux.

Distribuzione Linux	Nome del pacchetto	Come eseguire l'installazione
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make**	Il programma di installazione scaricherà e installerà i pacchetti automaticamente utilizzando l'abbonamento Red Hat.

© Acronis International GmbH, 2003-2024

	elfutils-libelf-devel	
	perl	Lanciare il seguente comando: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Il programma di installazione scaricherà e installerà i pacchetti automaticamente.
	perl	Lanciare il seguente comando: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Eseguire i seguenti comandi:
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

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

I pacchetti verranno scaricati dal repository della distribuzione e installati.

Per altre distribuzioni Linux, fare riferimento alla documentazione della distribuzione relativa ai nomi esatti dei pacchetti richiesti e ai modi per installarli.

Installazione manuale dei pacchetti

Potrebbe essere necessario installare i pacchetti **manualmente** se:

- La macchina non dispone di un abbonamento Red Hat attivo o di una connessione a Internet.
- Il programma di installazione non è grado di trovare la versione di **kernel-devel** o **gcc** corrispondente alla versione del kernel. Se il **kernel-devel** disponibile e più recente del kernel in uso, è necessario aggiornare il kernel o installare manualmente la versione corrispondente di **kernel-devel**.
- I pacchetti richiesti sono disponibili nella rete locale e non si vuole perdere tempo con la ricerca automatica e il download.

© Acronis International GmbH, 2003-2024

Scaricare i pacchetti dalla rete locale o da un sito Web di terze parti affidabile e installarli come indicato di seguito:

- In Red Hat Enterprise Linux, CentOS o Fedora, eseguire il seguente comando come utente root:

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

- In Ubuntu, eseguire il seguente comando:

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

Esempio: Installazione manuale dei pacchetti in Fedora 14

Seguire questi passaggi per installare i pacchetti richiesti in Fedora 14 su una macchina a 32 bit:

1. Eseguire il seguente comando per determinare la versione del kernel e la versione di GCC richiesta:

   ```
   cat /proc/version
   ```

   L'output di questo comando include quanto segue:

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

2. Ottenere i pacchetti **kernel-devel** e **gcc** che corrispondono a questa versione del kernel:

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

3. Ottenere il pacchetto **make** per Fedora 14:

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

4. Installare i pacchetti eseguendo i seguenti comandi come utente root:

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

   È possibile specificare tutti questi pacchetti in un unico comando `rpm`. L'installazione di questi pacchetti potrebbe richiedere l'installazione di pacchetti aggiuntivi per risolvere le dipendenze.

Configurazione delle impostazioni del server proxy

Gli agenti di protezione possono trasferire dati attraverso un server proxy HTTP/HTTPS. Il server deve operare tramite un tunnel HTTP senza analizzare né interferire con il traffico HTTP. Non sono supportati proxy di tipo man-in-the- middle.

© Acronis International GmbH, 2003-2024

Poiché la registrazione dell'agente nel cloud avviene durante l'installazione, è necessario configurare le impostazioni del server proxy durante l'installazione dell'agente o prima.

Per Windows

Se in **Pannello di controllo** > **Opzioni Internet** > **Connessioni** è configurato un server proxy, il programma di installazione legge le impostazioni del server proxy dal registro di sistema e le utilizza automaticamente.

Utilizzare questa procedura per eseguire le attività seguenti.

- Configurare le impostazioni del proxy prima dell'installazione dell'agente.
- Aggiornare le impostazioni del proxy dopo l'installazione dell'agente.

Per configurare le impostazioni del proxy durante l'installazione dell'agente, consultare "Installazione degli agenti di protezione in Windows" (pag. 77).

Nota
Questa procedura è valida solo quando nel sistema non è presente il file `http-proxy.yaml`. Se il file `http-proxy.yaml` è presente nel sistema, è necessario aggiornare le impostazioni del proxy nel file, così da sovrascrivere le impostazioni nel file `aakore.yaml`.

Il file `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml` viene creato quando si configurano le impostazioni del server proxy utilizzando Cyber Protection Monitor. Per ulteriori informazioni, consultare "Configurazione delle impostazioni del server proxy in Cyber Protect Monitor" (pag. 318).

Per aprire il file `http-proxy.yaml`, è necessario essere membri del gruppo Administrators di Windows.

Per configurare le impostazioni del proxy

1. Creare un nuovo documento di testo e aprirlo in un editor di testo, ad esempio Blocco note.
2. Copiare e incollare nel file le righe seguenti.

```
Windows Registry Editor Version 5.00

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

3. Sostituire `proxy.company.com` con il nome host/l'indirizzo IP del server proxy, e `000001bb` con il valore esadecimale del numero della porta. Ad esempio, `000001bb` è la porta 443.
4. Se il proxy server richiede l'autenticazione, sostituire `proxy_login` e `proxy_password` con le credenziali del server proxy. In alternativa, eliminare queste righe dal file.
5. Salvare il documento come `proxy.reg`.
6. Eseguire il file come amministratore.

© Acronis International GmbH, 2003-2024

7. Confermare che si desidera modificare il registro di Windows.
8. Se l'agente non è ancora installato su questo workload, installarlo ora. Se l'agente è già installato su questo workload, andare al passaggio successivo.
9. Aprire il file `%programdata%\Acronis\Agent\etc\aakore.yaml` in un editor di testo.
   Per aprire questo file, è necessario essere membri del gruppo Administrators di Windows.
10. Individuare la sezione **env** o crearla e aggiungere le righe seguenti.

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

11. Sostituire `proxy_login` e `proxy_password` con le credenziali del server proxy e `proxy_address:port` con l'indirizzo e il numero della porta del server proxy.
12. Nel menu **Start**, fare clic su **Esegui**, digitare: **cmd**, quindi fare clic su **OK**.
13. Riavviare il servizio aakore utilizzando i comandi seguenti.

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

14. Riavviare l'agente utilizzando i comandi seguenti.

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

Per macOS

Utilizzare questa procedura per eseguire le attività seguenti.

- Configurare le impostazioni del proxy prima dell'installazione dell'agente.
- Aggiornare le impostazioni del proxy dopo l'installazione dell'agente.

Per configurare le impostazioni del proxy durante l'installazione dell'agente, consultare "Installazione degli agenti di protezione in macOS" (pag. 82).

Per configurare le impostazioni del proxy

1. Creare il file `/Library/Application Support/Acronis/Registry/Global.config` e aprirlo in un editor di testo, ad esempio Text Edit.
2. Copiare e incollare nel file le righe seguenti.

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


© Acronis International GmbH, 2003-2024

```
    </key>
</registry>
```

3. Sostituire `proxy.company.com` con il nome host/l'indirizzo IP del proprio server proxy, e `443` con il valore decimale del numero della porta.
4. Se il proxy server richiede l'autenticazione, sostituire `proxy_login` e `proxy_password` con le credenziali del server proxy. In alternativa, eliminare queste righe dal file.
5. Salvare il file.
6. Se l'agente non è ancora installato su questo workload, installarlo ora. Se l'agente è già installato su questo workload, andare al passaggio successivo.
7. Aprire il file `/Library/Application Support/Acronis/Agent/etc/aakore.yaml` in editor di testo.
8. Individuare la sezione **env** o crearla e aggiungere le righe seguenti.

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

9. Sostituire `proxy_login` e `proxy_password` con le credenziali del server proxy e `proxy_address:port` con l'indirizzo e il numero della porta del server proxy.
10. Andare ad **Applicazioni** > **Utilità** > **Terminale**.
11. Riavviare il servizio aakore utilizzando i comandi seguenti.

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

12. Riavviare l'agente utilizzando i comandi seguenti.

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

Per Linux

Eseguire il file di installazione con i parametri `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`. Utilizzare la procedura seguente per aggiornare le impostazioni del proxy dopo l'installazione dell'agente di protezione.

Per configurare le impostazioni del proxy

1. Aprire il file `/etc/Acronis/Global.config` in un editor di testo.
2. Eseguire una delle seguenti operazioni:
   - Se le impostazioni del proxy sono state specificate durante l'installazione dell'agente, individuare la sezione seguente.

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


© Acronis International GmbH, 2003-2024

```
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- Se le impostazioni del proxy non sono state specificate durante l'installazione dell'agente, copiare le righe seguenti e incollarle nel file fra i tag `<registry name="Global">...</registry>`.

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

3. Sostituire `ADDRESS` con l'indirizzo IP/nome host del server proxy e `PORT` con il valore decimale del numero della porta.
4. Se il server proxy richiede l'autenticazione, sostituire `LOGIN` e `PASSWORD` con le credenziali del server proxy. In alternativa, eliminare queste righe dal file.
5. Salvare il file.
6. Aprire il file `/opt/acronis/etc/aakore.yaml` in un editor di testo.
7. Individuare la sezione **env** o crearla e aggiungere le righe seguenti:

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

8. Sostituire `proxy_login` e `proxy_password` con le credenziali del server proxy e `proxy_address:port` con l'indirizzo e il numero della porta del server proxy.
9. Riavviare il servizio aakore utilizzando il comando seguente.

```
sudo service aakore restart
```

10. Riavviare l'agente eseguendo il comando seguente in qualsiasi directory.

```
sudo service acronis_mms restart
```

Per il supporto di avvio

Quando si opera con il supporto di avvio, potrebbe essere necessario accedere al cloud storage tramite un server proxy. Per configurare le impostazioni del server proxy, fare clic su **Strumenti** > **Server proxy** e specificare il nome host/indirizzo IP, la porta e le credenziali del server proxy.

Installazione degli agenti di protezione

È possibile installare gli agenti sui computer che eseguono uno qualsiasi dei sistemi operativi indicati in "Sistemi operativi e ambienti supportati". I sistemi operativi che supportano le

© Acronis International GmbH, 2003-2024

funzionalità di Cyber Protect sono elencati in "Funzionalità di Cyber Protect supportate in base al sistema operativo".

Download degli agenti di protezione

Prima di installare un agente, è necessario scaricare il relativo file di installazione dalla console di Cyber Protect.

Per scaricare un agente durante l'aggiunta di un workload da proteggere

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Nell'angolo in alto a destra, fare clic su **Aggiungi dispositivo**.
3. Nel riquadro **Aggiungi periferiche**, nel menu a discesa **Canale di release**, selezionare una delle versioni dell'agente.
   - **Release precedente** - Per scaricare la versione dell'agente dalla release precedente.
   - **Corrente** - Per scaricare la versione disponibile più recente dell'agente.
4. Selezionare l'agente corrispondente al sistema operativo del workload da aggiungere.
   Viene visualizzata la finestra di dialogo **Salva come**.
5. [Solo per Mac con processori Apple Silicon (ad esempio Apple M1)] Fare clic su **Annulla**. Nel riquadro **Aggiungi Mac** visualizzato, fare clic sul link **Scarica programma di installazione ARM**.
6. Selezionare una posizione in cui salvare il file di installazione dell'agente e fare clic su **Salva**.

Per scaricare un agente da utilizzare successivamente

1. Nell'angolo in alto a sinistra della console di Cyber Protect, fare clic sull'icona **Utente**.
2. Fare clic su **Download**.
3. Nel riquadro **Download**, nel menu a discesa **Canale di release**, selezionare una delle versioni dell'agente.
   - **Release precedente** - Per scaricare la versione dell'agente dalla release precedente.
   - **Corrente** - Per scaricare la versione disponibile più recente dell'agente.
4. Scorrere l'elenco dei programmi di installazione disponibili per individuare il programma di installazione dell'agente necessario e fare clic sull'icona di download all'estremità della riga.
   Viene visualizzata la finestra di dialogo **Salva come**.
5. Selezionare una posizione in cui salvare il file di installazione dell'agente e fare clic su **Salva**.

Installazione degli agenti di protezione in Windows

Prerequisiti

Scaricare l'agente necessario sul workload da proteggere. Vedere "Download degli agenti di protezione" (pag. 77).

Per installare l'Agente per Windows

© Acronis International GmbH, 2003-2024

1. Accertarsi che la macchina sia connessa a Internet.
2. Accedere come amministratore e avviare il programma di installazione.
3. [Facoltativo] Fare clic su **Personalizza impostazioni di installazione** e apportare le modifiche idonee:
   - Per modificare i componenti da installare (ad esempio, per disabilitare l'installazione di Cyber Protection Monitor o dello strumento da riga di comando o per installare l'Agente per la protezione anti-malware e per il filtro degli URL).

     Nota
     Nei sistemi Windows, la funzionalità di protezione anti-malware richiede l'installazione dell'Agente per la protezione anti-malware e la funzionalità di filtro degli URL richiede l'installazione dell'Agente per il filtro URL. Tali agenti vengono installati automaticamente per i workload protetti se i moduli **Protezione antivirus e anti-malware** e/o **Filtro URL** sono abilitati nei rispettivi piani di protezione.

   - Per modificare il metodo di registrazione del workload al servizio Cyber Protection. È possibile passare da **Utilizza la console del servizio** (impostazione predefinita) a **Utilizza le credenziali** o **Utilizza il token di registrazione**.
   - Per modificare la posizione di installazione.
   - Per modificare l'account utente con cui viene eseguito il servizio agente. Per ulteriori informazioni, consultare "Modifica dell'account di accesso su sistemi Windows" (pag. 85).
   - Per verificare o modificare il nome host/l'indirizzo IP, la porta e le credenziali del server proxy. Se in Windows è abilitato un server proxy, verrà rilevato e utilizzato automaticamente.
4. Fare clic su **Installa**.
5. [Solo durante l'installazione dell'Agente per VMware] Specificare l'indirizzo e le credenziali di accesso per il vCenter Server o l'host ESXi autonomo per il quale eseguire il backup e il ripristino delle virtual machine, quindi fare clic su **Fine**.
   Si consiglia di utilizzare un account dedicato per accedere a vCenter Server o all'host ESXi, e non un account esistente con il ruolo Amministratore. Per ulteriori informazioni sui privilegi richiesti per l'account dedicato, fare riferimento a "Privilegi necessari per l'Agente per VMware" (pag. 714).
6. [Solo durante l'installazione su un controller di dominio] Specificare l'account utente utilizzato per l'esecuzione del servizio agente e quindi fare clic su **Fine**. Per motivi di sicurezza, il programma di installazione non crea automaticamente nuovi account su un controller di dominio.

   Nota
   All'account utente specificato deve essere assegnato il diritto `Accedi come servizio`. Questo account deve essere già stato utilizzato nel controller di dominio, affinché la cartella del relativo profilo possa essere creata in tale sistema.

© Acronis International GmbH, 2003-2024

Per ulteriori informazioni sull'installazione dell'agente in un controller di dominio di sola lettura, consultare questo articolo della Knowledge Base.

7. Se al passaggio 3 si è scelto di mantenere la modalità di registrazione predefinita **Utilizza la console del servizio**, attendere la comparsa della schermata di registrazione, quindi procedere al passaggio successivo. Altrimenti, non è necessaria alcuna azione aggiuntiva.
8. Eseguire una delle seguenti operazioni:
   - Se si accede con un account di amministratore dell'azienda, registrare i workload dell'azienda:
     a. Fare clic su **Registra workload**.
     b. Nella finestra del browser aperta, accedere alla console di Cyber Protect e controllare le informazioni di registrazione.
     c. Nell'elenco **Registra per l'account**, selezionare l'account utente nel quale registrare il workload.
     d. Fare clic su **Controlla codice**, quindi su **Conferma registrazione**.
   - Se si accede con un account di amministratore del partner, registrare i workload per i clienti:
     a. Fare clic su **Registra workload**.
     b. Nella finestra del browser aperta, accedere alla console di Cyber Protect e controllare le informazioni di registrazione.
     c. Nell'elenco **Registra per l'account**, selezionare l'account utente del cliente nel quale registrare il workload.
     d. Fare clic su **Controlla codice**, quindi su **Conferma registrazione**.
   - Fare clic su **Visualizza informazioni di registrazione**. Il programma di installazione mostra il link di registrazione e il codice di registrazione. Se non è possibile completare la registrazione del workload sul sistema in uso, copiare qui il link e il codice della registrazione e quindi eseguire i passaggi per la registrazione su un altro sistema. In questo caso, è necessario inserire il codice di registrazione nel modulo di registrazione. Il codice di registrazione resta valido per un'ora.

     In alternativa, è possibile accedere al modulo di registrazione nel modo seguente: fare clic su **Tutti i dispositivi** > **Aggiungi**, scorrere verso il basso fino all'opzione **Registrazione tramite codice**, fare clic su **Registra**.

     Nota
     Non uscire dal programma di installazione senza confermare la registrazione. Per riavviare la registrazione sarà necessario riavviare il programma di installazione e ripetere la procedura di installazione.

     Il workload viene assegnato all'account che è stato utilizzato per accedere alla console di Cyber Protect.
   - Registrare il workload manualmente utilizzando la riga di comando. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Registrazione e annullamento della registrazione di workload in modalità manuale" (pag. 122).

© Acronis International GmbH, 2003-2024

9. [Se l'agente è registrato in un account il cui tenant è in modalità Conformità] Impostare la password di crittografia.

Installazione degli agenti di protezione in Linux

Preparazione

- Scaricare l'agente necessario sul sistema da proteggere. Vedere "Download degli agenti di protezione" (pag. 77).
- Accertarsi che i pacchetti Linux necessari siano installati sulla macchina.
- Quando si installa l'agente in SUSE Linux, verificare di utilizzare il `su -` invece di `sudo`. In caso contrario, durante il tentativo di registrazione dell'agente tramite la console di Cyber Protect si verifica l'errore seguente: `Impossibile avviare il browser web. Nessun display disponibile.` Alcune distribuzioni Linux, come SUSE, non passano la variabile DISPLAY quando si utilizza sudo e il programma di installazione non può aprire il browser nell'interfaccia utente grafica.

Installazione

Per installare l'Agente per Linux, sono necessari almeno 2 GB di spazio libero su disco.

Per installare l'Agente per Linux

1. Accertarsi che la macchina sia connessa a Internet.
2. Come utente root, passare alla directory con il file di installazione, renderlo eseguibile ed eseguirlo.

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

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

   Se nella rete è abilitato un server proxy, quando si esegue il file di installazione, specificare il nome host o l'indirizzo IP e la porta del server nel formato seguente:`--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`.
   Se si desidera cambiare la modalità predefinita di registrazione della macchina al servizio Cyber Protection, eseguire il file di installazione con uno dei seguenti parametri:
   - `--register-with-credentials` - per chiedere nome utente e password durante l'installazione
   - `--token=STRING` - per utilizzare un token di registrazione
   - `--skip-registration` - per saltare la registrazione
3. Selezionare le caselle di controllo corrispondenti agli agenti da installare. Sono disponibili i seguenti agenti:
   - Agente per Linux
   - Agente per Virtuozzo

© Acronis International GmbH, 2003-2024

- Agente per Oracle
- Agente per MySQL/MariaDB

  Agente per Virtuozzo, Agente per Oracle e Agente per MySQL/MariaDB richiedono anche l'installazione dell'Agente per Linux (64-bit).

4. Se al passaggio 2 si è scelto di mantenere la modalità di registrazione predefinita, procedere al passaggio successivo. Altrimenti, inserire il nome utente e la password del servizio Cyber Protection oppure attendere la registrazione del sistema tramite il token.
5. Eseguire una delle seguenti operazioni:
   - Se si accede con un account di amministratore dell'azienda, registrare i workload dell'azienda:
     a. Fare clic su **Registra workload**.
     b. Nella finestra del browser aperta, accedere alla console di Cyber Protect e controllare le informazioni di registrazione.
     c. Nell'elenco **Registra per l'account**, selezionare l'account utente nel quale registrare il workload.
     d. Fare clic su **Controlla codice**, quindi su **Conferma registrazione**.
   - Se si accede con un account di amministratore del partner, registrare i workload per i clienti:
     a. Fare clic su **Registra workload**.
     b. Nella finestra del browser aperta, accedere alla console di Cyber Protect e controllare le informazioni di registrazione.
     c. Nell'elenco **Registra per l'account**, selezionare l'account utente del cliente nel quale registrare il workload.
     d. Fare clic su **Controlla codice**, quindi su **Conferma registrazione**.
   - Fare clic su **Visualizza informazioni di registrazione**. Il programma di installazione mostra il link di registrazione e il codice di registrazione. Se non è possibile completare la registrazione del workload sul sistema in uso, copiare qui il link e il codice della registrazione e quindi eseguire i passaggi per la registrazione su un altro sistema. In questo caso, è necessario inserire il codice di registrazione nel modulo di registrazione. Il codice di registrazione resta valido per un'ora.

     In alternativa, è possibile accedere al modulo di registrazione nel modo seguente: fare clic su **Tutti i dispositivi** > **Aggiungi**, scorrere verso il basso fino all'opzione **Registrazione tramite codice**, fare clic su **Registra**.

     Nota
     Non uscire dal programma di installazione senza confermare la registrazione. Per riavviare la registrazione sarà necessario riavviare il programma di installazione e ripetere la procedura di installazione.

     Il workload viene assegnato all'account che è stato utilizzato per accedere alla console di Cyber Protect.
   - Registrare il workload manualmente utilizzando la riga di comando. Per ulteriori informazioni

© Acronis International GmbH, 2003-2024

su come eseguire questa operazione, fare riferimento a "Registrazione e annullamento della registrazione di workload in modalità manuale" (pag. 122).

6. [Se l'agente è registrato in un account il cui tenant è in modalità Conformità] Impostare la password di crittografia.
7. Se UEFI Secure Boot è abilitato sul sistema, l'utente verrà informato della necessità di riavvio del sistema dopo l'installazione. Assicurarsi di ricordare la password da utilizzare (quella dell'utente root o "acronis").

   Nota
   L'istallazione genera una nuova chiave che viene utilizzata per la firma dei moduli del kernel. È necessario registrare questa nuova chiave nell'elenco MOK (Machine Owner Key) riavviando il sistema. Se la nuova chiave non viene registrata, l'agente non sarà operativo. Se si abilita UEFI Secure Boot dopo l'installazione dell'agente, è necessario reinstallare l'agente.

8. Al termine dell'installazione, eseguire una delle seguenti operazioni:
   - Se al passaggio precedente era stato richiesto di riavviare il sistema, fare clic su **Riavvia**. Durante il riavvio del sistema, dirigersi alla gestione del codice del proprietario della macchina, selezionare **Registrazione codice del proprietario della macchina**, quindi registrarlo utilizzando la password suggerita al passaggio precedente.
   - Altrimenti, fare clic su **Esci**.

Nel file sono fornite le informazioni per la risoluzione dei problemi:
`/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

Installazione degli agenti di protezione in macOS

Prerequisiti

Scaricare l'agente necessario sul workload da proteggere. Vedere "Download degli agenti di protezione" (pag. 77).

Per installare l'Agente per Mac (x64 o ARM64)

1. Accertarsi che la macchina sia connessa a Internet.
2. Fare doppio clic sul file di istallazione (.dmg).
3. Attendere mentre il sistema operativo monta l'immagine del disco di installazione.
4. Fare doppio clic su **Installa**.
5. Se nella rete è abilitato un server proxy, fare clic su **Agente di protezione** nella barra dei menu, quindi su **Impostazioni del server proxy** e specificare il nome host/indirizzo IP, la porta e le credenziali del server proxy.
6. Se richiesto, fornire le credenziali amministrative.
7. Fare clic su **Continua**.
8. Attendere che venga visualizzata la schermata di registrazione.

© Acronis International GmbH, 2003-2024

9. Eseguire una delle seguenti operazioni:
   - Se si accede con un account di amministratore dell'azienda, registrare i workload dell'azienda:
     a. Fare clic su **Registra workload**.
     b. Nella finestra del browser aperta, accedere alla console di Cyber Protect e controllare le informazioni di registrazione.
     c. Nell'elenco **Registra per l'account**, selezionare l'account utente nel quale registrare il workload.
     d. Fare clic su **Controlla codice**, quindi su **Conferma registrazione**.
   - Se si accede con un account di amministratore del partner, registrare i workload per i clienti:
     a. Fare clic su **Registra workload**.
     b. Nella finestra del browser aperta, accedere alla console di Cyber Protect e controllare le informazioni di registrazione.
     c. Nell'elenco **Registra per l'account**, selezionare l'account utente del cliente nel quale registrare il workload.
     d. Fare clic su **Controlla codice**, quindi su **Conferma registrazione**.
   - Fare clic su **Visualizza informazioni di registrazione**. Il programma di installazione mostra il link di registrazione e il codice di registrazione. Se non è possibile completare la registrazione del workload sul sistema in uso, copiare qui il link e il codice della registrazione e quindi eseguire i passaggi per la registrazione su un altro sistema. In questo caso, è necessario inserire il codice di registrazione nel modulo di registrazione. Il codice di registrazione resta valido per un'ora.

     In alternativa, è possibile accedere al modulo di registrazione nel modo seguente: fare clic su **Tutti i dispositivi** > **Aggiungi**, scorrere verso il basso fino all'opzione **Registrazione tramite codice**, fare clic su **Registra**.

     Nota
     Non uscire dal programma di installazione senza confermare la registrazione. Per riavviare la registrazione sarà necessario riavviare il programma di installazione e ripetere la procedura di installazione.

     Il workload viene assegnato all'account che è stato utilizzato per accedere alla console di Cyber Protect.
   - Registrare il workload manualmente utilizzando la riga di comando. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Registrazione e annullamento della registrazione di workload in modalità manuale" (pag. 122).
10. [Se l'agente è registrato in un account il cui tenant è in modalità Conformità] Impostare la password di crittografia.
11. Se la versione di macOS in uso è Mojave 10.14.x o successiva, concedere all'agente di protezione l'accesso completo al disco per abilitare le operazioni di backup.

    Per istruzioni, leggere l'articolo Grant the 'Full Disk Access' permission to the Cyber Protection agent (64657) (in inglese).

© Acronis International GmbH, 2003-2024

12. Per utilizzare la funzionalità di desktop remoto, concedere le autorizzazioni di sistema richieste a Connect Agent. Per ulteriori informazioni, consultare "Concedere le autorizzazioni di sistema richieste a Connect Agent" (pag. 84).

Concedere le autorizzazioni di sistema richieste a Connect Agent

Per abilitare tutte le funzionalità dal desktop remoto nei workload macOS, oltre alle autorizzazioni complete per l'accesso al disco è necessario garantire a Connect Agent le autorizzazioni seguenti:

- Registrazione dello schermo - Abilita la registrazione dello schermo del workload macOS tramite NEAR. Fino a quando questa autorizzazione non viene concessa, non sarà consentita nessuna connessione di controllo da remoto.
- Accessibilità - Abilita le connessioni remote in modalità di controllo tramite NEAR
- Microfono - Abilita il reindirizzamento dell'audio dal workload macOS remoto al workload locale tramite NEAR. Per abilitare la funzionalità di reindirizzamento dell'audio, nel workload deve essere installato un driver di acquisizione audio. Per ulteriori informazioni, consultare "Reindirizzamento audio remoto" (pag. 1017).
- Automazione - Abilita l'azione Svuota cestino

Dopo aver avviato l'agente nel workload macOS, il sistema controlla che l'agente abbia i diritti richiesti e chiede di concedere le autorizzazioni se necessario.

Per concedere l'autorizzazione Registrazione dello schermo

1. Nella finestra di dialogo **Concedi le autorizzazioni di sistema richieste** per l'agente Cyber Protect, fare clic su **Configura autorizzazioni di sistema**.
2. Nella finestra di dialogo **Autorizzazioni di sistema**, fare clic su **Richiedi autorizzazione Registrazione dello schermo**.
3. Fare clic su **Apri preferenze di sistema**.
4. Selezionare **Connect Agent**.

Se l'agente non ha l'autorizzazione quando si tenta di accedere al workload da remoto, verrà visualizzata la finestra di dialogo Richiedi autorizzazione Registrazione dello schermo. Solo l'utente locale potrà rispondere nella finestra.

Per concedere l'autorizzazione Accessibilità

1. Nella finestra di dialogo **Concedi le autorizzazioni di sistema richieste** per l'agente Cyber Protect, fare clic su **Configura autorizzazioni di sistema**.
2. Nella finestra di dialogo **Autorizzazioni di sistema**, fare clic su **Richiedi autorizzazione Accessibilità**.
3. Fare clic su **Apri preferenze di sistema**.
4. Fare clic sull'icona a lucchetto chiuso nell'angolo in basso a sinistra, in modo che cambi in lucchetto aperto. Il sistema chiederà una password di amministratore per apportare le modifiche.
5. Selezionare **Connect Agent**.

© Acronis International GmbH, 2003-2024

Per concedere l'autorizzazione Microfono

1. Nella finestra di dialogo **Concedi le autorizzazioni di sistema richieste** per Connect Agent, fare clic su **Configura autorizzazioni di sistema**.
2. Nella finestra di dialogo **Autorizzazioni di sistema**, fare clic su **Richiedi autorizzazione Microfono**.
3. Fare clic su **OK**.

Nota
È necessario installare un driver di acquisizione audio nel workload macOS affinché l'agente possa utilizzare l'autorizzazione concessa e reindirizzare l'audio del workload. Per ulteriori informazioni, consultare "Reindirizzamento audio remoto" (pag. 1017).

Per concedere l'autorizzazione Automazione

1. Nella finestra di dialogo **Concedi le autorizzazioni di sistema richieste** per Connect Agent, fare clic su **Configura autorizzazioni di sistema**.
2. Nella finestra di dialogo **Autorizzazioni di sistema**, fare clic su **Richiedi autorizzazione Automazione**.

Modifica dell'account di accesso su sistemi Windows

Nella schermata **Seleziona componenti**, definire l'account nel quale verranno eseguiti i servizi specificando **Account di accesso per il servizio agente**. È possibile selezionare una delle seguenti opzioni:

- **Usa gli account degli utenti del servizio** (impostazione predefinita per il servizio agente)
  Gli account degli utenti del servizio sono account di sistema Windows usati per eseguire i servizi. Questa impostazione è vantaggiosa perché i criteri di sicurezza del dominio non influiscono sui diritti utente di questi account. Per impostazione predefinita l'agente viene eseguito con l'account **Sistema locale**.
- **Crea un nuovo account**
  Il nome account sarà l'Agent User dell'agente.
- **Usa il seguente account**
  Se l'agente viene installato in un controller di dominio, il sistema chiede di specificare gli account esistenti (o lo stesso account) per l'agente. Per motivi di sicurezza, il sistema non crea automaticamente nuovi account su un controller di dominio.
  All'account utente specificato deve essere assegnato il diritto `Accedi come servizio` quando il programma di installazione viene eseguito su un controller di dominio. Questo account deve essere già stato utilizzato nel controller di dominio, affinché la cartella del relativo profilo possa essere creata in tale sistema.
  Per ulteriori informazioni sull'installazione dell'agente in un controller di dominio di sola lettura, consultare questo articolo della Knowledge Base.

© Acronis International GmbH, 2003-2024

Se si sceglie l'opzione **Crea un nuovo account** o **Usa il seguente account**, verificare che i criteri di sicurezza del dominio non influiscano sui diritti degli account correlati. Se un account viene privato dei diritti utente assegnati durante l'installazione, il componente potrebbe non funzionare correttamente.

Privilegi richiesti per l'account di accesso

Un agente di protezione viene eseguito come servizio MMS (Managed Machine Service) su un sistema Windows. L'account nel quale viene eseguito l'agente dispone delle credenziali per il corretto funzionamento dell'agente stesso. Pertanto, all'utente del servizio MMS devono essere assegnati i privilegi seguenti:

1. L'utente deve essere incluso nei gruppi **Operatori di Backup** e **Administrators**. Nel controller di dominio, l'utente deve essere incluso nel gruppo degli **amministratori di dominio**.
2. All'utente è concessa l'autorizzazione **Controllo completo** sulla cartella `%PROGRAMDATA%\Acronis` (in Windows XP e Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) e sulle relative cartelle secondarie.
3. All'utente è concessa l'autorizzazione **Controllo completo** per le chiavi di registro all'interno della chiave seguente: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. All'utente sono assegnati i diritti utente seguenti:
   - Accesso come servizio
   - Regolazione limite risorse memoria per un processo
   - Sostituzione di token a livello di processo
   - Modifica dei valori di ambiente firmware

Come assegnare i diritti utente

Attenersi alla procedura seguente per assegnare i diritti utente; questo esempio utilizza il diritto utente **Accesso come servizio**, ma i passaggi sono gli stessi per gli altri diritti utente:

1. Accedere al computer utilizzando un account con privilegi di amministrazione.
2. Nel **Pannello di controllo** aprire **Strumenti di amministrazione** (oppure fare clic su Win+R, digitare **control admintools** e premere Invio) e aprire **Criteri di sicurezza locali**.
3. Espandere i **Criteri locali** e fare clic su **Assegnazione diritti utente.**
4. Nel riquadro di destra, fare clic con il pulsante destro del mouse su **Accesso come servizio** e selezionare **Proprietà**.
5. Fare clic sul pulsante **Aggiungi utente o gruppo** per aggiungere un nuovo utente.
6. Nella finestra **Seleziona utenti, computer, account di servizio o gruppi**, individuare l'utente da aggiungere e fare clic su **OK**.
7. Fare clic su **OK** in **Accesso come servizio Proprietà** per salvare le modifiche.

© Acronis International GmbH, 2003-2024

Importante
Accertarsi che l'utente aggiunto al diritto utente **Accesso come servizio** non sia elencato nel criterio **Nega accesso come servizio** in **Criteri di sicurezza locali**.

Tenere presente che non è consigliabile modificare gli account di accesso manualmente una volta completata l'installazione.

Installazione e disinstallazione dinamica di componenti

Per i workload Windows protetti dalla versione dell'agente 15.0.26986 (rilasciata a maggio 2021) o versioni successive, i componenti seguenti vengono installati dinamicamente, ovvero solo quando richiesto da un piano di protezione:

- Agente per il filtro URL: richiesto per le funzionalità del filtro URL.
- Agente per la Protezione anti-malware: richiesto per le funzionalità di protezione anti-malware.
- Agente per la Prevenzione della perdita di dati: richiesto per le funzionalità di controllo dei dispositivi.

Per impostazione predefinita questi componenti non vengono installati. Il rispettivo componente viene installato automaticamente qualora un workload venga protetto da un piano per il quale è abilitato uno qualsiasi dei moduli seguenti:

- Protezione antivirus e anti-malware
- Filtro URL
- Controllo dispositivo

Allo stesso modo, se non è presente un piano di protezione che richiede le funzionalità di protezione anti-malware, filtro degli URL o controllo dei dispositivi, il rispettivo componente viene automaticamente disinstallato.

Successivamente alla modifica del piano di protezione, l'installazione o la disinstallazione dinamica dei componenti richiede 10 minuti. Tuttavia, se una qualsiasi delle seguenti operazioni è in esecuzione, l'installazione o la disinstallazione dinamica verrà avviata al termine dell'operazione:

- Backup
- Ripristino
- Replica di backup
- Replica della virtual machine
- Prova di una copia
- Esecuzione di una virtual machine da un backup (finalizzazione inclusa)
- Failover di disaster recovery
- Failback di disaster recovery

© Acronis International GmbH, 2003-2024

- Esecuzione di uno script (per la funzionalità di Cyber Scripting)
- Installazione patch
- Backup di configurazioni ESXi

Installazione o disinstallazione automatica

Installazione o disinstallazione automatica in Windows

In Windows, è possibile eseguire l'installazione o la disinstallazione automatica con le modalità seguenti:

- Utilizzando il file EXE per il programma di installazione e specificando i parametri di installazione nella riga di comando.
- Utilizzando il file MSI estratto dal programma di installazione e specificando i parametri di installazione con una delle modalità seguenti:
  - in un file MST
  - direttamente nella riga di comando

Installazione e disinstallazione automatica con un file EXE

Per questo tipo di installazione automatica, scaricare il programma di installazione e avviarlo dalla riga di comando con i parametri di installazione necessari. Per ulteriori informazioni sui parametri che è possibile utilizzare, consultare "Parametri per l'installazione automatica (EXE)" (pag. 90).

Non è necessario decomprimere i pacchetti di installazione e i file MSI e MST in anticipo.

Installare e disinstallare agenti e componenti (EXE)

Per eseguire l'installazione automatica con un file EXE, eseguire il programma di installazione e specificare i parametri di installazione nella riga di comando.

Per scaricare il programma di installazione, nella console di Cyber Protect, fare clic sull'icona dell'account nell'angolo in alto a destra e quindi su **Download**. Il collegamento per il download è disponibile nel pannello **Aggiungi dispositivi**.

Per installare agenti e componenti

1. Avviare l'interfaccia a riga di comando come amministratore, quindi individuare il file EXE del programma di installazione.
2. Per avviare il programma di installazione e specificare i parametri di installazione, eseguire il comando seguente:

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

   Utilizzare gli spazi per separare i parametri e le virgole senza spazi per separare i valori di un parametro. Per esempio:

© Acronis International GmbH, 2003-2024

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

Per verificare i parametri disponibili e i relativi valori, consultare "Parametri per l'installazione automatica (EXE)" (pag. 90).

Esempi

- Installazione dell'Agente per Windows, dell'Agente per la protezione anti-malware e per il filtro degli URL, dello strumento da riga di comando e di Cyber Protect Monitor. Registrazione del workload al servizio Cyber Protection utilizzando un nome utente e una password.

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

- Installazione dell'Agente per Windows, dello strumento da riga di comando e di Cyber Protect Monitor. Creazione di un nuovo account di accesso per il servizio agente in Windows. Registrazione del workload al servizio Cyber Protection utilizzando un token.

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

- Installazione dell'Agente per Windows, dello strumento da riga di comando, dell'Agente per Oracle e di Cyber Protect Monitor. Registrazione del sistema al servizio Cyber Protection utilizzando un nome utente e una password.

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

- Installazione dell'Agente per Windows, dello strumento da riga di comando e di Cyber Protect Monitor. Impostazione della lingua tedesca nell'interfaccia utente. Registrazione del sistema al servizio Cyber Protection utilizzando un token. Impostazione di un proxy HTTP.

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

Per rimuovere un componente installato

© Acronis International GmbH, 2003-2024

1. Avviare l'interfaccia a riga di comando come amministratore, quindi passare a `%ProgramFiles%\BackupClient\RemoteInstall`.
2. Lanciare il seguente comando:

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

   Per verificare i parametri disponibili e i relativi valori, consultare "Parametri per l'installazione automatica (EXE)" (pag. 90).

Esempio

- Disinstallazione di Cyber Protect Monitor.

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

Per disinstallare un agente

1. Avviare l'interfaccia a riga di comando come amministratore, quindi passare a `%Program Files%\Common Files\Acronis\BackupAndRecovery`.
2. Lanciare il seguente comando:

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

   Per verificare i parametri disponibili e i relativi valori, consultare "Parametri per l'installazione automatica (EXE)" (pag. 90).

Esempi

- Disinstallazione dell'Agente per Windows e di tutti i relativi componenti. Eliminazione di tutti i registri, le attività e le impostazioni di configurazione.

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

- Disinstallazione di un Agente per Windows protetto da password e di tutti i relativi componenti. Eliminazione di tutti i registri, le attività e le impostazioni di configurazione.

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

Parametri per l'installazione automatica (EXE)

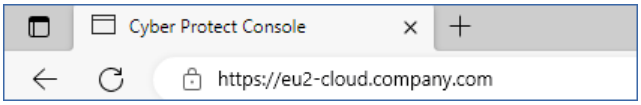
La tabella seguente riepiloga i parametri per l'installazione automatica con un file EXE.

Parametri	Descrizione
Parametri generici	

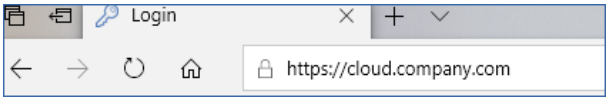
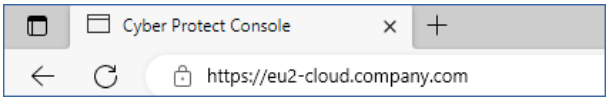
© Acronis International GmbH, 2003-2024

Parametri	Descrizione
`--add-components=`<component1,component2,...,componentN>	I componenti da installare. Per l'elenco completo dei componenti disponibili, consultare "Componenti per l'installazione automatica (EXE)" (pag. 95). Se si specificano più componenti, separarli con le virgole. Non aggiungere spazi prima o dopo la virgola. Se si specificano componenti già installati, questi vengono riparati o aggiornati, a seconda della versione del programma di installazione e dei componenti installati. Se questo parametro non viene specificato, viene installato un set di componenti predefinito, in base al sistema sul quale viene eseguita l'installazione. Ad esempio, Agente per SQL viene installato solo su sistemi che eseguono MS SQL Server.
`--install-dir=`<path>	La cartella nella quale vengono installati i componenti selezionati. Se la cartella specificata non esiste, viene creata. Se questo parametro non viene specificato, viene utilizzata una cartella predefinita: `C:\Programmi\BackupClient`.
`--log-dir=`<path>	La cartella nella quale vengono salvati i registri di installazione. Se questo parametro non viene specificato, viene utilizzata una cartella predefinita: `%ProgramData%\Acronis\InstallationLogs`.
`--language=`<code>	Lingua del prodotto. Sono disponibili le variabili seguenti: en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Se questo parametro non viene specificato, e se la lingua di sistema del sistema su cui viene eseguita l'installazione è indicata nell'elenco precedente, viene utilizzata la lingua di sistema. In tutti gli altri casi, il valore è impostato su en.
`--quiet`	Utilizzare questo parametro per eseguire il programma di installazione senza mostrare l'interfaccia utente grafica. Non utilizzare questo parametro insieme al parametro `--register-only`.

© Acronis International GmbH, 2003-2024

Parametri	Descrizione
`--help`	Utilizzare questo parametro per visualizzare un elenco di tutti i parametri disponibili che è possibile utilizzare nella riga di comando, con le relative descrizioni.
`--fss-onboarding-auto-start`	Utilizzare questo parametro insieme al parametro `--quiet` per visualizzare la procedura guidata di onboarding di File Sync & Share dopo un'installazione automatica.
Parametri di registrazione	
`--registration={skip | by-credentials | by-token | device-flow}`	Utilizzare questo parametro per scegliere la modalità di registrazione dell'agente dopo l'installazione. Per ignorare la registrazione, specificare `skip`. È possibile registrare l'agente in un secondo momento, utilizzando il parametro `--register-only`. Per registrare l'agente utilizzando le credenziali, specificare `by-credentials`, quindi utilizzare i parametri `--reg-login` e `--reg-password`. Inoltre, è possibile utilizzare solo i parametri `--reg-login` e `--reg-password`. In questo caso, è facoltativo specificare `--registration=by-credentials`. Per registrare l'agente con un token di registrazione, specificare `by-token`, quindi utilizzare il parametro `--reg-token`. È anche possibile utilizzare solo il parametro `--reg-token`. In questo caso, è facoltativo specificare `--registration=by-token`. Per registrare l'agente usando il protocollo OAuth 2.0, specificare `device-flow`. La pagina di registrazione viene visualizzata al completamento dell'installazione. Quando si utilizza il parametro `--registration=device-flow`, specificare l'indirizzo esatto del data center come valore del parametro `--reg-address`. Tale indirizzo corrisponde all'URL visualizzato **dopo aver fatto accesso** al servizio Cyber Protection. Ad esempio, `https://eu2-cloud.company.com`.  Non utilizzare `--registration=device-flow` con il parametro `--quiet`.
`--reg-address=<url>`	URL del servizio Cyber Protection. È possibile utilizzare questo parametro con i parametri `--reg-login` e `--reg-`

© Acronis International GmbH, 2003-2024

Parametri	Descrizione
	`password`, oppure con il parametro `--reg-token`. • Quando si utilizza con i parametri `--reg-login` e `--reg-password`, specificare l'indirizzo che si utilizza per **accedere** al servizio Cyber Protection. Ad esempio, `https://cloud.azienda.com`:  • Quando si utilizza con il parametro `--reg-token`, specificare l'indirizzo esatto del data center. Tale indirizzo corrisponde all'URL visualizzato **dopo aver fatto accesso** al servizio Cyber Protection. Ad esempio, `https://eu2-cloud.company.com`.  Non utilizzare `https://cloud.company.com` con il parametro `--reg-token`.
`--reg-login=`<login> `--reg-password=`<password>	Le credenziali dell'account con il quale l'agente viene registrato nel servizio Cyber Protection. Non può essere utilizzato l'account di un amministratore partner. Quando si utilizzano questi parametri, è facoltativo specificare il parametro `--registration`. Non utilizzare questi parametri con il parametro `--reg-token`.
`--reg-token=`<token>	Il token di registrazione. Il token di registrazione è costituito da una serie di 12 caratteri, divisi da trattini in tre segmenti. Per ulteriori informazioni su come generarne uno, consultare "Generazione del token di registrazione" (pag. 172). Quando si utilizza questo parametro, è facoltativo specificare il parametro `--registration`. Non utilizzare questo parametro con i parametri `--reg-login` e `--reg-password`.
`--register-only`	Utilizzare questo parametro per ignorare l'installazione e registrare l'agente usando il protocollo OAuth 2.0 (device-flow). La pagina di registrazione viene visualizzata al completamento dell'installazione. Non utilizzare `--register-only` con il parametro `--quiet`.

© Acronis International GmbH, 2003-2024

Parametri	Descrizione
Account di accesso per il servizio agente	
`--agent-account`={system | new | custom} oppure `--agent-account-login`=<login> `--agent-account-password`=<password>	Utilizzare questo parametro per specificare l'account di accesso con cui viene eseguito il servizio agente. Per ulteriori informazioni sugli account di accesso, consultare "Modifica dell'account di accesso su sistemi Windows" (pag. 85). Per utilizzare l'account **Local System**, specificare `--agent-account=system` oppure non utilizzare il parametro `--agent-account` nel comando. Affinché il servizio agente venga eseguito con un nuovo account di accesso, **Acronis Agent User**, che viene creato automaticamente, specificare `new`. Affinché il servizio agente venga eseguito con un account esistente, specificare le credenziali dell'account utilizzando i parametri `--agent-account-login` e `--agent-account-password`. In questo caso, è facoltativo specificare il parametro `--agent-account=custom`.
Parametri di vCenter/ESXi	
`--esxi-address`=<host>	Il nome host o l'indirizzo IP del vCenter Server o dell'host ESXi. Utilizzare questo parametro quando si installa Agente per VMware.
`--esxi-login`=<login> `--esxi-password`=<password>	Le credenziali per accedere a vCenter Server o all'host ESXi. Utilizzare questi parametri quando si installa Agente per VMware.
Parametri del proxy	
`--http-proxy`={none | system | custom}	Utilizzare questo parametro per indicare il server proxy HTTP da utilizzare per il backup e il ripristino dal cloud storage. Per disabilitare le connessioni al server proxy, specificare `--http-proxy=none`. Per utilizzare un server proxy valido per l'intero sistema, specificare `--http-proxy=system` oppure non utilizzare il parametro `--http-proxy` nel comando. Per utilizzare un altro server proxy, specificare l'indirizzo e le credenziali del server proxy utilizzando i parametri -

© Acronis International GmbH, 2003-2024

Parametri	Descrizione
	`-http-proxy-address`, `--http-proxy-login` e `--http-proxy-password`. In questo caso, è facoltativo specificare il parametro `--http-proxy=custom`.
`--http-proxy-address=`<host>:<port>	Il nome dell'host o l'indirizzo IP e la porta del server proxy HTTP personalizzato.
`--http-proxy-login=`<login>	Login del server proxy HTTP personalizzato.
`--http-proxy-password=`<password>	Password del server proxy HTTP personalizzato.
Parametri di disinstallazione	
`--remove-components=`<component1,component2,...,componentN>	I componenti da disinstallare. Per l'elenco completo dei componenti disponibili, consultare "Componenti per l'installazione automatica (EXE)" (pag. 95). Se si specificano più componenti, separarli con le virgole. Non aggiungere spazi prima o dopo la virgola. **Importante** Utilizzando questo parametro è possibile disinstallare solo i componenti. Per disinstallare completamente il prodotto, passare al Pannello di controllo di Windows > Programmi e funzionalità, selezionare il prodotto e quindi fare clic su **Disinstalla**.
`--delete-all-settings`	Utilizzare questo parametro facoltativo quando si usa il parametro `--remove-components` per eliminare tutti i registri, le attività e le impostazioni di configurazione del prodotto.
`--anti-tamper-password=`<password>	La password richiesta per disinstallare un Agente per Windows protetto con password o di modificarne i componenti.

Componenti per l'installazione automatica (EXE)

La tabella seguente riepiloga i componenti che è possibile utilizzare per l'installazione automatica tramite un file EXE. Utilizzare i nomi dei valori per specificare i valori per il parametro `--add-components`.

Per ulteriori informazioni, consultare "Parametri per l'installazione automatica (EXE)" (pag. 90)"Parametri per l'installazione automatica (MSI)" (pag. 100)

Nome del valore	Descrizione del componente
`agentForWindows`	Agente per Windows

© Acronis International GmbH, 2003-2024

Nome del valore	Descrizione del componente
`agentForSas`	Agente per File Sync & Share
`agentForAd`	Agente per Active Directory
`agentForAmp`	Agente per la protezione anti-malware e per il filtro URL
`agentForDlp`	Agente per la prevenzione della perdita di dati
`agentForEsx`	Agente per VMware (Windows)
`agentForExchange`	Agente per Exchange
`agentForHyperV`	Agente per Hyper-V
`agentForOffice365`	Agente per Office 365
`agentForOracle`	Agente per Oracle
`agentForSql`	Agente per SQL
`commandLine`	Strumento da riga di comando
`mediaBuilder`	Generatore di supporti riavviabili
`trayMonitor`	Cyber Protect Monitor
`all`	Questo valore combina tutti i componenti.
`allAgents`	Questo valore combina tutti gli agenti.

Installazione e disinstallazione automatica con un file MSI

Per questo tipo di installazione automatica, utilizzare Windows Installer (il programma `Msiexec`). Estrarre in anticipo i pacchetti di installazione e il file MSI utilizzando l'interfaccia utente grafica del programma di installazione.

Quando si installano i componenti con un file MSI, è possibile utilizzare un file di trasformazione MST per personalizzare i parametri di installazione. Per ulteriori informazioni su come utilizzare la combinazione di file MSI e MST, consultare "Installare agenti e componenti (combinazione di MSI e MST)" (pag. 97). È possibile utilizzare questo metodo di installazione in un dominio di Active Directory per installare gli agenti di protezione tramite Criteri di gruppo di Windows. Per ulteriori informazioni, consultare "Distribuzione di agenti tramite i Criteri di gruppo" (pag. 171).

In alternativa, è possibile specificare i parametri di installazione manualmente nella riga di comando. In questo caso, il file MST non è necessario. Per ulteriori informazioni, consultare "Esempi" (pag. 98).

© Acronis International GmbH, 2003-2024

Estrazione dei file MSI, MST e CAB

Estrarre i file MSI, MST e CAB con i pacchetti di installazione eseguendo l'interfaccia utente grafica del programma di installazione.

Per estrarre i file MSI, MST e CAB

1. Eseguire l'interfaccia utente grafica del programma di installazione, quindi fare clic su **Creare file .mst e .msi per l'installazione automatica**.
2. In **Cosa installare**, scegliere i componenti che si desidera installare, quindi fare clic su **Fine**.
   I pacchetti di installazione per questi componenti verranno estratti dal programma di installazione come file CAB.
3. In **Impostazioni di registrazione**, selezionare **Utilizza le credenziali** o **Utilizza il token di registrazione**. A seconda della scelta effettuata, specificare le credenziali o il token di registrazione e quindi fare clic su **Fine**.
   Per ulteriori informazioni su come generare un token di registrazione, consultare "Generazione del token di registrazione" (pag. 172).
4. [Solo durante l'installazione su un controller di dominio] In **Account di accesso per il servizio agente**, selezionare **Usa il seguente account**. Specificare l'account utente utilizzato per l'esecuzione del servizio agente e quindi fare clic su **Fine**. Per motivi di sicurezza, il programma di installazione non crea automaticamente nuovi account su un controller di dominio.

   Nota
   All'account utente specificato deve essere assegnato il diritto `Accedi come servizio`. Questo account deve essere già stato utilizzato nel controller di dominio, affinché la cartella del relativo profilo possa essere creata in tale sistema.

   Per ulteriori informazioni sull'installazione dell'agente in un controller di dominio di sola lettura, consultare questo articolo della Knowledge Base.
5. Rivedere o modificare le altre impostazioni di installazione che verranno aggiunte al file MST, quindi fare clic su **Procedi**.
6. Selezionare la cartella nella quale verranno estratti i file MSI, MST e CAB, quindi fare clic su **Genera**.

Installare agenti e componenti (combinazione di MSI e MST)

Utilizzare il file MST per personalizzare l'impostazione di installazione del file MSI. Utilizzare i file MSI e MST in combinazione quando si installano gli agenti su più sistemi tramite un criterio di gruppo Windows. Per ulteriori informazioni, consultare "Distribuzione di agenti tramite i Criteri di gruppo" (pag. 171).

Per installare i componenti con file MSI e MST

© Acronis International GmbH, 2003-2024

1. Estrarre i file MSI e MST come indicato in "Estrazione dei file MSI, MST e CAB" (pag. 97).
2. Nell'interfaccia a riga di comando del sistema in cui installare i componenti, eseguire il comando seguente:

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

   Per esempio:

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

Installare e disinstallare agenti e componenti (MSI e selezione diretta)

Eseguire il file MSI, selezionare manualmente i componenti da installare e specificare i rispettivi parametri di installazione nella riga di comando. In questo caso, il file MSR non è necessario.

Per installare agenti e componenti

1. Estrarre il file MSI e i pacchetti di installazione (file CAB) come indicato in "Estrazione dei file MSI, MST e CAB" (pag. 97).

   Per questo metodo di installazione sono necessari solo i file MSI e CAB. Il file MST non è necessario.
2. Nell'interfaccia a riga di comando del sistema, eseguire il comando seguente:

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

   Utilizzare gli spazi per separare i parametri e le virgole senza spazi per separare i valori di un parametro. Per esempio:

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

   Per verificare i parametri disponibili e i relativi valori, consultare "Parametri per l'installazione automatica (MSI)" (pag. 100).

Esempi

- Installazione dell'Agente per Windows, dell'Agente per la protezione anti-malware e per il filtro degli URL, dello strumento da riga di comando e di Cyber Protect Monitor. Registrazione del workload al servizio Cyber Protection utilizzando un nome utente e una password.

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


© Acronis International GmbH, 2003-2024

- Installazione dell'Agente per Windows, dello strumento da riga di comando e di Cyber Protect Monitor. Creazione di un nuovo account di accesso per il servizio agente in Windows. Registrazione del workload al servizio Cyber Protection utilizzando un token.

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

- Installazione dell'Agente per Windows, dello strumento da riga di comando, dell'Agente per Oracle e di Cyber Protect Monitor. Registrazione del sistema al servizio Cyber Protection utilizzando un nome utente e una password con codifica in Base64. Se la password contiene caratteri speciali o spazi, potrebbe essere necessario codificarla. Per ulteriori informazioni su come codificare una password, consultare "Password con caratteri speciali o spazi" (pag. 126).

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

- Installazione dell'Agente per Windows, dello strumento da riga di comando e di Cyber Protect Monitor. Registrazione del sistema al servizio Cyber Protection utilizzando un token. Impostazione di un proxy HTTP.

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

Per rimuovere un componente installato

1. Estrarre il file MSI e i pacchetti di installazione (file CAB) come indicato in "Estrazione dei file MSI, MST e CAB" (pag. 97).
   Per questo metodo di installazione sono necessari solo i file MSI e CAB. Il file MST non è necessario.
2. Nell'interfaccia a riga di comando del sistema, eseguire il comando seguente:

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

   Per verificare i parametri disponibili e i relativi valori, consultare "Parametri per l'installazione automatica (MSI)" (pag. 100).

© Acronis International GmbH, 2003-2024

Esempio

- Rimuovere Cyber Protect monitor.

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

Per disinstallare un agente

1. Estrarre il file MSI e i pacchetti di installazione (file CAB) come indicato in "Estrazione dei file MSI, MST e CAB" (pag. 97).

   Per questo metodo di installazione sono necessari solo i file MSI e CAB. Il file MST non è necessario.
2. Nell'interfaccia a riga di comando del sistema, eseguire il comando seguente:

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

   Per verificare i parametri disponibili e i relativi valori, consultare "Parametri per l'installazione automatica (MSI)" (pag. 100).

Esempi

- Disinstallazione dell'Agente per Windows e di tutti i relativi componenti. Eliminazione di tutti i registri, le attività e le impostazioni di configurazione.

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

- Disinstallazione di un Agente per Windows protetto da password e di tutti i relativi componenti. Eliminazione di tutti i registri, le attività e le impostazioni di configurazione.

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

Parametri per l'installazione automatica (MSI)

La tabella seguente riepiloga i parametri per l'installazione automatica quando si utilizza un file MSI.

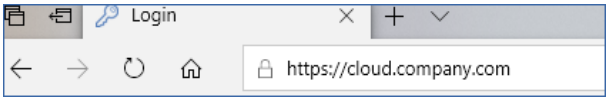
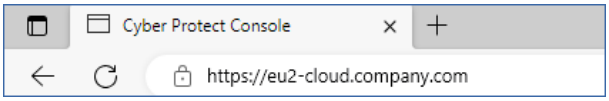
È inoltre possibile utilizzare parametri `msiexec` aggiuntivi. Ad esempio, il parametro `/qn` impedisce la visualizzazione di qualsiasi elemento dell'interfaccia utente grafica. Per ulteriori informazioni sui parametri `msiexec`, consultare la documentazione Microsoft.

Parametri	Descrizione
Parametri generici	
ADDLOCAL=	I componenti da installare. Per l'elenco completo dei

© Acronis International GmbH, 2003-2024

Parametri	Descrizione
<component1,component2,...,componentN>	componenti disponibili, consultare "Componenti per l'installazione automatica (MSI)" (pag. 104). Se si specificano più componenti, separarli con le virgole. Non aggiungere spazi prima o dopo la virgola. **Nota** È necessario estrarre i file di installazione di tutti i componenti da installare. Per ulteriori informazioni su come estrarre i file, consultare "Estrazione dei file MSI, MST e CAB" (pag. 97).
`TARGETDIR=`<path>	La cartella nella quale vengono installati i componenti selezionati. Se la cartella specificata non esiste, viene creata. Se questo parametro non viene specificato, viene utilizzata una cartella predefinita: `C:\Programmi\BackupClient`.
`REBOOT=ReallySuppress`	Specificare questo parametro per installare i componenti senza riavviare il sistema.
`/l*v` <log file>	Specificare questo parametro per salvare un registro dettagliato. Questo registro è utile se occorre indagare su eventuali problemi di installazione.
`CURRENT_LANGUAGE=`<language ID>	Lingua del prodotto. Sono disponibili le variabili seguenti: en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Se questo parametro non viene specificato, e se la lingua di sistema del sistema su cui viene eseguita l'installazione è indicata nell'elenco precedente, viene utilizzata la lingua di sistema. In tutti gli altri casi, il valore è impostato su en.
`SKIP_SHA2_KB_CHECK={0,1}`	Utilizzare questo parametro per scegliere se controllare se l'aggiornamento del supporto per la firma del codice SHA2 di Microsoft (KB4474419) è installato nel sistema. Il controllo viene eseguito solo sui sistemi operativi che richiedono tale aggiornamento. Per sapere se l'aggiornamento è richiesto per il sistema operativo in uso, consultare "Sistemi operativi e ambienti supportati" (pag. 23). Utilizzare questo parametro con il valore impostato su `1` per ignorare il controllo.

© Acronis International GmbH, 2003-2024

Parametri	Descrizione
	Se il parametro non viene specificato o se il relativo valore è impostato su `0`, e se l'aggiornamento del supporto per la firma del codice SHA2 non viene rilevato nel sistema, l'installazione non riesce.
`FSS_ONBOARDING_AUTO_START={0,1}`	Utilizzare questo parametro con il relativo valore impostato su `1` per visualizzare la procedura guidata di onboarding di File Sync & Share dopo un'installazione automatica. Se il parametro non viene specificato o se il relativo valore è impostato su `0`, la procedura guidata di onboarding non verrà visualizzata.
Parametri di registrazione	
`REGISTRATION_ADDRESS`	URL del servizio Cyber Protection. È possibile utilizzare questo parametro con i parametri `REGISTRATION_LOGIN` e `REGISTRATION_PASSWORD` , o con il parametro `REGISTRATION_TOKEN`. • Quando si utilizza con i parametri `REGISTRATION_LOGIN` e `REGISTRATION_PASSWORD`, specificare l'indirizzo utilizzato per **accedere** al servizio Cyber Protection. Ad esempio, `https://cloud.company.com`:  • Quando si utilizza con il parametro `REGISTRATION_TOKEN`, specificare l'indirizzo esatto del data center. Tale indirizzo corrisponde all'URL visualizzato **dopo aver fatto accesso** al servizio Cyber Protection. Ad esempio, `https://eu2-cloud.company.com`.  Non utilizzare `https://cloud.company.com` con il parametro `REGISTRATION_TOKEN`.

`REGISTRATION_LOGIN`
 	
`REGISTRATION_PASSWORD`
	Le credenziali dell'account con il quale l'agente viene registrato nel servizio Cyber Protection. Non può essere utilizzato l'account di un amministratore partner.
	
	Non utilizzare questi parametri con il parametro `REGISTRATION_TOKEN`.

`REGISTRATION_PASSWORD_ENCODED`	La password dell'account con il quale l'agente viene registrato al servizio Cyber Protection, codificato in Base64. Per ulteriori informazioni su come codificare la

© Acronis International GmbH, 2003-2024

Parametri	Descrizione
	password, consultare "Password con caratteri speciali o spazi" (pag. 126).
REGISTRATION_TOKEN	Il token di registrazione. Il token di registrazione è costituito da una serie di 12 caratteri, divisi da trattini in tre segmenti. Per ulteriori informazioni su come generarne uno, consultare "Generazione del token di registrazione" (pag. 172). Non utilizzare questo parametro con i parametri REGISTRATION_LOGIN e REGISTRATION_PASSWORD.
REGISTRATION_REQUIRED={0,1}	Utilizzare questo parametro per definire cosa accade se la registrazione non riesce. Se il valore è impostato su 1, anche l'installazione non riesce. Se il valore è impostato su 0, o se non si specifica il parametro, l'installazione riesce correttamente anche se la registrazione non ha esito positivo.
Account di accesso per il servizio agente	
MMS_USE_SYSTEM_ACCOUNT={0,1}	Utilizzare questo parametro con il valore 1 per fare in modo che il servizio venga eseguito con l'account di accesso **Sistema locale**. Per ulteriori informazioni sugli account di accesso, consultare "Modifica dell'account di accesso su sistemi Windows" (pag. 85).
MMS_CREATE_NEW_ACCOUNT={0,1}	Utilizzare questo parametro con il valore 1 per fare in modo che il servizio agente venga eseguito con un nuovo account di accesso, **Acronis Agent User**, che viene creato automaticamente.
MMS_SERVICE_USERNAME=<user name> MMS_SERVICE_PASSWORD=<password>	Utilizzare questi parametri per specificare un account di accesso esistente con cui verrà eseguito il servizio agente.
Parametri di vCenter/ESXi	
SET_ESX_SERVER={0,1}	Utilizzare questo parametro quando si installa Agente per VMware. Se il valore è impostato su 0, l'Agente per VMware non sarà connesso a un vCenter Server o a un host ESXi. Se il valore è impostato su 1, specificare i parametri seguenti: ESX_HOST, EXI_USER, ESX_PASSWORD.

© Acronis International GmbH, 2003-2024

Parametri	Descrizione
ESX_HOST=<nome host>	Il nome host o l'indirizzo IP del vCenter Server o dell'host ESXi.
ESX_USER=<user name> ESX_PASSWORD=<password>	Le credenziali per accedere a vCenter Server o all'host ESXi.
Parametri del proxy	
HTTP_PROXY_ADDRESS=<IP address> HTTP_PROXY_PORT=<port>	Utilizzare questi parametri per specificare il server proxy HTTP che l'agente utilizzerà. Se non si utilizza un server proxy, non specificare questi parametri.
HTTP_PROXY_LOGIN=<login> HTTP_PROXY_PASSWORD=<password>	Le credenziali per il server proxy HTTP. Utilizzare questi parametri se il server proxy richiede l'autenticazione.
Parametri di disinstallazione	
REMOVE={<list of components>|ALL}	I componenti da disinstallare. Se si specificano più componenti, separarli con le virgole. Non aggiungere spazi prima o dopo la virgola. Per rimuovere tutti i componenti del prodotto, impostare il valore su ALL.
DELETE_ALL_SETTINGS={0, 1}	Per eliminare tutti i registri, le attività e le impostazioni di configurazione del prodotto, impostare il valore su 1. Utilizzare questo parametro facoltativo quando si usa il parametro REMOVE.
ANTI_TAMPER_PASSWORD=<password>	La password richiesta per disinstallare un Agente per Windows protetto con password o di modificarne i componenti.

Componenti per l'installazione automatica (MSI)

La tabella seguente riepiloga i componenti che è possibile utilizzare per l'installazione automatica tramite un file MSI. Utilizzare i nomi dei valori per specificare i valori per il parametro ADDLOCAL. Per ulteriori informazioni, consultare "Parametri per l'installazione automatica (MSI)" (pag. 100).

Nome del valore	Descrizione del componente	Deve essere installato insieme a	Numero di bit
AgentFeature	Componenti principali per gli agenti		32-bit/64-bit

© Acronis International GmbH, 2003-2024

MmsMspComponents	Componenti principali per il backup	AgentFeature	32-bit/64-bit
BackupAndRecoveryAgent	Agente per Windows	MmsMspComponents	32-bit/64-bit
AmpAgentFeature	Agent for Antimalware protection	BackupAndRecoveryAgent	32-bit/64-bit
UrlFilteringAgentFeature	Agent for URL Filtering	BackupAndRecoveryAgent	32-bit/64-bit
DlpAgentFeature	Agente per la prevenzione della perdita di dati	BackupAndRecoveryAgent	32-bit/64-bit
SasAgentFeature	Agente per File Sync & Share	TrayMonitor	32-bit/64-bit
ArxAgentFeature	Agente per Exchange	MmsMspComponents	32-bit/64-bit
ArsAgentFeature	Agente per SQL	BackupAndRecoveryAgent	32-bit/64-bit
ARADAgentFeature	Agente per Active Directory	BackupAndRecoveryAgent	32-bit/64-bit
ArxOnlineAgentFeature	Agente per Microsoft 365	MmsMspComponents	32-bit/64-bit
OracleAgentFeature	Agente per Oracle	BackupAndRecoveryAgent	32-bit/64-bit
AcronisESXSupport	Agente per VMware ESX(i) (Windows)	BackupAndRecoveryAgent	64 bit
HyperVAgent	Agente per Hyper-V	BackupAndRecoveryAgent	32-bit/64-bit
CommandLineTool	Strumento da riga di comando		32-bit/64-bit
TrayMonitor	Cyber Protect Monitor	AgentFeature	32-bit/64-bit

© Acronis International GmbH, 2003-2024

BackupAndRecoveryBootableComponents	Generatore di supporti riavviabili		32-bit/64-bit

Installazione o disinstallazione automatica in Linux

Questa sezione descrive come installare o disinstallare gli agenti di protezione in modalità automatica su un sistema che esegue Linux, tramite la riga di comando.

Per installare un agente

1. Aprire il Terminal.

2. Eseguire una delle seguenti operazioni:

- Per avviare l'installazione specificando i parametri nella riga di comando, eseguire il comando seguente:

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

  Nel comando, `<package name>` è il nome del pacchetto di installazione (un file .i686 o .x86_64). Tutti i parametri disponibili e i relativi valori sono descritti in "Parametri per l'installazione o la disinstallazione automatica" (pag. 107).
- Per avviare l'installazione specificando i parametri in un file di testo separato, eseguire il comando seguente:

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

  Questo approccio potrebbe rivelarsi utile se non si desidera inserire informazioni sensibili nella riga di comando. In questo caso, è possibile specificare le impostazioni di configurazione in un file di testo separato al quale può accedere solo l'utente. Inserire ogni parametro su una nuova riga, seguita dal valore per quel parametro, ad esempio:

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

  oppure

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


© Acronis International GmbH, 2003-2024

Se lo stesso parametro è specificato sia sulla riga di comando sia nel file di testo, il valore della riga di comando viene per primo.

3. Se UEFI Secure Boot è abilitato sul sistema, l'utente verrà informato della necessità di riavvio del sistema dopo l'installazione. Assicurarsi di ricordare la password da utilizzare (quella dell'utente radice o "acronis"). Durante il riavvio del sistema, selezionare la gestione del codice del proprietario del sistema, selezionare **Registrazione codice del proprietario del sistema**, quindi registrare il codice utilizzando la password suggerita.

Se si abilita UEFI Secure Boot dopo l'installazione dell'agente, eseguire nuovamente l'installazione includendo il passaggio 3. In caso contrario, non sarà possibile eseguire i backup.

Per disinstallare un agente

1. Aprire il Terminal.
2. Eseguire una delle seguenti operazioni:
   - Per disinstallare l'agente e rimuovere tutti i registri, le attività e le impostazioni di configurazione, eseguire il comando seguente:

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

   - Per disinstallare l'agente ma mantenere il suo ID (ad esempio, se si prevede di installare l'agente in un secondo momento), eseguire il comando seguente:

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

   - Per disinstallare l'agente utilizzando il file di installazione, eseguire il seguente comando:

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

     Nel comando, `<package name>` è il nome del pacchetto di installazione (un file .i686 o .x86_64). Tutti i parametri disponibili e i relativi valori sono descritti in "Parametri per l'installazione o la disinstallazione automatica" (pag. 107).

     Nota
     Utilizzare questo comando solo se il pacchetto di installazione è della stessa versione dell'agente installato e se `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` è danneggiato o inaccessibile.

Parametri per l'installazione o la disinstallazione automatica

Questa sezione descrive i parametri usati durante l'installazione o la disinstallazione automatica in Linux.

La configurazione minima per l'installazione automatica include `-a` e i parametri di registrazione (ad esempio, i parametri `--login` e `--password`; i parametri `--rain` e `--token`). È possibile utilizzare più parametri per personalizzare l'installazione.

© Acronis International GmbH, 2003-2024

Parametri di installazione

Parametri di base

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

I componenti da installare, separati da virgole, senza caratteri di spazio. I componenti seguenti sono disponibili nel pacchetto di installazione .x86_64:

Componente	Descrizione del componente
BackupAndRecoveryAgent	Agente per Linux
AgentForPCS	Agente per Virtuozzo
OracleAgentFeature	Agente per Oracle
MySQLAgentFeature	Agente per MySQL/MariaDB

Se questo parametro non è specificato, tutti i componenti indicati vengono installati.

Agente per Virtuozzo, Agente per Oracle e Agente per MySQL/MariaDB richiedono anche l'installazione dell'Agente per Linux.

Il pacchetto di installazione .i686 contiene solo BackupAndRecoveryAgent.

`{-a|--auto}`

Il processo di installazione e registrazione viene completato senza alcuna interazione dell'utente. Quando si utilizza questo parametro, è necessario specificare l'account con il quale l'agente verrà registrato nel servizio Cyber Protection, utilizzando il parametro `--token`, o i parametri `--login` e `--password`.

`{-t|--strict}`

Se questo parametro è specificato, qualsiasi avviso generato durante l'installazione ha come conseguenza la mancata riuscita dell'installazione. Se questo parametro non è specificato, l'installazione viene completata anche in caso di messaggi di avviso.

`{-n|--nodeps}`

L'assenza dei pacchetti Linux richiesti viene ignorata durante l'installazione.

`{-d|--debug}`

Scrive il registro di installazione in modalità dettagliata.

`--options-file=<posizione>`

I parametri di installazione verranno letti da un file di testo e non dalla riga di comando.

`--language=<ID lingua>`

© Acronis International GmbH, 2003-2024

Lingua del prodotto. Sono disponibili i valori seguenti: `en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW`.
Se questo parametro non è specificato, la lingua del prodotto verrà definita in base alla lingua del sistema, a condizione che sia presente nell'elenco indicato. In caso contrario, la lingua del prodotto sarà impostata sull'inglese (`en`).

Parametri di registrazione

Specificare uno dei parametri seguenti:

- `{-g|--login=}<nome utente>` e `{-w|--password=}<password>`

  Credenziali dell'account con il quale l'agente verrà registrato al servizio Cyber Protection. Non può essere utilizzato l'account di un amministratore partner.

- `--token=<token>`

  Il token di registrazione è costituito da una serie di 12 caratteri separati da trattini e suddivisa in tre segmenti. È possibile generarne uno nella console di Cyber Protect, come descritto in "Distribuzione di agenti tramite Criteri di gruppo".

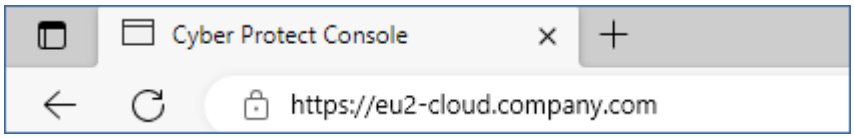
  Non è possibile utilizzare il parametro `--token` insieme ai parametri `--login`, `--password` e `--register-with-credentials`.

  - `{-C|--rain=}<indirizzo del servizio>`

    URL del servizio Cyber Protection.

    Non è necessario includere questo parametro in modo esplicito quando per la registrazione si utilizzano i parametri `--login` e `--password`, perché questo programma di installazione utilizza l'indirizzo corretto per impostazione predefinita; si tratta dell'indirizzo utilizzato per **accedere** al servizio Cyber Protection. Per esempio:

    Tuttavia, quando si utilizza `{-C|--rain=}` con il parametro `--token`, è necessario specificare l'indirizzo esatto del data center. Si tratta dell'URL visualizzato **dopo aver eseguito l'accesso** al servizio Cyber Protection. Per esempio:

- `--register-with-credentials`

  Se questo parametro è specificato, viene avviata l'interfaccia grafica del programma di installazione. Per completare la registrazione, immettere il nome utente e la password dell'account con il quale registrare l'agente al servizio Cyber Protection. Non può essere utilizzato l'account di un amministratore partner.

- `--skip-registration`

© Acronis International GmbH, 2003-2024

Utilizzare questo parametro se è necessario installare l'agente ma si pianifica di registrarlo al servizio Cyber Protection in un secondo momento. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Registrazione manuale dei sistemi".

Parametri aggiuntivi

`--http-proxy-host=<indirizzo IP>` e `--http-proxy-port=<porta>`

Il server proxy HTTP che l'agente utilizzerà per il backup e il ripristino dal cloud e per la connessione al server di gestione. Se questi parametri non sono specificati, non viene utilizzato alcun server proxy.

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

Le credenziali per il server proxy HTTP. Utilizzare questi parametri se il server richiede l'autenticazione.

`--tmp-dir=<posizione>`

Specifica la cartella in cui vengono memorizzati i file temporanei durante l'installazione. La cartella predefinita è **/var/tmp**.

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

Durante l'installazione verranno utilizzate le librerie ridistribuibili, anche se potrebbero essere già presenti nel sistema.

`--skip-prereq-check`

Non viene controllato se i pacchetti richiesti per compilare il modulo snapapi sono già installati.

`--force-weak-snapapi`

Il programma di installazione non compila il modulo snapapi. Utilizza invece un modulo già pronto che potrebbe non corrispondere esattamente al kernel Linux. Si consiglia di non utilizzare questa opzione.

`--skip-svc-start`

I servizi non vengono avviati automaticamente dopo l'installazione. In genere, questo parametro è utilizzato con il parametro `--skip-registration`.

Parametri informativi

`{-?|--help}`

Mostra la descrizione dei parametri.

`--usage`

Mostra una breve descrizione dell'utilizzo del comando.

`{-v|--version}`

© Acronis International GmbH, 2003-2024

Mostra la versione del pacchetto di installazione.

`--product-info`

Mostra il nome del prodotto e la versione del pacchetto di installazione.

`--snapapi-list`

Mostra i moduli snapapi già pronti disponibili.

`--components-list`

Mostra i componenti del programma di installazione.

Parametri per funzionalità già esistenti

Questi parametri sono correlati al componente già esistente agent.exe.

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

Specifica il percorso di un file di certificato personalizzato per la comunicazione SSL.

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

Specifica la porta sulla quale agent.exe è in ascolto per le connessioni. La porta predefinita è la 9876.

Parametri di disinstallazione

`{-u|--uninstall}`

Disinstalla il prodotto.

`--purge`

Disinstalla il prodotto e ne rimuove i registri, le attività e le impostazioni di configurazione. Non è necessario specificare esplicitamente il parametro `--uninstall` quando si utilizza il parametro `--purge`.

Esempi

- Installazione dell'Agente per Linux senza registrarlo.

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

- Installazione dell'Agente per Linux, dell'Agente per Oracle e dell'Agente per Virtuozzo e loro registrazione con le credenziali.

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

- Installazione dell'Agente per Linux e dell'Agente per Oracle e loro registrazione con un token di registrazione.

© Acronis International GmbH, 2003-2024

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

- Installazione dell'Agente per Linux, dell'Agente per Oracle e dell'Agente per Virtuozzo con impostazioni di configurazione inserite in un file di testo separato.

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

- Disinstallazione dell'Agente per Linux, dell'Agente per Virtuozzo e dell'Agente per Oracle, e rimozione di tutti i rispettivi registri, attività e impostazioni di configurazione.

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

Installazione e disinstallazione automatica in macOS

Questa sezione descrive come installare, registrare e disinstallare l'agente di protezione in modalità automatica su un sistema che esegue macOS, tramite la riga di comando.

Autorizzazioni richieste

Prima di avviare un'installazione automatica su un workload Mac, è necessario modificare il Controllo policy preferenze privacy in modo da consentire l'accesso app e le estensioni di kernel e sistema nel macOS del workload per abilitare l'istallazione dell'agente Cyber Protection. Vedere "Autorizzazioni richieste per l'installazione automatica in macOS" (pag. 114).

Dopo aver distribuito il payload PPPC, è possibile eseguire le procedure indicate di seguito.

Per scaricare il file di installazione (.dmg)

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic su **Aggiungi**, quindi su **Mac**.

Per installare un agente

1. Aprire il Terminal.
2. Creare una directory temporanea in cui verrà montato il file di installazione (.dmg).

   ```
   mkdir <dmg_root>
   ```

   Qui, `<dmg_root>` rappresenta un nome a scelta dell'utente.
3. Montare il file .dmg.

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

   Qui, `<dmg_file>` rappresenta il nome del file di installazione. Ad esempio, **Cyber_Protection_Agent_for_MAC_x64.dmg**.
4. Avviare il programma di installazione.

© Acronis International GmbH, 2003-2024

- Se si utilizza un programma di installazione completo per Mac, ad esempio `CyberProtect_AgentForMac_x64.dmg` o `CyberProtect_AgentForMac_arm64.dmg`, eseguire il comando seguente.

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

  Nota
  Se è necessario abilitare l'onboarding automatico per File Sync & Share, eseguire invece il comando seguente. Questa opzione richiede una password di amministratore.

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

- Se si utilizza un programma di installazione universale per Mac, ad esempio `CyberProtect_AgentForMac_web.dmg`, eseguire il comando seguente.

  ```
  sudo <dmg_root>/Install.app/Contents/MacOS/cyber_installer -a
  ```

5. Scollegare il file di istallazione (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Esempio

```
mkdir mydirectory
```

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

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

```
hdiutil detach mydirectory
```

Per disinstallare un agente

1. Aprire il Terminal.
2. Eseguire una delle seguenti operazioni:
   - Per disinstallare l'agente, eseguire il seguente comando:

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

   - Per disinstallare l'agente e rimuovere tutti i registri, le attività e le impostazioni di configurazione, eseguire il comando seguente:

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


© Acronis International GmbH, 2003-2024

Autorizzazioni richieste per l'installazione automatica in macOS

Prima di avviare un'installazione automatica su un workload Mac, è necessario modificare il Controllo policy preferenze privacy in modo da consentire l'accesso app e le estensioni di kernel e sistema nel macOS del workload per abilitare l'istallazione dell'agente Cyber Protection. Questa operazione può essere eseguita distribuendo un payload "Controllo politiche preferenze privacy" personalizzato o configurando le preferenze nell'interfaccia utente grafica del workload. Sono necessarie le autorizzazioni seguenti.

Requisiti per macOS 11 (Big Sur) o successivi

Scheda	Sezione	Campo	Valore

© Acronis International GmbH, 2003-2024

Controllo politiche preferenze privacy	Accesso app	Identificatore	com.acronis.backup

© Acronis International GmbH, 2003-2024

		Tipo di identificatore	ID pacchetto
		Requisiti del codice	identifier "com.acronis.backup" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APP o SERVIZIO	SystemPolicyAllFiles
		ACCESSO	Consenti
	Accesso app	Identificatore	com.acronis.backup.aakore
		Tipo di identificatore	ID pacchetto
		Requisiti del codice	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APP o SERVIZIO	SystemPolicyAllFiles
		ACCESSO	Consenti
	Accesso app	Identificatore	com.acronis.backup.activeprotection
		Tipo di identificatore	ID pacchetto
		Requisiti del codice	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APP o SERVIZIO	SystemPolicyAllFiles
		ACCESSO	Consenti

© Acronis International GmbH, 2003-2024

	Accesso app	Identificatore	cyber-protect-service
		Tipo di identificatore	ID pacchetto
		Requisiti del codice	`identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APP o SERVIZIO	SystemPolicyAllFiles
		ACCESSO	Consenti
Estensioni di sistema		Consenti agli utenti di approvare le estensioni di sistema	Abilitato
	ID dei team ed estensioni di sistema consentiti	Nome visualizzato	Acronis Cyber Protection Agent System Extensions
		Tipi di estensione di sistema	Identificatori team consentiti
		Identificatore del team	ZU2TV78AA6

Requisiti per versioni di macOS precedenti alla versione 11

Scheda	Sezione	Campo	Valore

© Acronis International GmbH, 2003-2024

Controllo politiche preferenze privacy	Accesso app	Identificatore	com.acronis.backup

© Acronis International GmbH, 2003-2024

		Tipo di identificatore	ID pacchetto

© Acronis International GmbH, 2003-2024

		Requisiti del codice	identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APP o SERVIZIO	SystemPolicyAllFiles
		ACCESSO	Consenti
	Accesso app	Identificatore	com.acronis.backup.aakore
		Tipo di identificatore	ID pacchetto
		Requisiti del codice	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APP o SERVIZIO	SystemPolicyAllFiles
		ACCESSO	Consenti
	Accesso app	Identificatore	com.acronis.backup.activeprotection
		Tipo di identificatore	ID pacchetto
		Requisiti del codice	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APP o SERVIZIO	SystemPolicyAllFiles
		ACCESSO	Consenti

© Acronis International GmbH, 2003-2024

	Accesso app	Identificatore	cyber-protect-service
		Tipo di identificatore	ID pacchetto
		Requisiti del codice	identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APP o SERVIZIO	SystemPolicyAllFiles
		ACCESSO	Consenti
Estensioni del kernel approvate		Consenti agli utenti di approvare le estensioni del kernel	Abilitato
		Consenti agli utenti standard di approvare le estensioni del kernel esistenti (macOS 11 o successive)	Abilitato
	ID del team ed estensioni del kernel approvate	ID del team approvato - Nome visualizzato	Acronis Cyber Protection Agent Kernel Extensions
		ID del team	ZU2TV78AA6
		ID del pacchetto di estensioni del kernel	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
Estensioni di sistema		Consenti agli utenti di approvare le estensioni di sistema	Abilitato
	ID dei team ed estensioni di sistema consentiti	Nome visualizzato	Acronis Cyber Protection Agent System Extensions
		Tipi di estensione di sistema	Identificatori team consentiti
		Identificatore del team	ZU2TV78AA6

© Acronis International GmbH, 2003-2024

Registrazione e annullamento della registrazione di workload in modalità manuale

Quando nei workload viene installato l'agente di protezione, essi vengono registrati automaticamente nel servizio Cyber Protection. Disinstallando l'agente di protezione, la registrazione dei workload viene automaticamente annullata, e non saranno più visibili nella console di Cyber Protect.

È possibile registrare un workload manualmente utilizzando l'interfaccia a riga di comando. La registrazione manuale può essere utile, ad esempio, se non riesce la registrazione automatica o se si desidera spostare un workload in un nuovo tenant o in un nuovo account utente.

Per registrare un workload utilizzando un nome utente e una password

In Windows

Nella riga di comando eseguire il comando seguente:

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

Per esempio:

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

In Linux

Nella riga di comando eseguire il comando seguente:

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

Per esempio:

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

In macOS

Nella riga di comando eseguire il comando seguente:

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

Per esempio:

© Acronis International GmbH, 2003-2024

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

Nota
Utilizzare il nome utente e la password dell'account nel quale si intende registrare il workload. Non può essere utilizzato l'account di un amministratore partner.

L'indirizzo del servizio è l'URL utilizzato per **accedere** al servizio Cyber Protection. Ad esempio, `https://cloud.company.com`.

Importante
Se la password contiene caratteri speciali o spazi, fare riferimento a "Password con caratteri speciali o spazi" (pag. 126).

Importante
Se si utilizza macOS 10.14 o versioni successive, concedere all'agente di protezione l'accesso completo al disco. Per eseguire questa operazione, accedere ad **Applicazioni** >**Utilità**, quindi eseguire **Assistente dell'agente di Cyber Protect**. Quindi, seguire le istruzioni nella finestra dell'applicazione.

Per registrare un workload utilizzando un token di registrazione

In Windows

Nella riga di comando eseguire il comando seguente:

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

Per esempio:

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

In Linux

Nella riga di comando eseguire il comando seguente:

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

Per esempio:

© Acronis International GmbH, 2003-2024

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

In macOS

Nella riga di comando eseguire il comando seguente:

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

Per esempio:

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

Importante
Se si utilizza macOS 10.14 o versioni successive, concedere all'agente di protezione l'accesso completo al disco. Per eseguire questa operazione, accedere ad **Applicazioni** >**Utilità**, quindi eseguire **Assistente dell'agente di Cyber Protect**. Quindi, seguire le istruzioni nella finestra dell'applicazione.

Appliance virtuale

1. Nella console dell'appliance virtuale, premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
2. Nel prompt dei comandi, eseguire il seguente comando:

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

   Per esempio:

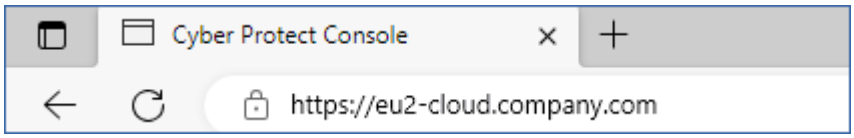
   ```
   register_agent -o register -t cloud -a https://eu2-cloud.company.com --token 34F6-
   8C39-4A5C
   ```

3. Premere ALT+F1 per tornare all'interfaccia grafica dell'appliance.

© Acronis International GmbH, 2003-2024

Nota

Quando si utilizza un token di registrazione, è necessario specificare l'indirizzo esatto del data center. Tale indirizzo corrisponde all'URL visualizzato **dopo aver fatto accesso** al servizio Cyber Protection. Ad esempio, `https://eu2-cloud.company.com`.



Non utilizzare `https://cloud.company.com` in questo caso.

Il token di registrazione è costituito da una serie di 12 caratteri separati da trattini e suddivisa in tre segmenti. Per ulteriori informazioni su come generarne uno, fare riferimento a "Generazione del token di registrazione" (pag. 172).

Per annullare la registrazione di un workload

In Windows

Nella riga di comando eseguire il comando seguente:

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

Per esempio:

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

In Linux

Nella riga di comando eseguire il comando seguente:

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

In macOS

Nella riga di comando eseguire il comando seguente:

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

Appliance virtuale

1. Nella console dell'appliance virtuale, premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
2. Nel prompt dei comandi, eseguire il seguente comando:

   ```
   register_agent -o unregister
   ```

3. Premere ALT+F1 per tornare all'interfaccia grafica dell'appliance.

© Acronis International GmbH, 2003-2024

Spostamento di un workload in un altro tenant

Lo spostamento di un workload in un altro tenant non è supportato in modalità nativa. In alternativa, è possibile annullare la registrazione del workload e quindi registrarlo in un altro tenant. Tutti i piani di protezione applicati al workload verranno revocati e il workload non potrà accedere ai backup nel cloud storage del tenant originario.

Per informazioni su come registrare un workload in un nuovo tenant o in un nuovo account utente, consultare "Modifica della registrazione di un workload" (pag. 126).

Password con caratteri speciali o spazi

Se la password contiene caratteri speciali o spazi, racchiuderli tra virgolette quando vengono digitati nella riga di comando.

Ad esempio, in Windows, eseguire questo comando:

Modello di comando:

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

Esempio di comando:

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

Se il comando non funziona, codificare la password in formato Base64 all'indirizzo https://www.base64encode.org/. Quindi, nella riga di comando, specificare la password codificata utilizzando il parametro -b oppure --base64.

Ad esempio, in Windows, eseguire questo comando:

Modello di comando:

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

Esempio di comando:

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

Modifica della registrazione di un workload

È possibile modificare la registrazione corrente di un workload registrandolo in un nuovo tenant o in un nuovo account utente.

© Acronis International GmbH, 2003-2024

Importante
Quando si modifica la registrazione di un workload, tutti i piani di protezione applicati al workload verranno revocati. Per continuare a proteggere il workload, applicare al workload un nuovo piano di protezione.

Se si registra il workload in un nuovo tenant, il workload non potrà accedere ai backup nel cloud storage del tenant originario. Resteranno tuttavia accessibili i backup negli storage non cloud.

È possibile modificare la registrazione di un workload utilizzando la riga di comando o il programma di installazione della GUI. Quando si utilizza la riga di comando, non è necessario disinstallare l'agente.

Per modificare la registrazione di un workload

Tramite la riga di comando

1. Annullare la registrazione dell'agente di protezione, come descritto in "Per annullare la registrazione di un workload" (pag. 125).
2. Registrare l'agente di protezione nel nuovo tenant o nel nuovo account utente, come descritto in "Per registrare un workload utilizzando un nome utente e una password" (pag. 122) o in "Per registrare un workload utilizzando un token di registrazione" (pag. 123).

Tramite il programma di installazione della GUI

1. Disinstallare l'agente di protezione.
2. Installare l'agente di protezione, quindi registrarlo nel nuovo tenant o nel nuovo account utente.

Per ulteriori informazioni su come installare e registrare un agente, fare riferimento a "Installazione degli agenti di protezione" (pag. 76).

Individuazione automatica dei sistemi

Utilizzando l'individuazione automatica è possibile:

- Automatizzare l'installazione degli agenti di protezione e la registrazione dei sistemi individuando quelli presenti nel dominio di Active Directory o nella rete locale.
- Installare e aggiornare gli agenti di protezione su più sistemi.
- Utilizzare la sincronizzazione con Active Directory, per ridurre l'impegno necessario al provisioning delle risorse e alla gestione dei sistemi nei domini di Active Directory di grandi dimensioni.

Prerequisiti

Per eseguire l'individuazione automatica, è necessario almeno un sistema con agente di protezione installato nella rete locale o nel dominio di Active Directory. Tale agente verrà utilizzato come agente di individuazione.

© Acronis International GmbH, 2003-2024

Importante
È possibile utilizzare come agenti di individuazione solo quelli installati su sistemi Windows. Qualora nell'ambiente non fossero presenti agenti di individuazione, non sarà possibile utilizzare l'opzione **Più dispositivi** nel riquadro **Aggiungi periferiche**.

L'installazione remota degli agenti è supportata solo per i sistemi che eseguono Windows (Windows XP non supportato). Per l'installazione remota su un sistema che esegue Windows Server 2012 R2, è necessario che in tale sistema sia installato l'aggiornamento Windows KB2999226.

Funzionamento dell'individuazione automatica

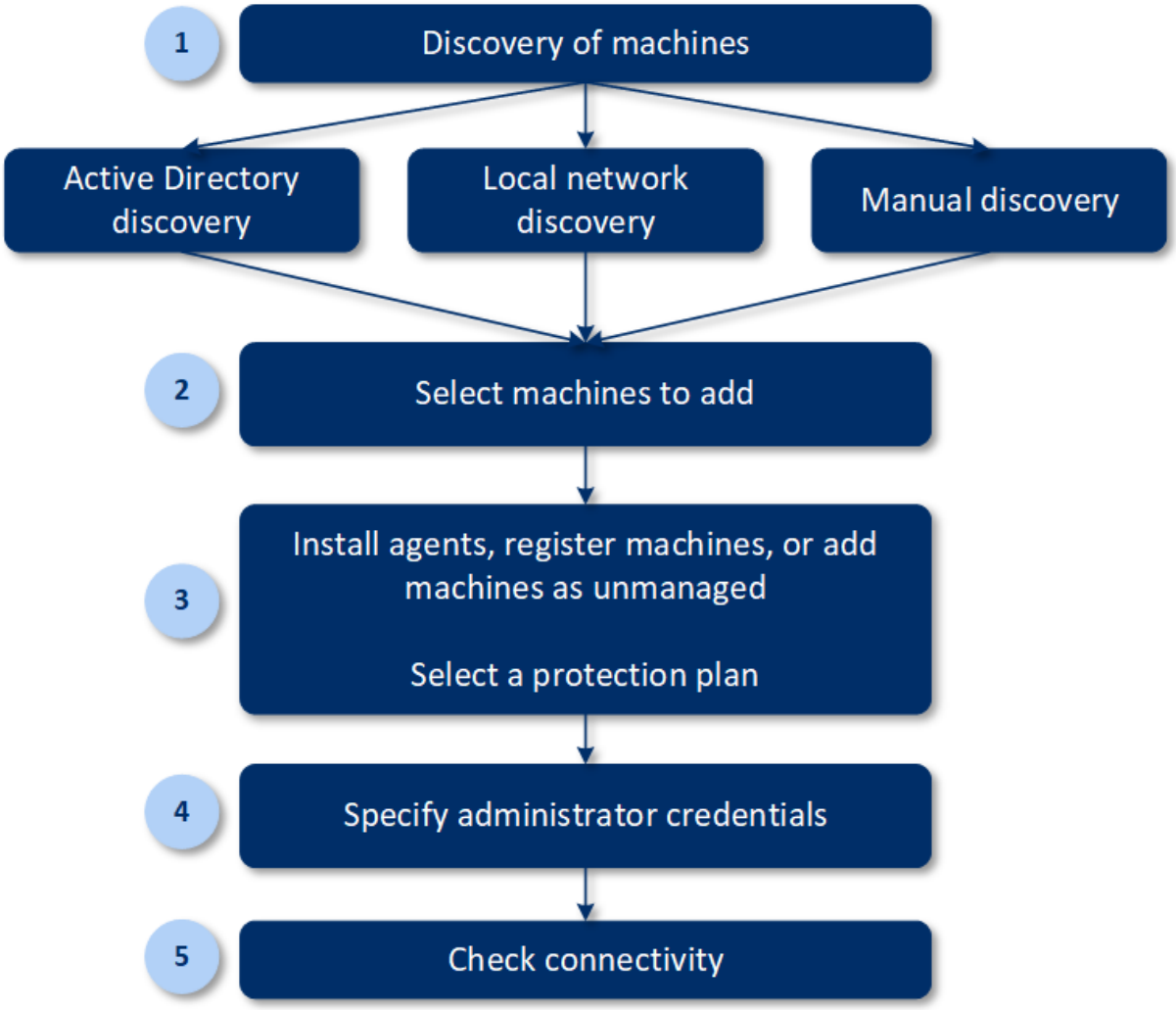
Durante l'individuazione della rete locale, l'agente di individuazione raccoglie le seguenti informazioni per ogni sistema della rete, utilizzando l'individuazione NetBIOS, Web Service Discovery (WSD) e la tabella Address Resolution Protocol (ARP):

- Nome (host nome abbreviato/NetBIOS)
- Nome di dominio completo (FQDN)
- Dominio/gruppo di lavoro
- Indirizzi IPv4/IPv6
- Indirizzi MAC
- Sistema operativo (nome/versione/famiglia)
- Categoria del sistema (workstation/server/controller di dominio)

Durante un'individuazione di Active Directory, l'agente di individuazione, oltre all'elenco sopra indicato, acquisisce informazioni sull'unità organizzativa dei sistemi e altri dati dettagliati relativi ai rispettivi nomi e sistemi operativi. Non vengono tuttavia acquisiti indirizzi IP e MAC.

Il diagramma seguente riepiloga il processo di individuazione automatica.

© Acronis International GmbH, 2003-2024



1. Selezionare il metodo di individuazione:
   - Individuazione basata su Active Directory
   - Individuazione sulla rete locale
   - Scansione manuale - Utilizzando l'indirizzo IP o il nome host del sistema, o importando un elenco dei sistemi da un file

   Nei risultati di un'individuazione di Active Directory o di un'individuazione di una rete locale non sono inclusi i sistemi sui quali sono installati gli agenti di protezione.

   Durante una individuazione manuale, gli agenti di protezione esistenti vengono aggiornati e nuovamente registrati. Quando si esegue l'individuazione automatica utilizzando lo stesso account con il quale è registrato un agente, quest'ultimo verrà soltanto aggiornato all'ultima versione. Se si esegue l'individuazione automatica utilizzando un altro account, l'agente verrà aggiornato alla versione più recente e nuovamente registrato nel tenant al quale appartiene l'account.
2. Selezionare i sistemi da aggiungere al tenant.
3. Selezionare la modalità con la quale aggiungere tali sistemi:

© Acronis International GmbH, 2003-2024

- Installare un agente di protezione e i componenti aggiuntivi nei sistemi e registrarli nella console di Cyber Protect.
- Registrare i sistemi nella console di Cyber Protect (se l'agente di protezione è già stato installato).
- Aggiungere i sistemi alla console di Cyber Protect come **Non gestiti**, senza installare alcun agente di protezione.

  È inoltre possibile applicare un piano di protezione esistente ai sistemi in cui è installato l'agente di protezione o che vengono registrati nella console di Cyber Protect.

4. Fornire le credenziali di amministratore per i sistemi selezionati.
5. Accertarsi di poter stabilire la connessione ai sistemi utilizzando le credenziali specificate.

I sistemi visualizzati nella console di Cyber Protect rientrano in una delle categorie seguenti:

- **Individuati** – Sistemi individuati, nei quali non è tuttavia installato l'agente di protezione.
- **Gestiti** – sistemi nei quali è installato l'agente di protezione.
- **Non protetti** – sistemi ai quali non è applicato il piano di protezione. Tra i sistemi non protetti sono inclusi sia i sistemi individuati e quelli gestiti ai quali non è applicato un piano di protezione.
- **Protetti** – sistemi ai quali è applicato un piano di protezione.

Funzionamento dell'installazione remota di agenti

1. L'agente di individuazione si connette ai sistemi di destinazione utilizzando il nome host, l'indirizzo IP e le credenziali di amministratore specificati nella procedura di individuazione guidata, quindi carica il file `web_installer.exe` su tali sistemi.
2. Il file `web_installer.exe` viene eseguito nei sistemi di destinazione in modalità automatica.
3. Il programma di installazione web recupera eventuali pacchetti di installazione dal cloud e quindi li installa nei sistemi di destinazione tramite il comando `msiexec`.
4. Una volta completata l'installazione, i componenti vengono registrati nel cloud.

Nota
L'installazione remota degli agenti non è supportata per i controller di dominio, a causa delle autorizzazioni aggiuntive richieste per l'esecuzione del servizio agente.

Esecuzione dell'individuazione automatica e dell'individuazione manuale

Prima di avviare l'individuazione, verificare che tutti i prerequisiti siano soddisfatti.

Nota
L'Individuazione automatica non è supportata per l'aggiunta dei controller di dominio, a causa delle autorizzazioni aggiuntive richieste per l'esecuzione del servizio agente.

Per individuare i sistemi

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic su **Aggiungi**.
3. In **Più dispositivi**, fare clic su **Solo per Windows**. Si apre la finestra dell'Individuazione automatica guidata.
4. [Se sono presenti unità nell'organizzazione] Selezionare un'unità. In **Agente di individuazione** è possibile selezionare gli agenti associati all'unità selezionata e alle relative alle unità figlio.
5. Selezionare l'agente di individuazione che eseguirà la scansione per individuare i sistemi.
6. Selezionare il metodo di individuazione:
   - **Cerca in Active Directory**. Verificare che il sistema con l'agente di individuazione sia membro del dominio di Active Directory.
   - **Scansiona rete locale**. Se l'agente di individuazione selezionato non è in grado di trovare alcun sistema, selezionarne un altro.
   - **Specifica manualmente o importa da file**. Definire manualmente i sistemi da aggiungere o importarli da un file di testo.
7. [Se è stato selezionato il metodo di individuazione da Active Directory] Selezionare come eseguire la ricerca dei sistemi:
   - **Nell'elenco delle unità organizzative**. Selezionare il gruppo di sistemi da aggiungere.
   - **Per query in dialetto LDAP**. Utilizzare query in dialetto LDAP per selezionare i sistemi. **Base di ricerca** definisce l'ambito in cui eseguire la ricerca, mentre **Filtro** consente di specificare i criteri per la selezione del sistema.
8. A seconda del metodo di individuazione selezionato, procedere come segue:

Metodo di individuazione	Azione
Cerca in Active Directory	Dall'elenco dei sistemi individuati, selezionare i sistemi da aggiungere.
Scansiona rete locale	Dall'elenco dei sistemi individuati, selezionare i sistemi da aggiungere.

Specifica manualmente o importa da file	Specificare gli indirizzi IP o i nomi host del sistema, oppure importare l'elenco dei sistemi da un file di testo. Il file deve contenere gli indirizzi IP o i nomi host, uno per riga. Di seguito è riportato un esempio di file:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Dopo aver aggiunto manualmente gli indirizzi dei sistemi o averli importati da un file, l'agente tenta di eseguire il ping ai sistemi aggiunti e ne definisce la disponibilità.

9. Selezionare le azioni da eseguire dopo l'individuazione:

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
Installa gli agenti e registra le macchine	È possibile selezionare quali componenti installare sui sistemi facendo clic su **Seleziona componenti**. Per ulteriori dettagli, consultare "Selezione dei componenti per l'installazione" (pag. 135).
Account di accesso per il servizio agente	Questa impostazione è disponibile nella schermata **Seleziona componenti**. L'impostazione definisce l'account con il quale verranno eseguiti i servizi. È possibile selezionare una delle opzioni seguenti: • **Usa gli account degli utenti del servizio** (impostazione predefinita per il servizio agente) Gli account degli utenti del servizio sono account di sistema Windows usati per eseguire i servizi. Questa impostazione è vantaggiosa perché i criteri di sicurezza del dominio non influiscono sui diritti utente di questi account. Per impostazione predefinita l'agente viene eseguito con l'account **Sistema locale**. • **Crea un nuovo account** Il nome account sarà l'Agent User dell'agente. • **Usa il seguente account** Se l'agente viene installato in un controller di dominio, il sistema chiede di specificare gli account esistenti (o lo stesso account) per l'agente. Per motivi di sicurezza, il sistema non crea automaticamente nuovi account su un controller di dominio. Se si sceglie l'opzione **Crea un nuovo account** o **Usa il seguente account**, verificare che i criteri di sicurezza del dominio non influiscano sui diritti degli account correlati. Se un account viene privato dei diritti utente assegnati durante l'installazione, il componente potrebbe non funzionare correttamente o non funzionare affatto.
Registra le macchine con agenti installati	Utilizzare questa opzione se l'agente è già installato sui sistemi e se è necessario solo registrarlo in Cyber Protection. Se non viene individuato nessun agente sui sistemi, questi verranno aggiunti come sistemi **Non gestiti**.
Aggiungi come macchine non gestite	Selezionando questa opzione, l'agente non viene installato sui sistemi. Sarà possibile visualizzare i sistemi nella console e installare o registrare l'agente in un secondo momento.
Riavviare la macchina, se necessario	Questa opzione viene visualizzata se è selezionata **Installa gli agenti e registra le macchine**. Selezionando questa opzione, il sistema viene riavviato il numero di volte necessario a completare l'installazione. Il riavvio del sistema può essere necessario in uno dei casi seguenti: • È stata completata l'installazione dei prerequisiti e il riavvio è richiesto per continuare l'installazione. • L'installazione è completa ma il riavvio è richiesto in quanto alcuni file vengono bloccati durante il processo.

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
	• L'installazione è completa ma il riavvio è richiesto per altro software installato in precedenza.
Non riavviare se l'utente ha effettuato l'accesso	Questa opzione viene visualizzata se è selezionata **Riavviare la macchina se necessario**. Se questa opzione è selezionata, il sistema non viene riavviato automaticamente se l'utente accede al sistema. Se, ad esempio, un utente sta lavorando quando l'installazione richiede il riavvio, il sistema non verrà riavviato. Se i prerequisiti sono stati installati ma il sistema non è stato riavviato perché un utente era collegato, per completare l'installazione è necessario riavviare il sistema, quindi avviare di nuovo l'installazione. Se l'agente è stato installato ma il sistema non è stato riavviato, è necessario riavviarlo.
Utente in cui registrare i sistemi	[Se sono presenti unità nell'organizzazione] Selezionare l'account utente dell'unità o delle unità secondarie per il quale registrare i sistemi. [Quando si esegue l'individuazione automatica a livello del tenant partner] Nell'elenco dei tenant cliente gestiti, espandere la struttura ad albero e selezionare l'account utente per il quale registrare i sistemi. [Quando si esegue l'individuazione automatica come amministratore del cliente] Se è stata selezionata l'opzione **Installa gli agenti e registra le macchine** o **Registra le macchine con agenti installati**, viene visualizzata anche un'opzione per applicare il piano di protezione ai sistemi. Se sono disponibili più piani di protezione, è possibile selezionare quale applicare.

10. Specificare le credenziali dell'utente che dispone dei diritti di amministratore per tutti i sistemi.

Importante
Tenere presente che l'installazione remota degli agenti funziona senza alcuna preparazione solo se vengono specificate le credenziali dell'account di amministrazione integrato (il primo account creato quando è stato installato il sistema operativo). Per definire alcune credenziali di amministratore personalizzate, è necessario procedere con i passaggi preparatori manuali descritti nella sezione "Preparazione di un sistema per l'installazione remota" (pag. 133).

11. Viene controllata la connessione verso tutti i sistemi. Se la connessione ad alcuni sistemi non riesce, è possibile modificare le credenziali dei sistemi in questione.

Una volta avviata l'individuazione dei sistemi, l'attività corrispondente viene visualizzata in **Monitoraggio** > **Attività** > **Attività di individuazione dei sistemi**.

Preparazione di un sistema per l'installazione remota

- Per eseguire correttamente l'installazione su un sistema remoto che esegue Windows 7 o versioni successive, l'opzione **Pannello di controllo** > **Opzioni cartella** > **Visualizza** > **Utilizza Configurazione guidata** deve essere *disabilitata* su tale sistema.

© Acronis International GmbH, 2003-2024

- Per eseguire correttamente l'installazione su una macchina remota che *non* è membro di un dominio di Active Directory, sulla macchina deve essere *disabilitato* Controllo account utente (UAC). Per ulteriori informazioni su come disabilitarlo, fare riferimento a "Requisiti per Controllo account utente (UAC)" > Per disabilitare UAC.
- Per impostazione predefinita, le credenziali dell'account amministratore integrato sono obbligatorie per l'installazione remota su qualsiasi sistema Windows. Per eseguire l'installazione remota utilizzando le credenziali di un altro account amministratore, è necessario *disabilitare* le limitazioni remote del controllo dell'account utente. Per ulteriori informazioni su come disabilitarlo, fare riferimento a "Requisiti per Controllo account utente (UAC)" > Per disabilitare le limitazioni remote di UAC.
- Condivisione file e stampanti deve essere *abilitata* sulla macchina remota. Per accedere a questa opzione:
  - Su un sistema che esegue Windows 2003 Server: passare a **Pannello di controllo** > **Windows Firewall** > **Eccezioni** > **Condivisione file e stampanti**.
  - Su un sistema che esegue Windows Server 2008, Windows 7 o versioni successive: passare a **Pannello di controllo** > **Windows Firewall** > **Centro connessioni di rete e condivisione** > **Modifica impostazioni di condivisione avanzate**.
- Cyber Protection utilizza le porte TCP 445, 25001 e 43234 per l'installazione remota.

  La porta 445 viene aperta automaticamente quando si abilita Condivisione file e stampanti. Le porte 43234 e 25001 vengono aperte automaticamente tramite Windows Firewall. Se si utilizza un firewall diverso, assicurarsi che queste tre porte siano aperte (aggiunte alle eccezioni) sia per le richieste in ingresso che per quelle in uscita.

  Dopo aver completato l'installazione remota, la porta 25001 viene chiusa automaticamente tramite Windows Firewall. Le porte 445 e 43234 devono rimanere aperte se si prevede, in futuro, di aggiornare l'agente in modalità remota. La porta 25001 viene automaticamente aperta e chiusa tramite Windows Firewall durante ogni aggiornamento. Se si utilizza un firewall diverso, tenere aperte tutte e tre le porte.

Requisiti per Controllo account utente (UAC)

Su un sistema che esegue Windows 7 o versioni successive e che non è membro di un dominio di Active Directory, le operazioni di gestione centralizzata (inclusa l'installazione remota) richiedono la disabilitazione di UAC e delle relative limitazioni remote.

Per disabilitare UAC

Eseguire una delle seguenti operazioni a seconda del sistema operativo:

- **In un sistema operativo Windows precedente a Windows 8:**

  Aprire **Pannello di controllo > Visualizza per: Icone piccole > Account utente > Modifica impostazioni di Controllo dell'account utente** e spostare il cursore su **Non notificare mai**. Quindi riavviare la macchina.
- **In tutti i sistemi operativi Windows:**:

© Acronis International GmbH, 2003-2024

1. Aprire l'Editor del Registro di sistema.
2. Individuare la seguente chiave di registro: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
3. Per il valore **EnableLUA**, modificare l'impostazione in **0**.
4. Riavviare la macchina.

Per disabilitare le limitazioni remote di UAC

1. Aprire l'Editor del Registro di sistema.
2. Individuare la seguente chiave di registro: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
3. Per il valore **LocalAccountTokenFilterPolicy**, modificare l'impostazione in **1**.

   Se il valore **LocalAccountTokenFilterPolicy** non è presente, crearlo come DWORD (32 bit). Per ulteriori informazioni su questo valore, fare riferimento alla documentazione Microsoft: https://support.microsoft.com/it-it/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Nota
Per ragioni di sicurezza, si consiglia, al termine dell'operazione di gestione (ad esempio dopo l'installazione remota), di riportare entrambe le impostazioni al loro stato originario: **EnableLUA**=**1** e **LocalAccountTokenFilterPolicy** = **0**

Selezione dei componenti per l'installazione

La tabella seguente descrive i componenti obbligatori e aggiuntivi:

Componente	Descrizione
Componente obbligatorio	
Agente per Windows	Questo agente esegue il backup di dischi, volumi e file e verrà installato sui sistemi Windows. Viene sempre installato, non è selezionabile.
Componenti aggiuntivi	
Agente per la prevenzione della perdita di dati	Questo agente consente di limitare l'accesso degli utenti a dispositivi periferici locali e reindirizzati, porte e appunti sui sistemi protetti da piani di protezione. Viene installato se selezionato.
Anti-malware e filtro URL	Questo componente attiva il modulo Protezione antivirus e anti-malware e il modulo Filtro URL nei piani di protezione. Anche se si decide di non installarlo, l'installazione avverrà automaticamente in un secondo momento qualora uno qualunque di tali moduli venga abilitato in un piano di protezione del sistema.
Agente per Hyper-V	Questo agente esegue il backup delle macchine virtuali Hyper-V e verrà installato negli host Hyper-V. Viene installato se selezionato e se viene individuato il ruolo Hyper-V nel

© Acronis International GmbH, 2003-2024

	sistema.
Agente per SQL	Questo agente esegue il backup dei database SQL Server e verrà installato nei sistemi che eseguono Microsoft SQL Server. Viene installato se selezionato e se viene individuata un'applicazione nel sistema.
Agente per Exchange	Questo agente esegue il backup dei database e delle caselle di posta di Exchange e verrà installato nei sistemi che eseguono il ruolo Cassette postali di Microsoft Exchange Server. Viene installato se selezionato e se viene individuata un'applicazione nel sistema.
Agente per Active Directory	Questo agente esegue il backup dei dati dei servizi di dominio di Active Directory e verrà installato nei controller di dominio. Viene installato se selezionato e se viene individuata un'applicazione nel sistema.
Agente per VMware (Windows)	Questo agente esegue il backup delle macchine virtuali VMware e verrà installato nei sistemi Windows che possono accedere tramite rete a VCenter Server. Viene installato se selezionato.
Agente per Microsoft 365	Questo agente esegue il backup delle caselle di posta di Microsoft 365 su una destinazione locale e verrà installato sui sistemi Windows. Viene installato se selezionato.
Agente per Oracle	Questo agente esegue il backup dei database Oracle e verrà installato nei sistemi che eseguono Oracle Database. Viene installato se selezionato.
Cyber Protection Monitor	Questo componente consente agli utenti di monitorare l'esecuzione delle attività in esecuzione nell'area di notifica e verrà installato nei sistemi Windows. Viene installato se selezionato. Supportato su Windows 7 Service Pack 1 e versioni successive, Windows Server 2008 R2 Service Pack 1 e versioni successive.

Gestione dei sistemi individuati

Dopo l'esecuzione del processo di individuazione, è possibile trovare tutti i sistemi individuati in **Dispositivi** > **Sistemi non gestiti**.

La sezione viene divisa in sottosezioni in base al metodo di individuazione utilizzato. L'elenco completo dei parametri dei sistemi viene indicato di seguito (può variare in base al metodo di individuazione):

Nome	Descrizione
Nome	Il nome del sistema. Se non è stato possibile individuare il nome del sistema, viene visualizzato l'indirizzo IP.
Indirizzo IP	L'indirizzo IP della macchina.
Tipo di individuazione	Il metodo di individuazione utilizzato per individuare il sistema.

© Acronis International GmbH, 2003-2024

Unità organizzativa	L'unità organizzativa in Active Directory alla quale appartiene il sistema. Questa colonna viene mostrata se l'elenco dei sistemi viene visualizzato in **Sistemi non gestiti** > **Active Directory**.
Sistema operativo	Il sistema operativo installato nel sistema.

È presente una sezione **Eccezioni**, nella quale è possibile aggiungere i sistemi da ignorare durante il processo di individuazione. Ad esempio, se sono presenti sistemi precisi da non individuare, è possibile aggiungerli all'elenco.

Per aggiungere un sistema alle **Eccezioni**, selezionarlo nell'elenco e fare clic su **Aggiungi alle eccezioni**. Per rimuovere un sistema dalle **Eccezioni**, passare a **Sistemi non gestiti** > **Eccezioni**, selezionare il sistema e fare clic su **Rimuovi dalle eccezioni**.

È possibile installare l'agente di protezione e registrare un batch di sistemi individuati in Cyber Protection selezionandoli nell'elenco e facendo clic su **Installa e registra**. La procedura guidata consente anche di assegnare un piano di protezione a un batch di sistemi.

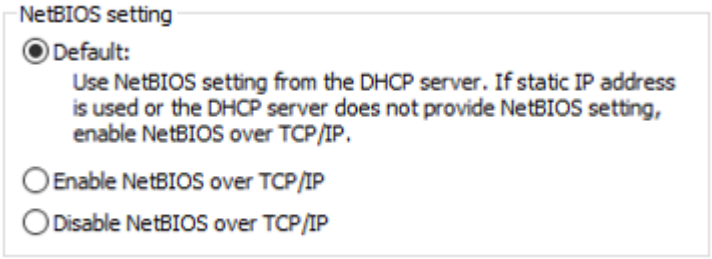
Dopo aver installato l'agente di protezione sui sistemi, questi vengono visualizzati nella sezione **Dispositivi** > **Macchine con agenti**.

Per verificare lo stato della protezione, passare a **Monitoraggio** > **Panoramica** e aggiungere il widget **Stato protezione** o il widget **Sistemi individuati**.

Risoluzione dei problemi

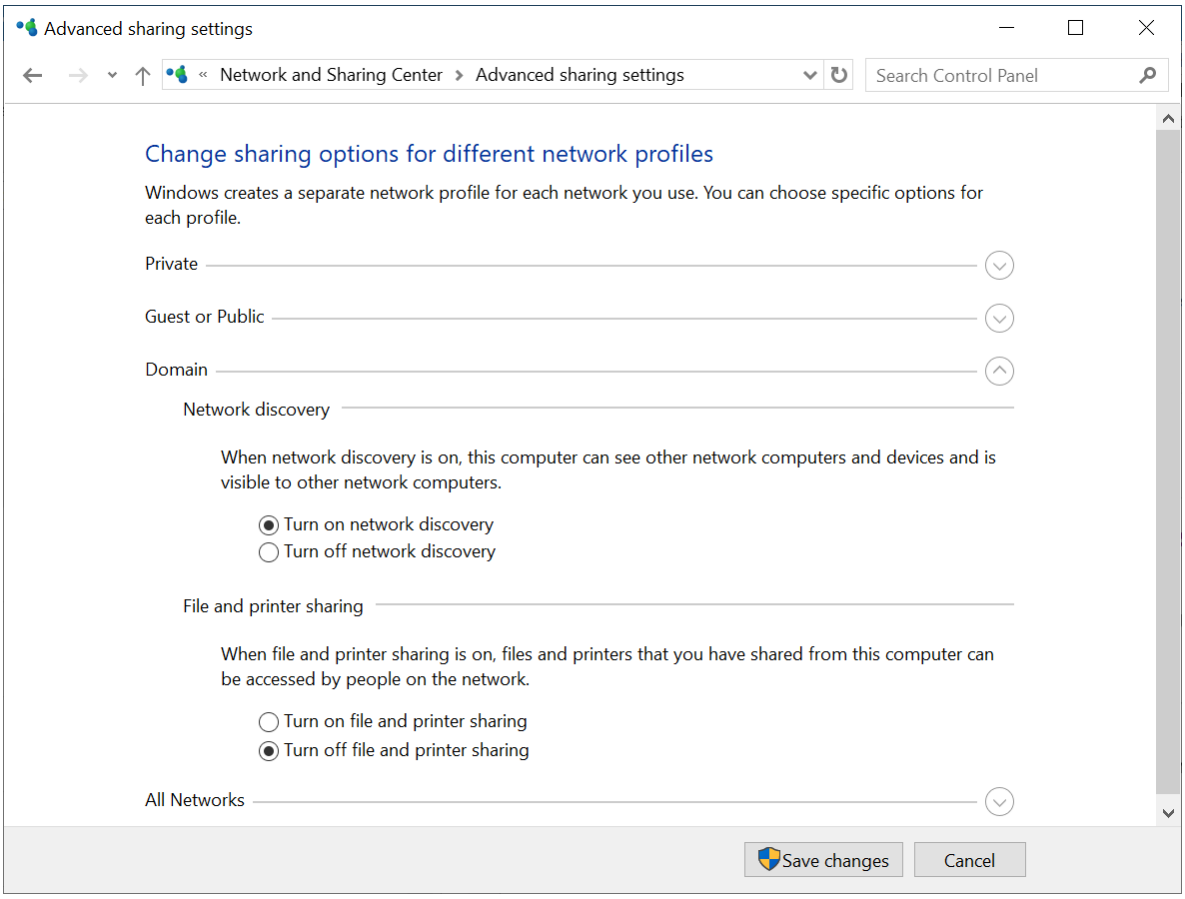
In caso di problemi con la funzione di individuazione automatica, verificare quanto segue:

- Verificare che l'impostazione NetBIOS su TCP/IP sia abilitata o impostata come predefinita.



- In "Pannello di controllo\Centro connessioni di rete e condivisione\impostazioni di condivisione avanzate" attivare l'individuazione della rete.

© Acronis International GmbH, 2003-2024



- Verificare che il servizio Host provider di individuazione funzioni sia in esecuzione nel sistema che esegue l'individuazione e nei sistemi da individuare.
- Verificare che il servizio Pubblicazione risorse per individuazione sia in esecuzione nei sistemi da individuare.

Distribuzione dell'Agente per VMware (Virtual Appliance)

Prima di iniziare

Requisiti di sistema per l'agente

Per impostazione predefinita, all'appliance virtuale sono assegnati 4 GB di RAM e 2 vCPU, sufficienti e ottimali per la maggior parte delle operazioni.

Per migliorare le prestazioni di backup ed evitare problemi causati dalla memoria RAM insufficiente, è consigliabile aumentare tali risorse a 16 GB di RAM e 4 vCPU nei casi di maggiore esigenza. Ad esempio, aumentare le risorse assegnate se si prevede che il traffico di backup superi i 100 MB al secondo (ad esempio, su reti 10-Gigabit) o se si esegue il backup simultaneo di più virtual machine con unità disco rigido di grandi dimensioni (500 GB o più).

Il disco virtuale dell'appliance non occupa più di 6 GB. Il formato del disco (thick o thin) non influisce sulle prestazioni dell'appliance.

© Acronis International GmbH, 2003-2024

Quanti agenti sono necessari?

Sebbene una appliance virtuale possa proteggere un intero ambiente vSphere, la procedura ottimale consiste nel distribuire un'appliance virtuale ogni cluster di vSphere cluster (o ogni host se non sono presenti cluster). Ciò accelera i backup perché l'appliance può collegare i dischi oggetto di backup tramite il trasporto HotAdd; di conseguenza il traffico di backup è diretto da un disco locale a un altro.

È normale usare l'appliance virtuale e l'Agente per VMware (Windows) contemporaneamente, a condizione che siano connessi allo stesso vCenter Server *oppure* a host ESXi diversi. È consigliabile evitare situazioni in cui un agente è connesso direttamente a un host ESXi e un altro gente è connesso al vCenter Server che gestisce tale ESXi.

Non è consigliabile l'utilizzo di uno storage collegato localmente (ad esempio per l'archiviazione di backup su dischi virtuali aggiunti all'appliance virtuale) se è presente più di un agente. Per altre informazioni, consultare "Utilizzo di un archivio collegato localmente" (pag. 707).

Disabilitare il servizio DRS automatico per l'agente

Se l'appliance virtuale è distribuita in un cluster vSphere, verificare di aver disabilitato vMotion. Nelle impostazioni di DRS del cluster, abilitare i singoli livelli di automazione della macchina virtuale e quindi impostare il **Livello di automazione** per l'appliance virtuale su **Disabilitato**.

Distribuzione del modello OVF

1. Fare clic su **Tutti i dispositivi** > **Aggiungi** > **VMware ESXi** > **Appliance virtuale (OVF)**.
   L'archivio in formato .zip viene scaricato nel computer.
2. Decomprimere l'archivio .zip. La cartella contiene un file .ovf e due file .vmdk.
3. Accertarsi che sia possibile accedere a questi file dal sistema che esegue il client vSphere.
4. Avviare il client vSphere e accedere al vCenter Server.
5. Distribuire il modello OVF.
   - Durante la configurazione dell'archivio, selezionare il datastore condiviso, se esistente. Il formato del disco (thick o thin) non influisce sulle prestazioni dell'appliance.
   - Durante la configurazione delle connessioni di rete, verificare di aver selezionato una rete che consente la connessione a Internet, in modo che l'agente possa registrarsi al cloud in modo idoneo.

Configurazione dell'appliance virtuale

Dopo aver distribuito l'appliance virtuale è necessario configurarla, così che possa accedere al vCenter Server o all'host ESXi e al servizio Cyber Protection.

Per configurare l'appliance virtuale

© Acronis International GmbH, 2003-2024

1. In vSphere Client, aprire la console dell'appliance virtuale.
2. Verificare che la connessione di rete sia configurata.

   La connessione viene configurata automaticamente tramite il protocollo Dynamic Host Configuration Protocol (DHCP).

   Per modificare la configurazione predefinita, in **Opzioni agente**, nel campo **eth0**, selezionare **Modifica** e specificare le impostazioni di rete.
3. Connettere l'appliance virtuale al vCenter Server o all'host ESXi.
   a. In **Opzioni agente**, nel campo **vCenter/ESX(i)**, selezionare **Modifica** e specificare quanto segue.
      - [Se si utilizza vCenter Server] Il nome o l'indirizzo IP del vCenter Server.
      - [Se non si utilizza vCenter Server] Specificare il nome o l'indirizzo IP dell'host ESXi sul quale eseguire il backup e il ripristino delle virtual machine. Per backup più rapidi, distribuire l'appliance virtuale sullo stesso host.
      - Le credenziali richieste per la connessione dell'appliance al vCenter Server o all'host ESXi.

        Si consiglia di utilizzare un account dedicato per accedere a vCenter Server o all'host ESXi, e non un account esistente con il ruolo Amministratore. Per ulteriori informazioni sui privilegi richiesti per l'account dedicato, fare riferimento a "Privilegi necessari per l'Agente per VMware" (pag. 714).
   b. Fare clic su **Controlla connessione** per verificare che le credenziali siano corrette.
   c. Fare clic su **OK**.
4. Registrare l'appliance nel servizio Cyber Protection usando uno dei metodi seguenti.
   - [Solo per i tenant senza autenticazione a due fattori] Registrare l'appliance nella rispettiva interfaccia grafica.
     a. In **Opzioni agente**, nel campo **Management Server**, fare clic su **Modifica**.
     b. Nel campo **Nome/IP server**, selezionare **Cloud**.

        Viene visualizzato l'indirizzo del servizio Cyber Protection. Non modificare questo indirizzo se non si ricevono indicazioni in merito.
     c. Nei campi **Nome utente** e **Password**, immettere le credenziali dell'account per il servizio Cyber Protection. L'appliance virtuale e le virtual machine che l'appliance gestisce vengono registrate in questo account.
     d. Fare clic su **OK**.
   - Registrare l'appliance nell'interfaccia a riga di comando.

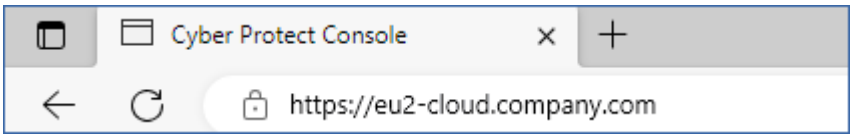
     Nota
     Se si sceglie questo metodo, è necessario un token di registrazione. Per ulteriori informazioni su come generarne uno, fare riferimento a "Generazione del token di registrazione" (pag. 172).

     a. Premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
     b. Lanciare il seguente comando:

 © Acronis International GmbH, 2003-2024

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

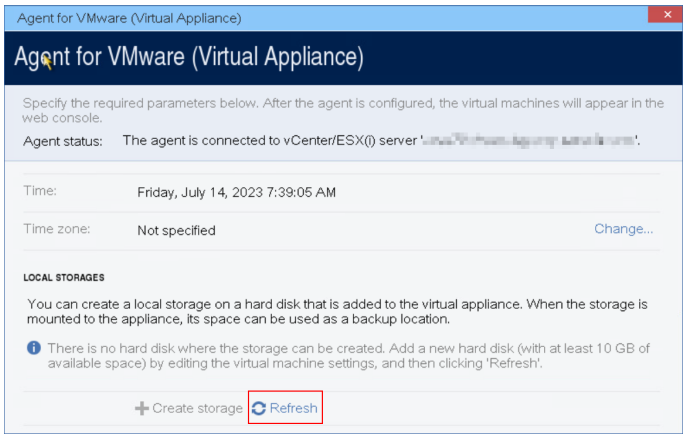
Nota
Quando si utilizza un token di registrazione, è necessario specificare l'indirizzo esatto del data center. Tale indirizzo corrisponde all'URL visualizzato **dopo aver fatto accesso** alla console di Cyber Protect. Ad esempio, `https://eu2-cloud.company.com`.



Non utilizzare `https://cloud.company.com` in questo caso.

c. Premere ALT+F1 per tornare all'interfaccia grafica dell'appliance.

5. [Facoltativo] Aggiungere uno storage locale.
   a. In vSphere Client, connettere un disco virtuale all'appliance virtuale. Il disco virtuale deve avere almeno 10 GB di spazio libero.
   b. Nell'interfaccia utente grafica dell'appliance, fare clic su **Aggiorna**.



   Il pulsante **Crea storage** si attiva.
   c. Fare clic su **Crea storage**.
   d. Specificare un'etichetta per lo storage, quindi fare clic su **OK**.
   e. Confermare la selezione facendo clic su **Sì**.

6. [Se è abilitato un server proxy nella rete] Configurare il proxy server.
   a. Premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
   b. Aprire il file **/etc/Acronis/Global.config** in un editor di testo.
   c. Eseguire una delle seguenti operazioni:
      - Se le impostazioni del proxy sono state specificate durante l'installazione dell'agente, individuare la sezione seguente:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
```


© Acronis International GmbH, 2003-2024

```
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- Altrimenti, copiare le righe indicate e incollarle nel file fra i tag `<registry name="Global">...</registry>`.

d. Sostituire `ADDRESS` con l'indirizzo IP/nome host del server proxy e `PORT` con il valore decimale del numero della porta.

e. Se il server proxy richiede l'autenticazione, sostituire `LOGIN` e `PASSWORD` con le credenziali del server proxy. In alternativa, eliminare queste righe dal file.

f. Salvare il file.

g. Aprire il file **/opt/acronis/etc/aakore.yaml** in un editor di testo.

h. Individuare la sezione **env** o crearla e aggiungere le righe seguenti:

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

i. Sostituire `proxy_login` e `proxy_password` con le credenziali del server proxy e `proxy_address:port` con l'indirizzo e il numero della porta del server proxy.

j. Eseguire il comando `reboot`.

Nota

Per poter aggiornare un'appliance virtuale distribuita dietro a un proxy, modificare il file dell'appliance `config.yaml` (`/opt/acronis/etc/va-updater/config.yaml`) aggiungendo la riga seguente in fondo al file, inserendo quindi i valori specifici per il proprio ambiente:

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

Per esempio:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Distribuzione dell'Agente per Scale Computing HC3 (appliance virtuale)

Prima di iniziare

Quest'appliance è una virtual machine preconfigurata che viene distribuita in un cluster Scale Computing HC3. Contiene un agente di protezione che consente di gestire la protezione informatica per tutte le virtual machine presenti nel cluster.

© Acronis International GmbH, 2003-2024

Requisiti di sistema per l’agente

Per impostazione predefinita, la virtual machine con l'agente utilizza 2 vCPU e 4 GiB di RAM. Queste impostazioni sono sufficienti per la maggior parte delle operazioni, ma è possibile modificarle agendo sulla virtual machine nell'interfaccia web di Scale Computing HC3.

Per migliorare le prestazioni di backup ed evitare problemi causati dalla memoria RAM insufficiente, si consiglia di aumentare tali risorse a 8 GiB di RAM e 4 vCPU nei casi di maggiore esigenza. Ad esempio, aumentare le risorse assegnate se si prevede che il traffico di backup superi i 100 MB al secondo (ad esempio, su reti 10-Gigabit) o se si esegue il backup simultaneo di più virtual machine con unità disco rigido di grandi dimensioni (500 GB o più).

La dimensione del disco dell'appliance virtuale è di circa 9 GB.

Quanti agenti sono necessari?

Un agente può proteggere l'intero cluster. Tuttavia, nel cluster possono essere presenti più agenti, nel caso in cui sia necessario distribuire il carico della larghezza di banda del traffico di backup.

Nei cluster in cui sono presenti più agenti, le virtual machine vengono automaticamente distribuite in modo omogeneo tra gli agenti, in modo che ogni agente gestisca un numero simile di sistemi.

La ridistribuzione automatica avviene quando lo squilibrio del carico tra gli agenti raggiunge il 20%. Ciò si verifica, ad esempio, quando un agente o un sistema vengono aggiunti o rimossi. Per esempio, si comprende che sono necessari più agenti per incrementare la produttività e pertanto si distribuisce un'appliance virtuale aggiuntiva sul cluster. Il server di gestione assegna le macchine più appropriate al nuovo agente. Il carico dei vecchi agenti si ridurrà. Quando si rimuove un agente dal management server, i sistemi assegnati all'agente vengono ridistribuiti tra gli agenti rimanenti. Tuttavia, ciò non accade se un agente risulta danneggiato o se viene eliminato manualmente dal cluster Scale Computing HC3. La ridistribuzione verrà avviata solo dopo la rimozione dell'agente dalla console di Cyber Protect.

Per controllare quale agente gestisce un sistema specifico

1. Nella console di Cyber Protect, fare clic su **Dispositivi** e selezionare **Scale Computing**.
2. Fare clic sull'icona ingranaggio nell'angolo in alto a destra della tabella e, in **Sistema**, selezionare la casella di controllo **Agente**.
3. Controllare il nome dell'agente nella colonna visualizzata.

Distribuzione del modello QCOW2

1. Accedere all'account Cyber Protection.
2. Fare clic su **Dispositivi** > **Tutti i dispositivi** > **Aggiungi** > **Scale Computing HC3**.
   L’archivio in formato .zip viene scaricato nel computer.
3. Decomprimere l'archivio zip e quindi salvare il file .qcow2 e il file .xml in una cartella chiamata **ScaleAppliance**.

© Acronis International GmbH, 2003-2024

4. Caricare la cartella **ScaleAppliance** in una condivisione di rete e verificare che il cluster Scale Computing HC3 possa accedervi.
5. Accedere al cluster Scale Computing HC3 come amministratore con il ruolo **Crea/Modifica VM** assegnato. Per ulteriori informazioni sui ruoli richiesti per eseguire le operazioni con le virtual machine di Scale Computing HC3, fare riferimento a "Agente per Scale Computing HC3 - ruoli necessari" (pag. 147).
6. Nell'interfaccia web di Scale Computing HC3, importare il modello di virtual machine dalla cartella **ScaleAppliance**.
   a. Fare clic sull'icona **Import VM HC3**.
   b. Nella finestra **Import HC3 VM**, specificare quanto segue:
      - Il nome della nuova macchina virtuale.
      - La condivisione di rete su cui si trova la cartella **ScaleAppliance**.
      - Il nome utente e la password necessarie per accedere a questa condivisione di rete.
      - [Facoltativo] Una tag di dominio per la nuova virtual machine.
      - Il percorso alla cartella **ScaleAppliance** nella condivisione di rete.
   c. Fare clic su **Importa**.

Una volta completato il deployment, è necessario configurare l'appliance virtuale. Per ulteriori informazioni su come procedere per la configurazione, fare riferimento a "Configurazione dell'appliance virtuale" (pag. 144).

Nota
Se nel cluster sono necessarie più appliance virtuali, ripetere questi passaggi ed eseguire il deployment delle appliance virtuali aggiuntive. Non clonare un'appliance virtuale esistente utilizzando l'opzione **Clone VM** nell'interfaccia web di Scale Computing HC3.

Configurazione dell'appliance virtuale

Dopo aver distribuito l'appliance virtuale è necessario configurarla, così che possa raggiungere sia il cluster di Scale Computing HC3 che deve proteggere, sia il servizio Cyber Protection.

Per configurare l'appliance virtuale

1. Accedere all'account Scale Computing HC3.
2. Selezionare l'appliance virtuale da configurare, quindi fare clic sull'icona **Console**.
3. Nel campo **eth0**, configurare le interfacce di rete dell'appliance.
   Verificare che gli indirizzi DHCP assegnati automaticamente (se presenti) siano validi per le reti utilizzate dalla virtual machine, in caso contrario assegnarli manualmente. Potrebbe essere necessario configurare una o più interfacce, a seconda del numero di reti utilizzate dall'appliance.
4. Nel campo **Scale Computing**, fare clic su **Modifica** per specificare l'indirizzo del cluster Scale Computing HC3 e le credenziali per accedervi.

© Acronis International GmbH, 2003-2024

a. Nel campo **Nome/IP server**, immettere il nome DNS o l'indirizzo IP del cluster.

b. Nei campi **Nome utente** e **Password**, immettere le credenziali dell'account amministratore di Scale Computing HC3.

   Verificare che questo account abbia i ruoli necessari per eseguire operazioni con virtual machine Scale Computing HC3. Per ulteriori informazioni su questi ruoli, consultare "Agente per Scale Computing HC3 - ruoli necessari" (pag. 147).

c. Fare clic su **Controlla connessione** per verificare che le credenziali siano corrette.

d. Fare clic su **OK**.

5. Registrare l'appliance nel servizio Cyber Protection usando uno dei metodi seguenti.

- [Solo per i tenant senza autenticazione a due fattori] Registrare l'appliance nella rispettiva interfaccia grafica.

  a. In **Opzioni agente**, nel campo **Management Server**, fare clic su **Modifica**.

  b. Nel campo **Nome/IP server**, selezionare **Cloud**.

     Viene visualizzato l'indirizzo del servizio Cyber Protection. Non modificare questo indirizzo se non si ricevono indicazioni in merito.

  c. Nei campi **Nome utente** e **Password**, immettere le credenziali dell'account per il servizio Cyber Protection. L'appliance virtuale e le virtual machine che l'appliance gestisce vengono registrate in questo account.

  d. Fare clic su **OK**.

- Registrare l'appliance nell'interfaccia a riga di comando.

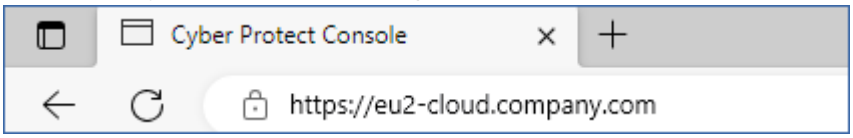
  Nota
  Se si sceglie questo metodo, è necessario un token di registrazione. Per ulteriori informazioni su come generarne uno, fare riferimento a "Generazione del token di registrazione" (pag. 172).

  a. Premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.

  b. Lanciare il seguente comando:

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

  Nota
  Quando si utilizza un token di registrazione, è necessario specificare l'indirizzo esatto del data center. Tale indirizzo corrisponde all'URL visualizzato **dopo aver fatto accesso** alla console di Cyber Protect. Ad esempio, `https://eu2-cloud.company.com`.

© Acronis International GmbH, 2003-2024

Non utilizzare `https://cloud.company.com` in questo caso.

c. Premere ALT+F1 per tornare all'interfaccia grafica dell'appliance.

6. [Facoltativo] Nel campo **Nome**, fare clic su **Modifica** per modificare il nome predefinito dell'appliance virtuale, che è **localhost**. Tale nome viene visualizzato nella console di Cyber Protect.
7. [Facoltativo] Nel campo **Orario**, fare clic su **Modifica**, quindi selezionare il fuso orario della propria posizione per fare in modo che le operazioni pianificate vengano eseguite all'ora adeguata.
8. [Se è abilitato un server proxy nella rete] Configurare il proxy server.
   a. Premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
   b. Aprire il file **/etc/Acronis/Global.config** in un editor di testo.
   c. Eseguire una delle seguenti operazioni:
      - Se le impostazioni del proxy sono state specificate durante l'installazione dell'agente, individuare la sezione seguente:

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

      - Altrimenti, copiare le righe indicate e incollarle nel file fra i tag `<registry name="Global">...</registry>`.
   d. Sostituire `ADDRESS` con l'indirizzo IP/nome host del server proxy e `PORT` con il valore decimale del numero della porta.
   e. Se il server proxy richiede l'autenticazione, sostituire `LOGIN` e `PASSWORD` con le credenziali del server proxy. In alternativa, eliminare queste righe dal file.
   f. Salvare il file.
   g. Aprire il file **/opt/acronis/etc/aakore.yaml** in un editor di testo.
   h. Individuare la sezione **env** o crearla e aggiungere le righe seguenti:

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

   i. Sostituire `proxy_login` e `proxy_password` con le credenziali del server proxy e `proxy_address:port` con l'indirizzo e il numero della porta del server proxy.
   j. Eseguire il comando `reboot`.

© Acronis International GmbH, 2003-2024

Nota

Per poter aggiornare un'appliance virtuale distribuita dietro a un proxy, modificare il file dell'appliance `config.yaml` (`/opt/acronis/etc/va-updater/config.yaml`) aggiungendo la riga seguente in fondo al file, inserendo quindi i valori specifici per il proprio ambiente:

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

Per esempio:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Per proteggere le virtual machine nel cluster Scale Computing HC3

1. Accedere all'account Cyber Protection.
2. Passare a **Dispositivi** > **Scale Computing HC3**> <cluster personale> oppure individuare i sistemi in **Dispositivi** > **Tutti i dispositivi**.
3. Selezionare i sistemi e applicare i piani di protezione.

Agente per Scale Computing HC3 - ruoli necessari

Questa sezione descrive i ruoli necessari per operazioni con virtual machine Scale Computing HC3.

Operazione	Ruolo
Backup di una virtual machine	Backup Crea/Modifica VM Elimina VM
Ripristino su una virtual machine esistente	Backup Crea/Modifica VM Controllo delle opzioni energetiche della VM Elimina VM Impostazioni del cluster
Ripristino su una nuova virtual machine	Backup Crea/Modifica VM Controllo delle opzioni energetiche della VM Elimina VM Impostazioni del cluster

© Acronis International GmbH, 2003-2024

Distribuzione dell'Agente per Virtuozzo Hybrid Infrastructure (appliance virtuale)

Prima di iniziare

Questa appliance è una macchina virtuale pre-configurata che viene distribuita in Virtuozzo Hybrid Infrastructure. Contiene un agente di protezione che consente di gestire la protezione informatica per tutte le macchine virtuali presenti in un cluster di Virtuozzo Hybrid Infrastructure.

Nota
Per accertarsi che i backup con l'opzione di backup **Servizio Copia Shadow del volume per virtual machine** abilitata vengano eseguiti correttamente e acquisiscano i dati in uno stato coerente con l'applicazione più recente, verificare che gli strumenti Virtuozzo Guest Tools siano installati e aggiornati sulle virtual machine protette.

Requisiti di sistema per l'agente

Durante la distribuzione dell'appliance virtuale è possibile scegliere tra diverse combinazioni predefinite di vCPU e RAM (versioni). È inoltre possibile creare versioni personalizzate.

4 GB di RAM e 2 vCPU (versione media) sono sufficienti e ottimali per la maggior parte delle operazioni. Per migliorare le prestazioni di backup ed evitare problemi causati dalla memoria RAM insufficiente, è consigliabile aumentare tali risorse a 8 GB di RAM e 4 vCPU nei casi di maggiore esigenza. Ad esempio, aumentare le risorse assegnate se si prevede che il traffico di backup superi i 100 MB al secondo (ad esempio, su reti 10-Gigabit) o se si esegue il backup simultaneo di più virtual machine con unità disco rigido di grandi dimensioni (500 GB o più).

Quanti agenti sono necessari?

Un agente può proteggere l'intero cluster. Tuttavia, nel cluster possono essere presenti più agenti, nel caso in cui sia necessario distribuire il carico della larghezza di banda del traffico di backup.

Nei cluster in cui sono presenti più agenti, le virtual machine vengono automaticamente distribuite in modo omogeneo tra gli agenti, in modo che ogni agente gestisca un numero simile di sistemi.

La ridistribuzione automatica avviene quando lo squilibrio del carico tra gli agenti raggiunge il 20%. Ciò si verifica, ad esempio, quando un agente o un sistema vengono aggiunti o rimossi. Per esempio, si comprende che sono necessari più agenti per incrementare la produttività e pertanto si distribuisce un'appliance virtuale aggiuntiva sul cluster. Il server di gestione assegna le macchine più appropriate al nuovo agente. Il carico dei vecchi agenti si ridurrà. Quando si rimuove un agente dal management server, i sistemi assegnati all'agente vengono ridistribuiti tra gli agenti rimanenti. Tuttavia, ciò non accade se un agente risulta danneggiato o se viene eliminato manualmente dal nodo Virtuozzo Hybrid Infrastructure. La ridistribuzione verrà avviata solo dopo la rimozione dell'agente dall'interfaccia web di Cyber Protection.

© Acronis International GmbH, 2003-2024

Per controllare quale agente gestisce un sistema specifico

1. Nella console di Cyber Protect, fare clic su **Dispositivi** e selezionare **Virtuozzo Hybrid Infrastructure**.
2. Fare clic sull'icona ingranaggio nell'angolo in alto a destra della tabella e, in **Sistema**, selezionare la casella di controllo **Agente**.
3. Controllare il nome dell'agente nella colonna visualizzata.

Limitazioni

- Non è possibile distribuire l'appliance Virtuozzo Hybrid Infrastructure in modalità remota.
- Il backup application-aware delle macchine virtuali non è supportato.

Configurazione delle reti in Virtuozzo Hybrid Infrastructure

Prima di distribuire e configurare l'appliance virtuale, è necessario configurare le reti in Virtuozzo Hybrid Infrastructure.

Requisiti di rete per Agente per Virtuozzo Hybrid Infrastructure (appliance virtuale)

- L'appliance virtuale richiede due schede di rete.
- L'appliance virtuale deve essere connessa alle reti Virtuozzo con le tipologie di traffico di rete seguenti:
  - Compute API
  - Backup MV
  - ABGW Public
  - VM Public

Per ulteriori informazioni sulla configurazione delle reti, vedere l'articolo relativo ai requisiti del cluster di elaborazione nella documentazione di Virtuozzo.

Configurazione degli account utente in Virtuozzo Hybrid Infrastructure

Per configurare l'appliance virtuale, occorre un account utente di Virtuozzo Hybrid Infrastructure. L'account deve disporre del ruolo di **Amministratore** nel dominio **Default**. Per ulteriori informazioni sugli utenti, vedere l'articolo relativo alla gestione degli utenti del pannello di amministrazione nella documentazione di Virtuozzo Hybrid Infrastructure. Assicurarsi di aver concesso l'accesso a tutti i progetti all'account nel dominio **Default**.

Per concedere l'accesso a tutti i progetti nel dominio Default

1. Creare un file di ambiente per l'amministratore di sistema. A tal fine, eseguire il seguente script nel cluster di Virtuozzo Hybrid Infrastructure tramite l'interfaccia a riga di comando di OpenStack. Per ulteriori informazioni sulla connessione a questa interfaccia, vedere il capitolo

© Acronis International GmbH, 2003-2024

relativo alla connessione all'interfaccia a riga di comando di OpenStack nella documentazione di Virtuozzo Hybrid Infrastructure.

```
su - vstoradmin
kolla-ansible post-deploy
exit
```

2. Utilizzare il file di ambiente per autorizzare ulteriori comandi di OpenStack:

```
. /etc/kolla/admin-openrc.sh
```

3. Eseguire i seguenti comandi:

```
openstack --insecure user set --project admin --project-domain Default --domain
Default <username>
openstack --insecure role add --domain Default --user <username> --user-domain
Default compute --inherited
```

Qui, <username> rappresenta l'account di Virtuozzo Hybrid Infrastructure con il ruolo di **Amministratore** nel dominio **Default**. L'appliance virtuale utilizzerà questo account per eseguire il backup e il ripristino delle macchine virtuali nei progetti figlio del dominio **Default**.

Esempio

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

Per gestire i backup delle virtual machine in un dominio diverso da quello di **Default**, eseguire anche il comando seguente.

Per concedere l'accesso a tutti i progetti in un altro dominio

```
openstack --insecure role add --domain <domain name> --inherited --user <username> --
user-domain Default admin
```

Qui, <domain name> rappresenta il dominio dei progetti in cui l'account <username> avrà accesso.

Esempio

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-
domain Default admin
```

Dopo aver autorizzato l'accesso ai progetti, verificare quali ruoli sono assegnati all'account.

© Acronis International GmbH, 2003-2024

Per verificare i ruoli assegnati

```
openstack --insecure role assignment list --user <username> --names
```

Qui, <username> rappresenta l'account di Virtuozzo Hybrid Infrastructure.

Esempio

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | MyNewDomain |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

In questo esempio, le opzioni `-c Role`, `-c User`, `-c Project` e `-c Domain` sono utilizzate per abbreviare l'output del comando affinché si adatti alla pagina.

Per controllare i ruoli effettivi assegnati all'account in tutti i progetti, eseguire anche il comando seguente.

Per controllare i ruoli effettivi in tutti i progetti

```
openstack --insecure role assignment list --user <username> --names --effective
```

Qui, <username> rappresenta l'account di Virtuozzo Hybrid Infrastructure.

Esempio

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
```


© Acronis International GmbH, 2003-2024

```
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

In questo esempio, le opzioni `-c Role`, `-c User`, `-c Project` e `-c Domain` sono utilizzate per abbreviare l'output del comando affinché si adatti alla pagina.

Distribuzione del modello QCOW2

1. Accedere all'account Cyber Protection.
2. Fare clic su **Dispositivi** > **Tutti i dispositivi** > **Aggiungi** > **Virtuozzo Hybrid Infrastructure**. L'archivio in formato .zip viene scaricato nel computer.
3. Decomprimere l'archivio .zip. L'archivio contiene un file di immagine .qcow2.
4. Accedere all'account Virtuozzo Hybrid Infrastructure personale.
5. Aggiungere il file di immagine .qcow2 al cluster di elaborazione di Virtuozzo Hybrid Infrastructure come indicato di seguito:
   - Nella scheda **Compute** > **Virtual machines** > **Images**, fare clic su **Add image**.
   - Nella finestra **Add image** fare clic su **Browse** e quindi selezionare il file .qcow2.
   - Specificare il nome dell'immagine, selezionare il tipo **Generic Linux OS** e quindi fare clic su **Add**.
6. Nella scheda **Compute** > **Virtual machines** > **Virtual machines**, fare clic su **Create virtual machine**. Viene visualizzata una finestra nella quale è necessario specificare i parametri seguenti:
   - Il nome della nuova macchina virtuale.
   - In **Deploy from**, selezionare **Image**.
   - Nella finestra **Images**, selezionare il file di immagine .qcow2 dell'appliance, quindi fare clic su **Fine**.
   - Nella finestra **Volumes** non è necessario aggiungere alcun volume. Il volume aggiunto in modo automatico per il disco di sistema è infatti sufficiente.
   - Nella finestra **Flavor**, scegliere la combinazione desiderata di vCPU e RAM e quindi fare clic su **Fine**. In genere sono sufficienti 2 vCPU e 4 GB di RAM.
   - Nella finestra **Network interfaces**, fare clic su **Add**, selezionare le reti virtuali di tipo *pubblico*, quindi fare clic su **Add**. La rete verrà visualizzata nell'elenco **Network interfaces**.
     Se si utilizza una configurazione con più di una rete fisica (e di conseguenza con più di una rete virtuale di tipo pubblico), ripetere questo passaggio e selezionare le reti virtuali necessarie.
7. Fare clic su **Fine**.
8. Tornare alla finestra **Create virtual machine** e fare clic su **Deploy** per creare e avviare la macchina virtuale.

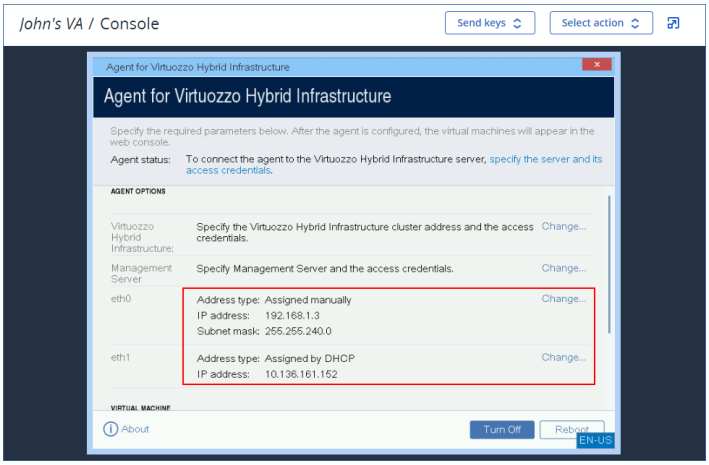
© Acronis International GmbH, 2003-2024

Configurazione dell'appliance virtuale

Dopo aver distribuito l' Agente per Virtuozzo Hybrid Infrastructure (appliance virtuale) è necessario configurarla così che possa raggiungere sia il cluster di Virtuozzo Hybrid Infrastructure che deve proteggere, sia il servizio cloud Cyber Protection.

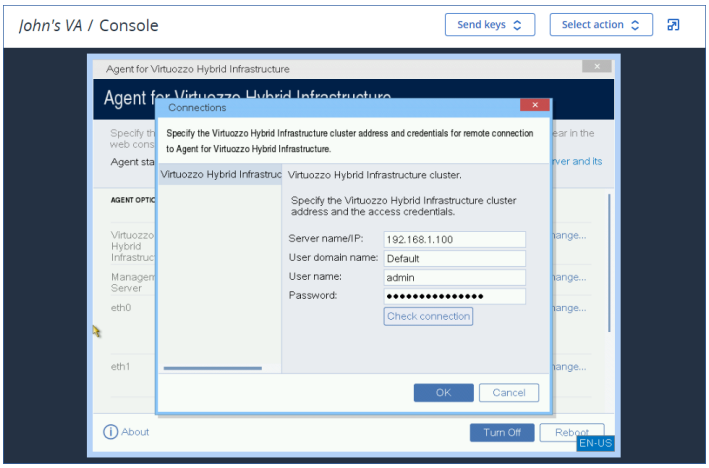
Per configurare l'appliance virtuale

1. Accedere all'account Virtuozzo Hybrid Infrastructure personale.
2. Nella scheda **Compute** > **Virtual machines** > **Virtual machines**, selezionare la macchina virtuale creata. Fare clic su **Console**.
3. Configurare le interfacce di rete dell'appliance. Potrebbe essere necessario configurare una o più interfacce, a seconda del numero di reti virtuali utilizzate dall'appliance. Verificare che gli indirizzi DHCP assegnati automaticamente (se presenti) siano validi per le reti utilizzate dalla virtual machine, in caso contrario assegnarli manualmente.



4. Specificare le credenziali e l'indirizzo del cluster Virtuozzo:
   - Nome DNS o indirizzo IP del cluster Virtuozzo Hybrid Infrastructure – si tratta dell'indirizzo del nodo di gestione del cluster. Viene automaticamente impostata la porta predefinita 5000. Per utilizzare una porta differente è necessario specificarla manualmente.
   - Nel campo **Nome dell'utente di dominio**, specificare il dominio in Virtuozzo Hybrid Infrastructure. Ad esempio, **Default**.
     Il nome del dominio fa distinzione tra maiuscole e minuscole.
   - Nei campi **Nome utente** e **Password**, immettere le credenziali dell'account utente Virtuozzo Hybrid Infrastructure che dispone del ruolo **Amministratore** nel dominio specificato. Per ulteriori informazioni su utenti, ruoli e domini, consultare Configurazione degli account utente in Virtuozzo Hybrid Infrastructure.

© Acronis International GmbH, 2003-2024



5. Registrare l'appliance nel servizio Cyber Protection usando uno dei metodi seguenti.
   - [Solo per i tenant senza autenticazione a due fattori] Registrare l'appliance nella rispettiva interfaccia grafica.
     a. In **Opzioni agente**, nel campo **Management Server**, fare clic su **Modifica**.
     b. Nel campo **Nome/IP server**, selezionare **Cloud**.
        Viene visualizzato l'indirizzo del servizio Cyber Protection. Non modificare questo indirizzo se non si ricevono indicazioni in merito.
     c. Nei campi **Nome utente** e **Password**, immettere le credenziali dell'account per il servizio Cyber Protection. L'appliance virtuale e le virtual machine che l'appliance gestisce vengono registrate in questo account.
     d. Fare clic su **OK**.
   - Registrare l'appliance nell'interfaccia a riga di comando.

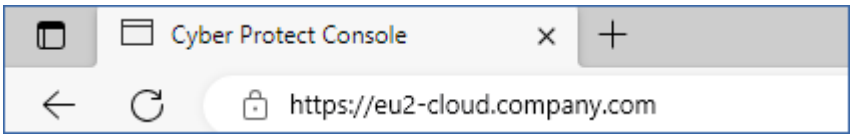
     Nota
     Se si sceglie questo metodo, è necessario un token di registrazione. Per ulteriori informazioni su come generarne uno, fare riferimento a "Generazione del token di registrazione" (pag. 172).

     a. Premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
     b. Lanciare il seguente comando:

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


© Acronis International GmbH, 2003-2024

Nota
Quando si utilizza un token di registrazione, è necessario specificare l'indirizzo esatto del data center. Tale indirizzo corrisponde all'URL visualizzato **dopo aver fatto accesso** alla console di Cyber Protect. Ad esempio, `https://eu2-cloud.company.com`.



Non utilizzare `https://cloud.company.com` in questo caso.

c. Premere ALT+F1 per tornare all'interfaccia grafica dell'appliance.

6. [Se è abilitato un server proxy nella rete] Configurare il proxy server.
   a. Premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
   b. Aprire il file **/etc/Acronis/Global.config** in un editor di testo.
   c. Eseguire una delle seguenti operazioni:
      - Se le impostazioni del proxy sono state specificate durante l'installazione dell'agente, individuare la sezione seguente:

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

      - Altrimenti, copiare le righe indicate e incollarle nel file fra i tag `<registry name="Global">...</registry>`.
   d. Sostituire `ADDRESS` con l'indirizzo IP/nome host del server proxy e `PORT` con il valore decimale del numero della porta.
   e. Se il server proxy richiede l'autenticazione, sostituire `LOGIN` e `PASSWORD` con le credenziali del server proxy. In alternativa, eliminare queste righe dal file.
   f. Salvare il file.
   g. Aprire il file **/opt/acronis/etc/aakore.yaml** in un editor di testo.
   h. Individuare la sezione **env** o crearla e aggiungere le righe seguenti:

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

   i. Sostituire `proxy_login` e `proxy_password` con le credenziali del server proxy e `proxy_address:port` con l'indirizzo e il numero della porta del server proxy.
   j. Eseguire il comando `reboot`.

© Acronis International GmbH, 2003-2024

Nota

Per poter aggiornare un'appliance virtuale distribuita dietro a un proxy, modificare il file dell'appliance `config.yaml` (`/opt/acronis/etc/va-updater/config.yaml`) aggiungendo la riga seguente in fondo al file, inserendo quindi i valori specifici per il proprio ambiente:

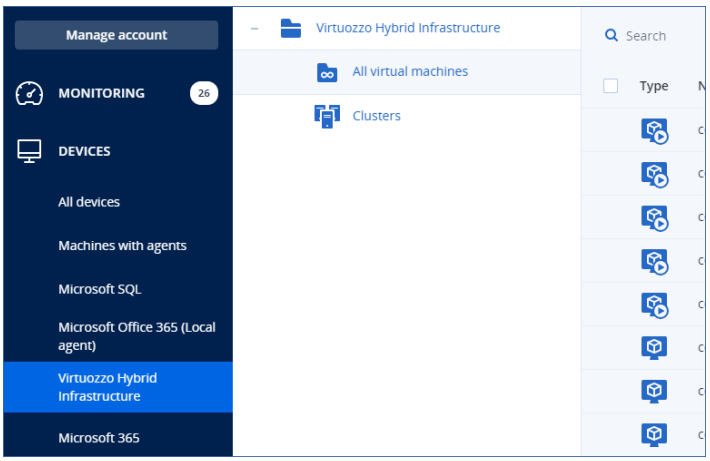
```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Per esempio:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Per proteggere le macchine virtuali nel cluster Virtuozzo Hybrid Infrastructure

1. Accedere all'account Cyber Protection.
2. Passare a **Dispositivi** > **Virtuozzo Hybrid Infrastructure**> <cluster personale> > **Progetto predefinito** > **amministratore** oppure individuare i sistemi in **Dispositivi** > **Tutti i dispositivi**.
3. Selezionare i sistemi e applicare i piani di protezione.



Distribuzione dell'Agente per oVirt (Virtual Appliance)

Prima di iniziare

Quest'appliance è una virtual machine preconfigurata che viene distribuita in un data center Red Hat Virtualization/oVirt. Contiene un agente di protezione che consente di gestire la protezione informatica di tutte le virtual machine presenti nel data center.

Requisiti di sistema per l'agente

Per impostazione predefinita, la virtual machine con l'agente utilizza 2 vCPU e 4 GiB di RAM. Queste impostazioni sono sufficienti per la maggior parte delle operazioni, ma è possibile modificarle nel portale di amministrazione di Red Hat Virtualization/oVirt.

© Acronis International GmbH, 2003-2024

Per migliorare le prestazioni di backup ed evitare problemi causati dalla memoria RAM insufficiente, si consiglia di aumentare tali risorse a 8 GiB di RAM e 4 vCPU nei casi di maggiore esigenza. Ad esempio, aumentare le risorse assegnate se si prevede che il traffico di backup superi i 100 MB al secondo (ad esempio, su reti 10-Gigabit) o se si esegue il backup simultaneo di più virtual machine con unità disco rigido di grandi dimensioni (500 GB o più).

La dimensione del disco dell'appliance virtuale è 8 GiB.

Quanti agenti sono necessari?

Un agente può proteggere l'intero data center. Tuttavia, nel data center possono essere presenti più agenti, nel caso in cui sia necessario distribuire il carico della larghezza di banda del traffico di backup.

Nei data center in cui sono presenti più agenti, le virtual machine vengono distribuite in modo automatico tra gli agenti, in modo che ogni agente gestisca un numero simile di sistemi.

La ridistribuzione automatica avviene quando lo squilibrio del carico tra gli agenti raggiunge il 20%. Ciò si verifica, ad esempio, quando un agente o un sistema vengono aggiunti o rimossi. Per esempio, si comprende che sono necessari più agenti per incrementare la produttività e pertanto si distribuisce un'appliance virtuale aggiuntiva nel data center. Il server di gestione assegna le macchine più appropriate al nuovo agente. Il carico dei vecchi agenti si ridurrà. Quando si rimuove un agente, i sistemi assegnati all'agente vengono ridistribuiti tra gli agenti rimanenti. Tuttavia, ciò non accade se un agente risulta danneggiato o se viene eliminato manualmente dal portale di amministrazione di Red Hat Virtualization/oVirt. La ridistribuzione verrà avviata solo dopo la rimozione dell'agente dalla console di Cyber Protect.

Per controllare quale agente gestisce un sistema specifico

1. Nella console di Cyber Protect, fare clic su **Dispositivi** e selezionare **oVirt**.
2. Fare clic sull'icona ingranaggio nell'angolo in alto a destra della tabella e, in **Sistema**, selezionare la casella di controllo **Agente**.
3. Controllare il nome dell'agente nella colonna visualizzata.

Limitazioni

Le seguenti operazioni non sono supportate per le virtual machine Red Hat Virtualization/oVirt:

- Backup compatibile con l’applicazione
- Esecuzione di una virtual machine da un backup
- Replica di macchine virtuali
- Changed block tracking (CBT)

© Acronis International GmbH, 2003-2024

Distribuzione del modello OVA

1. Accedere all'account Cyber Protection.
2. Fare clic su **Dispositivi** > **Tutti i dispositivi** > **Aggiungi** > **Red Hat Virtualization (oVirt)**.
   L'archivio in formato .zip viene scaricato nel computer.
3. Decomprimere l'archivio .zip. Contiene un file con estensione .ova.
4. Scaricare il file .ova nell'host nel data center Red Hat Virtualization/oVirt da proteggere.
5. Accedere al portale di amministrazione di Red Hat Virtualization/oVirt come amministratore. Per ulteriori informazioni sui ruoli richiesti per eseguire le operazioni con le virtual machine, fare riferimento a "Agente per oVirt – ruoli e porte richiesti" (pag. 162).
6. Nel menu di navigazione, selezionare **Compute** > **Virtual machines**.
7. Fare clic sull'icona dei puntini di sospensione in verticale , e quindi su **Import**.
8. Nella finestra **Import Virtual Machine(s)**, procedere come segue:
   a. In **Data center**, selezionare il data center da proteggere.
   b. In **Source**, selezionare **Virtual Appliance (OVA)**.
   c. In **Host**, selezionare l'host nel quale è stato caricato il file .ova.
   d. In **File Path**, specificare il percorso alla directory che contiene il file .ova.
   e. Fare clic su **Load**.
      Il modello di appliance virtuale oVirt del file .ova viene visualizzato nel riquadro **Virtual Machines on Source**.
      Se il modello non viene visualizzato in questo riquadro, verificare di aver specificato il percorso corretto al file, che il file non sia danneggiato e che l'host sia raggiungibile.
   f. In **Virtual Machines on Source**, selezionare il modello di appliance virtuale oVirt, quindi fare clic sulla freccia a destra.
      Il modello viene visualizzato nel riquadro **Virtual machines to import**.
   g. Fare clic su **Avanti**.
9. Nella finestra successiva, fare clic sul nome dell'appliance, quindi configurare le impostazioni seguenti:
   - Nella scheda **Network interfaces** configurare le interfacce di rete.
   - [Facoltativo] Nella scheda **Informazioni generali**, modificare il nome predefinito della virtual machine con l'agente.

Il deployment è completo. A questo punto è necessario configurare l'appliance virtuale. Per ulteriori informazioni su come procedere per la configurazione, fare riferimento a "Configurazione dell'appliance virtuale" (pag. 159).

© Acronis International GmbH, 2003-2024

Nota
Se nel data center è necessario installare più di un'appliance virtuale, ripetere i passaggi precedenti e distribuire le ulteriori appliance richieste. Non clonare un'appliance virtuale esistente utilizzando l'opzione **Clone VM** nel portale di amministrazione di Red Hat Virtualization/oVirt.

Per escludere l'appliance virtuale dal backup di gruppi dinamici, è necessario escluderla anche dall'elenco di virtual machine nella console di Cyber Protect. Per escluderla, nel portale di amministrazione di Red Hat Virtualization/oVirt, selezionare la virtual machine con l'agente, quindi assegnare la tag `acronis_virtual_appliance`.

Configurazione dell'appliance virtuale

Dopo aver distribuito l'appliance virtuale è necessario configurarla, così che possa raggiungere sia il motore oVirt sia il servizio Cyber Protection.

Per configurare l'appliance virtuale

1. Accedere al portale di amministrazione di Red Hat Virtualization/oVirt.
2. Selezionare l'appliance virtuale da configurare, quindi fare clic sull'icona **Console**.
3. Nel campo **eth0**, configurare le interfacce di rete dell'appliance.
   Verificare che gli indirizzi DHCP assegnati automaticamente (se presenti) siano validi per le reti utilizzate dalla virtual machine, in caso contrario assegnarli manualmente. Potrebbe essere necessario configurare una o più interfacce, a seconda del numero di reti utilizzate dall'appliance.
4. Nel campo **oVirt**, fare clic su **Modifica** per specificare l'indirizzo del motore oVirt e le credenziali per accedervi:
   a. Nel campo **Nome/IP server**, immettere il nome DNS o l'indirizzo IP del motore.
   b. Nei campi **Nome utente** e **Password**, immettere le credenziali dell'amministratore per questo motore.
      Verificare che questo account amministratore disponga dei ruoli richiesti per eseguire operazioni con virtual machine Red Hat Virtualization/oVirt. Per ulteriori informazioni su questi ruoli, consultare "Agente per oVirt – ruoli e porte richiesti" (pag. 162).
      Se Keycloak è il provider di SSO per la tecnologia oVirt (per impostazione predefinita oVirt 4.5.1), utilizzare il formato di Keycloak per specificare il nome utente. Per esempio, specificare l'account dell'amministratore predefinito nel formato `admin@ovirt@internalsso` e non `admin@internal`.
   c. [Facoltativo] Fare clic su **Controlla connessione** per assicurarsi che le credenziali fornite siano corrette.
   d. Fare clic su **OK**.
5. Registrare l'appliance nel servizio Cyber Protection usando uno dei metodi seguenti.
   - [Solo per i tenant senza autenticazione a due fattori] Registrare l'appliance nella rispettiva interfaccia grafica.

© Acronis International GmbH, 2003-2024

a. In **Opzioni agente**, nel campo **Management Server**, fare clic su **Modifica**.

b. Nel campo **Nome/IP server**, selezionare **Cloud**.

   Viene visualizzato l'indirizzo del servizio Cyber Protection. Non modificare questo indirizzo se non si ricevono indicazioni in merito.

c. Nei campi **Nome utente** e **Password**, immettere le credenziali dell'account per il servizio Cyber Protection. L'appliance virtuale e le virtual machine che l'appliance gestisce vengono registrate in questo account.

d. Fare clic su **OK**.

- Registrare l'appliance nell'interfaccia a riga di comando.

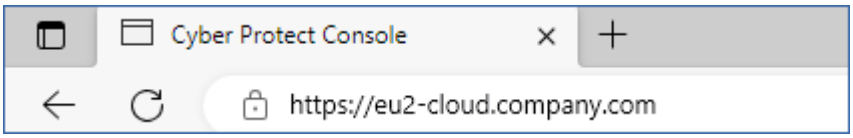
  Nota
  Se si sceglie questo metodo, è necessario un token di registrazione. Per ulteriori informazioni su come generarne uno, fare riferimento a "Generazione del token di registrazione" (pag. 172).

  a. Premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.

  b. Lanciare il seguente comando:

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

  Nota
  Quando si utilizza un token di registrazione, è necessario specificare l'indirizzo esatto del data center. Tale indirizzo corrisponde all'URL visualizzato **dopo aver fatto accesso** alla console di Cyber Protect. Ad esempio, `https://eu2-cloud.company.com`.

  Non utilizzare `https://cloud.company.com` in questo caso.

  c. Premere ALT+F1 per tornare all'interfaccia grafica dell'appliance.

6. [Facoltativo] Nel campo **Nome**, fare clic su **Modifica** per modificare il nome predefinito dell'appliance virtuale, che è **localhost**. Tale nome viene visualizzato nella console di Cyber Protect.
7. [Facoltativo] Nel campo **Orario**, fare clic su **Modifica**, quindi selezionare il fuso orario della propria posizione per fare in modo che le operazioni pianificate vengano eseguite all'ora adeguata.
8. [Facoltativo] [Se è abilitato un server proxy nella rete] Configurare il proxy server.
   a. Premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
   b. Aprire il file **/etc/Acronis/Global.config** in un editor di testo.

© Acronis International GmbH, 2003-2024

c. Eseguire una delle seguenti operazioni:
   - Se le impostazioni del proxy sono state specificate durante l'installazione dell'agente, individuare la sezione seguente:

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

   - Altrimenti, copiare le righe indicate e incollarle nel file fra i tag `<registry name="Global">...</registry>`.

d. Sostituire `ADDRESS` con l'indirizzo IP/nome host del server proxy e `PORT` con il valore decimale del numero della porta.
e. Se il server proxy richiede l'autenticazione, sostituire `LOGIN` e `PASSWORD` con le credenziali del server proxy. In alternativa, eliminare queste righe dal file.
f. Salvare il file.
g. Aprire il file **/opt/acronis/etc/aakore.yaml** in un editor di testo.
h. Individuare la sezione **env** o crearla e aggiungere le righe seguenti:

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

i. Sostituire `proxy_login` e `proxy_password` con le credenziali del server proxy e `proxy_address:port` con l'indirizzo e il numero della porta del server proxy.
j. Eseguire il comando `reboot`.

Nota
Per poter aggiornare un'appliance virtuale distribuita dietro a un proxy, modificare il file dell'appliance `config.yaml` (`/opt/acronis/etc/va-updater/config.yaml`) aggiungendo la riga seguente in fondo al file, inserendo quindi i valori specifici per il proprio ambiente:

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

Per esempio:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Per proteggere le virtual machine nel data center Red Hat Virtualization/oVirt

1. Accedere all'account Cyber Protection.
2. Passare a **Dispositivi** > **oVirt** > <cluster personale> oppure individuare i sistemi in **Dispositivi** >

© Acronis International GmbH, 2003-2024

Tutti i dispositivi.

3. Selezionare i sistemi e applicare i piani di protezione.

Agente per oVirt – ruoli e porte richiesti

Ruoli richiesti

Per il deployment e il funzionamento, Agente per oVirt richiede un account di amministratore al quale siano assegnati i seguenti ruoli.

oVirt/Red Hat Virtualization 4.2 e 4.3/Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4, 4.5

- SuperUser

Porte richieste

L'Agente per oVirt si connette al motore oVirt utilizzando l'URL specificato al momento della configurazione dell'appliance virtuale. In genere il motore degli URL ha il seguente formato: `https://ovirt.azienda.com`. In questo caso vengono utilizzati il protocollo HTTPS e la porta 443.

Le impostazioni non predefinite di oVirt possono richiedere un'altra porta. È possibile individuare la porta corretta analizzando il formato dell'URL. Per esempio:

URL del motore oVirt	Porta	Protocollo
`https://ovirt.azienda.com/`	443	HTTPS
`http://ovirt.azienda.com/`	80	HTTP
`https://ovirt.azienda.com:1234/`	1234	HTTPS

Non sono richieste porte aggiuntive per le operazioni di lettura/scrittura del disco, perché il backup viene eseguito in modalità HotAdd.

© Acronis International GmbH, 2003-2024

Distribuzione dell'Agente per Synology

Prima di iniziare

L'Agente per Synology consente di eseguire il backup di file e cartelle da e verso i dispositivi NAS di Synology. Vengono mantenute le proprietà specifiche del NAS e le autorizzazioni di accesso per condivisioni, cartelle e file.

L'Agente per Synology viene eseguito nel dispositivo NAS. Pertanto, è possibile utilizzare le risorse del dispositivo per le operazioni di elaborazione dei dati esternamente all'host come la replica, la convalida e la pulizia del backup. Per ulteriori informazioni su queste operazioni, fare riferimento a "Elaborazione dei dati al di fuori dell'host" (pag. 201).

Nota
L'Agente per Synology supporta soltanto i dispositivi NAS con processori x86_64. I processori ARM non sono supportati.

È possibile recuperare un backup nella posizione originale o in una nuova nel dispositivo NAS, e su una cartella di rete che sia accessibile da tale dispositivo. È inoltre possibile recuperare i backup nel cloud storage in un dispositivo NAS non originale sul quale sia installato l'Agente per Synology.

La tabella seguente riepiloga le origini e le destinazioni di backup disponibili.

Oggetto del backup	Elementi da sottoporre a backup (Origine di backup)	Dove eseguire il backup (Destinazione di backup)
File/cartelle	Cartella locale*	Archiviazione nel cloud
		Cartella locale*
	Cartella di rete (SMB)**	Cartella di rete (SMB)**
		Cartella NFS

* Incluse unità USB collegate al dispositivo NAS.

Nota
Le cartelle crittografate non sono supportate. Queste cartelle non vengono visualizzate nell'interfaccia utente grafica di Cyber Protection.

** L'utilizzo delle condivisioni di rete esterne come origine o destinazione di backup tramite il protocollo SMB è disponibile solo per gli agenti eseguiti su Synology DiskStation Manager 6.2.3 e versioni successive. È possibile eseguire il backup senza limitazioni dei dati archiviati sul dispositivo NAS di Synology, incluse le condivisioni di rete in hosting.

© Acronis International GmbH, 2003-2024

Limitazioni

- L'Agente per Synology supporta soltanto i dispositivi NAS con processori x86_64. I processori ARM non sono supportati.
- I backup delle condivisioni crittografate vengono ripristinati come non crittografati.
- Le condivisioni di cui è stato eseguito il backup per le quali è abilitata l'opzione di **compressione dei file** vengono ripristinate con l'opzione disabilitata.
- Su un dispositivo NAS Synology è possibile ripristinare solo i backup creati da Agente per Synology.

Download del programma di installazione

Il programma di installazione di Agente per Synology è disponibile come file SPK.

Agente per Synology 7.x

Per scaricare il programma di installazione

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Nell'angolo in alto a destra fare clic su **Aggiungi**.
3. In **Dispositivi NAS**, fare clic su **Synology**.
   Il programma di installazione di installazione viene scaricato nel sistema.

Agente per Synology 6.x

Per scaricare il programma di installazione

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Nell'angolo in alto a destra fare clic su **Aggiungi**.
3. In **Dispositivi NAS**, fare clic su **Synology**.
   Il programma di installazione per Agente per Synology 7.x viene scaricato nel sistema.
   È possibile arrestare il processo di download o ignorare il file scaricato.
4. Fare clic su **Scarica Agente per Synology 6.x**.
   Il programma di installazione per Agente per Synology 6.x viene scaricato nel sistema.

Installazione dell'Agente per Synology

Per installare l'Agente per Synology, eseguire il file SPK in Synology DiskStation Manager.

Nota
L'Agente per Synology supporta soltanto i dispositivi NAS con processori x86_64. I processori ARM non sono supportati.

Agente per Synology 7.x

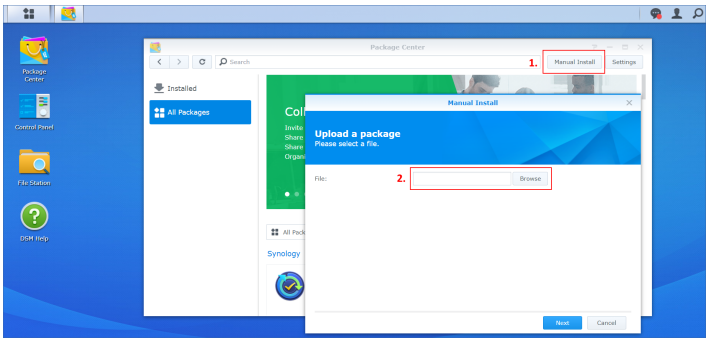
© Acronis International GmbH, 2003-2024

Prerequisiti

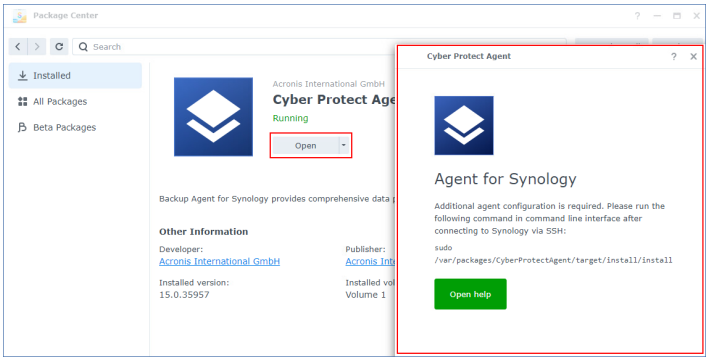
- Il dispositivo NAS esegue DiskStation Manager 7.x.
- L'utente fa parte del gruppo degli **amministratori** nel dispositivo NAS.
- Sul volume NAS nel quale si intende installare l'agente sono presenti almeno 200 MB di spazio libero.
- Nel sistema è disponibile un client SSH. Per l'esempio di questo documento viene utilizzato Putty.

Per installare l'Agente per Synology

1. Accedere a Synology DiskStation Manager.
2. Aprire il **Centro pacchetti**.
3. Fare clic su **Installazione manuale** e quindi su **Sfoglia**.



4. Selezionare il file SPK scaricato dalla console di Cyber Protect, quindi fare clic su **Avanti**.
   Viene visualizzato un avviso indicante l'installazione in corso di un software di terze parti. Il messaggio fa parte della procedura di installazione standard.
5. Per confermare di voler installare il pacchetto, fare clic su **Conferma**.
6. Selezionare il volume sul quale installare l'agente, quindi fare clic su **Avanti**.
7. Controllare le impostazioni, quindi fare clic su **Fine**.
8. Nel **Centro pacchetti** di Synology DiskStation Manager, aprire Cyber Protect Agente per Synology, quindi verificare che sia visibile la schermata seguente.



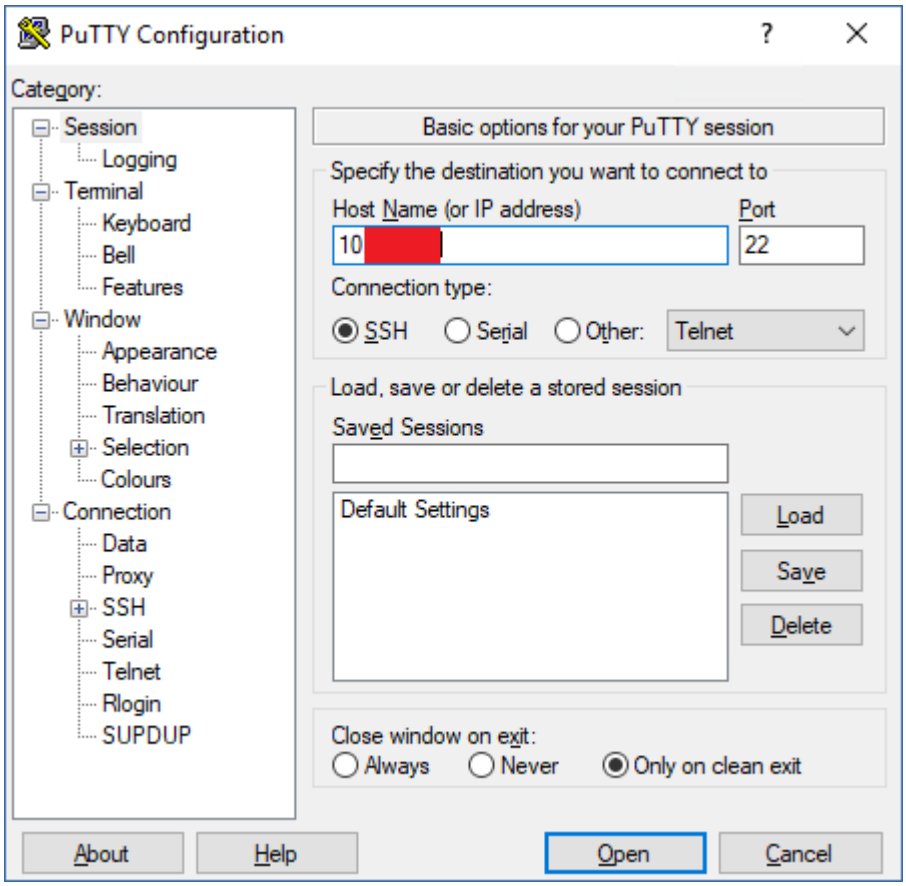
9. Nel **pannello di controllo** di Synology DiskStation Manager, passare a **Terminale e SNMP**, quindi abilitare l'accesso SSH al dispositivo NAS.

© Acronis International GmbH, 2003-2024

10. Eseguire lo script `install` nel dispositivo NAS utilizzando un client SSH (in questo esempio, Putty).

    Lo script abilita l'accesso root a DSM 7.0 o versione successiva, necessario per configurare l'agente.

    a. Avviare Putty, quindi specificare l'indirizzo IP o il nome host del dispositivo NAS Synology.



    b. Fare clic su **Apri**, quindi accedere come amministratore di Synology DSM.

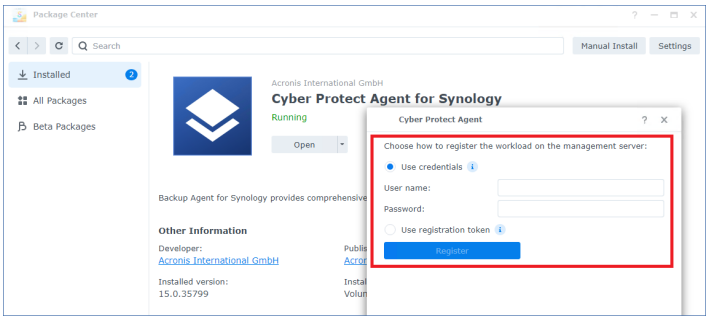
    c. Eseguire il comando seguente:

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

    Dopo l'avvio dello script, attendere 15 secondi per l'inizializzazione dei servizi Cyber Protection.

11. Nel **pannello di controllo** di Synology DiskStation Manager, passare a **Terminale e SNMP**, quindi disabilitare l'accesso SSH al dispositivo NAS. L'accesso SSH non è più necessario.
12. Nel **Centro pacchetti** di Synology DiskStation Manager, aprire Cyber Protect Agente per Synology.
13. Selezionare il metodo di registrazione.

© Acronis International GmbH, 2003-2024



- [Per registrare l'agente utilizzando le credenziali]
  - Nei campi **Nome utente** e **Password**, specificare le credenziali per l'account nel quale l'agente verrà registrato. Non può essere utilizzato l'account di un amministratore Partner.
- [Per registrare l'agente utilizzando un token di registrazione]
  - In **Indirizzo di registrazione**, specificare l'indirizzo esatto del data center. L'indirizzo esatto del data center è l'URL visualizzato dopo aver effettuato l'accesso alla console di Cyber Protect, ad esempio `https://us5-cloud.acronis.com`.

    Nota
    Non utilizzare un formato URL senza l'indirizzo del data center. Ad esempio, non utilizzare `https://cloud.acronis.com`.

  - Nel campo **Token**, specificare il token di registrazione.

    Per ulteriori informazioni su come generare un token di registrazione, consultare "Generazione del token di registrazione" (pag. 172).

14. Fare clic su **Registra**.

Agente per Synology 6.x

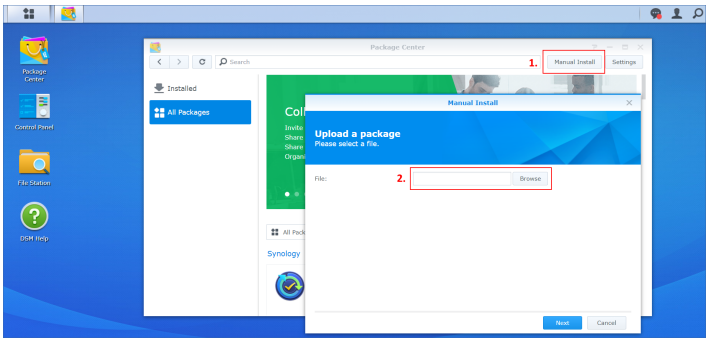
Prerequisiti

- Il dispositivo NAS esegue DiskStation Manager 6.2.x.
- L'utente fa parte del gruppo degli **amministratori** nel dispositivo NAS.
- Sul volume NAS nel quale si intende installare l'agente sono presenti almeno 200 MB di spazio libero.

Per installare l'Agente per Synology

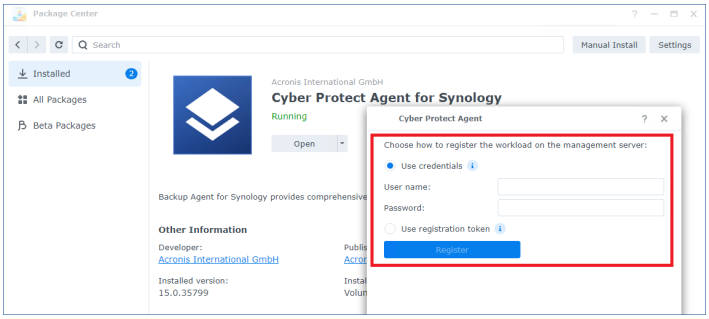
1. Accedere a Synology DiskStation Manager.
2. Aprire il **Centro pacchetti**.
3. Fare clic su **Installazione manuale** e quindi su **Sfoglia**.

© Acronis International GmbH, 2003-2024



4. Selezionare il file SPK scaricato dalla console di Cyber Protect, quindi fare clic su **Avanti**.

   Viene visualizzato un avviso indicante l'installazione in corso di un pacchetto senza firma digitale. Il messaggio fa parte della procedura di installazione standard.
5. Per confermare di voler installare il pacchetto, fare clic su **Sì**.
6. Selezionare il volume sul quale installare l'agente, quindi fare clic su **Avanti**.
7. Controllare le impostazioni, quindi fare clic su **Applica**.
8. Nel **Centro pacchetti** di Synology DiskStation Manager, aprire Cyber Protect Agente per Synology.
9. Selezionare il metodo di registrazione.



   - [Per registrare l'agente utilizzando le credenziali]
     - Nei campi **Nome utente** e **Password**, specificare le credenziali per l'account nel quale l'agente verrà registrato. Non può essere utilizzato l'account di un amministratore Partner.
   - [Per registrare l'agente utilizzando un token di registrazione]
     - In **Indirizzo di registrazione**, specificare l'indirizzo esatto del data center. L'indirizzo esatto del data center è l'URL visualizzato dopo aver effettuato l'accesso alla console di Cyber Protect, ad esempio `https://us5-cloud.acronis.com`.

       Nota
       Non utilizzare un formato URL senza l'indirizzo del data center. Ad esempio, non utilizzare `https://cloud.acronis.com`.

     - Nel campo **Token**, specificare il token di registrazione.

       Per ulteriori informazioni su come generare un token di registrazione, consultare "Generazione del token di registrazione" (pag. 172).
10. Fare clic su **Registra**.

© Acronis International GmbH, 2003-2024

Al termine della registrazione, il dispositivo NAS Synology viene visualizzato nella console di Cyber Protect, nella scheda **Dispositivi** > **Dispositivi NAS**.

Per eseguire il backup dei dati sul dispositivo NAS, applicare un piano di protezione.

Aggiornamento di Agente per Synology

È possibile aggiornare Agente per Synology 6.x a una versione successiva. In modo analogo, è possibile aggiornare anche Agente per Synology 7.x a una versione successiva.

Per aggiornare l'agente, eseguire la versione più recente del programma di installazione in Synology DiskStation Manager. La registrazione originale dell'agente, le relative impostazioni e i piani applicati ai workload protetti vengono conservati.

Nota
Non è possibile aggiornare l'agente dalla console di Cyber Protect.

L'aggiornamento di Agente per Synology 6.x ad Agente per Synology 7.x è possibile solo se si disinstalla l'agente obsoleto e si installa quello più recente. In questo caso, tutti i piani di protezione vengono revocati e devono essere riapplicati manualmente.

Agente per Synology 7.x

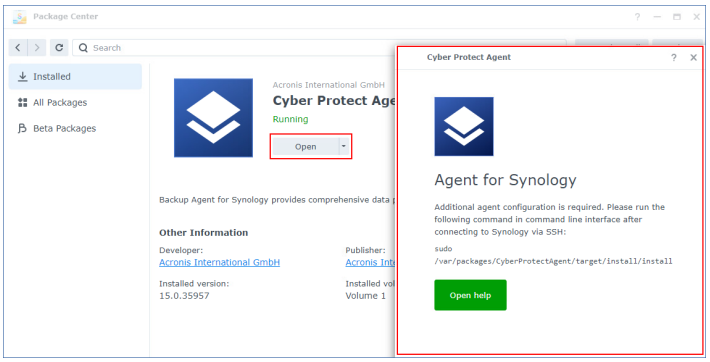
Prerequisiti

- L'utente fa parte del gruppo degli **amministratori** nel dispositivo NAS.
- Sul volume NAS nel quale si intende installare l'agente sono presenti almeno 200 MB di spazio libero.
- Nel sistema è disponibile un client SSH. Per l'esempio di questo documento viene utilizzato Putty.

Per aggiornare l'Agente per Synology

1. In DiskStation Manager, aprire il **Centro pacchetti**.
2. Fare clic su **Installazione manuale** e quindi su **Sfoglia**.
3. Selezionare il file SPK più recente di Agente per Synology 7.x scaricato dalla console di Cyber Protect, quindi fare clic su **Avanti**.
   Viene visualizzato un avviso indicante l'installazione in corso di un software di terze parti. Il messaggio fa parte della procedura di installazione standard.
4. Per confermare di voler installare il pacchetto, fare clic su **Conferma**.
5. Controllare le impostazioni, quindi fare clic su **Fine**.
6. Nel **Centro pacchetti** di Synology DiskStation Manager, aprire Cyber Protect Agente per Synology, quindi verificare che sia visibile la schermata seguente.

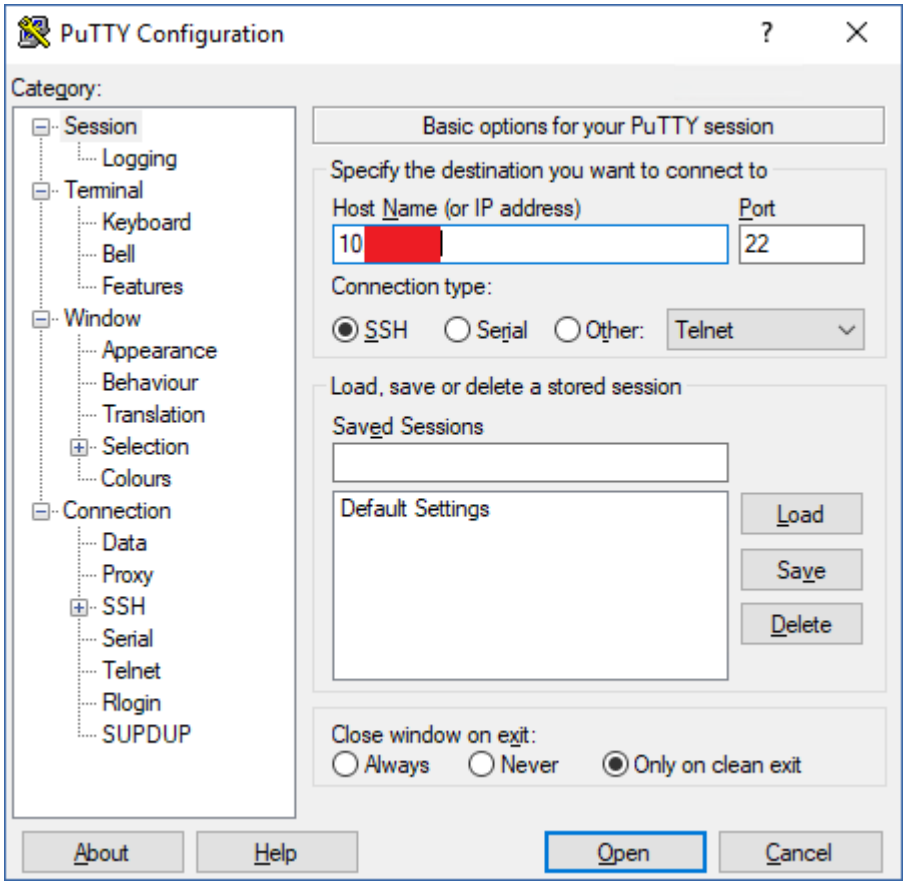
© Acronis International GmbH, 2003-2024



7. Nel **pannello di controllo** di Synology DiskStation Manager, passare a **Terminale e SNMP**, quindi abilitare l'accesso SSH al dispositivo NAS.
8. Eseguire lo script `install` nel dispositivo NAS utilizzando un client SSH (in questo esempio, Putty).

   Lo script abilita l'accesso root a DSM 7.0 o versione successiva, necessario per configurare l'agente.

   a. Avviare Putty, quindi specificare l'indirizzo IP o il nome host del dispositivo NAS Synology.



   b. Fare clic su **Apri**, quindi accedere come amministratore di Synology DSM.

   c. Eseguire il comando seguente:

```
sudo /var/packages/CyberProtectAgent/target/install/install
```


© Acronis International GmbH, 2003-2024

9. Nel **pannello di controllo** di Synology DiskStation Manager, passare a **Terminale e SNMP**, quindi disabilitare l'accesso SSH al dispositivo NAS. L'accesso SSH non è più necessario.

Agente per Synology 6.x

Prerequisiti

- L'utente fa parte del gruppo degli **amministratori** nel dispositivo NAS.
- Sul volume NAS nel quale si intende installare l'agente sono presenti almeno 200 MB di spazio libero.

Per aggiornare l'Agente per Synology

1. In DiskStation Manager, aprire il **Centro pacchetti**.
2. Fare clic su **Installazione manuale** e quindi su **Sfoglia**.
3. Selezionare il file SPK più recente di Agente per Synology 6.x scaricato dalla console di Cyber Protect, quindi fare clic su **Avanti**.
   Viene visualizzato un avviso indicante l'installazione in corso di un pacchetto senza firma digitale. Il messaggio fa parte della procedura di installazione standard.
4. Per confermare di voler installare il pacchetto, fare clic su **Sì**.
5. Controllare le impostazioni, quindi fare clic su **Applica**.

Distribuzione di agenti tramite i Criteri di gruppo

È possibile installare (o distribuire) a livello centralizzato l'Agente per Windows su sistemi membri di un dominio di Active Directory tramite i Criteri di gruppo di Windows.

In questa sezione verrà illustrata l'impostazione di un oggetto Criteri di gruppo per la distribuzione di agenti nei sistemi in un intero dominio o in un'unità organizzativa di un dominio.

Ogni volta che un sistema accede al dominio, l'oggetto Criteri di gruppo derivante assicurerà che l'agente sia installato e registrato.

Prerequisiti

- Dominio di Active Directory con un controller di dominio che esegue Microsoft Windows Server 2003 o versioni successive.
- È necessario essere membro del gruppo **Amministratori di dominio** in questo dominio.
- Il programma di installazione **Tutti gli agenti per Windows** sia stato scaricato.
  Per scaricare il programma di installazione, nella console di Cyber Protect, fare clic sull'icona dell'account nell'angolo in alto a destra e quindi su **Download**. Il collegamento per il download è disponibile nel pannello **Aggiungi dispositivi**.

Per distribuire gli agenti tramite i Criteri di gruppo

© Acronis International GmbH, 2003-2024

1. Generare un token di registrazione come descritto in "Generazione del token di registrazione" (pag. 172).
2. Creare il file .mst, il file .msi e i file .cab come descritto in "Creazione del file di trasformazione ed estrazione dei pacchetti di installazione" (pag. 175).
3. Impostare l'oggetto Criteri di gruppo come descritto in "Impostazione dell'oggetto Criteri di gruppo" (pag. 176).

Generazione del token di registrazione

Un token di registrazione trasferisce l'identità di un utente al programma di installazione dell'agente, senza archiviare le credenziali utente della console di Cyber Protect. In questo modo gli utenti possono registrare qualsiasi numero di sistemi con il proprio account, oppure applicare piani di protezione ai propri workload senza dover accedere.

Nota
I piani di protezione non vengono applicati automaticamente durante la registrazione del sistema. L'applicazione di un piano di protezione è un'attività distinta.

Per ragioni di sicurezza, i token hanno una durata limitata, ma regolabile dall'utente. Il periodo di durata predefinito è di 3 giorni.

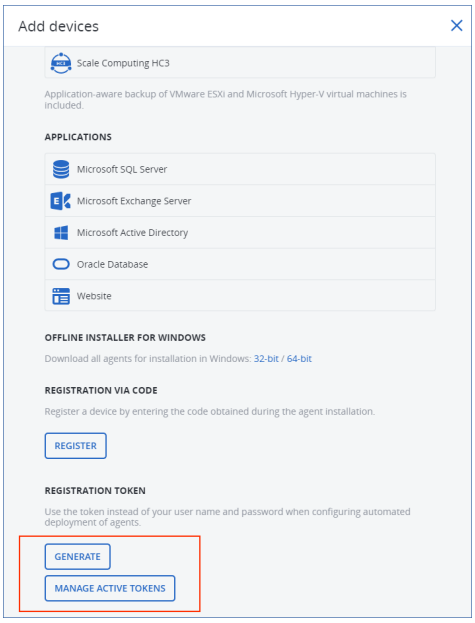
Gli utenti possono generare i token di registrazione solo per i propri account. Gli amministratori possono generare token di registrazione per tutti gli account utente nel tenant che gestiscono.

Per generare un token di registrazione

Come utente

1. Accedere alla console di Cyber Protect.
2. Fare clic su **Dispositivi** > **Tutti i dispositivi** > **Aggiungi**.
   A sinistra viene aperto il pannello **Aggiungi dispositivi**.
3. Scorrere verso il basso fino a **Token di registrazione** e quindi fare clic su **Genera**.

© Acronis International GmbH, 2003-2024



4. Specificare la durata del token.
5. Fare clic su **Genera token**.
6. Fare clic su **Copia** per copiare il token negli appunti del dispositivo, o scrivere il token down manualmente.

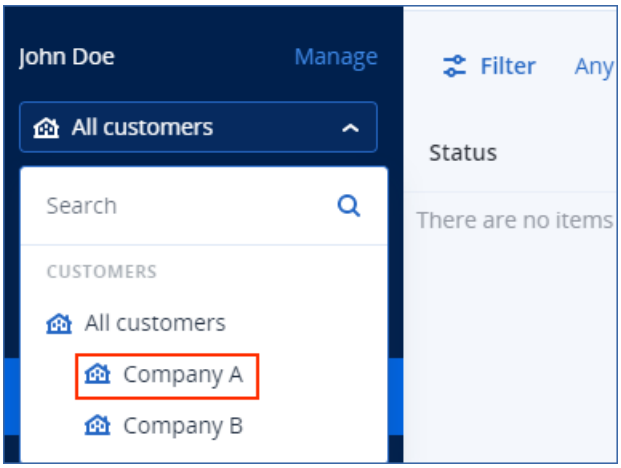
Come amministratore

1. Accedere alla console di Cyber Protect come amministratore.

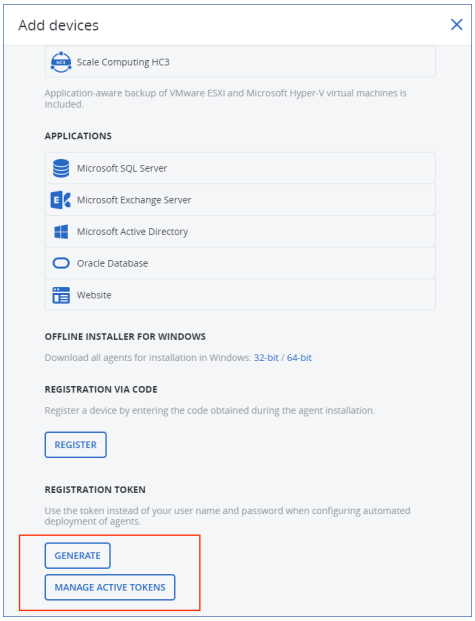
   Se si è già eseguito l'accesso al portale di gestione, aprire la console di Cyber Protect passando a **Monitoraggio** > **Utilizzo**, quindi nella scheda **Protezione**, fare clic su **Gestisci servizio**.

   [Per gli amministratori del partner che gestiscono i tenant cliente] Nella console di Cyber Protect, selezionare il tenant con l'utente per il quale generare il token. Non è possibile generare un token al livello **Tutti i clienti**.

© Acronis International GmbH, 2003-2024



2. In **Dispositivi**, fare clic su **Tutti i dispositivi** > **Aggiungi**.
   A sinistra viene aperto il pannello **Aggiungi dispositivi**.
3. Scorrere verso il basso fino a **Token di registrazione** e quindi fare clic su **Genera**.



4. Specificare la durata del token.
5. Selezionare l'utente per il quale generare il token.

   Nota
   Quando si utilizzano i token, i workload verranno registrati nell'account utente qui selezionato.

6. [Facoltativo] Per abilitare l'utente del token all'applicazione e alla revoca di un piano di protezione per i workload aggiunti, selezionare il piano dall'elenco a discesa.
   È necessario eseguire uno script che applica o revoca un piano di protezione ai workload aggiunti. Fare riferimento a questo articolo della Knowledge Base per ulteriori dettagli.
7. Fare clic su **Genera token**.
8. Fare clic su **Copia** per copiare il token negli appunti del dispositivo, o scrivere il token down manualmente.

© Acronis International GmbH, 2003-2024

Per visualizzare o eliminare i token di registrazione

1. Accedere alla console di Cyber Protect.
2. Fare clic su **Dispositivi** > **Tutti i dispositivi** > **Aggiungi**.
3. Scorrere verso il basso fino a **Token di registrazione** e quindi fare clic su **Gestisci token attivi**.
   A sinistra si apre un elenco con i token attivi generati per il tenant.

   Nota
   Per ragioni di sicurezza, nella colonna **Token** vengono visualizzati solo i primi due caratteri del valore del token.

4. [Per eliminare un token] Selezionare il token, quindi fare clic su **Elimina**.

Creazione del file di trasformazione ed estrazione dei pacchetti di installazione

Per distribuire gli agenti di protezione tramite Criteri di gruppo di Windows, sono necessari un file di trasformazione (.mst) e i pacchetti di installazione (file .msi e .cab).

Nota
La procedura seguente si avvale dell'opzione di registrazione predefinita, ovvero la registrazione con token. Per informazioni su come generare un token di registrazione, fare riferimento a "Generazione del token di registrazione" (pag. 172).

Per creare il file di trasformazione .mst ed estrarre i pacchetti di installazione (file .msi e .cab)

1. Accedere come amministratore su qualsiasi sistema del dominio di Active Directory.
2. Creare una cartella condivisa che conterrà i pacchetti di installazione. Assicurarsi che gli utenti del dominio possano accedere alla cartella condivisa, ad esempio, lasciando le impostazioni di condivisione predefinite per **Tutti**.
3. Eseguire il programma di installazione dell'agente.
4. Fare clic su **Creare file .mst e .msi per l'installazione automatica**.
5. In **Cosa installare**, scegliere i componenti da includere nell'installazione, quindi fare clic su **Fine**.
6. In **Impostazioni di registrazione**, fare clic su **Specificare**, inserire un token di registrazione, quindi fare clic su **Fine**.
   È possibile cambiare il metodo di registrazione da **Utilizza il token di registrazione** (impostazione predefinita) a **Utilizza le credenziali** o **Ignora la registrazione**. L'opzione **Ignora la registrazione** presume che l'utente registrerà il workload manualmente in un secondo momento.
7. Rivedere o modificare le impostazioni di installazione che verranno aggiunte al file .mst, quindi fare clic su **Procedi**.

© Acronis International GmbH, 2003-2024

8. In **Salvare i file in**, specificare il percorso della cartella condivisa creata.
9. Fare clic su **Genera**.

   Il file .mst, il file .msi e i file .cab vengono creati e copiati nella cartella condivisa specificata dall'utente.

   Il passaggio successivo prevede la configurazione dell'oggetto Criteri di gruppo di Windows. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Impostazione dell'oggetto Criteri di gruppo" (pag. 176).

Impostazione dell'oggetto Criteri di gruppo

In questa procedura vengono utilizzati i pacchetti di installazione creati in "Creazione del file di trasformazione ed estrazione dei pacchetti di installazione" (pag. 175) per configurare un oggetto Criteri di gruppo. L'oggetto Criteri di gruppo distribuisce gli agenti nei sistemi del dominio.

Per configurare l'oggetto Criteri di gruppo

1. Accedere al controller di dominio come amministratore di dominio.
   Se il dominio dispone di più controller di dominio, accedere a ciascuno di essi come amministratore di dominio.
2. [Se gli agenti vengono distribuiti in un'unità organizzativa] Accertarsi che l'unità nella quale si intende distribuire gli agenti esista in questo dominio.
3. Nel menu **Start** di Windows, scegliere **Strumenti di amministrazione** e fare clic su **Gestione Criteri di gruppo** (o su **Utenti e computer di Active Directory** in Windows Server 2003).
4. [Per Windows Server 2008 o versioni successive] Fare clic con il pulsante destro del mouse sul nome del dominio o dell'unità organizzativa, quindi selezionare **Crea un oggetto Criteri di gruppo in questo dominio e crea qui un collegamento**.
5. [Per Windows Server 2003] Fare clic con il pulsante destro del mouse sul nome del dominio o dell'unità organizzativa, quindi fare clic su **Proprietà**. Nella finestra di dialogo, fare clic sulla scheda **Criteri di gruppo** e quindi su **Nuovo**.
6. Nominare il nuovo oggetto Criteri di gruppo **Agente per Windows.**
7. Aprire l'oggetto Criteri di gruppo **Agente per Windows** per la modifica:
   - [In Windows Server 2008 o versioni successive] In **Oggetti Criteri di gruppo**, fare clic con il pulsante destro del mouse sull'oggetto Criteri di gruppo, quindi su **Modifica**.
   - [In Windows Server 2003] Selezionare l'oggetto Criteri di gruppo e fare clic su **Modifica**.
8. Nello snap-in dell'editor dell'oggetto Criteri di gruppo, espandere **Configurazione computer**.
9. [In Windows Server 2012 o versioni successive] Espandere **Criteri** > **Impostazioni del software**.
10. [In Windows Server 2003 e Windows Server 2008] Espandere **Impostazioni del software**.
11. Fare clic con il pulsante destro del mouse su **Installazione software**, selezionare **Nuovo**, quindi fare clic su **Pacchetto**.
12. Selezionare il pacchetto di installazione .msi dell'agente nella cartella condivisa creata, quindi fare clic su **Apri**.

© Acronis International GmbH, 2003-2024

13. Nella finestra di dialogo **Distribuisci software** fare clic su **Avanzate** e quindi su **OK**.
14. Nella scheda **Modifiche**, fare clic su **Aggiungi** e selezionare il file di trasformazione .mst nella cartella condivisa creata.
15. Fare clic su **OK** per chiudere la finestra di dialogo **Distribuisci software.**

Connessioni SSH a un'appliance virtuale

Utilizzare una connessione Secure Socket Shell (SSH) quando si accede da remoto a un'appliance virtuale per attività di manutenzione.

Avvio del daemon Secure Shell

Per consentire le connessioni SSH a un'appliance virtuale, avviare il daemon Secure Shell (sshd) nell'appliance.

Per avviare il daemon Secure Shell

1. Nel software hypervisor, aprire la console dell'appliance virtuale.
2. Nell'interfaccia utente grafica dell'appliance, premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
3. Lanciare il seguente comando:

   ```
   /bin/sshd
   ```

4. [Solo durante la prima connessione all'appliance] Impostare la password per l'utente `root`.

   Per ulteriori informazioni su come impostare la password, consultare "Impostazione della password radice su un'appliance virtuale" (pag. 177).

Nota
Si consiglia di arrestare il daemon Secure Shell quando la connessione SSH non è in uso.

Impostazione della password radice su un'appliance virtuale

Prima di stabilire per la prima volta una connessione SSH con un'appliance virtuale, è necessario impostare la password radice nell'appliance.

Per impostare la password radice

1. Nel software hypervisor, aprire la console dell'appliance virtuale.
2. Nell'interfaccia utente grafica dell'appliance, premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
3. Lanciare il seguente comando:

   ```
   passwd
   ```

4. Specificare una password, quindi premere Invio.

© Acronis International GmbH, 2003-2024

La password deve contenere almeno nove caratteri e avere un punteggio di complessità pari a tre o superiore. Il punteggio di complessità viene calcolato automaticamente. Per ottenere un punteggio più alto, utilizzare una combinazione di simboli speciali, caratteri maiuscoli e minuscoli e numeri.

5. Confermare la password, quindi premere Invio.

Accesso a un'appliance virtuale tramite un client SSH

Prerequisiti

- Sul sistema remoto deve essere disponibile un client SSH. La procedura seguente utilizza come esempio il client WinSCP. È possibile utilizzare qualsiasi client SSH, adattando i passaggi di conseguenza.
- Nell'appliance virtuale deve essere avviato il daemon Secure Shell (sshd). Per ulteriori informazioni, consultare "Avvio del daemon Secure Shell" (pag. 177).

Per accedere a un'appliance virtuale tramite WinSCP

1. Sul sistema remoto, aprire WinSCP.
2. Fare clic su **Sessione** > **Nuova sessione**.
3. In **Protocollo file**, selezionare **SCP**.
4. In **Nome host**, specificare l'indirizzo IP dell'appliance virtuale.
5. In **Nome utente** e **Password**, specificare la `root` e la password per l'utente `root`.
6. Fare clic su **Accedi**.

Viene visualizzato un elenco di tutte le directory nell'appliance virtuale.

Aggiornamento di agenti

È possibile aggiornare tutti gli agenti manualmente tramite la console di Cyber Protect o scaricando ed eseguendo il file di installazione.

È possibile configurare gli aggiornamenti automatici per i seguenti agenti:

- Agente per Windows
- Agente per Linux
- Agente per Mac
- Cyber Files Cloud Agente per File Sync & Share

Nella posizione seguente sono necessari 4,2 GB di spazio libero per aggiornare un agente automaticamente o manualmente tramite la console di Cyber Protect:

- Per Linux: la directory radice
- Per Windows - il volume in cui è installato l'agente

© Acronis International GmbH, 2003-2024

Nella posizione seguente sono necessari 5 GB di spazio libero per aggiornare un agente in macOS: nella directory radice.

Nota
[Per tutti gli agenti forniti in forma di appliance virtuale, incluso Agente per VMware, Agente per Scale Computing, Agente per Virtuozzo Hybrid Infrastructure, Agente per RHV (oVirt)]

Per eseguire un aggiornamento automatico o manuale di un'appliance virtuale posizionata dietro un proxy, è necessario configurare il server proxy in ogni appliance come segue.

Nel file `/opt/acronis/etc/va-updater/config.yaml`, aggiungere la riga seguente alla fine del file e inserire i valori specifici dell'ambiente corrente:

```
httpProxy: http://proxy_login:proxy_password@indirizzo_proxy:porta
```

Aggiornamento manuale degli agenti

È possibile aggiornare gli agenti tramite la console di Cyber Protect o scaricando ed eseguendo il file di installazione.

Le appliance virtuali con le seguenti versioni possono essere aggiornate solo utilizzando la console di Cyber Protect:

- Agente per VMware (appliance virtuale): versione 12.5.23094 e successive.
- Agente per Virtuozzo Hybrid Infrastructure (appliance virtuale): versione 12.5.23094 e successive.

Gli agenti con le seguenti versioni possono essere aggiornati anche con la console di Cyber Protect:

- Agente per Windows, Agente per VMware (Windows), Agente per Hyper-V: versione 12.5.21670 e successive.
- Agente per Linux: versione 12.5.23094 e successive.
- Altri agenti: versione 12.5.23094 e successive.

Per trovare la versione dell'agente, nella console di Cyber Protect selezionare il sistema e fare clic su **Dettagli**.

Per aggiornare le versioni precedenti di tali agenti, scaricare e installare manualmente la versione più recenti. Per trovare i collegamenti per il download, fare clic su **Tutti i dispositivi** > **Aggiungi**.

Prerequisiti

Sui sistemi Windows, le funzionalità di Cyber Protect richiedono Microsoft Visual C++ 2017 Redistributable. Verificare che sia già installato nel sistema o installarlo prima di procedere con l'aggiornamento dell'agente. Dopo l'installazione, potrebbe essere necessario un riavvio. Il pacchetto Microsoft Visual C++ Redistributable è disponibile sul sito web di Microsoft all'indirizzo https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Per aggiornare un agente utilizzando la console di Cyber Protect

© Acronis International GmbH, 2003-2024

1. Fare clic su **Impostazioni** > **Agenti**.

   Viene visualizzato l'elenco dei sistemi. I sistemi con versioni di agenti obsolete sono contrassegnati da un punto esclamativo arancione.
2. Selezionare i sistemi su cui si desidera aggiornare gli agenti. I sistemi devono essere online.
3. Fare clic su **Aggiorna agente**.

Nota
Durante l'aggiornamento, qualsiasi backup in corso non avrà esito positivo.

Per aggiornare l'Agente per VMware (appliance virtuale) con versioni precedenti alla 12.5.23094

1. Fare clic su **Impostazioni** > **Agenti** > l'agente che si desidera aggiornare > **Dettagli**, e quindi controllare la sezione **Macchine virtuali assegnate**. È necessario reinserire queste impostazioni dopo l'aggiornamento.
   a. Annotare la condizione dell'opzione **Assegnazione automatica**.
   b. Per individuare quali macchine virtuali sono state assegnate manualmente all'agente, fare clic sul collegamento **Assegnate:**. Il software visualizza l'elenco delle macchine virtuali assegnate. Annotare le macchine nelle quali è presente `(M)` dopo il nome dell'agente nella colonna **Agente**.
2. Rimuovere l'Agente per VMware (appliance virtuale) come descritto in "Disinstallazione di agenti". Nel passaggio 5 eliminare l'agente da **Impostazioni** > **Agenti**, anche se si prevede di installare nuovamente l'agente.
3. Distribuire l'Agente per VMware (appliance virtuale) come descritto in "Distribuzione del modello OVF".
4. Configurare l'Agente per VMware (appliance virtuale) come descritto in "Configurazione dell'appliance virtuale".

   Per ricostruire lo storage connesso in locale, nel passaggio 7 attenersi alla procedura seguente:
   a. Aggiungere il disco contenente lo storage locale all'appliance virtuale.
   b. Fare clic su **Aggiorna** > **Crea archivio** > **Monta**.
   c. Vengono visualizzate la **Lettera** e l'**Etichetta** originali del disco. Non modificarle.
   d. Fare clic su **OK**.
5. Fare clic su **Impostazioni** > **Agenti** > l'agente che si desidera aggiornare > **Dettagli**, e quindi reinserire le impostazioni di cui si è preso nota nel passaggio 1. Se alcune macchine virtuali sono state assegnate manualmente all'agente, riassegnarle come descritto in "Associazione delle macchine virtuali".

   Dopo aver completato la configurazione dell'agente, i piani di protezione applicati al vecchio agente vengono riapplicati automaticamente al nuovo agente.
6. Per essere nuovamente immessi, i piani per i quali sono stati abilitati i backup compatibili con l'applicazione richiedono le credenziali del sistema operativo guest. Modificare tali piani e immettere nuovamente le credenziali.

© Acronis International GmbH, 2003-2024

7. I piani che eseguono il backup della configurazione ESXi richiedono la password radice per essere nuovamente immessi. Modificare tali piani e immettere nuovamente la password.

Per aggiornare le definizioni di Cyber Protection in un sistema

1. Fare clic su **Impostazioni** > **Agenti**.
2. Selezionare il sistema sul quale aggiornare le definizioni di Cyber Protection e fare clic su **Aggiorna definizioni**. Il sistema deve essere online.

Per assegnare il Ruolo di chi esegue l'aggiornamento a un agente

1. Fare clic su **Impostazioni** > **Agenti**.
2. Selezionare il sistema al quale assegnare il Ruolo di chi esegue l'aggiornamento, fare clic su **Dettagli**, quindi nella sezione **Definizioni di Cyber Protection** abilitare la casella **Utilizzare questo agente per scaricare e distribuire patch e aggiornamenti**.

   Nota
   Un agente con il Ruolo di chi esegue l'aggiornamento può scaricare ed distribuire le patch solo per i prodotti Windows di terze parti. La distribuzione delle patch per i prodotti Microsoft non è supportata dall'agente del programma di aggiornamento.

Per cancellare i dati della cache in un agente

1. Fare clic su **Impostazioni** > **Agenti**.
2. Selezionare il sistema di cui cancellare i dati della cache (file di aggiornamento e dati di gestione delle patch) e fare clic su **Cancella cache**.

Aggiornamento automatico degli agenti

Per semplificare la gestione di più workload, è possibile configurare gli aggiornamenti automatici di Agente per Windows, Agente per Linux e Agente per Mac. Gli aggiornamenti automatici sono disponibili per gli agenti nella versione 15.0.26986 (rilasciata a maggio 2021) e versioni successive. Gli agenti meno recenti devono essere prima aggiornati manualmente alla versione più recente.

Gli aggiornamenti automatici sono supportati sui sistemi che eseguono i sistemi operativi seguenti:

- Windows XP SP 3 e versioni successive
- Red Hat Enterprise Linux 6 e versioni successive, CentOS 6 e versioni successive
- OS X 10.9 Mavericks e versioni successive

Le impostazioni degli aggiornamenti automatici vengono preconfigurate a livello di data center. Tali impostazioni possono essere personalizzate dall'amministratore della società, sia per tutti i sistemi aziendali o di unità che per i singoli sistemi. Se non vengono applicate impostazioni personalizzate, vengono utilizzate le impostazioni del livello superiore, nell'ordine seguente:

1. Data center Cyber Protection
2. Azienda (tenant cliente)

© Acronis International GmbH, 2003-2024

3. Unità
4. Macchina

Ad esempio, un amministratore di unità può configurare impostazioni di aggiornamento automatico personalizzate per tutti i sistemi dell'unità; tali impostazioni potrebbero differire da quelle applicate ai sistemi a livello aziendale. L'amministratore può inoltre configurare diverse impostazioni per uno o più sistemi singoli dell'unità, ai quali non verranno applicate né le impostazioni dell'unità né quelle aziendali.

Dopo aver abilitato gli aggiornamenti automatici, sarà possibile configurare le opzioni seguenti:

- **Canale di aggiornamento**
  Questa impostazione definisce quale versione degli agenti verrà utilizzata, se quella più aggiornata o quella più recente dalla release precedente.
- **Intervallo di manutenzione**
  L'intervallo di manutenzione definisce gli orari in cui è possibile installare gli aggiornamenti. Se l'impostazione è disabitata, gli aggiornamenti possono essere eseguiti in qualsiasi momento.
  Anche se l'intervallo di manutenzione è abilitato, gli aggiornamenti non verranno installati se l'agente sta eseguendo una qualsiasi delle operazioni seguenti:
  - Backup
  - Ripristino
  - Replica di backup
  - Replica della virtual machine
  - Prova di una copia
  - Esecuzione di una virtual machine da un backup (finalizzazione inclusa)
  - Failover di disaster recovery
  - Failback di disaster recovery
  - Esecuzione di uno script (per la funzionalità di Cyber Scripting)
  - Installazione patch
  - Backup di configurazioni ESXi

Per personalizzare le impostazioni di aggiornamento automatico

1. Nella console di Cyber Protect, passare a **Impostazioni** > **Agenti**.
2. Selezionare l'ambito delle impostazioni:
   - Per modificare le impostazioni per tutti i sistemi, fare clic su **Modifica impostazioni di aggiornamento predefinite dell'agente**.
   - Per modificare le impostazioni di sistemi specifici, selezionare i sistemi desiderati e fare clic su **Impostazioni di aggiornamento dell'Agente**.
3. Modificare le impostazioni in base alle necessità e quindi fare clic su **Applica**.

Per rimuovere le impostazioni di aggiornamento automatico

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Impostazioni** > **Agenti**.
2. Selezionare l'ambito delle impostazioni:
   - Per rimuovere le impostazioni personalizzate per tutti i sistemi, fare clic su **Modifica impostazioni di aggiornamento predefinite dell'agente**.
   - Per rimuovere le impostazioni personalizzate per sistemi specifici, selezionare i sistemi desiderati e fare clic su **Impostazioni di aggiornamento dell'Agente**.
3. Fare clic su **Ripristina impostazioni predefinite**, quindi fare clic su **Applica**.

Per controllare lo stato dell'aggiornamento automatico

1. Nella console di Cyber Protect, passare a **Impostazioni** > **Agenti**.
2. Fare clic sull'icona ingranaggio nell'angolo in alto a destra della tabella e verificare che la casella di controllo **Aggiornamento automatico** sia selezionata.
3. Verificare lo stato che è mostrato nella colonna **Aggiornamento automatico**.

Aggiornamento degli agenti sui workload protetti da BitLocker

Gli aggiornamenti dell'agente che introducono modifiche a Startup Recovery Manager interferiscono con BitLocker sui workload in cui sono abilitati sia BitLocker che Startup Recovery Manager. In questo caso, dopo aver effettuato il riavvio, è necessaria la chiave di ripristino di BitLocker. Per attenuare questo problema, sospendere o disattivare BitLocker prima di aggiornare l'agente.

Versioni dell'agente interessate:

- 23.12.36943, rilasciato a dicembre 2023

È anche possibile verificare se un aggiornamento introduce modifiche a Startup Recovery Manager nelle note di rilascio dell'agente di protezione.

Per aggiornare l'agente su un workload con BitLocker e su cui è abilitato Startup Recovery Manager

1. Sul workload su cui si desidera aggiornare l'agente, sospendere o disattivare BitLocker.
2. Aggiornare l'agente.
3. Riavviare il workload.
4. Abilitare BitLocker.

Impedire la disinstallazione o la modifica non autorizzate degli agenti

È possibile proteggere l'Agente per Windows da disinstallazione o modifica non autorizzate abilitando l'impostazione **Protezione con password** in un piano di protezione. Questa

© Acronis International GmbH, 2003-2024

impostazione è disponibile soltanto se l'impostazione **Auto-protezione** è attivata.

Per abilitare la protezione con password

1. In un piano di protezione, espandere il modulo **Protezione antivirus e anti-malware** (modulo **Active Protection** nelle edizioni Cyber Backup).
2. Fare clic su **Auto-protezione** e verificare che l'interruttore **Auto-protezione** sia abilitato.
3. Abilitare l'interruttore **Protezione con password**.
4. Nella finestra visualizzata, copiare la password da disinstallare o modificare i componenti dell'Agente per Windows protetto.
   Questa password è univoca e non sarà possibile ripristinarla dopo aver chiuso la finestra. Se la password viene persa o dimenticata, è possibile modificare il piano di protezione e creare una nuova password.
5. Fare clic su **Chiudi**.
6. Nel riquadro **Auto-protezione**, fare clic su **Fine**.
7. Salvare il piano di protezione.

La protezione con password verrà abilitata per i sistemi ai quali è applicato questo piano di protezione. La protezione con password è disponibile solo per l'Agente per Windows versione *15.0.25851* o successive. I sistemi devono essere online.

È possibile applicare un piano di protezione con Protezione con password abilitata in un sistema che esegue macOS, ma non verrà fornita alcuna protezione. Non è possibile applicare il piano di protezione in un sistema che esegue Linux.

Inoltre, non è possibile applicare più di un piano di protezione con Protezione con password abilitata allo stesso sistema Windows. Per approfondire come risolvere un possibile conflitto, fare riferimento a Risoluzione dei conflitti tra piani.

Per modificare la password di un piano di protezione esistente

1. Nel piano di protezione, espandere il modulo **Protezione antivirus e anti-malware** (modulo **Active Protection** nelle edizioni Cyber Backup).
2. Fare clic su **Auto-protezione**.
3. Fare clic su **Crea nuova password**.
4. Nella finestra visualizzata, copiare la password da disinstallare o modificare i componenti dell'Agente per Windows protetto.
   Questa password è univoca e non sarà possibile ripristinarla dopo aver chiuso la finestra. Se la password viene persa o dimenticata, è possibile modificare il piano di protezione e creare una nuova password.
5. Fare clic su **Chiudi**.
6. Nel riquadro **Auto-protezione**, fare clic su **Fine**.
7. Salvare il piano di protezione.

© Acronis International GmbH, 2003-2024

Disinstallazione di agenti

Quando si disinstalla un agente da un workload, il workload viene automaticamente rimosso dalla console di Cyber Protect. Se il workload è ancora visualizzato dopo aver disinstallato l'agente, ad esempio a causa di un problema di rete, rimuovere manualmente il workload dalla console. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Eliminazione di workload dalla console di Cyber Protect" (pag. 341).

Nota
La disinstallazione di un agente non implica l'eliminazione dei piani o dei backup.

Per disinstallare un agente

Windows

1. Accedere come amministratore al sistema con l'agente.
2. Nel **Pannello di controllo** selezionare **Programmi e funzionalità** (**Installazione applicazioni** in Windows XP).
3. Fare clic con il pulsante destro su **Acronis Cyber Protect**, quindi selezionare **Disinstalla**.
4. [Per gli agenti protetti con password] Specificare la password necessaria per disinstallare l'agente, quindi fare clic su **Avanti**.
5. [Facoltativo] Selezionare la casella di controllo **Rimuovere impostazioni di registri e configurazioni**.

   Se si prevede di installare nuovamente l'agente, lasciare deselezionata questa casella di controllo. Se la casella di controllo è selezionata e si installa di nuovo l'agente, il workload potrebbe risultare duplicato nella console di Cyber Protect e i backup del sistema precedente potrebbero non essere associati al nuovo sistema.
6. Fare clic su **Disinstalla**.

Linux

1. Sul sistema con l'agente, eseguire `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` come utente root.
2. [Facoltativo] Selezionare la casella di controllo **Eliminare tutte le tracce del prodotto (eliminare registri, attività, depositi e impostazioni di configurazione)**.

   Se si prevede di installare nuovamente l'agente, lasciare deselezionata questa casella di controllo. Se la casella di controllo è selezionata e si installa di nuovo l'agente, il workload potrebbe risultare duplicato nella console di Cyber Protect e i backup del sistema precedente potrebbero non essere associati al nuovo sistema.
3. Confermare la propria decisione.

macOS

© Acronis International GmbH, 2003-2024

1. Nel sistema con l'agente, fare doppio clic sul file di installazione .dmg.
2. Attendere mentre il sistema operativo monta l'immagine del disco di installazione.
3. Fare doppio clic su **Disinstalla** all'interno dell'immagine.
4. Se richiesto, fornire le credenziali amministrative.
5. Confermare la propria decisione.

Per disinstallare i componenti distribuiti nel pacchetto con l'Agente per Windows

È possibile disinstallare singoli componenti inclusi nel pacchetto con l'Agente per Windows, ad esempio Cyber Protect Monitor, Agente per Prevenzione della perdita di dati o Generatore di supporti riavviabili, senza disinstallare l'Agente per Windows.

1. Accedere come amministratore al sistema con l'agente.
2. Eseguire il programma di installazione quindi fare clic su **Modificare componenti installati**.
3. Deselezionare le caselle di controllo accanto ai nomi dei componenti da disinstallare, quindi fare clic su **Fine**.

Per rimuovere l'Agente per VMware (appliance virtuale)

1. Utilizzando vSphere Client, accedere a vCenter Server.
2. [Se l'appliance virtuale è attiva] Fare clic con il pulsante destro sull'appliance virtuale, quindi su **Accensione** > **Spegni**. Confermare la propria decisione.
3. [Se l'appliance virtuale utilizza uno storage collegato localmente su un disco virtuale e si desidera conservare i dati su tale disco] Rimuovere lo storage virtuale dall'appliance virtuale.
   a. Fare clic con il pulsante destro sull'appliance virtuale, quindi selezionare **Modifica impostazioni**.
   b. Selezionare il disco con l'archivio, quindi fare clic su **Rimuovi**.
   c. In **Opzioni di rimozione**, fare clic su **Rimuovi dalla macchina virtuale**.
   d. Fare clic su **OK**.

   Di conseguenza, il disco rimarrà nel datastore. È possibile collegare il disco a un'altra appliance virtuale.
4. Fare clic con il pulsante destro sull'appliance virtuale, quindi selezionare **Elimina da disco**. Confermare la propria decisione.
5. [Facoltativo] [Se non si prevede di utilizzare l'appliance di nuovo] Nella console di Cyber Protect, passare a **Archivio di backup** > **Posizioni** ed eliminare la posizione corrispondente allo storage collegato in locale.

Impostazioni di protezione

Per configurare le impostazioni di protezione generali per Cyber Protection, nella console di Cyber Protect passare a **Impostazioni** > **Protezione**.

© Acronis International GmbH, 2003-2024

Aggiornamenti automatici dei componenti

Per impostazione predefinita, tutti gli agenti possono connettersi a Internet e scaricare gli aggiornamenti.

Un amministratore può ridurre al minimo il traffico sulla larghezza di banda della rete selezionando nell'ambiente uno o più agenti e assegnando a questi il Ruolo di chi esegue l'aggiornamento. Tutti gli agenti dedicati potranno connettersi a Internet e scaricare gli aggiornamenti. Tutti gli altri agenti si connetteranno agli agenti di aggiornamento dedicati utilizzando la tecnologia peer-to-peer, ed eseguendo quindi da questi il download degli aggiornamenti.

Gli agenti senza Ruolo di chi esegue l'aggiornamento si connettono a Internet se non è presente alcun agente di aggiornamento dedicato nell'ambiente o se non è possibile stabilire la connessione a un agente di aggiornamento dedicato per più di cinque minuti.

L'agente che esegue l'aggiornamento distribuisce aggiornamenti e patch per le funzionalità Protezione antivirus e anti-malware, Vulnerability assessment e Patch management, ma non include gli aggiornamenti della versione dell'agente.

Nota
Un agente con il Ruolo di chi esegue l'aggiornamento può scaricare ed distribuire le patch solo per i prodotti Windows di terze parti. La distribuzione delle patch per i prodotti Microsoft non è supportata dall'agente del programma di aggiornamento.

Prima di assegnare il Ruolo di chi esegue l'aggiornamento a un agente, verificare che il sistema sul quale viene eseguito l'agente sia sufficientemente potente, disponga di una connessione a Internet stabile e ad alta velocità e di spazio su disco sufficiente.

Per preparare un sistema per il Ruolo di chi esegue l'aggiornamento

1. Sul sistema dell'agente sul quale si intende abilitare il Ruolo di chi esegue l'aggiornamento, applicare le regole del firewall:
   - In entrata (in arrivo) "updater_incoming_tcp_ports": consente la connessione alle porte TCP 18018 e 6888 per tutti i profili del firewall (pubblico, privato e dominio).
   - In entrata (in arrivo) "updater_incoming_udp_ports": consente la connessione alla porta UDP 6888 per tutti i profili del firewall (pubblico, privato e dominio).
2. Riavviare Acronis Agent Core Service.
3. Riavviare il servizio Firewall.

Se queste regole non vengono applicate e il firewall è abilitato, gli agenti peer scaricheranno gli aggiornamenti dal cloud.

Per assegnare il Ruolo di chi esegue l'aggiornamento a un agente di protezione

1. Nella console di Cyber Protect, passare a **Impostazioni** > **Agenti**.
2. Selezionare il sistema con l'agente al quale assegnare il Ruolo di chi esegue l'aggiornamento.

© Acronis International GmbH, 2003-2024

3. Fare clic su **Dettagli**, quindi abilitare l'opzione **Utilizzare questo agente per scaricare e distribuire patch e aggiornamenti**.

L'aggiornamento peer-to-peer funziona come indicato di seguito.

1. L'agente con il Ruolo di chi esegue l'aggiornamento controlla secondo la pianificazione il file di indice fornito dal service provider per aggiornare i componenti principali.
2. L'agente con il Ruolo di chi esegue l'aggiornamento inizia il download e la distribuzione degli aggiornamenti a tutti gli agenti.

È possibile assegnare il Ruolo di chi esegue l'aggiornamento a più agenti dell'ambiente. Pertanto, se un agente con il Ruolo di chi esegue l'aggiornamento è offline, altri agenti con lo stesso ruolo possono fungere come origine degli aggiornamenti delle definizioni.

Aggiornamento delle definizioni di Cyber Protection in base alla pianificazione

Nella scheda **Pianificazione** è possibile definire la pianificazione per l'aggiornamento automatico delle definizioni di Cyber Protection per ognuno dei seguenti componenti:

- Anti-malware
- Valutazione delle vulnerabilità
- Gestione patch

Per modificare l'impostazione di aggiornamento delle definizioni, passare a **Impostazioni** > **Protezione** > **Aggiornamento delle definizioni di protezione** > **Pianificazione**.

Tipo di pianificazione:

- **Ogni giorno** – Definire in quali giorni della settimana aggiornare le definizioni.
  Ora di avvio – Selezionare l'ora di aggiornamento delle definizioni.
- **Ogni ora** – Definire una pianificazione oraria più dettagliata per gli aggiornamenti.
  Esegui ogni – Definire la periodicità di esecuzione degli aggiornamenti.
  Da... **A** – Definire un intervallo di orario specifico per gli aggiornamenti.

Aggiornamento delle definizioni di Cyber Protection su richiesta

Per aggiornare le definizioni di Cyber Protection per uno specifico sistema su richiesta

1. Nella console di Cyber Protect, passare a **Impostazioni** > **Agenti**.
2. Selezionare i sistemi sui quali aggiornare le definizioni di protezione e fare clic su **Aggiorna definizioni**.

Archiviazione cache

La posizione dei dati memorizzati nella cache è la seguente:

© Acronis International GmbH, 2003-2024

- Su sistemi Windows: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Su sistemi Linux: `/opt/acronis/var/atp-downloader/Cache`
- Su sistemi MacOS: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Per modificare l'impostazione di archiviazione della cache, passare a **Impostazioni** > **Protezione** > **Aggiornamento delle definizioni di protezione** > **Archiviazione cache**.

Nel campo **File di aggiornamento e dati di gestione patch obsoleti**, specificare il periodo dopo il quale rimuovere i dati memorizzati nella cache.

Massima dimensione archivio cache (GB) per gli agenti:

- **Ruolo di chi esegue l'aggiornamento** – definire la dimensione della cache sui sistemi con il Ruolo di chi esegue l'aggiornamento.
- **Altri ruoli** – definire la dimensione della cache sugli altri sistemi.

Nota
Cyber Protection raccoglie esempi dei malware rilevati per ulteriori analisi in modo da poter migliorare il software. È possibile modificare questa impostazione in qualsiasi momento nella scheda **Protezione**, disattivando l'interruttore **Raccogli e carica su CPOC esempi di malware**.

Modifica della quota di servizio dei sistemi

Una quota di servizio viene automaticamente assegnata quando un piano di protezione viene applicato per la prima volta a un sistema.

Viene assegnata la quota più appropriata in funzione del tipo di sistema protetto, del suo sistema operativo, del livello di protezione richiesto e di disponibilità della quota. Se nell'organizzazione non è disponibile una quota appropriata, verrà assegnata la seconda migliore quota disponibile. Se, ad esempio, la quota più appropriata è **Server di web hosting** ma questa non è disponibile, verrà assegnata la quota **Server**.

Esempi di assegnazione delle quote:

- A un sistema fisico che esegue un sistema operativo Windows Server o Linux Server (come Ubuntu Server) viene assegnata la quota **Server**.
- A un sistema fisico che esegue un sistema operativo desktop Windows o Linux (come Ubuntu Desktop) viene assegnata la quota **Workstation**.
- A un sistema fisico che esegue il sistema operativo Windows 10 con un ruolo di Hyper-V abilitato, viene assegnata la quota **Workstation**.
- A un sistema desktop che viene eseguito su un'infrastruttura desktop virtuale e il cui agente di protezione è installato nel sistema operativo guest (ad esempio, Agente per Windows), viene assegnata la quota **Macchina virtuale**. Questo tipo di sistema può inoltre utilizzare la quota **Workstation** se la quota **Macchina virtuale** non è disponibile.

© Acronis International GmbH, 2003-2024

- A un sistema desktop che viene eseguito su un'infrastruttura desktop virtuale e il cui backup viene eseguito in modalità agentless (ad esempio, Agente per VMware o Agente per Hyper-V), viene assegnata la quota **Macchina virtuale**.
- A un server Hyper-V o vSphere viene assegnata la quota **Server**.
- A un server con cPanel o Plesk viene assegnata la quota **Server di web hosting**. Questo tipo di sistema può inoltre utilizzare la quota **Macchina virtuale** o la quota **Server**, a seconda del tipo di sistema sul quale viene eseguito il server web, se la quota **Server di web hosting** non è disponibile.
- Il backup application-aware richiede la quota **Server** anche per una workstation.

È possibile modificare manualmente l'assegnazione originaria in un secondo momento. Ad esempio, per applicare un piano di protezione più avanzato allo stesso sistema, potrebbe essere necessario aggiornare la quota di servizio del sistema. Se le funzionalità richieste dal piano di protezione in questione non sono supportate dalla quota di servizio correntemente assegnata, il piano di protezione non avrà esito positivo.

In alternativa, è possibile modificare la quota di servizio se si acquistano quote più appropriate dopo l'assegnazione di quella originaria. Ad esempio, la quota **Workstation** viene assegnata a una virtual machine. Dopo aver acquistato una quota **Macchina virtuale**, è possibile assegnarla manualmente al sistema al posto della quota **Workstation** originaria.

È inoltre possibile rilasciare la quota di servizio attualmente assegnata e quindi assegnarla a un altro sistema.

È possibile modificare la quota di servizio di un singolo sistema o di un gruppo di sistemi.

Per modificare la quota di servizio di un singolo sistema

1. Nella console di Cyber Protect, passare a **Dispositivi**.
2. Selezionare il sistema desiderato e fare clic su **Dettagli**.
3. Nella sezione **Quota di servizio**, fare clic su **Modifica**.
4. Nella finestra **Modifica quota**, selezionare la quota di servizio desiderata o la voce **Nessuna quota**, quindi fare clic su **Modifica**.

Per modificare la quota di servizio di un gruppo di sistemi

1. Nella console di Cyber Protect, passare a **Dispositivi**.
2. Selezionare più di un sistema, quindi fare clic su **Assegna quota**.
3. Nella finestra **Modifica quota**, selezionare la quota di servizio desiderata o la voce **Nessuna quota**, quindi fare clic su **Modifica**.

Servizi di Cyber Protection installati nell'ambiente

Cyber Protection installa alcuni o tutti i seguenti servizi, in base alle opzioni di Cyber Protection utilizzate.

© Acronis International GmbH, 2003-2024

Servizi installati in Windows

Nome del servizio	Scopo
Acronis Managed Machine Service	Fornisce funzionalità di backup, ripristino, replica, conservazione, convalida
Acronis Scheduler2 Service	Esegue le attività pianificate al verificarsi di determinati eventi
Acronis Active Protection Service	Fornisce protezione contro il ransomware
Acronis Cyber Protection Service	Fornisce protezione contro i malware

Servizi installati in macOS

Nome e posizione del servizio	Scopo
`/Library/LaunchDaemons/com.acronis.aakore.plist`	Facilita la comunicazione tra l'agente e i componenti di gestione
`/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist`	Consente il rilevamento del malware
`/Library/LaunchDaemons/com.acronis.mms.plist`	Fornisce funzionalità di backup e ripristino
`/Library/LaunchDaemons/com.acronis.schedule.plist`	Esegue le attività pianificate

Salvataggio di un file del registro agente

È possibile salvare un registro agente in un file .zip. Se un backup non riesce per un motivo non precisato, questo file consente al personale del supporto tecnico di identificare il problema.

Per impostazione predefinita, le informazioni nel registro sono ottimizzate rispetto agli ultimi tre giorni, ma è possibile modificare il periodo.

Per raccogliere i registri agente

1. Eseguire una delle seguenti operazioni:
   - In **Dispositivi**, selezionare il sistema da cui raccogliere i registri, quindi fare clic su **Attività**.
   - In **Impostazioni** > **Agenti**, selezionare il sistema da cui raccogliere i registri, quindi fare clic su **Dettagli**.
2. [Facoltativo] Per modificare il periodo predefinito per il quale includere le informazioni di sistema, fare clic sulla freccia accanto al pulsante **Raccogliere le informazioni di sistema** e quindi selezionare il periodo.

© Acronis International GmbH, 2003-2024

3. Fare clic su **Raccogliere le informazioni di sistema**.
4. Se richiesto dal browser Web, specificare dove salvare il file.

Open VPN site-to-site - Informazioni aggiuntive

Durante la configurazione di un server di ripristino, vengono configurati l'**indirizzo IP nella rete produttiva** e l'**indirizzo IP di prova**.

Successivamente all'esecuzione del failover (esecuzione della virtual machine nel cloud) e all'accesso alla virtual machine per controllare l'indirizzo IP del server, viene visualizzato l'**indirizzo IP nella rete produttiva**.

Durante l'esecuzione del failover di prova, è possibile raggiungere il server di prova solo utilizzando l'**indirizzo IP di prova**, visibile soltanto nella configurazione del server di ripristino.

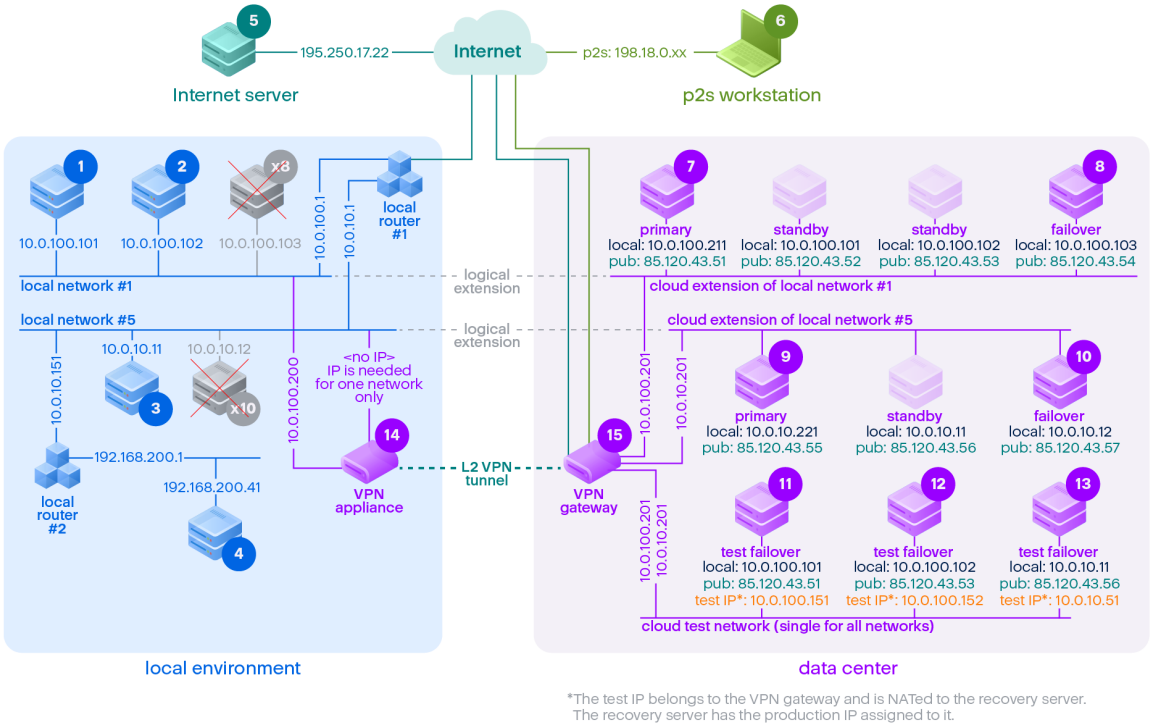
Per raggiungere un server di prova dal sito locale, è necessario utilizzare l'**indirizzo IP di prova**.

Nota
La configurazione di rete del server mostra sempre l'**indirizzo IP nella rete produttiva**, perché il server di prova rispecchia la configurazione del server di produzione. Ciò accade perché l'indirizzo IP di prova non appartiene al server di prova ma al gateway VPN, e viene tradotto nell'indirizzo IP di produzione tramite NAT.

Il diagramma seguente illustra un esempio di configurazione di Open VPN da sito a sito. Alcuni dei server nell'ambiente locale vengono ripristinati nel cloud tramite il failover (mentre l'infrastruttura di rete non presenta problema).

1. Il cliente ha abilitato il Disaster Recovery nei seguenti modi:
   a. configurando l'appliance VPN (14) e connettendola al server VPN cloud dedicato (15)
   b. proteggendo alcuni dei server locali con il Disaster Recovery (1, 2, 3, x8 e x10)
      Alcuni server nel sito locale (come il 4) sono collegati a reti non connesse all'appliance VPN. Questi server non sono protetti con Disaster Recovery.
2. Parte dei server (connessi a reti differenti) funzionano nel sito locale: (1, 2, 3 e 4)
3. Questi server protetti (1, 2 e 3) vengono sottoposti a test con il failover di prova (11, 12 e 13)
4. Alcuni server del sito locale non sono disponibili (x8, x10). Dopo l'esecuzione del failover, diventano disponibili nel cloud (8 e 10)
5. Alcuni server primari (7 e 9), connessi a reti differenti, sono disponibili nell'ambiente cloud
6. (5) è un server in Internet con un indirizzo IP pubblico
7. (6) è una workstation connessa al cloud tramite una connessione VPN da punto a sito (p2s)

© Acronis International GmbH, 2003-2024



In questo esempio, è disponibile la seguente configurazione di connessione (ad esempio, "ping") da un server nella riga **Da:** a un server nella colonna **A:**.

	A:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Da:		locale	locale	locale	locale	internet	p2s	primario	failover	primario	failover	failover di prova	failover di prova	failover di prova	applianc e VPN	server VPN
1	locale		diretto	tramite router locale 1	tramite router locale 2	tramite router locale 1 e Internet	no	tramite tunnel: locale tramite router locale 1 e Internet:	tramite tunnel: locale tramite router locale 1 e Internet:	tramite tunnel: locale tramite router locale 1 e Internet:	tramite tunnel: locale tramite router locale 1 e Internet:	tramite tunnel: NAT (server VPN) tramite router locale 1	tramite tunnel: NAT (server VPN) tramite router locale 1	tramite router locale 1 e tunnel: NAT (server VPN) tra	diretto	no

© Acronis International GmbH, 2003-2024

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								pub	pub	pub	pub	e Internet: pub	e Internet: pub	mite router locale 1 e Internet: pub		
2	locale	diretto		tramite router locale 1	tramite router locale 2	tramite router locale 1 e Internet	no	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	tramite router locale 1 e tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	diretto	no
3	locale	tramite router locale 1	tramite router locale 1		tramite router locale 2	tramite router locale 1 e	no	tramite tunnel: locale tramite	tramite tunnel: locale tramite	tramite tunnel: locale tramite	tramite tunnel: locale tramite	tramite tunnel: NAT (server VP	tramite tunnel: NAT (server VP	tramite router locale 1 e tun	tramite router locale	no

© Acronis International GmbH, 2003-2024

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						Internet		router locale 1 e Internet: pub	router locale 1 e Internet: pub	router locale 1 e Internet: pub	router locale 1 e Internet: pub	N) tramite router locale 1 e Internet: pub	N) tramite router locale 1 e Internet: pub	nel: NAT (server VPN) tramite router locale 1 e Internet: pub		
4	locale	tramite router locale 2 e router 1	tramite router locale 2 e router 1	tramite router locale 2		tramite router locale 2, router 1 e Internet	no	tramite router locale 2 e tunnel: locale tramite router locale 2, router locale 1 e Internet: pub	tramite router locale 2 e tunnel: locale tramite router locale 2, router locale 1 e Internet: pub	tramite router locale 2 e tunnel: locale tramite router locale 2, router locale 1 e Internet: pub	tramite router locale 2 e tunnel: locale tramite router locale 2, router locale 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 2, router 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 2, router 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 2, router 1 e Internet: pub	tramite router locale 2	no

© Acronis International GmbH, 2003-2024

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
5	internet	no	no	no	no		n/d	tramite Internet: pub	tramite Internet: pub	tramite Internet: pub	tramite Internet: pub	tramite Internet: pub	tramite Internet: pub	tramite Internet: pub	no	no
6	p2s	no	no	no	no	tramite Internet		tramite VPN p2s (server VPN): locale tramite Internet: pub	tramite VPN p2s (server VPN): locale tramite Internet: pub	tramite VPN p2s (server VPN): locale tramite Internet: pub	tramite VPN p2s (server VPN): locale tramite Internet: pub	tramite VPN p2s - NAT (server VPN) tramite Internet: pub	tramite VPN p2s - NAT (server VPN) tramite Internet: pub	tramite VPN p2s - NAT (server VPN) tramite Internet: pub	no	no
7	primario	tramite tunnel	tramite tunnel	tramite tunnel e router locale 1	tramite tunnel e router locale 1 e 2	tramite Internet (tramite server VPN)	no		diretto in cloud: locale	tramite tunnel e router locale 1: locale	tramite tunnel e router locale 1: locale	tramite server VPN: NAT	tramite server VPN: NAT	tramite tunnel e router locale 1: NAT	no	Solo protocolli DHCP e DNS
8	failover	tramite tunnel	tramite tunnel	tramite tunnel e router loc	tramite tunnel e router loc	tramite Internet (tramite ser	no	diretto in cloud: locale		tramite tunnel e router locale 1:	tramite tunnel e router locale 1:	tramite server VPN: NAT	tramite server VPN: NAT	tramite tunnel e router locale 1:	no	Solo protocolli DHCP e DNS

© Acronis International GmbH, 2003-2024

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				ale 1	ale 1 e 2	ver VPN)				locale	locale			NAT		
9	primario	tramite tunnel e router locale 1	tramite tunnel e router locale 1	tramite tunnel	tramite tunnel	tramite Internet (tramite server VPN)	no	tramite tunnel e router locale 1: locale	tramite tunnel e router locale 1: locale		diretto in cloud: locale	tramite tunnel e router locale 1: NAT	tramite tunnel e router locale 1: NAT	tramite server VPN: NAT	no	Solo protocolli DHCP e DNS
10	failover	tramite tunnel e router locale 1	tramite tunnel e router locale 1	tramite tunnel	tramite tunnel	tramite Internet (tramite server VPN)	no	tramite tunnel e router locale 1: locale	tramite tunnel e router locale 1: locale	diretto in cloud: locale		tramite tunnel e router locale 1: NAT	tramite tunnel e router locale 1: NAT	tramite server VPN: NAT	no	Solo protocolli DHCP e DNS
11	failover di prova	no	no	no	no	tramite Internet (tramite server VPN)	no	no	no	no	no		diretto in cloud: locale	tramite server VPN: locale (routing)	no	Solo protocolli DHCP e DNS
12	failover di prov	no	no	no	no	tramite	no	no	no	no	no	diretto in clou		tramite serv	no	Solo protocolli

© Acronis International GmbH, 2003-2024

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	a					Internet (tramite server VPN)						d: locale		er VPN: locale (routing)		DHCP e DNS
13	failover di prova	no	no	no	no	tramite Internet (tramite server VPN)	no	no	no	no	no	tramite server VPN: locale (routing)	tramite server VPN: locale (routing)		no	Solo protocolli DHCP e DNS
14	appliance VPN	diretto	diretto	tramite router locale 1	tramite router locale 2	tramite Internet (router locale 1)	no	no	no	no	no	no	no	no		no
15	server VPN	no	no	no	no	no	no	no	no	no	no	no	no	no	no	

Gestione delle licenze per i management server in locale

Per informazioni dettagliate su come attivare un management server in locale o su come allocare a questo le licenze, fare riferimento alla sezione Licenze del manuale utente di Cyber Protect.

© Acronis International GmbH, 2003-2024

Definizione degli elementi da proteggere e delle modalità di protezione

Scheda Gestione

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Tutti i piani creati sono disponibili nella scheda **Gestione** della console di Cyber Protect.

Sono disponibili le sezioni seguenti:

- **Piani di protezione**
- **Piani di gestione remota**
- **Piani di scripting**
- **Piani di monitoraggio**
- **Archivio degli script**
- **Backup delle applicazioni cloud**
- **Scansione del backup**
- **Replica backup**
- **Convalida**
- **Pulizia**
- **Conversione in MV**
- **Replica di MV**

Stati del piano

Per i piani di protezione e i piani di replica delle VM, è disponibile una barra di stato che mostra i seguenti stati con classificazione basata su colori:

- OK (Verde)
- Avviso (Arancione)
- Errore (Arancione scuro)
- Critico (Rosso)
- Piano in esecuzione (Blu)
- Piano disabilitato (Grigio)

Fare clic sulla barra di stato per visualizzare i dettagli sugli stati del piano su tutti i workload ai quali è applicato il piano.

© Acronis International GmbH, 2003-2024

Fare clic su uno stato specifico per visualizzare un elenco di tutti i workload con questo stato.

Piani di protezione

Nella scheda **Management** > **Piani di protezione**, è possibile visualizzare informazioni sui piani di protezione esistenti, eseguire azioni con i piani e crearne di nuovi.

Per ulteriori informazioni sui piani di protezione, fare riferimento a "Piani e moduli di protezione" (pag. 217).

Piani di backup per applicazioni cloud

La sezione **Gestione** > **Backup delle applicazioni cloud** mostra i piani di backup cloud-to-cloud. Questi piani eseguono il backup delle applicazioni in esecuzione nel cloud tramite agenti che vengono eseguiti nel cloud e utilizzano l'archivio nel cloud come posizione di backup.

In questa sezione è possibile eseguire le seguenti operazioni:

- Creazione, visualizzazione, esecuzione, arresto, modifica ed eliminazione di un piano di backup
- Visualizzazione delle attività correlate a ogni piano di backup
- Visualizzazione degli avvisi correlati a ogni piano di backup

Per ulteriori informazioni sul backup delle applicazioni cloud, fare riferimento a:

- Protezione dei dati di Microsoft 365
- Protezione dei dati di Google Workspace

Esecuzione manuale dei backup da cloud a cloud

Per evitare interruzioni del servizio Cyber Protection, il numero di operazioni di backup manuale cloud-to-cloud è limitato a 10 per organizzazione di Microsoft 365 o Google Workspace ogni ora. Una volta raggiunto questo numero, il numero di esecuzioni consentite viene ripristinato a una ogni ora, e da questo momento in poi è possibile eseguire un'esecuzione aggiuntiva ogni ora (ad esempio: ora 1, 10 esecuzioni; ora 2, 1 esecuzione; ora 3, 2 esecuzioni) fino a quando non viene raggiunto il totale di 10 esecuzioni per ora.

Non è possibile eseguire manualmente i piani di backup applicati a gruppi di dispositivi (caselle di posta, unità, siti) o contenenti più di 10 dispositivi.

Piani di scansione del backup

Per scansionare i backup alla ricerca di malware (incluso il ransomware), creare un piano di scansione dei backup.

Importante
I piani di scansione del backup non sono supportati per tutti i workload e gli storage di backup. Per ulteriori informazioni, consultare "Limitazioni" (pag. 883).

 © Acronis International GmbH, 2003-2024

Per creare un piano di scansione del backup

1. Nella console di Cyber Protect, passare a **Gestione** > **Scansione del backup**.
2. Fare clic su **Crea piano**.
3. Specificare il nome del piano e i parametri seguenti:
   - **Tipo scansione**:
     - **Cloud**: non è possibile modificare questa opzione. La scansione del backup verrà eseguita da un agente cloud selezionato automaticamente.
   - **Backup da scansionare**:
     - **Posizioni**: selezionare le posizioni con i set di backup da scansionare.
     - **Backup**: selezionare i set di backup da scansionare.
   - **Scansiona per**:
     - **Malware**: non è possibile modificare questa opzione. La scansione controlla i set di backup selezionati alla ricerca del malware (incluso il ransomware).
   - **Crittografia**: per scansionare i set di backup crittografati, specificare la password di crittografia. Se si seleziona una posizione o più set di backup e la password specificata non corrisponde a un set di backup, viene generato un avviso.
   - **Pianificazione**: non è possibile modificare questa opzione. Nel cloud storage la scansione si avvia automaticamente.
4. Fare clic su **Crea**.

Viene creato un piano per la scansione del backup e un agente cloud scansionerà le posizioni o i set di backup specificati alla ricerca del malware.

Elaborazione dei dati al di fuori dell'host

Nota
Questa funzionalità è disponibile nei tenant cliente per i quali la quota di **Advanced Backup - Server** o la quota di **Advanced Backup - NAS** è abilitata come parte del pacchetto Advanced Backup.

Le operazioni di replica, convalida e pulizia vengono in genere eseguite dall'agente di protezione che esegue anche il backup. Ciò aggiunge un ulteriore carico al sistema in cui l'agente è in esecuzione, anche una volta completato il processo di backup. Per ridurre il carico sul sistema, è possibile creare piani di protezione dati con elaborazione esterna all'host, ovvero piano distinti per la replica, la convalida, la pulizia e la conversione in virtual machine.

I piani di protezione dati con elaborazione esterna all'host consentono di:

- Scegliere agenti differenti per le operazioni di backup e protezione dati esterne all'host
- Pianificare le operazioni di elaborazione dei dati esternamente all'host durante le ore di minor utilizzo per ridurre il consumo di larghezza di banda della rete

© Acronis International GmbH, 2003-2024

- Pianificare le operazioni di elaborazione dei dati esternamente all'host durante le ore non lavorative, se non si desidera installare un agente dedicato a tali attività

Nota
I piani che prevedono l'elaborazione dei dati esterna all'host vengono eseguiti in base alle impostazioni orarie (compreso il fuso orario) del sistema su cui è installato l'agente di protezione. Per un'appliance virtuale (ad esempio l'Agente per VMware o l'Agente per Scale Computing HC3), è possibile configurare il fuso orario nell'interfaccia utente dell'agente.

Replica di backup

Nota
Questa funzionalità è disponibile nei tenant cliente per i quali la quota di **Advanced Backup - Server** o la quota di **Advanced Backup - NAS** è abilitata come parte del pacchetto Advanced Backup.

Con replica di backup si intende la copia del backup in una posizione diversa. In quanto operazione di elaborazione dei dati esternamente all'host, questa attività viene configurata nel piano di replica di un backup.

La replica di backup può anche far parte di un piano di protezione. Per ulteriori informazioni su questa opzione, fare riferimento a "Replica" (pag. 447).

Creazione di un piano di replica del backup

Per replicare i backup come un'operazione di elaborazione dei dati esternamente all'host, occorre creare un piano di replica di backup.

Per creare un piano di replica del backup

1. Nella console di Cyber Protect, fare clic su **Gestione** > **Replica backup**.
2. Fare clic su **Crea piano**.
3. In **Agente**, selezionare l'agente che eseguirà la replica.
   È possibile selezionare qualsiasi agente che abbia accesso sia alla posizione di origine che alle posizioni di replica.
4. In **Elementi da replicare**, selezionare gli archivi o le posizioni di backup da replicare.
   È possibile alternare la selezione degli archivi e delle posizioni tramite l'opzione **Posizioni**/**Backup** nell'angolo in alto a destra.
   Se si selezionano più archivi crittografati, la loro password di crittografia deve essere la stessa. Per gli archivi che usano password di crittografia diverse, creare piani di backup separati.
5. In **Destinazione**, specificare la posizione della replica.
6. In **Come eseguire la replica**, selezionare i backup (anche noti come punti di ripristino) di cui eseguire la replica.
   Sono disponibili le seguenti opzioni:

 © Acronis International GmbH, 2003-2024

- **Tutti i backup**
- **Solo backup completi**
- **Solo l'ultimo backup**

Per ulteriori informazioni su queste opzioni, consultare "Elementi della replica" (pag. 203).

7. In **Pianificazione**, configurare la pianificazione della replica.
   Quando si configura la pianificazione del piano di replica di backup, verificare che l'ultimo backup replicato sia ancora disponibile nella sua posizione originale all'avvio della replica di backup. Se il backup non è disponibile nella posizione originale, perché ad esempio è stato eliminato da una regola di conservazione, l'intero archivio verrà replicato come backup completo. Questa attività può essere lunga e laboriosa e utilizzare spazio di storage aggiuntivo.
8. In **Regole di conservazione**, specificare le regole di conservazione per la posizione di destinazione.
   Sono disponibili le seguenti opzioni:
   - **Per numero di backup**
   - **Per durata backup** (impostazioni distinte per backup mensili, settimanali, giornalieri e orari)
   - **Per dimensione totale dei backup**
   - **Conserva i backup per un periodo illimitato**

     Nota
     La selezione di questa opzione implicherà un maggiore utilizzo dell'archivio. È necessario eliminare manualmente i backup superflui.
9. [Se sono stati selezionati archivi crittografati in **Elementi da replicare**] Attivare l'opzione **Password di backup**, quindi fornire la password di crittografia.
10. [Facoltativo] Per modificare le opzioni del piano, fare clic sull'icona ingranaggio e configurare le opzioni come richiesto.
11. Fare clic su **Crea**.

Elementi della replica

Nota
Alcune operazioni di replica, come la replica di un'intera posizione o la replica di tutti i backup in un set di backup possono richiedere molto tempo.

È possibile replicare singoli set di backup o intere posizioni di backup. La replica di una posizione di backup riguarda tutti i set di backup che contiene.

I set di backup sono costituiti da backup (anche noti come punti di ripristino). È necessario selezionare i backup di cui eseguire la replica.

Sono disponibili le seguenti opzioni:

© Acronis International GmbH, 2003-2024

- **Tutti i backup**
  Tutti i backup nel set di backup vengono replicati ogni volta che viene eseguito il piano di replica.
- **Solo backup completi**
  Vengono replicati solo i backup completi del set di backup.
- **Solo l'ultimo backup**
  Viene replicato solo il backup più recente nel set di backup, a prescindere da quale sia il tipo di backup (completo, differenziale o incrementale).

Selezionare un'opzione in base alle esigenze e allo schema di backup in uso. Se, ad esempio, si utilizza lo schema di backup **Sempre incrementale (a file singolo)** e si desidera replicare solo il più recente backup incrementale, nel piano di replica di backup selezionare **Solo ultimo backup**.

La tabella seguente riepiloga i backup che verranno replicati con i diversi schemi di backup.

	Sempre incrementale (a file singolo)	**Sempre completo**	**Settimanale completo, Giornaliero incrementale**	**Mensile completo, Settimanale differenziale, Giornaliero incrementale (GFS)**
Tutti i backup	Tutti i backup nel set di backup	Tutti i backup nel set di backup	Tutti i backup nel set di backup	Tutti i backup nel set di backup
Solo backup completi	Solo il primo backup, che è completo	Tutti i backup	Un backup ogni settimana*	Un backup ogni mese*
Solo ultimo backup	Solo il backup più recente nel set di backup*	Solo il backup più recente nel set di backup*	Solo il backup più recente nel set di backup, a prescindere dal tipo*	Solo il backup più recente nel set di backup, a prescindere dal tipo*

*Quando si configura la pianificazione del piano di replica di backup, verificare che l'ultimo backup replicato sia ancora disponibile nella sua posizione originale all'avvio della replica di backup. Se il backup non è disponibile nella posizione originale, perché ad esempio è stato eliminato da una regola di conservazione, l'intero archivio verrà replicato come backup completo. Questa attività può essere lunga e laboriosa e utilizzare spazio di storage aggiuntivo.

Posizioni supportate

La tabella seguente riepiloga le posizioni di backup supportate dai piani di replica del backup.

Posizione del backup	**Supportato come origine**	**Supportato come destinazione**
Archiviazione nel cloud	+	+

© Acronis International GmbH, 2003-2024

Posizione del backup	Supportato come origine	Supportato come destinazione
Cartella locale	+	+
Cartella di rete	+	+
Cloud pubblico	+	+
Cartella NFS	–	–
Secure Zone	–	–

Convalida

Nota
Questa funzionalità è disponibile nei tenant cliente per i quali la quota di **Advanced Backup - Server** o la quota di **Advanced Backup - NAS** è abilitata come parte del pacchetto Advanced Backup.

La convalida di un backup consente di verificare che sia possibile recuperare i dati che questo contiene.

Per convalidare un backup come un'operazione di elaborazione dei dati esternamente all'host, occorre creare un piano di convalida. Per ulteriori informazioni su come creare un piano di convalida, fare riferimento a "Creazione di un piano di convalida" (pag. 206).

Sono disponibili i seguenti metodi di convalida:

- Verifica checksum
- Esegui come macchina virtuale
  - Heartbeat MV
  - Convalida screenshot

È possibile selezionare uno o più metodi. Selezionando uno o più metodi di convalida, le operazioni di ogni metodo vengono eseguite consecutivamente. Per ulteriori informazioni sui metodi, fare riferimento a "Heartbeat MV" (pag. 209).

È possibile convalidare set di backup o posizioni di backup. La convalida di una posizione di backup riguarda tutti i set di backup che questa contiene.

Posizioni supportate

La tabella seguente mostra le posizioni di backup e i metodi di convalida supportati.

Nota
L'opzione di convalida non è disponibile per i backup nel cloud pubblico a causa dei costi proibitivi della lettura di un intero archivio da un cloud pubblico.

© Acronis International GmbH, 2003-2024

Posizione del backup	Verifica checksum	Esegui come macchina virtuale	
		Heartbeat MV	Convalida screenshot
Archiviazione nel cloud	+	+	+
Cartella locale	+	+	+
Cartella di rete	+	+	+
Cartella NFS	–	–	–
Secure Zone	–	–	–

Stato di convalida

Dopo la riuscita di una convalida, il backup viene contrassegnato con un punto verde e con l'etichetta **Convalidato**.

Se la convalida non riesce, il backup viene convalidato con un punto rosso. La convalida non ha esito positivo anche se uno solo dei metodi di convalida non riesce. In alcuni casi, la mancata riuscita potrebbe essere causata dall'errata configurazione del piano di convalida, ad esempio l'utilizzo del metodo **Heartbeat MV** per le virtual machine su un host errato.

Lo stato di convalida di un backup viene aggiornato a ogni nuova operazione di convalida. Lo stato di ogni metodo di convalida viene aggiornato separatamente. Per questa ragione la convalida di un backup in cui un metodo non ha dato esito positivo verrà visualizzata come non riuscita fino a quando lo stesso metodo di convalida non da esito positivo, anche quando l'ultima operazione di convalida non utilizza il metodo non riuscito e viene completata correttamente.

Per ulteriori informazioni su come controllare lo stato di convalida, fare riferimento a "Controllo dello stato di convalida di un backup" (pag. 212).

Creazione di un piano di convalida

Per convalidare un set di backup come un'operazione di elaborazione dei dati esternamente all'host, occorre creare un piano di convalida.

Per creare un piano di convalida

1. Nella console di Cyber Protect, fare clic su **Gestione** > **Convalida**.
2. Fare clic su **Crea piano**.
   Viene aperto il modello di un piano di convalida.
3. [Facoltativo] Per modificare il nome del piano, fare clic sul nome predefinito.
4. In **Agente**, selezionare l'agente che eseguirà la convalida, quindi fare clic su **OK**.

© Acronis International GmbH, 2003-2024

Per eseguire la convalida avviando una virtual machine da un backup, selezionare un sistema con l'Agente per VMware o l'Agente per Hyper-V. In alternativa, selezionare qualsiasi virtual machine che ha accesso alla posizione del backup.

5. In **Elementi da convalidare**, selezionare i set di backup da convalidare.
   a. Selezionare l'ambito del piano, ovvero singoli set di backup o intere posizioni, facendo clic su **Posizioni** o su **Backup** nell'angolo in alto a destra.
      Se i backup selezionati sono crittografati, è necessario che usino tutti la stessa password di crittografia. Per i backup che usano password di crittografia diverse, creare piani di backup separati.
   b. Fare clic su **Aggiungi**.
   c. A seconda dell'ambito del piano di convalida, selezionare le posizioni o una posizione e i set di backup, quindi fare clic su **Fine**.
   d. Fare clic su **Fine**.
6. In **Cosa convalidare**, selezionare i backup (anche denominati punti di ripristino) nel set di backup da convalidare. Sono disponibili le seguenti opzioni:
   - **Tutti i backup**
   - **Solo l'ultimo backup**
7. In **Come eseguire la convalida**, selezionare il metodo di convalida.
   È possibile selezionare una o entrambe le opzioni seguenti:
   - **Verifica checksum**
   - **Esegui come macchina virtuale**

   Per ulteriori informazioni sui metodi, fare riferimento a "Heartbeat MV" (pag. 209).
8. [Se è selezionata **Verifica checksum**] Fare clic su **Fine**.
9. [Se è selezionata **Esegui come macchina virtuale**]. Configurare le impostazioni per questo metodo.
   a. In **Macchina di destinazione**, selezionare il tipo di virtual machine (ESXi o Hyper-V), l'host e il modello di nome del sistema, quindi fare clic su **OK**.
      Il nome predefinito è **[Nome macchina]_convalidato**.
   b. In **Datastore** (per ESXi) o **Percorso** (per Hyper-V), selezionare il datastore della virtual machine.
   c. Selezionare uno o entrambi i metodi di convalida forniti da **Esegui come macchina virtuale**:
      - **Heartbeat MV**
      - **Convalida screenshot**
   d. [Facoltativo] Fare clic su **Impostazioni VM** per cambiare le dimensioni della memoria e le connessioni di rete della virtual machine.
      Per impostazione predefinita, la macchina virtuale non è connessa a una rete e la dimensione della memoria è pari a quella della macchina originale.
   e. Fare clic su **Fine**.

© Acronis International GmbH, 2003-2024

10. [Facoltativo] Nel modello del piano di convalida, fare clic su **Pianificazione**, quindi avviare la configurazione.
11. [Se i set di backup selezionati in **Elementi da convalidare** sono crittografati] Attivare l'opzione **Password di backup**, quindi fornire la password di crittografia.
12. [Facoltativo] Per modificare le opzioni del piano, fare clic sull'icona ingranaggio.
13. Fare clic su **Crea**.

Il piano di convalida è pronto e potrà essere eseguito in base alla pianificazione configurata. Per eseguire il piano immediatamente, selezionarlo in **Gestione** > **Convalida**, quindi fare clic su **Esegui ora**.

Una volta avviato il piano, è possibile controllare le attività in esecuzione e i relativi dettagli nella console di Cyber Protect, in **Monitoraggio** > **Attività**.

Un piano di convalida può includere più backup e un backup può essere convalidato da più piani di backup.

Nota
Tutti i backup vengono elaborati in sequenza, uno alla volta, da una singola attività di convalida.

È possibile eseguire una sola attività di convalida alla volta su un determinato agente. Più attività di convalida possono essere eseguite in parallelo se vengono eseguite da agenti diversi: due attività simultanee richiedono due agenti, tre attività tre agenti, e così via.

La tabella seguente riepiloga i possibili stati dell'attività di convalida.

Risultato attività	Piano con un backup	Piano con più backup
Esito positivo	Tutti i metodi di convalida hanno esito positivo	Tutti i metodi di convalida hanno esito positivo in tutti i backup
Esito positivo con avvisi	N/D	Almeno un metodo di convalida non ha avuto esito positivo in almeno un backup
Fallito	Almeno un metodo di convalida non ha avuto esito positivo	Almeno un metodo di convalida non ha avuto esito positivo in tutti i backup

Metodi di convalida

In un piano di convalida sono disponibili i seguenti metodi di convalida:

- Verifica checksum
- Esegui come macchina virtuale
  - Heartbeat MV
  - Convalida screenshot

© Acronis International GmbH, 2003-2024

Verifica checksum

La convalida tramite verifica checksum calcola un checksum per ogni blocco dati che è possibile recuperare dal backup, e quindi lo confronta con il checksum originale di quel blocco di dati, che è stato scritto durante il processo di backup. L'unica eccezione è rappresentata dalla convalida di backup a livello di file posizionati nell'archivio nel cloud. Tali backup vengono convalidati mediante il controllo della coerenza dei metadati salvati nel backup.

La convalida tramite verifica checksum è un processo che richiede tempo, anche per i backup incrementali o differenziali, che sono di piccole dimensioni. Il motivo sta nel fatto che l'operazione di convalida non controlla solo i dati fisicamente contenuti in un determinato backup, ma tutti i dati che devono essere recuperati; ciò significa che potrebbe essere necessario convalidare anche i backup precedenti.

La riuscita di una convalida tramite verifica checksum implica un'alta probabilità di riuscita del recupero dei dati. Tuttavia, questo metodo non controlla tutti i fattori che influenzano la procedura di ripristino.

Se si esegue il backup di un sistema operativo, è consigliabile utilizzare alcune delle seguenti operazioni aggiuntive:

- Ripristino di prova da un supporto di avvio a un disco rigido sostitutivo.
- Esecuzione di una virtual machine dal backup in un ambiente ESXi o Hyper-V.
- Esecuzione di un piano di convalida nel quale è abilitato il metodo di convalida **Esegui come macchina virtuale**.

Esegui come macchina virtuale

Questo metodo funziona solo per i backup dei dischi contenenti un sistema operativo. Per utilizzare questo metodo, sono necessari un host ESXi o Hyper-V e un agente di protezione (Agente per VMware o Agente per Hyper-V) in grado di gestire l'host.

Il metodo di convalida **Esegui come macchina virtuale** è disponibile nelle varianti seguenti:

- Heartbeat MV
- Convalida screenshot

È necessario selezionarne almeno uno.

Heartbeat MV

Con questo metodo di convalida, l'agente esegue una virtual machine da un backup, quindi si connette a Strumenti VMware o a Hyper-V Integration Services e infine controlla la risposta hearthbeat per garantire il corretto avvio del sistema operativo. Se la connessione non riesce, l'agente tenta di nuovo ogni due minuti, per un totale di cinque tentativi. Se nessun tentativo ha esito positivo, la convalida non riesce.

© Acronis International GmbH, 2003-2024

Indipendentemente dal numero di piani di convalida e di backup convalidati, l'agente che esegue la convalida esegue una macchina virtuale alla volta. Non appena i risultati della convalida sono chiari, l'agente elimina la macchina virtuale e passa all'esecuzione di quella successiva.

Nota
Utilizzare questo metodo solo per la convalida dei backup di virtual machine VMware, eseguendo questi backup come virtual machine su host ESXi e i backup di virtual machine Hyper-V come virtual machine su host Hyper-V.

Convalida screenshot

Con questo metodo di convalida, l'agente esegue una virtual machine dal backup e, durante il suo avvio, acquisisce degli screenshot. Un modulo di machine intelligence (MI) controlla gli screenshot e se individua tra questi una schermata di accesso, contrassegna il backup come convalidato.

Lo screenshot viene allegato al punto di ripristino e potrà essere scaricato nella console di Cyber Protect entro un anno dalla convalida. Per ulteriori informazioni su come controllare lo screenshot, fare riferimento a "Controllo dello stato di convalida di un backup" (pag. 212).

Se sono state abilitate le notifiche per l'account utente, il sistema invia un'e-mail sullo stato di convalida del backup, alla quale è allegato lo screenshot. Per ulteriori informazioni sulle notifiche, fare riferimento a Modifica delle impostazioni di notifica per un utente.

Convalida screenshot è supportata dagli agenti a partire dalla versione 15.0.30971 (rilasciata a novembre 2022) e versioni successive.

Nota
La convalida screenshot funziona al meglio con i backup dei sistemi Windows e Linux con schermate di accesso con interfaccia grafica. Il metodo non è stato ottimizzato per i sistemi Linux con schermata di accesso da console.

Modifica del timeout per l'heartbeat della VM e convalida degli screenshot

Quando si convalida un backup eseguendolo come virtual machine, è possibile configurare il timeout tra l'avvio della virtual machine e l'invio della richiesta di heartbeat o l'acquisizione di uno screenshot.

I periodi predefiniti sono indicati di seguito.

- Un minuto: per i backup archiviati in una cartella locale o su una condivisione di rete
- Cinque minuti: per i backup archiviati nel cloud

È possibile modificare questa impostazione modificando il file di configurazione per l'Agente per VMware o per l'Agente per Hyper-V.

Per modificare il timeout

© Acronis International GmbH, 2003-2024

1. Aprire il file di configurazione per la modifica. È possibile trovare il file nelle posizioni seguenti:
   - Per l'Agente per VMware o l'Agente per Hyper-V eseguiti in Windows: `C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - Per l'Agente per VMware (appliance virtuale): `/bin/mms_settings.config`

     Per ulteriori informazioni su come accedere al file di configurazione su un'appliance virtuale, consultare "Connessioni SSH a un'appliance virtuale" (pag. 177).
2. In `<validation>`, modificare i valori per i backup locali e per i backup cloud come necessario:

```
<validation>
<run_vm>
<initial_timeout_minutes>
<local_backups>1</local_backups>
<cloud_backups>5</cloud_backups>
</initial_timeout_minutes>
</run_vm>
</validation>
```

3. Salvare il file di configurazione.
4. Riavviare l'agente.
   - [Per l'Agente per VMware o l'Agente per Hyper-V eseguiti in Windows] Eseguire i comandi seguenti nel prompt dei comandi:

```
net stop mms
```

```
net start mms
```

   - [Per l'Agente per VMware (appliance virtuale)] Riavviare la virtual machine con l'agente.

Configurazione del numero di nuovi tentativi in caso di errore

Per ottimizzare il numero di convalide riuscite, è possibile configurare un numero di nuovi tentativi automatici per le operazioni di convalida che si concludono con un errore.

Per configurare i nuovi tentativi automatici

1. Durante la creazione di un piano di convalida, fare clic sull'icona ingranaggio,
2. Nel pannello **Opzioni**, selezionare **Gestione degli errori**.
3. In **Riprova se si verifica un errore**, fare clic su **Sì**.
4. In **Numero di tentativi**, configurare il numero massimo di tentativi da eseguire se si verifica un errore.

   L'operazione di convalida verrà eseguita di nuovo fino a quando non viene completata correttamente o fino a quando non viene raggiunto il numero massimo di nuovi tentativi.
5. In **Intervallo tra i tentativi**, configurare il timeout tra due tentativi consecutivi.
6. Fare clic su **Fine**.

© Acronis International GmbH, 2003-2024

Controllo dello stato di convalida di un backup

È possibile controllare lo stato di convalida del backup nella scheda **Dispositivi** o nella scheda **Archivio di backup**.

È inoltre possibile visualizzare lo stato di ogni metodo di convalida e scaricare lo screenshot acquisito con il metodo di convalida dello screenshot.

Per ulteriori informazioni sul funzionamento degli stati, fare riferimento a "Stato di convalida" (pag. 206).

Per controllare lo stato di convalida di un backup

Dispositivi

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare i workload di cui controllare lo stato di convalida del backup, quindi fare clic su **Ripristino**.
3. [Se sono disponibili più posizioni di backup] Selezionare la posizione del backup.
4. Selezionare il backup di cui controllare lo stato.

Archiviazione di backup

1. Nella console di Cyber Protect, passare a **Archivio di backup**.
2. Selezionare la posizione in cui è archiviato il set di backup.
3. Selezionare il set di backup, quindi fare clic su **Mostra backup**.
4. Selezionare il backup di cui controllare lo stato di convalida.

Pulizia

L'operazione di pulizia consente di eliminare i backup obsoleti in base a regole di conservazione ed è applicabile solo agli agenti e ai workload e non ai backup cloud-to-cloud (che possono essere eliminati solo manualmente).

Nota
Questa funzionalità è disponibile nei tenant cliente per i quali la quota di **Advanced Backup - Server** o la quota di **Advanced Backup - NAS** è abilitata come parte del pacchetto Advanced Backup.

Posizioni supportate

Per i piani di pulizia sono supportate tutte le posizioni di backup, ad eccezione delle cartelle NFS e di Secure Zone.

Per creare un piano di pulizia

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, fare clic su **Gestione** > **Pulizia**.
2. Fare clic su **Crea piano**.
3. In **Agente**, selezionare l'agente che eseguirà la pulizia.
   È possibile selezionare qualsiasi agente che abbia accesso alla posizione del backup.
4. In **Elementi da pulire**, selezionare gli archivi o le posizioni di backup da pulire.
   È possibile alternare la selezione degli archivi e delle posizioni tramite l'opzione **Posizioni**/**Backup** nell'angolo in alto a destra.
   Se si selezionano più archivi crittografati, la loro password di crittografia deve essere la stessa. Per gli archivi che usano password di crittografia diverse, creare piani di backup separati.
5. In **Pianificazione**, configurare la pianificazione della pulizia.
6. In **Regole di conservazione**, specificare le regole di conservazione.
   Sono disponibili le seguenti opzioni:
   - **Per numero di backup**
   - **Per durata backup** (impostazioni distinte per backup mensili, settimanali, giornalieri e orari)
   - **Per dimensione totale dei backup**
7. [Se sono stati selezionati archivi crittografati in **Elementi da replicare**] Attivare l'opzione **Password di backup**, quindi fornire la password di crittografia.
8. [Facoltativo] Per modificare le opzioni del piano, fare clic sull'icona ingranaggio e configurare le opzioni come richiesto.
9. Fare clic su **Crea**.

Conversione in macchina virtuale

La conversione in macchina virtuale è disponibile solo per i backup del disco. Se il backup include il volume di sistema e contiene tutte le informazioni necessarie per l'avvio del sistema operativo, la macchina virtuale che ne risulta potrà avviarsi autonomamente. In caso contrario è possibile aggiungere i dischi virtuali a un'altra macchina virtuale.

Nota
Non è possibile eseguire il backup delle VM replicate tramite la funzionalità nativa di replica delle VM di Scale Computing.

È possibile creare un piano distinto per la conversione in virtual machine ed eseguire tale piano manualmente o secondo una pianificazione.

Per informazioni su prerequisiti e limiti, fare riferimento a "Informazioni sulla conversione" (pag. 215).

Nota
Questa funzionalità è disponibile nei tenant cliente per i quali la quota di **Advanced Backup - Server** o la quota di **Advanced Backup - NAS** è abilitata come parte del pacchetto Advanced Backup.

© Acronis International GmbH, 2003-2024

Per creare un piano per la conversione in macchina virtuale

1. Fare clic su **Gestione** > **Conversione in VM**.
2. Fare clic su **Crea piano**.
   Il software visualizza un nuovo modello di piano.
3. [Facoltativo] Per modificare il nome del piano, fare clic sul nome predefinito.
4. In **Converti in**, selezionare il tipo di macchina virtuale di destinazione. **È possibile selezionare uno tra i seguenti**:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **File VHDX**

   Nota
   Per risparmiare spazio di archiviazione, ogni conversione in file VHDX o VMware Workstation sovrascrive i file VHDX/VMDK nella posizione di destinazione creati durante la conversione precedente.

5. Eseguire una delle seguenti operazioni:
   - [Per VMware ESXi, Hyper-V e Scale Computing HC3] Fare clic su **Host**, selezionare l'host di destinazione e specificare il modello di nome del nuovo sistema.
   - [Per altri tipi di virtual machine] In **Percorso**, specificare dove salvare i file della virtual machine e il modello del nome del file.

   Il nome predefinito è **[Nome macchina]_convertito**.
6. Fare clic su **Agente**, quindi selezionare l'agente che eseguirà la conversione.
7. Fare clic su **Elementi da convertire**, quindi selezionare i backup che saranno convertiti in macchine virtuali da questo piano.
   È possibile alternare la selezione dei backup e la selezione di intere posizioni tramite l'opzione **Posizioni** / **Backup** nell'angolo in alto a destra.
   Se i backup selezionati sono crittografati, è necessario che usino tutti la stessa password di crittografia. Per i backup che usano password di crittografia diverse, creare piani di backup separati.
8. [Solo per VMware ESXi e Hyper-V] Fare clic su **Datastore** per ESXi o su **Percorso** per Hyper-V, quindi selezionare il datastore (archivio) per la macchina virtuale.
9. [Solo per VMware ESXi e Hyper-V] Selezionare la modalità di provisioning del disco.
   L'impostazione predefinita è **Thin** per VMware ESXi e **Espansione dinamica** per Hyper-V.
10. [Facoltativo] [Per VMware ESXi, Hyper-V e Scale Computing HC3] Per cambiare la dimensione della memoria, il numero di processori e le connessioni di rete della virtual machine fare clic su **Impostazioni VM**.
11. [Facoltativo] Fare clic su **Pianificazione**, quindi cambiare la pianificazione.

© Acronis International GmbH, 2003-2024

12. Se i backup selezionati in **Elementi da convertire** sono crittografati, attivare l'opzione **Password di backup**, quindi fornire la password di crittografia. Altrimenti, ignorare questo passaggio.
13. [Facoltativo] Per modificare le opzioni del piano, fare clic sull'icona ingranaggio.
14. Fare clic su **Crea**.

Informazioni sulla conversione

Tipi di macchina virtuale supportati

La conversione di un backup in una macchina virtuale può essere eseguita dallo stesso agente che ha creato il backup o da un altro agente.

Per eseguire una conversione a VMware ESXi, Hyper-V o Scale Computing HC3, è necessario, rispettivamente, un host ESXi, Hyper-V o Scale Computing HC3 e un agente di protezione (Agente per VMware, Agente per Hyper-V o Agente per Scale Computing HC3) che gestisca tale host.

La conversione in file VHDX presuppone che i file vengano connessi come dischi virtuali a una macchina virtuale Hyper-V.

La tabella seguente riepiloga i tipi di virtual machine che è possibile creare con l'operazione **Converti in VM**. Le righe della tabella mostrano il tipo di virtual machine convertite. Le colonne mostrano gli agenti che eseguono la conversione.

Tipo di MV	Agente per VMware	Agente per Hyper-V	Agente per Windows	Agente per Linux	Agente per Mac	Agente per Scale Computing HC3	Agente per oVirt (KVM)	Agente per Virtuozzo Hybrid Infrastructure	Agente per Virtuozzo
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–
VMware Workstation	+	+	+	+	–	–	–	–	–
File VHDX	+	+	+	+	–	–	–	–	–
Scale Computing HC3	–	–	–	–	–	+	–	–	–

© Acronis International GmbH, 2003-2024

Limitazioni

- I backup archiviati su NFS non possono essere convertiti.
- I backup archiviati nella Secure Zone possono essere convertiti esclusivamente dall'agente in esecuzione nello stesso sistema.
- I backup che contengono volumi logici Linux (LVM) possono essere convertiti solo se sono stati creati con l'Agente per VMware, l'Agente per Hyper-V e l'Agente per Scale Computing HC3 e se vengono indirizzati allo stesso hypervisor. La conversione tra hypervisor non è supportata.
- Quando i backup di una macchina Windows vengono convertiti in workstation VMware o file VHDX, le macchine virtuali risultanti ereditano il tipo di CPU dalla macchina che ha eseguito la conversione. I driver della CPU corrispondenti vengono quindi installati nel sistema operativo. Di conseguenza, se il sistema guest viene avviato su un host con un tipo di CPU differente verrà visualizzato un errore di driver. È necessario aggiornare il driver manualmente.

Confronto tra conversione regolare in virtual machine ed esecuzione di una virtual machine da un backup

Entrambe le attività consentono di ottenere una macchina virtuale che può essere avviata in pochi secondi in caso di arresto della macchina originale.

La conversione regolare in virtual machine impegna risorse di CPU e memoria. I file della macchina virtuale occupano sempre spazio nel datastore (spazio di archiviazione). Ciò può rivelarsi poco pratico se per la conversione viene utilizzato un host di produzione. Tuttavia, le prestazioni della macchina virtuale risultano limitate solo dalle risorse dell'host.

L'esecuzione di una virtual machine da un backup consuma risorse solo mentre la virtual machine è in esecuzione. Il datastore (spazio di archiviazione) è necessario soltanto per conservare le modifiche apportate ai dischi virtuali. La macchina virtuale può tuttavia risultare più lenta, perché l'host non accede direttamente ai dischi virtuali ma comunica con l'agente che legge i dati dal backup. Inoltre la macchina virtuale è temporanea.

Funzionamento della conversione regolare in virtual machine

Il funzionamento della conversione regolare dipende da dove si sceglie di creare la virtual machine.

- **Se si sceglie di salvare la macchina virtuale come set di file:** ogni conversione crea nuovamente la macchina virtuale da zero.
- **Se si sceglie di creare la virtual machine su un server di virtualizzazione:** quando si esegue la conversione di un backup incrementale o differenziale, il software aggiorna in modo incrementale la virtual machine esistente invece di crearla nuovamente. Tale conversione di solito è più rapida. Consente di risparmiare traffico di rete e risorse CPU dell'host che esegue la conversione. Se l'aggiornamento della macchina virtuale non è possibile, il software la crea nuovamente da zero.

Di seguito è indicata una descrizione dettagliata di entrambi i casi.

© Acronis International GmbH, 2003-2024

Se si sceglie di salvare la macchina virtuale come set di file

Come conseguenza della prima conversione, verrà creata una nuova macchina virtuale. Ogni conversione successiva creerà nuovamente questa macchina da zero. Prima di tutto, la vecchia macchina verrà rinominata temporaneamente. Quindi, verrà creata una nuova macchina virtuale con il nome precedente della macchina vecchia. Se l'operazione viene eseguita correttamente, la vecchia macchina viene eliminata. Se questa operazione fallisce, la nuova macchina viene eliminata e alla vecchia macchina viene fornito il suo nome precedente. In questo modo, la conversione termina sempre con una sola macchina. Tuttavia, durante la conversione è necessario spazio di archiviazione aggiuntivo per archiviare la vecchia macchina.

Se si sceglie di creare la macchina virtuale su un server di virtualizzazione

La prima conversione crea una nuova macchina virtuale. Ogni conversione successiva funziona come segue:

- Se è stato creato un *backup completo* dall'ultima conversione, la virtual machine viene creata nuovamente da zero, come descritto precedentemente in questa sezione.
- Altrimenti, la macchina virtuale esistente viene aggiornata per riflettere le modifiche dall'ultima conversione. Se l'aggiornamento non è possibile (per esempio, se si eliminano gli snapshot intermedi, vedere di seguito), la macchina virtuale è creata nuovamente da zero.

Snapshot intermedi

Per poter eseguire in sicurezza l'aggiornamento della virtual machine convertita, il software archivia uno snapshot intermedio dell'hypervisor del sistema. Tale snapshot è denominato **Replica...** e deve essere conservato.

Lo snapshot **Replica...** corrisponde al risultato dell'ultima conversione. È possibile passare a questo snapshot se si vuole riportare il sistema al relativo stato; per esempio, se si lavorava con il sistema e si desidera scartare le modifiche che sono state apportate.

Per le virtual machine Scale Computing HC3 convertite, viene creata un'**Utility Snapshot** aggiuntiva. Verrà utilizzata solo dal servizio Cyber Protection.

Piani e moduli di protezione

Per proteggere i dati, è necessario creare i piani di protezione e quindi applicarli ai workload.

Un piano di protezione è composto da diversi moduli di protezione. Per creare piani di protezione che soddisfano le esigenze specifiche dell'utente, è possibile abilitare i moduli necessari e configurare le rispettive impostazioni.

Sono disponibili i moduli seguenti:

© Acronis International GmbH, 2003-2024

- Backup. Consente di eseguire il backup delle origini dati nel cloud storage e in locale.
- "Implementazione del disaster recovery" (pag. 749). Consente di avviare copie esatte dei sistemi nel sito cloud e di trasferire i workload dai sistemi originali danneggiati ai server di ripristino nel cloud.
- Protezione antivirus e anti-malware. Controlla i workload utilizzando una soluzione anti-malware integrata.
- Endpoint Detection and Response (EDR). Rileva qualsiasi attività sospetta in un workload, inclusi gli attacchi passati inosservati, e genera un elenco di problemi che consente di comprendere come si è verificato un attacco e come impedire che accada di nuovo.
- Filtro URL. Protegge i sistemi dalle minacce provenienti da Internet, bloccando l'accesso agli URL e ai contenuti da scaricare potenzialmente dannosi.
- Windows Defender Antivirus. Consente di gestire le impostazioni di Windows Defender Antivirus per proteggere l'ambiente.
- Microsoft Security Essentials. Consente di gestire le impostazioni di Microsoft Security Essentials per proteggere l'ambiente.
- Valutazione delle vulnerabilità. Controlla le vulnerabilità dei sistemi operativi Windows, Linux, macOS e dei prodotti Microsoft e macOS di terze parti installati nei sistemi e invia all'utente le notifiche pertinenti.
- Gestione patch. Consente di installare patch e aggiornamenti per i sistemi operativi Windows, Linux, macOS e per i prodotti Microsoft e macOS di terze parti installati nei sistemi, per risolvere le vulnerabilità individuate.
- Mappa di protezione dati. Consente di individuare i dati per monitorare lo stato di protezione dei file più importanti.
- Controllo dispositivo. Consente di specificare i dispositivi il cui utilizzo è consentito o proibito sui sistemi dell'utente.
- Advanced Data Loss Prevention. Previene la perdita di dati sensibili da dispositivi periferici (come stampanti o storage rimovibili) o tramite trasferimenti su rete interna ed esterna, utilizzando una policy di flusso dei dati.

Creazione di un piano di protezione

È possibile creare un piano di protezione con le procedure indicate di seguito:

- Nella scheda **Dispositivi**. Selezionare uno o più workload da proteggere, quindi creare un piano di protezione dedicato.
- Nella scheda **Gestione** > **Piani di protezione**. Creare un piano di protezione, quindi selezionare uno o più workload ai quali applicare il piano.

Quando viene creato un piano di protezione, vengono visualizzati solo i moduli applicabili al tipo di workload dell'utente.

È possibile applicare un piano di protezione a più di un workload. È inoltre possibile applicare più piani di protezione allo stesso workload. Per ulteriori informazioni sui possibili conflitti, consultare "Risoluzione dei conflitti tra piani" (pag. 224).

© Acronis International GmbH, 2003-2024

Per creare un piano di protezione

Dispositivi

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare i workload da proteggere, quindi fare clic su **Proteggi**.
3. [Se sono già presenti piani applicati] Fare clic su **Aggiungi piano**.
4. Fare clic su **Crea piano** > **Protezione**.
   Viene visualizzato il pannello del piano di protezione.
5. [Facoltativo] Per rinominare il piano di protezione, fare clic sull'icona a matita, quindi inserire il nuovo nome.
6. [Facoltativo] Per abilitare o disabilitare un modulo nel piano, fare clic sull'opzione accanto al nome del modulo.
7. [Facoltativo] Per configurare un modulo, fare clic per espanderlo, quindi modificare le impostazioni secondo necessità.
8. Al termine, fare clic su **Crea**.

Nota
Per creare un piano di protezione con crittografia, specificare una password di crittografia. Per ulteriori informazioni, consultare "Crittografia" (pag. 449).

Gestione > Piani di protezione

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di protezione**.
2. Fare clic su **Crea piano**.
   Viene aperto il modello di un piano di protezione.
3. [Facoltativo] Per rinominare il piano di protezione, fare clic sull'icona a matita, quindi inserire il nuovo nome.
4. [Facoltativo] Per abilitare o disabilitare un modulo nel piano, fare clic sull'opzione accanto al nome del modulo.
5. [Facoltativo] Per configurare un modulo, fare clic per espanderlo, quindi modificare le impostazioni secondo necessità.
6. [Facoltativo] Per selezionare i workload ai quali applicare il piano, fare clic su **Aggiungi periferiche**.

Nota
È possibile creare un piano senza applicarlo a nessun workload. I workload possono essere aggiunti in un secondo momento, modificando il piano. Per ulteriori informazioni su come aggiungere un workload a un piano, consultare "Applicazione di un piano di protezione a un workload" (pag. 221).

7. Al termine, fare clic su **Crea**.

© Acronis International GmbH, 2003-2024

Nota
Per creare un piano di protezione con crittografia, specificare una password di crittografia. Per ulteriori informazioni, consultare "Crittografia" (pag. 449).

Per eseguire un modulo su richiesta (ad esempio **Backup**, **Protezione antivirus e anti-malware**, **Vulnerability assessment**, **Patch Management** o **Mappa di protezione dati**) fare clic su **Esegui ora**.

Guardare il video dimostrativo Creazione del primo piano di protezione.

Per ulteriori informazioni sul modulo Disaster recovery, consultare "Creare un piano di protezione di disaster recovery" (pag. 755).

Per ulteriori informazioni sul modulo Controllo dispositivo, consultare "Lavorare con il modulo Controllo dispositivo" (pag. 371).

Azioni eseguibili con i piani di protezione

Dopo aver creato un piano di protezione, è possibile eseguire le azioni seguenti:

- Applicare un piano a un workload o a un gruppo di dispositivi.
- Rinominare un piano.
- Modificare un piano.
  È possibile abilitare e disabilitare i moduli di un piano e modificarne le impostazioni.
- Abitare o disabilitare un piano.
  Un piano disabilitato non viene eseguito nei workload ai quali è applicato.
  Questa azione è utile agli amministratori che intendono proteggere lo stesso workload con lo stesso piano in un secondo momento. Il piano non viene revocato dal workload ed è possibile ripristinare rapidamente la protezione abilitando nuovamente il piano.
- Revocare un piano da un workload.
  Un piano revocato non viene più applicato al workload.
  Questa azione è utile agli amministratori che non intendono avvalersi di nuovo della protezione rapida per lo stesso workload con lo stesso piano. Per ripristinare la protezione fornita da un piano revocato, è necessario conoscere il nome del piano, selezionarlo dall'elenco dei piani disponibili e quindi riapplicare il piano al rispettivo workload.
- Arrestare un piano.
  Questa azione blocca tutte le operazioni di backup in esecuzione su tutti i workload ai quali il piano è applicato. I backup verranno di nuovo avviati in base alla pianificazione configurata nel piano.
  Questa azione non interessa la scansione anti-malware, che proseguirà secondo la pianificazione configurata nel piano.
- Clonare un piano.

© Acronis International GmbH, 2003-2024

È possibile creare una copia esatta di un piano esistente. Il nuovo piano non viene assegnato ad alcun workload.

- Esportare e importare un piano.

  È possibile esportare un piano in un file JSON, che potrà essere reimportato in un secondo momento. In questo modo non è necessario creare manualmente un nuovo piano e configurarne le impostazioni.

  Nota
  È possibile importare i piani di protezione creati con Cyber Protection 9.0 (rilasciata a marzo 2020) e versioni successive. I piani creati con le versioni precedenti del prodotto non sono compatibili con Cyber Protection versione 9.0 e successive.

- Controllare i dettagli di un piano.
- È possibile controllare le attività e gli avvisi relativi a un piano.
- Eliminare un piano.

Applicazione di un piano di protezione a un workload

Per garantirne la protezione di un workload, è necessario applicare a questo un piano di protezione.

Il piano può essere applicato dalla scheda **Dispositivi** e dalla scheda **Gestione** > **Piani di protezione**.

Dispositivi

1. Selezionare uno o più workload da proteggere.
2. Fare clic su **Proteggi**.
3. [Se ai workload selezionati è già applicato un piano di protezione] Fare clic su **Aggiungi piano**.
4. Viene visualizzato un elenco dei piani di protezione disponibili.
5. Selezionare il piano di protezione da applicare, quindi fare clic su **Applica**.

Gestione > Piani di protezione

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di protezione**.
2. Selezionare il piano di protezione da applicare.
3. Fare clic su **Modifica**.
4. Fare clic su **Gestisci dispositivi**.
5. Nella finestra **Dispositivi**, fare clic su **Aggiungi**.
6. Selezionare i workload ai quali applicare il piano, quindi fare clic su **Aggiungi**.
7. Nella finestra **Dispositivi**, fare clic su **Fine**.
8. Nel pannello del piano di protezione, fare clic su **Salva**.

© Acronis International GmbH, 2003-2024

Per informazioni su come applicare un piano di protezione a un gruppo di dispositivi, consultare "Applicazione di un piano a gruppo" (pag. 369).

Modifica di un piano di protezione

Quando si modifica un piano, è possibile abilitare e disabilitare i moduli che questo contiene e modificarne le impostazioni.

È possibile modificare un piano di protezione per tutti i workload a cui è applicato o solo per alcuni workload selezionati.

È possibile modificare un piano dalla scheda **Dispositivi** e dalla scheda **Gestione** > **Piani di protezione**.

Dispositivi

1. Selezionare uno o più workload ai quali è applicato il piano.
2. Fare clic su **Proteggi**.
3. Selezionare il piano di protezione da modificare.
4. Fare clic sull'icona dei puntini di sospensione accanto al nome del piano, quindi fare clic su **Modifica**.
5. Fare clic sul modulo da modificare, quindi configurarne le impostazioni secondo necessità.
6. Fare clic su **Salva**.
7. [Se non sono stati selezionati tutti i workload ai quali è applicato il piano] Selezionare l'ambito della modifica:
   - Per modificare il piano di protezione per tutti i workload a cui è applicato, fare clic su **Applica le modifiche a questo piano di protezione (verranno modificati altri dispositivi)**.
   - Per modificare il piano solo per i workload selezionati, fare clic su **Crea un nuovo piano di protezione solo per i dispositivi selezionati**.

     Il piano esistente viene revocato dai workload selezionati. Viene creato un nuovo piano di protezione con le impostazioni configurate che sarà quindi applicato a questi workload.

Gestione > Piani di protezione

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di protezione**.
2. Selezionare il piano di protezione da modificare.
3. Fare clic su **Modifica**.
4. Fare clic sui moduli da modificare, quindi configurarne le impostazioni secondo necessità.
5. Fare clic su **Salva**.

Nota
La modifica apportata a un piano dalla scheda **Gestione** > **Piani di protezione** ha effetto su tutti i workload ai quali il piano è applicato.

© Acronis International GmbH, 2003-2024

Revoca di un piano di protezione

Quando si revoca un piano, questo viene rimosso da uno o più workload. Il piano continuerà a proteggere gli altri workload a cui è applicato.

Il piano può essere revocato dalla scheda **Dispositivi** e dalla scheda **Gestione** > **Piani di protezione**.

Dispositivi

1. Selezionare i workload da cui revocare il piano.
2. Fare clic su **Proteggi**.
3. Selezionare il piano di protezione da revocare.
4. Fare clic sull'icona dei puntini di sospensione accanto al nome del piano, quindi fare clic su **Revoca**.

Gestione > Piani di protezione

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di protezione**.
2. Selezionare il piano di protezione da revocare.
3. Fare clic su **Modifica**.
4. Fare clic su **Gestisci dispositivi**.
5. Nella finestra **Dispositivi**, selezionare i workload da cui revocare il piano.
6. Fare clic su **Rimuovi**.
7. Nella finestra **Dispositivi**, fare clic su **Fine**.
8. Nel modello del piano di protezione, fare clic su **Salva**.

Abilitazione o disabilitazione di un piano di protezione

Un piano abilitato è attivo e viene eseguito sui workload ai quali è applicato. Un piano disabilitato non è attivo, il che significa che è ancora applicato ai workload ma non viene eseguito su questi.

Quando si abilita o disabilita un piano di protezione dalla scheda **Dispositivi**, l'azione ha effetto solo sui workload selezionati.

Quando si abilita o disabilita un piano di protezione dalla scheda **Gestione** > **Piani di protezione**, l'azione ha effetto su tutti i workload ai quali il piano è applicato. È inoltre possibile abilitare o disabilitare più piani di protezione.

Dispositivi

1. Selezionare i workload da cui disabilitare i piani.
2. Fare clic su **Proteggi**.
3. Selezionare il piano di protezione da disabilitare.

© Acronis International GmbH, 2003-2024

4. Fare clic sull'icona dei puntini di sospensione accanto al nome del piano, quindi fare clic rispettivamente su **Abilita** o su **Disabilita**.

Gestione > Piani di protezione

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di protezione**.
2. Selezionare uno o più piani di protezione da abilitare o disabilitare.
3. Fare clic su **Modifica**.
4. Fare clic rispettivamente su **Abilita** o **Disabilita**.

Nota
Questa azione non ha effetto sui piani di protezione che sono già nello stato desiderato. Se, ad esempio, la selezione include sia piani abilitati che piani disabilitati, facendo clic su **Abilita** verranno abilitati tutti i piani selezionati.

Eliminazione di un piano di protezione

Quando si elimina un piano, questo viene revocato da tutti i workload e rimosso dalla console di Cyber Protect.

Il piano può essere eliminato dalla scheda **Dispositivi** e dalla scheda **Gestione** > **Piani di protezione**.

Dispositivi

1. Selezionare qualsiasi workload a cui è applicato il piano di protezione che si desidera eliminare.
2. Fare clic su **Proteggi**.
3. Selezionare il piano di protezione da eliminare.
4. Fare clic sull'icona dei puntini di sospensione accanto al nome del piano, quindi fare clic su **Elimina**.

Gestione > Piani di protezione

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di protezione**.
2. Selezionare il piano di protezione da eliminare.
3. Fare clic su **Elimina**.
4. Confermare la scelta effettuata selezionando la casella di controllo **Confermo l'eliminazione del piano**, quindi fare clic su **Elimina**.

Risoluzione dei conflitti tra piani

È possibile applicare più piani di protezione allo stesso workload. Ad esempio, è possibile applicare un piano di protezione nel quale è stato configurato solo il modulo **Antivirus e anti-malware** e un altro piano di protezione in cui è stato abilitato e configurato solo il modulo **Backup**.

© Acronis International GmbH, 2003-2024

È possibile combinare piani di protezione nei quali sono abilitati moduli differenti. È inoltre possibile combinare più piani di protezione nei quali è abilitato solo il modulo **Backup**. Tuttavia, se qualsiasi altro modulo è abilitato in più di un piano si verifica un conflitto. Per applicare il piano, è innanzitutto necessario risolvere il conflitto.

Conflitto tra un piano nuovo e uno esistente

Se un nuovo piano entra in conflitto con un piano esistente, è possibile risolvere il conflitto in uno dei modi seguenti:

- Creare un nuovo piano, applicarlo e quindi disabilitare il piano esistente che è in conflitto con il nuovo.
- Creare un nuovo piano e disabilitarlo.

Conflitto tra un piano individuale e un piano di gruppo

Se un piano di protezione individuale entra in conflitto con un piano di gruppo applicato a un gruppo di dispositivi, è possibile risolvere il conflitto in uno dei modi seguenti:

- Rimuovere il workload dal gruppo di dispositivi, quindi applicare a questo il piano di protezione individuale.
- Modificare il piano di gruppo esistente o applicare un nuovo piano di gruppo al gruppo di dispositivi.

Problema con le licenze

Un modulo di un piano di protezione può richiedere l'assegnazione di una quota di servizio specifica al workload protetto. Se la quota di servizio assegnata non è appropriata, non sarà possibile eseguire, aggiornare o applicare il piano di protezione nel quale il rispettivo modulo è abilitato.

Per risolvere un problema con le licenze, eseguire una delle seguenti operazioni:

- Disabilitare il modulo che non è supportato dalla quota di servizio attualmente assegnata e continuare a utilizzare il piano di protezione.
- Modificare manualmente la quota di servizio assegnata. Per istruzioni su come eseguire questa operazione, consultare "Modifica della quota di servizio dei sistemi" (pag. 189).

Piani di protezione predefiniti

Un piano di protezione predefinito è un modello preconfigurato che è possibile applicare ai workload per garantire una protezione rapida. Utilizzando un piano di protezione predefinito, non è necessario creare nuovi piani di protezione da zero.

Quando un piano predefinito viene applicato per la prima volta, il modello viene copiato nel tenant ed è possibile modificare i moduli del piano e le relative impostazioni.

Sono disponibili i piani predefiniti seguenti:

© Acronis International GmbH, 2003-2024

- Cyber Protect Essentials

  Questo piano fornisce funzionalità di protezione di base e backup a livello di file.
- Lavoratori da remoto

  Questo piano è ottimizzato per gli utenti che lavorano da remoto. Prevede le attività più frequenti (backup, protezione anti-malware, valutazione delle vulnerabilità), azioni di protezione più rigide e opzioni per l'ottimizzazione delle prestazioni e del consumo energetico.
- Lavoratori in ufficio (Antivirus di terze parti)

  Questo piano è ottimizzato per gli utenti che lavorano in ufficio e preferiscono utilizzare un software antivirus di terze parti. In questo piano, il modulo **Protezione anti-malware e antivirus** è disabilitato.
- Lavoratori in ufficio (Acronis Antivirus)

  Questo piano è ottimizzato per gli utenti che lavorano in ufficio e preferiscono utilizzare un software antivirus di Acronis.

Confronto tra i piani di protezione predefiniti

Moduli e opzioni	**Piani di protezione predefiniti**			
	Cyber Protect Essentials	**Lavoratori da remoto**	**Lavoratori in ufficio (Antivirus di terze parti)**	**Lavoratori in ufficio (Acronis Antivirus)**
Backup	Disponibili	Disponibili	Disponibili	Disponibili
Cosa includere nel backup Elementi di cui eseguire il backup	File/cartelle [Cartella Tutti i profili]	Intera macchina	Intera macchina	Intera macchina
Protezione continua dei dati (CDP)	Disabilitato	Abilitato	Disabilitato	Disabilitato
Dove eseguire il backup	Archiviazione nel cloud	Archiviazione nel cloud	Archiviazione nel cloud	Archiviazione nel cloud
Pianificazione	Da lunedì a venerdì alle 11:00 PM	Da lunedì a venerdì alle 12:00 AM Opzioni e condizioni di avvio aggiuntive abilitate: • Se la macchina è spenta,	Da lunedì a venerdì alle 11:00 PM	Da lunedì a venerdì alle 11:00 PM

© Acronis International GmbH, 2003-2024

Moduli e opzioni	Piani di protezione predefiniti			
	Cyber Protect Essentials	**Lavoratori da remoto**	**Lavoratori in ufficio (Antivirus di terze parti)**	**Lavoratori in ufficio (Acronis Antivirus)**
		esegui le attività mancanti all'avvio della macchina • Riattiva dalla modalità di sospensione o ibernazione per avviare un backup pianificato • Risparmia carica della batteria: Non avviare se è attiva l'alimentazione con batteria • Non avviare se è attiva una connessione a consumo		
Schema di backup	Sempre incrementale	Sempre incrementale	Sempre incrementale	Sempre incrementale
Tempo di conservazione	Conserva i backup all'infinito	Mensilmente: 12 mesi Settimanalmente: 4 settimane Giornalmente: 7 giorni	Mensilmente: 12 mesi Settimanalmente: 4 settimane Giornalmente: 7 giorni	Mensilmente: 12 mesi Settimanalmente: 4 settimane Giornalmente: 7 giorni
Opzioni di backup	Opzioni predefinite	Opzioni predefinite, più: • Prestazioni e finestra di backup (insieme verde): Priorità CPU:	Opzioni predefinite	Opzioni predefinite

© Acronis International GmbH, 2003-2024

Moduli e opzioni	Piani di protezione predefiniti			
	Cyber Protect Essentials	**Lavoratori da remoto**	**Lavoratori in ufficio (Antivirus di terze parti)**	**Lavoratori in ufficio (Acronis Antivirus)**
		Basso Velocità output: 50%		
Protezione antivirus e anti-malware	Disponibili	Disponibili	Non disponibile	Disponibili
Active Protection	Disattivato	Disattivato	–	Disattivato
Advanced Antimalware	Attiva	Attiva	–	Attiva
Protezione delle cartelle di rete	Attiva	Attiva	–	Attiva
Protezione lato server	Disattivato	Disattivato	–	Disattivato
Autoprotezione	Attiva	Attiva	–	Attiva
Individuazione dei processi di mining delle criptovalute	Attiva	Attiva	–	Attiva
Quarantena	Rimuovi i file posti in quarantena dopo 30 giorni	Rimuovi i file posti in quarantena dopo 30 giorni	–	Rimuovi i file posti in quarantena dopo 30 giorni
Motore comportamentale	Quarantena	Quarantena	–	Quarantena
Prevenzione degli exploit	Notifica e arresta il processo	Notifica e arresta il processo	–	Notifica e arresta il processo
Protezione in tempo reale	Quarantena	Quarantena	–	Quarantena
Pianifica scansione	Scansione rapida:Quarantena Alle 02:20 PM, da domenica a sabato Scansione completa:Disattivata	Scansione rapida: Disattivato Scansione completa: Quarantena Alle 01:55 PM, da domenica a	–	Scansione rapida: Quarantena Alle 02:20 PM, da domenica a sabato Scansione completa:

© Acronis International GmbH, 2003-2024

Moduli e opzioni	Piani di protezione predefiniti			
	Cyber Protect Essentials	**Lavoratori da remoto**	**Lavoratori in ufficio (Antivirus di terze parti)**	**Lavoratori in ufficio (Acronis Antivirus)**
		sabato Opzioni e condizioni di avvio aggiuntive abilitate: • Se la macchina è spenta, esegui le attività mancanti all'avvio della macchina • Riattiva dalla modalità di sospensione o ibernazione per avviare un backup pianificato • Risparmia carica della batteria: Non avviare se è attiva l'alimentazione con batteria		Disattivato
Esclusioni	Nessuno	Nessuno	–	Nessuno
Filtro URL	Disponibili	Disponibili	Disponibili	Disponibili
Accesso a siti web dannosi	Chiedi sempre all'utente	Blocca	Chiedi sempre all'utente	Chiedi sempre all'utente
Categorie da filtrare	Opzioni predefinite	Opzioni predefinite	Opzioni predefinite	Opzioni predefinite
Esclusioni	Nessuno	Nessuno	Nessuno	Nessuno
Valutazione delle vulnerabilità	Disponibili	Disponibili	Disponibili	Disponibili

© Acronis International GmbH, 2003-2024

Moduli e opzioni	Piani di protezione predefiniti			
	Cyber Protect Essentials	**Lavoratori da remoto**	**Lavoratori in ufficio (Antivirus di terze parti)**	**Lavoratori in ufficio (Acronis Antivirus)**
Ambito di valutazione delle vulnerabilità	Prodotti Microsoft, prodotti di terze parti per Windows	Prodotti Microsoft, prodotti di terze parti per Windows	Prodotti Microsoft, prodotti di terze parti per Windows	Prodotti Microsoft, prodotti di terze parti per Windows
Pianificazione	Alle 01:15 PM, solo il lunedì	Alle 02:20 PM, solo il lunedì	Alle 01:15 PM, solo il lunedì	Alle 01:15 PM, solo il lunedì
Gestione patch	Disponibili	Disponibili	Disponibili	Disponibili
Prodotti Microsoft	Tutti gli aggiornamenti	Tutti gli aggiornamenti	Tutti gli aggiornamenti	Tutti gli aggiornamenti
Prodotti di terze parti per Windows	Solo aggiornamenti principali	Solo aggiornamenti principali	Solo aggiornamenti principali	Solo aggiornamenti principali
Pianificazione	Alle 03:10 PM, solo il lunedì	Alle 02:20 PM, da lunedì a venerdì	Alle 03:10 PM, solo il lunedì	Alle 03:10 PM, solo il lunedì
Backup precedente all'aggiornamento	Disattivato	Attiva	Disattivato	Disattivato
Mappa di protezione dati	Non disponibile	Disponibili	Disponibili	Disponibili
Regole di estensione ed eccezione	–	Opzioni predefinite ed estensioni aggiuntive seguenti: **Immagini** • .jpeg • .jpg • .png • .gif • .bmp • .ico • .wbmp • .xcf • .psd • .tiff	Opzioni predefinite (66 estensioni da rilevare)	Opzioni predefinite (66 estensioni da rilevare)

© Acronis International GmbH, 2003-2024

Moduli e opzioni	Piani di protezione predefiniti			
	Cyber Protect Essentials	**Lavoratori da remoto**	**Lavoratori in ufficio (Antivirus di terze parti)**	**Lavoratori in ufficio (Acronis Antivirus)**
		• .dwg **Audio e video** • .avi • .mov • .mpeg • .mpg • .mkv • .wav • .aif • .aifc • .aiff • .au • .snd • .mid • .midi • .mpga • .mp3 • .oga • .flac • .opus • .spx • .ogg • .ogx • .mp4		
Pianificazione	–	Alle 03:35 PM, da lunedì a venerdì	Alle 03:40 PM, da lunedì a venerdì	Alle 03:40 PM, da lunedì a venerdì

Nota
Il numero di moduli nel piano di protezione predefinito può variare in base alla licenza di Cyber Protection in uso.

Applicazione di un piano di protezione predefinito

Il piano di protezione predefinito iniziale è un modello per il quale non è possibile modificare le impostazioni. Quando un piano predefinito viene applicato per la prima volta, il modello viene copiato nel tenant come piano di protezione preconfigurato ed è abilitato nei workload selezionati.

© Acronis International GmbH, 2003-2024

Il piano di protezione viene visualizzato nella scheda **Gestione** > **Piani di protezione**, dove è possibile gestirlo.

Per applicare un piano di protezione predefinito per la prima volta

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare i workload da proteggere.
3. Fare clic su **Proteggi**.
4. Selezionare uno dei piani predefiniti, quindi fare clic su **Applica**.

Modifica di un piano di protezione predefinito

È possibile modificare un piano di protezione predefinito dopo averlo applicato per la prima volta.

Per modificare un piano di protezione predefinito applicato

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di protezione**.
2. Selezionare il piano da modificare, quindi fare clic su **Modifica**.
3. Modificare i moduli inclusi nel piano o le loro opzioni, quindi fare clic su **Salva**.

Importante
Alcune opzioni non sono modificabili.

Piani di protezione individuali per le integrazioni con pannelli di controllo per l'hosting

Quando vengono abilitate le integrazioni con pannelli di controllo per l'hosting nei server di web hosting che utilizzano DirectAdmin, cPanel o Plesk, il servizio Cyber Protection crea automaticamente un piano di protezione individuale per ogni workload nell'account utente. Questo piano di protezione è associato al workload specifico che ha avviato la creazione del piano di protezione e non può essere revocato o assegnato ad altri workload.

Per arrestare l'utilizzo di un piano di protezione individuale, è possibile eliminarlo dalla console di Cyber Protect. È possibile identificare i piani di protezione individuali perché sono contrassegnati dal segno accanto al proprio nome.

Per fare in modo che un piano di protezione protegga più server di web hosting che utilizzano le integrazioni con pannelli di controllo per l'hosting, creare un piano di protezione standard nella console di Cyber Protect e assegnare a questo piano i workload desiderati. Tenere presente che qualsiasi modifica a un piano di protezione che viene condiviso da più pannelli di controllo di web hosting potrà essere eseguita solo dalla console di Cyber Protect e non dalle integrazioni.

© Acronis International GmbH, 2003-2024

#CyberFit Score dei sistemi

#CyberFit Score offre una valutazione della sicurezza e un meccanismo di assegnazione del punteggio che valuta lo stato della sicurezza del sistema. Identifica le lacune nella sicurezza dell'ambiente IT e i potenziali vettori di attacco agli endpoint, e offre report contenenti le azioni consigliate per eventuali migliorie. Questa funzionalità è disponibile in tutte le edizioni di Cyber Protect.

La funzionalità #CyberFit Score è supportata in:

- Windows 7 (prima versione) e versioni successive
- Windows Server 2008 R2 e versioni successive

Come funziona

L'agente di protezione installato in un sistema esegue una valutazione della sicurezza e calcola il #CyberFit Score del sistema. Tale punteggio viene ricalcolato periodicamente in modo automatico.

Meccanismo di assegnazione del Punteggio #CyberFit

Il #CyberFit Score di un sistema viene calcolato in base alle metriche seguenti:

- Protezione anti-malware 0-275
- Protezione del backup 0-175
- Firewall 0-175
- VPN (Virtual Private Network, rete privata virtuale) 0-75
- Crittografia dell'intero disco 0-125
- Sicurezza della rete 0-25

Il #CyberFit Score massimo per un sistema è 850.

Metrica	Elementi valutati	Raccomandazioni per gli utenti	Punteggio
Anti-malware	L'agente controlla se nel sistema è installato o meno un software anti-malware.	Risultati: • È presente e abilitata una soluzione di protezione anti-malware (+275 punti) • Non è presente alcuna protezione anti-malware; il sistema potrebbe essere a rischio (0 punti) Raccomandazioni fornite da #CyberFit Score: Per essere protetti dai rischi della sicurezza, è necessario aver installato e abilitato una soluzione anti-malware nel sistema.	275 - software anti-malware installato nel sistema 0 - nessun software anti-malware installato nel sistema

© Acronis International GmbH, 2003-2024

		Per un elenco delle soluzioni anti-malware consigliate, fare riferimento a siti quali AV-Test o AV-Comparatives.	
Backup	L'agente controlla se nel sistema è installata una soluzione di backup.	Risultati: • È presente una soluzione di backup a protezione dei dati (+175 punti) • Non è stata individuata alcuna soluzione di backup; i dati potrebbero essere a rischio (0 punti) Raccomandazioni fornite da #CyberFit Score: È consigliabile eseguire regolarmente il backup dei dati per prevenire la perdita di dati o gli attacchi ransomware. Di seguito vengono indicate alcune soluzioni di backup il cui utilizzo è consigliato: • Acronis Cyber Protect/Cyber Backup/True Image • Windows Server Backup (Windows Server 2008 R2 e versioni successive)	175 - software di backup installato nel sistema 0 - nessun software di backup installato nel sistema
Firewall	L'agente controlla se nell'ambiente è o meno disponibile e abilitato un firewall. L'agente esegue quanto indicato di seguito: 1. Controlla l'opzione Protezione firewall e della rete di Windows per verificare se è attivato o meno un firewall pubblico. 2. Controlla l'opzione Protezione firewall e della rete di Windows per verificare se è attivato o meno un firewall privato. 3. Controlla l'agente/soluzione	Risultati: • Il firewall per le reti pubbliche e private è abilitato, oppure è stata individuata una soluzione firewall di terze parti (+175 punti) • Il firewall è abilitato solo per le reti pubbliche (+100 punti) • Il firewall è abilitato solo per le reti private (+75 punti) • Nessun firewall abilitato; la connessione di rete non è sicura (0 punti) Raccomandazioni fornite da #CyberFit Score: Si consiglia di abilitare un firewall per le reti pubbliche e private, per migliorare la protezione delle funzioni di sicurezza contro attacchi potenzialmente dannosi perpetrati verso il sistema in uso. Di seguito vengono indicate alcune guide dettagliate per la configurazione del firewall di Windows, in base alle esigenze di sicurezza e all'architettura di rete: Guide per dipendenti/utenti finali: Come configurare Windows Defender Firewall su un PC	100 - Il firewall pubblico di Windows è abilitato 75 - Il firewall privato di Windows è abilitato 175 - I firewall pubblici e privati di Windows sono abilitati OPPURE è abilitata una soluzione firewall di terze parti 0 - non sono abilitati né un firewall Windows né una soluzione firewall di

© Acronis International GmbH, 2003-2024

	firewall di terzi nel caso in cui i firewall pubblici e privati di Windows siano disabilitati.	Come configurare Windows Firewall su un PC Guide per amministratori e ingegneri di sistemi: Come distribuire Window Defender Firewall con Advanced Security Come creare regole avanzate in Windows Firewall	terze parti
Rete VPN (Virtual Private Network)	L'agente controlla se nel sistema è installata o meno una soluzione VPN e se è o meno abilitata e in esecuzione una rete VPN.	Risultati: • È presente una soluzione VPN ed è possibile inviare e ricevere in sicurezza i dati sulle reti pubbliche e condivise (+75 punti) • Non è stata individuata una soluzione VPN; la connessione alle reti pubbliche e condivise non è sicura (0 punti) Raccomandazioni fornite da #CyberFit Score: Si consiglia di utilizzare una VPN per accedere alla rete aziendale e ai dati riservati. È importante utilizzare una VPN per salvaguardare la sicurezza e la privacy delle comunicazioni, soprattutto quando si utilizza un accesso a Internet gratuito in un locale pubblico come un bar, una biblioteca, un aeroporto o altro. Di seguito vengono indicate alcune soluzioni VPN il cui utilizzo è consigliato: • Acronis Business VPN • OpenVPN • Cisco AnyConnect • NordVPN • TunnelBear • ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81 • VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	75 - VPN abilitata e in esecuzione 0 - VPN non abilitata
Crittografia del disco	L'agente controlla se nel sistema è abilitata o meno la crittografia del	Risultati: • La crittografia dell'intero disco è abilitata; il sistema è protetto dalla manomissione fisica	125 - tutti i dischi sono crittografati

© Acronis International GmbH, 2003-2024

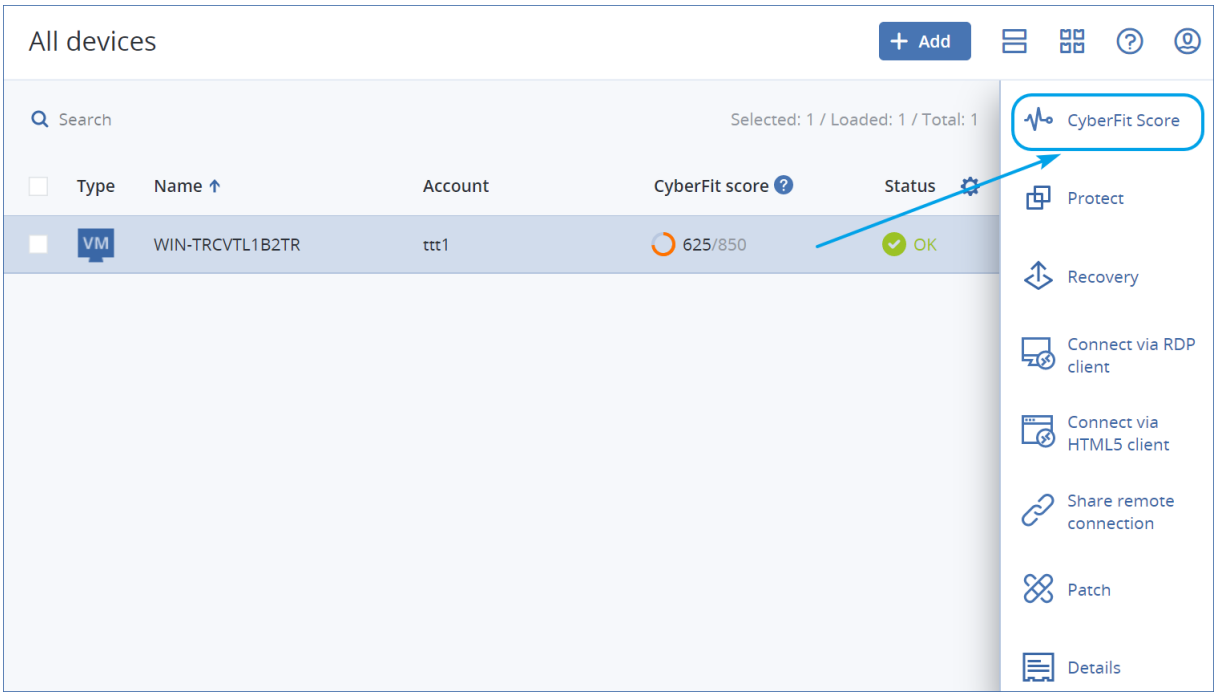
	disco. L'agente controlla se Windows BitLocker è attivato o meno.	(+125 punti) • Solo alcune unità sono crittografate; i sistemi sono a rischio di manomissione fisica (+ 75 punti) • Non è stata individuata alcuna crittografia del disco; il sistema è a rischio di manomissione fisica (0 punti) Raccomandazioni fornite da #CyberFit Score: Si consiglia di attivare Windows BitLocker per migliorare la protezione di dati e file. Guida: Come attivare la crittografia dei dispositivi in Windows	75 - almeno un disco è crittografato ma sono presenti anche dischi non crittografati 0 - nessun disco crittografato
Sicurezza di rete (traffico NTLM in uscita verso i server remoti)	L'agente controlla la presenza nel sistema di limitazioni del traffico NTLM in uscita verso i server remoti.	Risultati: • Il traffico NTLM in uscita verso i server remoti è negato; le credenziali sono protette (+25 punti) • Il traffico NTLM in uscita verso i server remoti non è negato; le credenziali sono potenzialmente esposte e vulnerabili (0 punti) Raccomandazioni fornite da #CyberFit Score: Per migliorare la protezione delle funzioni di sicurezza, si consiglia di negare tutto il traffico NTLM in uscita verso i server remoti. Ulteriori informazioni su come modificare le impostazioni NTLM e aggiungere eccezioni sono disponibili al link seguente. Guida: Limitare il traffico NTLM in uscita verso i server remoti	25 - il traffico NTLM in uscita è impostato su DenyAll 0 - il traffico NTLM in uscita è impostato su un altro valore

In base alla somma dei punti assegnati per ogni metrica, il #CyberFit Score totale di un sistema può corrispondere a uno dei punteggi seguenti che riflettono il livello di protezione dell'endpoint:

- 0 - 579 - Scarso
- 580 - 669 - Discreto
- 670 - 739 - Buono
- 740 - 799 - Molto buono
- 800 - 850 - Eccellente

È possibile visualizzare il #CyberFit Score dei sistemi presenti nella console di Cyber Protect passando a **Dispositivi** > **Tutti i dispositivi**. Nell'elenco dei dispositivi è visibile la colonna **#CyberFit Score**. È inoltre possibile eseguire la scansione #CyberFit Score su un sistema per verificarne le condizioni di sicurezza.

© Acronis International GmbH, 2003-2024



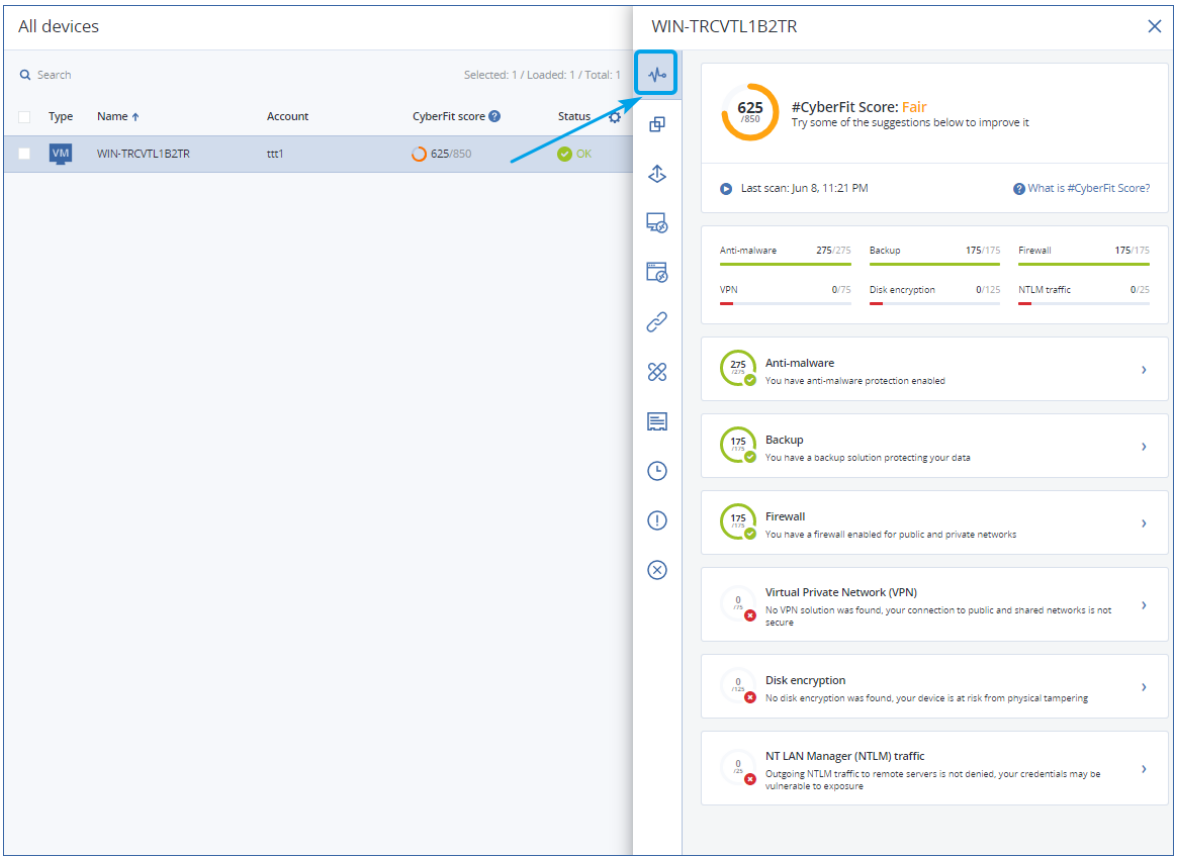
Le informazioni sul #CyberFit Score sono inoltre reperibili nel widget e nel report corrispondenti.

Esecuzione di una scansione #CyberFit Score

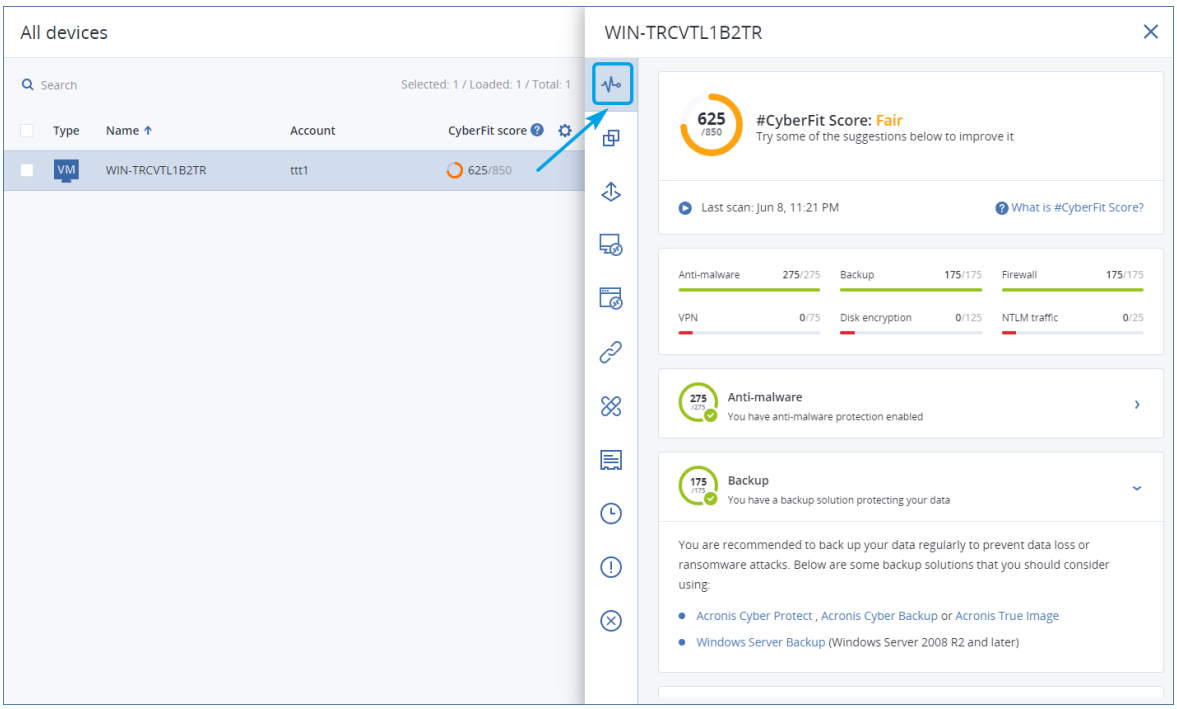
Per eseguire una scansione #CyberFit Score

1. Nella console di Cyber Protect, passare a **Dispositivi**.
2. Selezionare il sistema e fare clic su **#CyberFit Score**.
3. Se il sistema non è mai stato analizzato prima, fare clic su **Eseguire una prima scansione**.
4. Una volta completata la scansione, verrà visualizzato il #CyberFit Score totale del sistema, insieme ai punteggi di ciascuna delle sei metriche valutate: Anti-malware, Backup, Firewall, Virtual Private Network (VPN), Crittografia del disco e Traffico NTLM.

© Acronis International GmbH, 2003-2024



5. Per comprendere come aumentare il punteggio di ogni metrica per la quale è possibile migliorare le configurazioni di sicurezza, espandere la sezione corrispondente e leggere le raccomandazioni.



6. Dopo aver seguito le raccomandazioni, è sempre possibile ricalcolare il #CyberFit Score del sistema facendo clic sul pulsante freccia destra nel #CyberFit Score totale.

© Acronis International GmbH, 2003-2024

Cyber Scripting

Cyber Scripting consente di utilizzare gli script per automatizzare le operazioni di routine sui sistemi Windows e macOS nell'ambiente, ad esempio l'installazione di software, la modifica di configurazioni, l'avvio o l'arresto di servizi e la creazione di account. Pertanto è possibile ridurre il tempo impiegato in tali operazioni e il rischio di errore durante la loro esecuzione manuale.

Cyber Scripting è disponibile ad amministratori e utenti a livello di cliente, nonché agli amministratori di partner (Service Provider). Per ulteriori informazioni sui diversi livelli di amministrazione, consultare "Supporto per ambienti multitenant" (pag. 334).

Gli script che l'utente può utilizzare devono essere precedentemente approvati. Solo gli amministratori con il ruolo **Amministratore Cyber** possono approvare e testare i nuovi script. Per ulteriori informazioni sulla modifica dello stato di uno script, consultare "Modifica dello stato dello script" (pag. 250).

A seconda del ruolo utente, è possibile eseguire diverse operazioni con script e piani di scripting. Per ulteriori informazioni sui ruoli, consultare "Ruoli utente e diritti di Cyber Scripting" (pag. 240).

Prerequisiti

- La funzionalità Cyber Scripting richiede il pacchetto Advanced Management.
- Per utilizzare tutte le funzioni di Cyber Scripting, come la modifica di script, l'esecuzione di script, la creazione di piani di scripting e così via, è necessario abilitare l'autenticazione a due fattori per l'account.

Limitazioni

- Sono supportati i seguenti linguaggi di scripting:
  - PowerShell
  - Bash
- Le operazioni di Cyber Scripting possono essere eseguite soltanto su sistemi di destinazione sui quali è stato installato un agente di protezione.

Piattaforme supportate

Cyber Scripting è disponibile per i workload Windows e macOS.

La seguente tabella riassume le versioni supportate.

© Acronis International GmbH, 2003-2024

Sistema operativo	Versione
Windows	Windows 7 SP1 e versioni successive – tutte le edizioni
	Windows 8/8.1 – tutte le edizioni (x86, x64), eccetto le edizioni Windows RT
	Windows 10 – edizioni Home, Pro, Education, Enterprise, IoT Enterprise
	Windows 11
	Windows Server 2008 R2 SP1 e versioni successive – edizioni Standard, Enterprise, Datacenter, Foundation e Web
	Windows Server 2012/2012 R2 - tutte le edizioni
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Storage Server (2008 R2, 2012, 2012 R2, 2016)
macOS	macOS Mojave 10.14
	macOS Catalina 10.15
	macOS Big Sur 11
	macOS Monterey 12

Ruoli utente e diritti di Cyber Scripting

Le azioni disponibili con gli script e i piani di scripting dipendono dallo stato dello script e dal ruolo dell'utente.

Gli amministratori possono gestire oggetti nei propri tenant e nei rispettivi tenant figlio. Non possono visualizzare o accedere agli oggetti a un livello di amministrazione superiore, se presente.

Gli amministratori di livello più basso possono accedere esclusivamente in sola lettura ai piani di scripting applicati ai propri workload da un amministratore di livello superiore.

I ruoli seguenti forniscono diritti per Cyber Scripting:

- **Amministratore dell'azienda**

  Questo ruolo concede diritti di amministratore completi per tutti i servizi. Per quanto riguarda Cyber Scripting, garantisce gli stessi diritti del ruolo Amministratore Cyber.

- **Amministratore Cyber**

  Questo ruolo garantisce autorizzazioni complete, inclusa l'autorizzazione degli script che possono essere utilizzati nel tenant e la possibilità di eseguire script con lo stato **Prova in corso**.
- **Amministratore**

© Acronis International GmbH, 2003-2024

Questo ruolo garantisce autorizzazioni parziali, con la possibilità di eseguire script approvati e di creare ed eseguire piani di scripting che utilizzano script approvati.

- **Amministratore di sola lettura**

  Questo ruolo garantisce autorizzazioni limitate, con la possibilità di visualizzare gli script e i piani di protezione utilizzati nel tenant.
- **Utente**

  Questo ruolo garantisce autorizzazioni parziali, con la possibilità di eseguire script approvati e di creare ed eseguire piani di scripting che utilizzano script approvati, esclusivamente sul sistema dell'utente.

La tabella seguente riepiloga le azioni disponibili in base allo stato dello script e al ruolo dell'utente.

Ruolo	Oggetto	Stato dello script		
		Bozza	**Prova in corso**	**Approvato**
Amministratore Cyber **Amministratore dell'azienda**	Piano di scripting	Modifica (rimozione di una bozza di script da un piano) Elimina Revoca Disabilita Arresta	Crea Modifica Applica Abilita Esegui Elimina Revoca Disabilita Arresta	Crea Modifica Applica Abilita Esegui Elimina Revoca Disabilita Arresta
	Script	Crea Modifica Modifica stato Clona Elimina Annulla esecuzione	Crea Modifica Modifica stato Esegui Clona Elimina Annulla esecuzione	Crea Modifica Modifica stato Esegui Clona Elimina Annulla esecuzione
Amministratore **Utente** (per i propri workload)	Piano di scripting	Visualizzazione Revoca Disabilita Arresta	Visualizzazione Annulla esecuzione	Crea Modifica Applica Abilita

© Acronis International GmbH, 2003-2024

				Esegui Elimina Revoca Disabilita Arresta
	Script	Crea Modifica Clona Elimina Annulla esecuzione	Visualizzazione Clona Annulla esecuzione	Esegui Clona Annulla esecuzione
Amministratore di sola lettura	Piano di scripting	Visualizzazione	Visualizzazione	Visualizzazione
	Script	Visualizzazione	Visualizzazione	Visualizzazione

Script

Uno script consiste in una serie di istruzioni che vengono interpretate in fase di runtime ed eseguite in un sistema di destinazione. Costituisce una soluzione pratica per l'automazione di attività ripetitive o complesse.

In Cyber Scripting è possibile eseguire uno script predefinito o crearne uno personalizzato. Tutti gli script disponibili all'utente sono visualizzabili in **Gestione** > **Archivio degli script**. Gli script predefiniti sono disponibili nella sezione **Libreria**. Gli script creati o clonati nel tenant dell'utente sono posizionati nella sezione **Script personali**.

È possibile utilizzare uno script includendolo in un piano di scripting o avviando un'operazione di **Esecuzione rapida dello script**.

Nota
È possibile utilizzare soltanto script approvati, creati o clonati nel tenant dell'utente. Se uno script è stato rimosso dall'archivio degli script o se il suo stato è stato modificato in **Bozza**, lo script non viene eseguito. È possibile controllare i dettagli relativi a un'operazione di scripting o cancellarla in **Monitoraggio** > **Attività**.

La tabella seguente offre più informazioni sulle possibili azioni eseguibili con uno script in base al relativo stato.

© Acronis International GmbH, 2003-2024

Stato	Azioni possibili
Bozza	I nuovi script creati e gli script clonati nel repository sono nello stato **Bozza**. Non è possibile eseguire questi script o includerli nei piani di scripting.
Prova in corso	Gli amministratori con il ruolo di **Amministratore Cyber** possono eseguire questi script e includerli nei piani di scripting.
Approvato	È possibile eseguire questi script e includerli nei piani di scripting.

Solo gli amministratori con il ruolo **Amministratore Cyber** possono modificare lo stato di uno script o eliminare uno script approvato. Per ulteriori informazioni, consultare "Modifica dello stato dello script" (pag. 250).

Creazione di uno script

È possibile creare uno script scrivendo manualmente il codice.

Per creare uno script

1. Nella console di Cyber Protect, passare a **Gestione** > **Archivio degli script**.
2. In **Script personali**, fare clic su **Crea script utilizzando l'intelligenza artificiale**.
3. Nel riquadro principale scrivere il corpo dello script.

   Importante
   Durante la creazione di uno script è necessario includere i controlli per il codice di uscita per ogni operazione. In caso contrario, un'operazione non riuscita potrebbe essere ignorata e lo stato dell'attività dello scripting in **Monitoraggio** > **Attività** potrebbe essere visualizzato erroneamente come **Riuscita**.

4. Specificare le impostazioni dello script.

Impostazione	Descrizione
Nome dello script	Nome dello script. Il campo viene popolato automaticamente, ma è possibile modificare il valore.
Descrizione	Descrizione dello script. Questa impostazione è facoltativa. [Per script generati da AI] Il campo viene popolato automaticamente al momento della generazione dello script. È possibile modificare la descrizione fornita dall'intelligenza artificiale.
Lingua	Linguaggio dello script. I valori disponibili sono: • **PowerShell**. Questo è il valore predefinito. • **Bash** [Per script generati da AI] Questa impostazione viene configurata prima della generazione dello script.

© Acronis International GmbH, 2003-2024

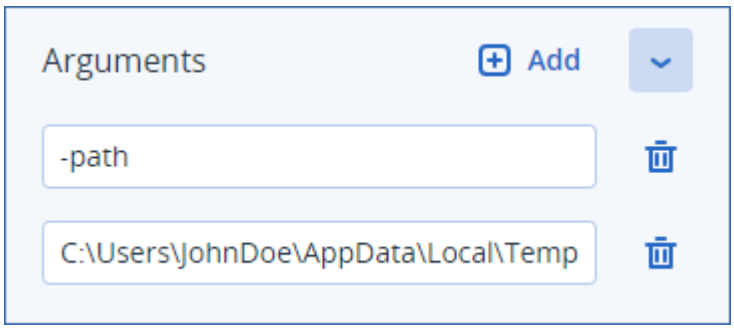
Impostazione	Descrizione
Sistema operativo	Sistema operativo installato sul workload di destinazione nel quale verrà eseguito lo script. I valori disponibili sono: • **Windows**. Questo è il valore predefinito. • **macOS** [Per script generati da AI] Questa impostazione viene configurata prima della generazione dello script.
Stato	Stato dello script. • **Bozza**. Questo è il valore predefinito. I nuovi script creati e gli script clonati nel repository sono nello stato **Bozza**. Non è possibile eseguire gli script nello stato **Bozza** né includerli nei piani di scripting. • **Prova in corso**. Solo gli amministratori con il ruolo **Amministratore Cyber** possono modificare lo stato di uno script nello stato **Prova in corso**, eseguire script nello stato **Prova in corso**, ed eseguire piani di scripting contenenti script con tali stati. • **Approvato**. È possibile eseguire script con lo stato **Approvato** e includerli nei piani di scripting. Solo gli amministratori con il ruolo **Amministratore Cyber** possono modificare lo stato di uno script o eliminare uno script approvato. Per ulteriori informazioni, consultare "Modifica dello stato dello script" (pag. 250).
Etichette	Le etichette non distinguono tra maiuscole e minuscole e possono contenere un massimo di 32 caratteri. Non è possibile utilizzare parentesi tonde o quadre, virgole e spazi. Questa impostazione è facoltativa. [Per script generati da AI] L'etichetta **Generato da AI** viene aggiunto automaticamente al momento della generazione dello script. È possibile eliminare questa etichetta o aggiungere altre etichette manualmente.

5. [Solo per gli script che richiedono credenziali] Specificare le credenziali.
   È possibile utilizzare una singola credenziale (ad esempio, un token) o una coppia di credenziali (ad esempio, un nome utente e una password).
6. [Solo per gli script che richiedono argomenti] Specificare gli argomenti e i rispettivi valori, come indicato di seguito.
   a. Fare clic su **Aggiungi**.
   b. Nel campo **Aggiungi argomenti**, specificare l'argomento.
   c. Fare clic su **Aggiungi**.
   d. Nel secondo campo visualizzato, specificare il valore dell'argomento.

© Acronis International GmbH, 2003-2024

Nota
È possibile specificare solo argomenti già definiti nel corpo dello script.

Per esempio:



e. Ripetere questi passaggi se è necessario aggiungere più di un argomento.

7. Fare clic su **Salva**.

Lo script viene salvato nel repository personale nello stato **Bozza**.

Non è possibile utilizzare lo script fino a quando un amministratore con il ruolo di **Amministratore Cyber** non cambia lo stato in **Approvato**. Per ulteriori informazioni, consultare "Modifica dello stato dello script" (pag. 250).

Per utilizzare lo script in un altro tenant gestito, è necessario clonare lo script nel tenant desiderato. Per ulteriori informazioni, consultare "Clonazione di uno script" (pag. 248).

Creazione di uno script utilizzando l'IA

Nota
Questa funzionalità richiede il pacchetto Advanced Management.

È possibile utilizzare l'IA per trasformare i prompt in script funzionali, risparmiando tempo e impegno. È possibile utilizzare la funzionalità nei modi seguenti:

- Immettere un prompt per chiedere all'IA di generare un script dall'inizio.

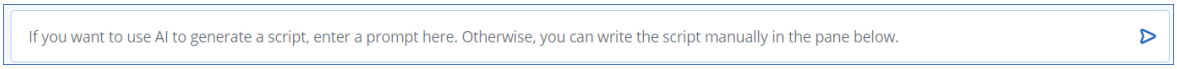
© Acronis International GmbH, 2003-2024

- Immettere un prompt per chiedere all'IA di rivedere e completare un codice inserito nel corpo dello script. È possibile utilizzare questa funzionalità quando si hanno difficoltà con codici più complessi.

Questa funzionalità utilizza il modello GPT-4 di OpenAI. È possibile utilizzarla per creare fino a 100 script aziendali al mese, gratuitamente.

Per creare uno script utilizzando l'intelligenza artificiale

1. Nella console di Cyber Protect, passare a **Gestione** > **Archivio degli script**.
2. In **Script personali**, fare clic su **Crea script utilizzando l'intelligenza artificiale**.
3. Nel prompt, immettere una descrizione di ciò che lo script deve fare. Inserire una descrizione che sia il più chiara e dettagliata possibile.

   Per esempio:

   ```
   I need a script that deletes Temporary files for all users (including user profiles +
   Windows Temps) and disable Windows Update Service to allow the script to run
   ```

4. Nel prompt, fare clic sul pulsante freccia.
5. Nella finestra di conferma, selezionare Lingua e Sistema operativo, quindi fare clic su **Genera**.

   Lo script generato dall'intelligenza artificiale viene visualizzato nel pannello principale. Il nome e la descrizione dello script sono generati automaticamente dall'intelligenza artificiale in modo da corrispondere allo script. Allo script viene assegnata automaticamente l'etichetta **Generato da IA**.
6. Rivedere lo script generato dall'intelligenza artificiale e, se necessario, modificalo manualmente.
7. Se necessario, modificare le impostazioni dello script.

Impostazione	Descrizione
Nome dello script	Nome dello script. Il campo viene popolato automaticamente, ma è possibile modificare il valore.
Descrizione	Descrizione dello script. Questa impostazione è facoltativa. [Per script generati da AI] Il campo viene popolato automaticamente al momento della generazione dello script. È possibile modificare la descrizione fornita dall'intelligenza artificiale.
Lingua	Linguaggio dello script. I valori disponibili sono: • **PowerShell**. Questo è il valore predefinito. • **Bash** [Per script generati da AI] Questa impostazione viene configurata prima della generazione dello script.
Sistema	Sistema operativo installato sul workload di destinazione nel quale verrà eseguito

© Acronis International GmbH, 2003-2024

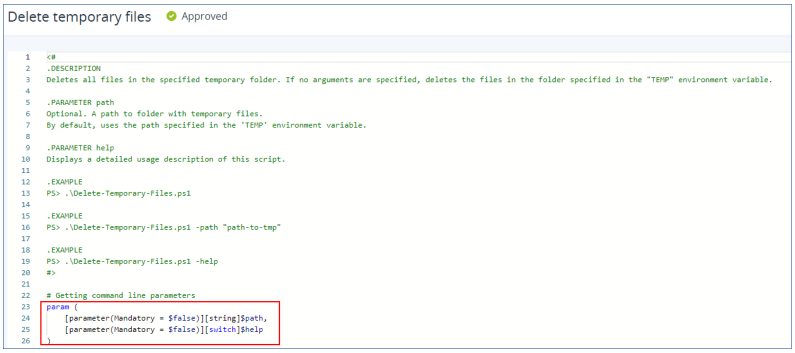
Impostazione	Descrizione
operativo	lo script. I valori disponibili sono: • **Windows**. Questo è il valore predefinito. • **macOS** [Per script generati da AI] Questa impostazione viene configurata prima della generazione dello script.
Stato	Stato dello script. • **Bozza**. Questo è il valore predefinito. I nuovi script creati e gli script clonati nel repository sono nello stato **Bozza**. Non è possibile eseguire gli script nello stato **Bozza** né includerli nei piani di scripting. • **Prova in corso**. Solo gli amministratori con il ruolo **Amministratore Cyber** possono modificare lo stato di uno script nello stato **Prova in corso**, eseguire script nello stato **Prova in corso**, ed eseguire piani di scripting contenenti script con tali stati. • **Approvato**. È possibile eseguire script con lo stato **Approvato** e includerli nei piani di scripting. Solo gli amministratori con il ruolo **Amministratore Cyber** possono modificare lo stato di uno script o eliminare uno script approvato. Per ulteriori informazioni, consultare "Modifica dello stato dello script" (pag. 250).
Etichette	Le etichette non distinguono tra maiuscole e minuscole e possono contenere un massimo di 32 caratteri. Non è possibile utilizzare parentesi tonde o quadre, virgole e spazi. Questa impostazione è facoltativa. [Per script generati da AI] L'etichetta **Generato da AI** viene aggiunto automaticamente al momento della generazione dello script. È possibile eliminare questa etichetta o aggiungere altre etichette manualmente.

8. [Facoltativo] [Solo per gli script che richiedono credenziali] Specificare le credenziali.
   È possibile utilizzare una singola credenziale (ad esempio, un token) o una coppia di credenziali (ad esempio, un nome utente e una password).
9. [Solo per gli script che richiedono argomenti] Specificare gli argomenti e i rispettivi valori, come indicato di seguito.
   a. Fare clic su **Aggiungi**.
   b. Nel campo **Aggiungi argomenti**, specificare l'argomento.
   c. Fare clic su **Aggiungi**.
   d. Nel secondo campo visualizzato, specificare il valore dell'argomento.

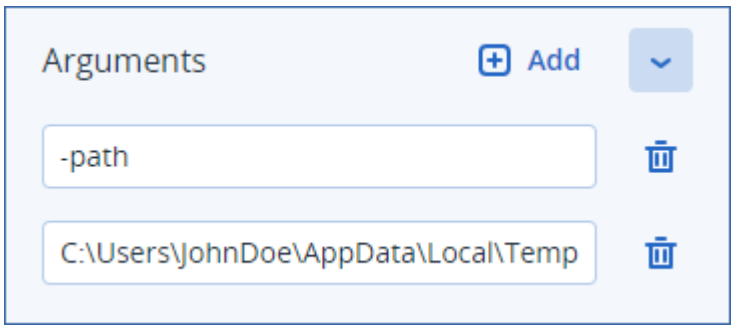
© Acronis International GmbH, 2003-2024

Nota

È possibile specificare solo argomenti già definiti nel corpo dello script.



Per esempio:



e. Ripetere questi passaggi se è necessario aggiungere più di un argomento.

10. Fare clic su **Salva**.

    Lo script viene salvato nel repository personale nello stato **Bozza**.

    Non è possibile utilizzare lo script fino a quando un amministratore con il ruolo di **Amministratore Cyber** non cambia lo stato in **Approvato**. Per ulteriori informazioni, consultare "Modifica dello stato dello script" (pag. 250).

    Per utilizzare lo script in un altro tenant gestito, è necessario clonare lo script nel tenant desiderato. Per ulteriori informazioni, consultare "Clonazione di uno script" (pag. 248).

Clonazione di uno script

La clonazione di uno script è necessaria nei casi seguenti:

- Prima di utilizzare uno script incluso nella **Libreria**. In questo caso, è innanzitutto necessario clonare lo script nella sezione **Script personali**.
- Quando si desidera clonare script creati in un tenant padre nelle unità o nei tenant figlio.

Per clonare uno script

1. In **Archivio degli script**, individuare lo script da clonare.
2. Eseguire una delle seguenti operazioni:
   - [Se si clona uno script da **Script personali**] Fare clic sull'icona dei puntini di sospensione accanto al nome dello script, quindi su **Clona**.

© Acronis International GmbH, 2003-2024

- [Se si clona uno script da **Libreria**] Fare clic su **Clona** accanto al nome dello script selezionato.

3. Nella finestra a comparsa **Clona script**, selezionare uno dei seguenti stati dello script dall'elenco a discesa **Stato**:
   - **Bozza** (per impostazione predefinita): questo stato non consente di eseguire lo script immediatamente.
   - **Test**: questo stato consente di eseguire lo script.
   - **Approvato**: questo stato consente di eseguire lo script.
4. [Se si gestisce più di un tenant o unità] Selezionare la posizione in cui clonare lo script.
   Nella finestra di dialogo **Clona script** vengono visualizzati solo i tenant che è possibile gestire e ai quali è applicato il pacchetto Advanced Management.

Lo script viene clonato nella sezione **Script personali** del tenant o dell'unità selezionata. Se si gestisce un solo tenant che non contiene unità, lo script viene copiato automaticamente nella sezione **Script personali**.

Importante
Le credenziali utilizzate da uno script non vengono copiate quando si clona uno script in un tenant diverso dall'originale.

Modifica o eliminazione di uno script

Nota
A seconda del ruolo utente, è possibile eseguire diverse operazioni con script e piani di scripting. Per ulteriori informazioni sui ruoli, consultare "Ruoli utente e diritti di Cyber Scripting" (pag. 240).

Per modificare uno script

1. In **Archivio degli script**, passare a **Script personali** e individuare lo script da modificare.
2. Fare clic sull'icona dei puntini di sospensione accanto al nome dello script, quindi su **Modifica**.
3. Apportare le modifiche necessarie allo script e fare clic su **Salva**.
4. [Se si modifica uno script utilizzato in un piano di scripting] Confermare la scelta facendo clic su **Salva script**.

   Nota
   Alla successiva esecuzione del piano di scripting viene utilizzata la versione più recente dello script.

Versioni dello script

Se si modifica uno qualunque dei seguenti attributi dello script viene creata una nuova versione dello script:

© Acronis International GmbH, 2003-2024

- corpo dello script
- nome dello script
- descrizione
- lingua dello script
- credenziali
- argomenti

Se si modificano altri attributi, le modifiche verranno aggiunte alla versione corrente dello script. Per ulteriori informazioni sulle versioni e su come confrontarle, fare riferimento a "Confronto tra versioni di uno script" (pag. 251).

Nota
Lo stato dello script viene aggiornato solo quando vengono modificati i valori nel campo **Stato**. Solo gli amministratori con il ruolo Amministratore Cyber possono modificare lo stato di uno script.

Per eliminare uno script

1. In **Archivio degli script**, passare a **Script personali** e individuare lo script da eliminare.
2. Fare clic sull'icona dei puntini di sospensione accanto al nome dello script, quindi su **Elimina**.
3. Fare clic su **Elimina**.
4. [Se si elimina uno script utilizzato in un piano di scripting] Confermare la scelta facendo clic su **Salva script**.

   Nota
   I piani di scripting che utilizzano lo script eliminato non potranno essere eseguiti.

Modifica dello stato dello script

Uno script appena creato e impostato sullo stato **Bozza** non può essere utilizzato fino a quando lo stato non viene modificato in **Approvato**. A seconda del caso d'uso, uno script può avere lo stato **Prova in corso** per un certo periodo prima di essere approvato.

Nota
A seconda del ruolo utente, è possibile eseguire diverse operazioni con script e piani di scripting. Per ulteriori informazioni sui ruoli, consultare "Ruoli utente e diritti di Cyber Scripting" (pag. 240).

Prerequisiti

- L'utente è un amministratore a cui è stato assegnato il ruolo di **Amministratore Cyber**.
- È disponibile uno script con lo stato corrispondente.

Per modificare lo stato dello script

 © Acronis International GmbH, 2003-2024

1. In **Archivio degli script**, passare a **Script personali**.
2. Fare clic sull'icona dei puntini di sospensione accanto al nome dello script, quindi su **Modifica**.
3. Nell'elenco a discesa **Stato**, selezionare lo stato.
4. Fare clic su **Salva**.
5. [Se si modifica lo stato di uno script approvato] Confermare la modifica facendo clic su **Salva script**.

Nota
Se lo stato dello script è stato impostato su **Bozza**, i piani di scripting che utilizzano tale script non potranno essere eseguiti.
Solo gli amministratori con il ruolo **Amministratore Cyber** possono eseguire gli script con lo stato **Prova in corso** e i piani di scripting che contengono script con questo stato.

Confronto tra versioni di uno script

È possibile confrontare due versioni di uno script e ripristinare una versione precedente. È anche possibile controllare chi è l'autore di una versione specifica e la data di creazione.

Per confrontare versioni di uno script

1. In **Archivio degli script**, passare a **Script personali** e individuare lo script con le versioni da confrontare.
2. Fare clic sull'icona dei puntini di sospensione accanto al nome dello script, quindi su **Cronologia delle versioni**.
3. Selezionare due versioni da confrontare, quindi fare clic su **Confronta versioni**.
   Qualsiasi modifica al corpo, agli argomenti o alle credenziali dello script viene evidenziata.

Per ripristinare una versione precedente

1. Nella finestra **Confronta versioni dello script** fare clic su **Ripristina questa versione**.
2. Nella finestra a comparsa **Ripristina a una versione precedente**, nell'elenco a discesa **Stato**, selezionare lo stato dello script.

La versione selezionata viene ripristinata e salvata come quella più recente nella cronologia delle versioni.

Per ripristinare uno script è anche possibile selezionare una versione dalla finestra **Cronologia versioni** e quindi fare clic sul pulsante **Ripristina**.

Importante
È possibile eseguire soltanto script con stato **Prova in corso** o **Approvato**. Per ulteriori informazioni, consultare "Modifica dello stato dello script" (pag. 250).

© Acronis International GmbH, 2003-2024

Scaricare l'output di un'operazione di scripting

È possibile scaricare l'output di un'operazione di scripting come file zip. Lo zip contiene due file – `stdout` e `stderr`. Nel file `stdout` vengono visualizzati i risultati di un'operazione di scripting completata senza errori. Il file `stderr` contiene informazioni sugli errori che si sono verificati durante l'operazione di scripting.

Per scaricare il file di output

1. Nella console di Cyber Protect, passare a **Monitoraggio** > **Attività**.
2. Fare clic sull'attività di Cyber Scripting di cui si desidera scaricare l'output.
3. Nella schermata **Dettagli attività**, fare clic su **Scarica output**.

Repository di script

È possibile individuare l'archivio degli script nella scheda **Gestione**. Nell'archivio, è possibile cercare gli script utilizzando il loro nome e descrizione. È anche possibile utilizzare i filtri o ordinare gli script in base al proprio nome o stato.

Per gestire uno script, fare clic sull'icona dei puntini di sospensione accanto al nome dello script, quindi selezionare l'azione desiderata. In alternativa, fare clic su uno script e utilizzare i pulsanti nella schermata che viene visualizzata.

L'archivio degli script contiene le sezioni seguenti:

- **Script personali**
  Questa sezione contiene gli script che è possibile utilizzare direttamente nell'ambiente. Si tratta degli script creati da zero e di quelli clonati in questa sezione.
  È possibile filtrare gli script della sezione secondo i seguenti criteri:
  - Etichette
  - Stato
  - Lingua
  - Sistema operativo
  - Proprietario dello script
- **Libreria**
  La libreria contiene gli script predefiniti che è possibile utilizzare nell'ambiente dopo averli clonati nella sezione **Script personali**. L'utente può solo ispezionare e clonare tali script.
  È possibile filtrare gli script della sezione secondo i seguenti criteri:
  - Etichette
  - Lingua
  - Sistema operativo

© Acronis International GmbH, 2003-2024

Per ulteriori informazioni, consultare l'articolo 70595 della Knowledge Base sugli script approvati dal fornitore.

Piani di scripting

Un piano di scripting consente di eseguire uno script su più workload, di pianificare l'esecuzione di uno script e di configurare impostazioni aggiuntive.

I piani di scripting creati e quelli applicati ai workload sono visualizzati in **Management** > **Piani di scripting**. Da qui è possibile controllare la posizione di esecuzione del piano, il proprietario o lo stato.

Una barra interattiva mostra i seguenti stati con classificazione basata su colori per i piani di scripting:

- In esecuzione (blu)
- Controllo di compatibilità in corso (grigio scuro)
- Disabilitato (grigio chiaro)
- OK (Verde)
- Avviso critico (rosso)
- Errore (arancione)
- Attenzione (giallo)

Facendo clic sulla barra è possibile visualizzare qual è lo stato di un piano e su quanti workload è applicato. È possibile fare clic su qualsiasi stato.

Nella scheda **Piani di scripting** è possibile gestire i piani eseguendo le azioni indicate di seguito:

- Esegui
- Arresta
- Modifica
- Rinomina
- Disabilita
- Abilita
- Clona
- Esportazione. La configurazione del piano viene esportata in formato JSON sul sistema locale.
- Elimina

La visibilità di un piano di scripting e le azioni che è possibile eseguire con tale piano dipendono dal proprietario del piano e dal ruolo dell'utente. Ad esempio, gli amministratori dell'azienda possono solo vedere i piani di scripting di proprietà del partner che sono applicati ai propri workload, e non possono eseguire alcuna azioni con tali piani.

© Acronis International GmbH, 2003-2024

Per ulteriori informazioni su chi può creare e gestire i piani di scripting, fare riferimento a "Ruoli utente e diritti di Cyber Scripting" (pag. 240).

Per gestire un piano di scripting

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di scripting**.
2. Individuare il piano che si desidera gestire e quindi fare clic sull'icona con i puntini di sospensione accanto al nome del servizio.
3. Selezionare l'azione desiderata, quindi seguire le istruzioni sullo schermo.

Creazione di un piano di scripting

È possibile creare un piano di scripting con le procedure indicate di seguito:

- Nella scheda **Dispositivi**
  Selezionare i workload e quindi creare il rispettivo piano di scripting.
- Nella scheda **Gestione** > **Piani di scripting**
  Creare un piano di scripting e quindi selezionare i workload ai quali applicare il piano.

Per creare un piano di scripting nella scheda Dispositivi

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Selezionare i workload o il gruppo di dispositivi ai quali applicare il piano di scripting, quindi fare clic rispettivamente su **Proteggi** o su **Proteggi gruppo**.
3. [Se sono già presenti piani applicati] Fare clic su **Aggiungi piano**.
4. Fare clic su **Crea piano** > **Piano di scripting**.
   Viene aperto un modello per il piano di scripting.
5. [Facoltativo] Per modificare il nome del piano di scripting, fare clic sull'icona a forma di matita.
6. Fare clic su **Scegli script**, selezionare lo script da utilizzare, quindi fare clic su **Fine**.

   Nota
   È possibile utilizzare solo gli script approvati in **Archivio degli script** > **Script personali**. Solo un amministratore con il ruolo **Amministratore Cyber** può utilizzare gli script con lo stato **Prova in corso**. Per ulteriori informazioni sui ruoli, consultare "Ruoli utente e diritti di Cyber Scripting" (pag. 240).

7. Configurare la pianificazione e le condizioni di avvio del piano di scripting.
8. Scegliere l'account con il quale lo script verrà eseguito nel workload di destinazione. Sono disponibili le seguenti opzioni:
   - Account di sistema (in macOS si tratta dell'account principale)
   - Account attualmente connesso
9. Specificare per quanto tempo lo script potrà essere eseguito nel workload di destinazione.
   Se l'esecuzione dello script non può concludersi nell'intervallo di tempo specificato, l'attività di Cyber Scripting non riuscirà.

© Acronis International GmbH, 2003-2024

Il valore minimo che è possibile specificare è un minuto, quello massimo è 1440 minuti.

10. [Solo per gli script di PowerShell] Configurare la policy di esecuzione di PowerShell.
    Per ulteriori informazioni su questa policy, fare riferimento alla documentazione Microsoft.
11. Fare clic su **Crea**.

Per creare un piano di scripting nella scheda Piani di scripting

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di scripting**.
2. Fare clic su **Crea piano**.
   Viene aperto un modello per il piano di scripting.
3. [Facoltativo] Per selezionare i workload o il gruppo di dispositivi ai quali applicare il nuovo piano, fare clic su **Aggiungi workload**.
   a. Fare clic su **Macchine con agenti** per espandere l'elenco e quindi selezionare i workload o i gruppi di dispositivi desiderati.
   b. Fare clic su **Aggiungi**.

   Per ulteriori informazioni su come creare gruppi di dispositivi a livello del partner, fare riferimento a "Scheda Dispositivi" (pag. 329).

   Nota
   È inoltre possibile selezionare workload o gruppi di dispositivi dopo aver creato il piano.

4. [Facoltativo] Per modificare il nome del piano di scripting, fare clic sull'icona a forma di matita.
5. Fare clic su **Scegli script**, selezionare lo script da utilizzare, quindi fare clic su **Fine**.

   Nota
   È possibile utilizzare solo gli script approvati in **Archivio degli script** > **Script personali**. Solo un amministratore con il ruolo **Amministratore Cyber** può utilizzare gli script con lo stato **Prova in corso**. Per ulteriori informazioni sui ruoli, consultare "Ruoli utente e diritti di Cyber Scripting" (pag. 240).

6. Configurare la pianificazione e le condizioni di avvio del piano di scripting.
7. Scegliere l'account con il quale lo script verrà eseguito nel workload di destinazione. Sono disponibili le seguenti opzioni:
   - Account di sistema (in macOS si tratta dell'account principale)
   - Account attualmente connesso
8. Specificare per quanto tempo lo script potrà essere eseguito nel workload di destinazione.
   Se l'esecuzione dello script non può concludersi nell'intervallo di tempo specificato, l'attività di Cyber Scripting non riuscirà.
   Il valore minimo che è possibile specificare è un minuto, quello massimo è 1440 minuti.
9. [Solo per gli script di PowerShell] Configurare la policy di esecuzione di PowerShell.
   Per ulteriori informazioni su questa policy, fare riferimento alla documentazione Microsoft.
10. Fare clic su **Crea**.

© Acronis International GmbH, 2003-2024

Pianificazione e condizioni di avvio

Pianificazione

È possibile configurare un piano di scripting affinché venga eseguito una volta o ripetutamente, avviato in base a una pianificazione o attivato da un determinato evento.

Sono disponibili le seguenti opzioni:

- Esegui una volta

  Per questa opzione, è necessario configurare la data e l'ora di esecuzione del piano.
- Pianificazione oraria

  Con questa opzione è possibile configurare l'esecuzione oraria, giornaliera o mensile dei piani di scripting.

  Per rendere effettiva la pianificazione solo temporaneamente, selezionare la casella di controllo **Esegui entro un intervallo di date** e quindi configurare il periodo durante il quale verrà eseguito il piano pianificato.
- Quando l'utente accede al sistema

  È possibile scegliere se il piano di scripting verrà attivato dall'accesso di uno specifico utente o di qualsiasi utente specifico.
- Quando l'utente si disconnette dal sistema

  È possibile scegliere se il piano di scripting verrà attivato dalla disconnessione di uno specifico utente o di qualsiasi utente specifico.
- All'avvio del sistema
- Quando il sistema viene arrestato

  Nota
  Questa opzione di pianificazione funziona solo con gli script eseguiti nell'account di sistema.
- Quando il sistema è online

Condizioni di avvio

Le condizioni di avvio aggiungono più flessibilità ai piani programmati. Se si configurano più condizioni, è necessario che tutte vengano soddisfatte contemporaneamente per consentire l'avvio del piano.

Le condizioni di avvio non sono valide se il piano viene eseguito manualmente mediante l'opzione **Esegui ora**.

Condizione	Descrizione
Esegui solo se il workload è online	Lo script verrà eseguito quando il workload di destinazione viene connesso a Internet.

© Acronis International GmbH, 2003-2024

Condizione	Descrizione
L'utente è inattivo	Questa condizione è soddisfatta quando uno screen saver è in esecuzione nel sistema o il sistema è bloccato.
Utente disconnesso	Con questa condizione è possibile posticipare un piano di scripting pianificato fino a quando l'utente del workload di destinazione non si disconnette.
Si adatta all'intervallo di tempo	Con questa condizione, un piano di scripting può essere avviato solo entro l'intervallo di tempo specificato. Ad esempio, è possibile utilizzare questa condizione per limitare la condizione **Utente disconnesso**.
Risparmia carica della batteria	Con questa condizione è possibile fare in modo che il piano di scripting non venga interrotto a causa di una batteria scarica. Sono disponibili le seguenti opzioni: • Non avviare se è attiva l'alimentazione con batteria Il piano viene avviato solo se il sistema è collegato a una fonte di alimentazione. • Avvia se è attiva l'alimentazione con batteria e il livello della batteria è superiore a Il piano viene avviato solo se il sistema è collegato a una fonte di alimentazione o se il livello della batteria è superiore al valore specificato.
Non avviare se è attiva una connessione a consumo	Questa condizione impedisce l'avvio del piano se il workload di destinazione accede a Internet tramite una connessione a consumo.
Non avviare se è attiva la connessione alle reti Wi-Fi seguenti	Questa condizione impedisce l'avvio del piano se il workload di destinazione è connesso a una qualsiasi delle reti wireless specificate. Per utilizzare questa condizione è necessario specificare il SSID della rete non consentita. La limitazione è valida per tutte le reti che contengono nel proprio nome il nome specificato come stringa secondaria, senza distinzione tra maiuscole e minuscole. Se, ad esempio, si specifica `telefono` come nome della rete, il piano non si avvia quando il dispositivo è connesso a una qualsiasi delle seguenti reti: `Telefono iPhone di John`, `wifi_telefono` oppure `wifi_TELEFONO_personale`.
Controlla gli indirizzi IP del dispositivo	Questa condizione impedisce l'avvio del piano se uno qualsiasi degli indirizzi IP del workload di destinazione è incluso o escluso dall'intervallo di indirizzi IP specificato. Sono disponibili le seguenti opzioni: • Avvia se è fuori dall'intervallo IP • Avvia se rientra nell'intervallo IP Sono supportati solo indirizzi IPv4.
Se le condizioni di avvio non sono soddisfatte, esegui comunque	Questa opzione consente di impostare l'intervallo di tempo dopo il quale verrà eseguito il piano, indipendentemente da qualsiasi altra condizione. Il piano si avvierà non appena le altre condizioni sono soddisfatte oppure il periodo

© Acronis International GmbH, 2003-2024

Condizione	Descrizione
l'attività	specificato termina, a seconda di quale si verifica prima. Questa opzione non è disponibile se il piano di scripting è stato configurato per essere eseguito una sola volta.

Gestione dei workload di destinazione di un piano

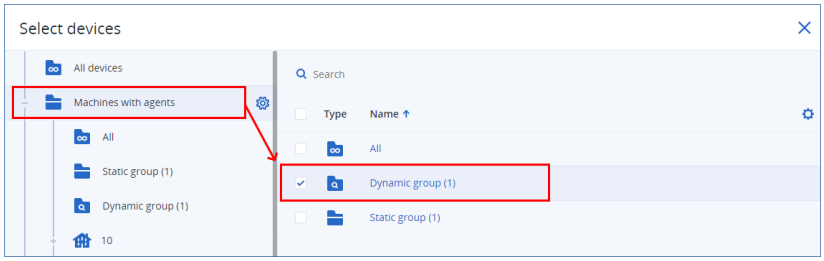
È possibile selezionare i workload o i gruppi di dispositivi ai quali applicare il piano di scripting durante la creazione del piano o in un secondo momento.

Gli amministratori di partner possono applicare lo stesso piano ai workload di diversi clienti e creare gruppi di dispositivi che contengono workload di diversi clienti. Per ulteriori informazioni su come creare un gruppo di dispositivi statico o dinamico al livello del partner, fare riferimento a "Scheda Dispositivi" (pag. 329).

Per aggiungere i workload iniziali a un piano

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di scripting**.
2. Fare clic sul nome del piano per il quale specificare i workload di destinazione.
3. Fare clic su **Aggiungi workload**.
4. Selezionare i workload o i gruppi di dispositivi desiderati, quindi fare clic su **Aggiungi**.

   Nota
   Per selezionare un gruppo di dispositivi, fare clic sul livello padre e quindi, nel riquadro principale, selezionare la casella di controllo accanto al suo nome.

5. Fare clic su **Salva** per salvare il piano modificato.

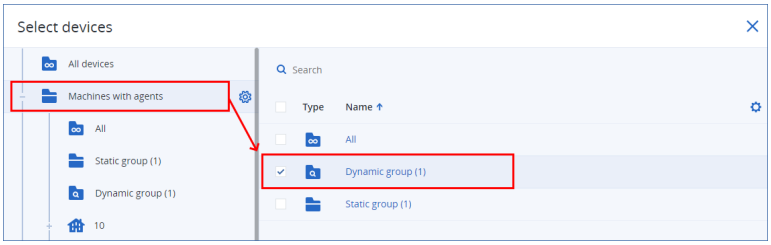
Per gestire i workload esistenti di un piano

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di scripting**.
2. Fare clic sul nome del piano di cui si desidera modificare i workload di destinazione.
3. Fare clic su **Gestisci workload**.
   La schermata **Dispositivi** elenca i workload ai quali è attualmente applicato il piano di scripting. Se si gestisce più di un tenant, i workload sono ordinati in base al tenant.

© Acronis International GmbH, 2003-2024

- Per aggiungere nuovi workload o gruppi di dispositivi, fare clic su **Aggiungi**.
  a. Selezionare i workload o i gruppi di dispositivi desiderati. È possibile aggiungere workload appartenenti a tutti i tenant gestiti.

  Nota
  Per selezionare un gruppo di dispositivi, fare clic sul livello padre e quindi, nel riquadro principale, selezionare la casella di controllo accanto al suo nome.

  b. Fare clic su **Aggiungi**.
- Per rimuovere workload o gruppi di dispositivi, selezionarli e quindi fare clic su **Rimuovi**.

4. Fare clic su **Fine**.
5. Fare clic su **Salva** per salvare il piano modificato.

Piani ai diversi livelli di amministrazione

La tabella seguente riepiloga i piani che possono essere visualizzati e gestiti dagli amministratori di diversi livelli.

Amministratore	Livello amministratore	Piani	Diritti
Amministratori di partner	Livello del partner	Propri piani	Accesso completo
		Piani del cliente (inclusi i piani nelle unità)	Accesso completo
		Piani delle unità	Accesso completo
	Livello del cliente (per i clienti gestiti dal service provider)	Piani del partner applicati ai workload di questo cliente	Sola lettura
		Piani del cliente (inclusi i piani nelle unità)	Accesso completo
		Piani delle unità	Accesso completo
	Livello dell'unità (per i clienti gestiti dal service provider)	Piani del partner applicati ai workload di questa unità	Sola lettura
		Piani del cliente applicati ai workload di	Sola lettura

© Acronis International GmbH, 2003-2024

Amministratore	Livello amministratore	Piani	Diritti
		questa unità	
		Piani delle unità	Accesso completo
Amministratore società	Livello del cliente	Piani del partner applicati ai workload di questo cliente o unità	Sola lettura
		Piani del cliente (inclusi i piani nelle unità)	Accesso completo
		Piani delle unità	Accesso completo
	Livello dell'unità	Piani del partner applicati ai workload di questa unità	Sola lettura
		Piani del cliente applicati ai workload di questa unità	Sola lettura
		Piani delle unità	Accesso completo
Amministratore unità	Livello dell'unità	Piani del partner applicati ai workload di questa unità	Sola lettura
		Piani del cliente applicati ai workload di questa unità	Sola lettura
		Piani delle unità	Accesso completo

Importante
Il proprietario di un piano è il tenant nel quale il piano è stato creato. Pertanto, se un amministratore di partner ha creato un piano al livello del tenant cliente, il tenant cliente è il proprietario del piano.

Problemi di compatibilità con piani di scripting

In alcuni casi, applicare un piano di script a un workload può causare problemi di compatibilità. Potrebbero registrarsi i problemi di compatibilità seguenti:

- Sistema operativo non compatibile: questo problema si verifica quando il sistema operativo del workload non è supportato.
- Agente non supportato: questo problema si verifica quando una versione dell'agente di protezione nel workload è obsoleta e non supporta la funzionalità Cyber Scripting.
- Quota non sufficiente: questo problema si verifica quando la quota di servizio nel tenant non è sufficiente per essere assegnata ai workload selezionati.

© Acronis International GmbH, 2003-2024

Se il piano di scripting è applicato a un massimo di 150 workload selezionati singolarmente, verrà richiesto di risolvere i conflitti esistenti prima di salvare il piano. Per risolvere i conflitti, rimuovere la causa principale che li causa oppure rimuovere i workload interessati dal piano. Per ulteriori informazioni, consultare "Risoluzione dei problemi di compatibilità con piani di scripting" (pag. 261). Se si salva il piano senza risolvere i conflitti, il piano verrà automaticamente disabilitato per i workload non compatibili e verranno mostrati i relativi avvisi.

Se il piano di scripting è applicato a più di 150 workload o a gruppi di dispositivi, verrà salvato e quindi ne verrà controllata la compatibilità. Il piano verrà automaticamente disabilitato per i workload incompatibili e verranno visualizzati i relativi avvisi.

Risoluzione dei problemi di compatibilità con piani di scripting

A seconda della causa che provoca i problemi di compatibilità, è possibile eseguire azioni differenti per risolverli durante il processo di creazione di un nuovo piano di scripting.

Nota
Quando si tenta di risolvere un problema di compatibilità rimuovendo i workload da un piano, non è possibile rimuovere i workload che fanno parte di un gruppo di dispositivi.

Per risolvere i problemi di compatibilità

1. Fare clic su **Rivedi problemi**.
2. [Per risolvere i problemi di compatibilità con sistemi operativi incompatibili]
   a. Nella scheda **Sistema operativo incompatibile** selezionare i workload da eliminare.
   b. Fare clic su **Rimuovi i workload dal piano**.
   c. Fare clic su **Rimuovi** e quindi su **Chiudi**.
3. [Per risolvere i problemi di compatibilità con agenti non supportati rimuovendo i workload dal piano]
   a. Nella scheda **Agenti non supportati** selezionare i workload da eliminare.
   b. Fare clic su **Rimuovi i workload dal piano**.
   c. Fare clic su **Rimuovi** e quindi su **Chiudi**.
4. [Per risolvere i problemi di compatibilità con agenti non supportati aggiornando la versione dell'agente] Fare clic su **Passare all'elenco degli agenti**.

   Nota
   Questa opzione è disponibile solo per gli amministratori del cliente.

5. [Per risolvere i problemi di compatibilità con quote insufficienti rimuovendo i workload dal piano]
   a. Nella scheda **Quota insufficiente** selezionare i workload da eliminare.
   b. Fare clic su **Rimuovi i workload dal piano**.
   c. Fare clic su **Rimuovi** e quindi su **Chiudi**.

© Acronis International GmbH, 2003-2024

6. [Per risolvere i problemi di compatibilità con quote insufficienti aumentando la quota del tenant]

   Nota
   Questa opzione è disponibile solo per gli amministratori del partner.

   a. Nella scheda **Quota insufficiente**, fare clic su **Vai al portale di gestione**.

   b. Aumentare la quota di servizio per il cliente.

Esecuzione rapida dello script

È possibile eseguire uno script immediatamente, senza includerlo in un piano di scripting. Questa operazione non può essere utilizzata su più di 150 workload, su workload offline o su gruppi di dispositivi.

Al workload di destinazione deve essere assegnata una quota di servizio che supporti la funzionalità Esecuzione rapida dello script; per il rispettivo tenant deve essere abilitato il pacchetto Advanced Management. Se è disponibile nel tenant, la quota di servizio appropriata verrà assegnata automaticamente.

Nota
È possibile utilizzare solo gli script approvati in **Archivio degli script** > **Script personali**. Solo un amministratore con il ruolo **Amministratore Cyber** può utilizzare gli script con lo stato **Prova in corso**. Per ulteriori informazioni sui ruoli, consultare "Ruoli utente e diritti di Cyber Scripting" (pag. 240).

È possibile avviare l'esecuzione rapida con le procedure indicate di seguito:

- Dalla scheda **Dispositivi**
  Selezionare uno o più workload e quindi lo script da eseguire su questi.
- Nella scheda **Gestione** > **Archivio degli script**
  Selezionare uno script e quindi uno o più workload di destinazione.

Per eseguire uno script nella scheda Dispositivi

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare i workload in cui eseguire lo script, quindi fare clic su **Proteggi**.
3. Fare clic su **Esecuzione rapida dello script**.
4. Fare clic su **Scegli script**, selezionare lo script da utilizzare, quindi fare clic su **Fine**.
5. Scegliere l'account con il quale lo script verrà eseguito nel workload di destinazione. Sono disponibili le seguenti opzioni:
   - Account di sistema (in macOS si tratta dell'account principale)
   - Account attualmente connesso
6. Specificare per quanto tempo lo script potrà essere eseguito nel workload di destinazione.

© Acronis International GmbH, 2003-2024

Se l'esecuzione dello script non può concludersi nell'intervallo di tempo specificato, l'attività di Cyber Script non riuscirà.

È possibile utilizzare valori tra 1 e 1440 minuti.

7. [Solo per gli script di PowerShell] Configurare la policy di esecuzione di PowerShell.

   Per ulteriori informazioni su questi valori, consultare la documentazione Microsoft.
8. Fare clic su **Esegui ora**.

Per eseguire uno script dalla scheda Archivio degli script

1. Nella console di Cyber Protect, passare a **Gestione** > **Archivio degli script**.
2. Selezionare lo script da eseguire, quindi fare clic su **Esecuzione rapida dello script**.
3. Fare clic su **Aggiungi workload** per selezionare i workload di destinazione, quindi fare clic su **Aggiungi**.
4. Fare clic su **Scegli script**, selezionare lo script da utilizzare, quindi fare clic su **Fine**.
5. Scegliere l'account con il quale lo script verrà eseguito nel workload di destinazione. Sono disponibili le seguenti opzioni:
   - Account di sistema (in macOS si tratta dell'account principale)
   - Account attualmente connesso
6. Specificare per quanto tempo lo script potrà essere eseguito nel workload di destinazione.

   Se l'esecuzione dello script non può concludersi nell'intervallo di tempo specificato, l'attività di Cyber Script non riuscirà.

   È possibile utilizzare valori tra 1 e 1440 minuti.
7. [Solo per gli script di PowerShell] Configurare la policy di esecuzione di PowerShell.

   Per ulteriori informazioni su questi valori, consultare la documentazione Microsoft.
8. Fare clic su **Esegui ora**.

Protezione di applicazioni di collaborazione e comunicazione

Zoom, Cisco Webex Meetings, Citrix Workspace e Microsoft Teams sono al momento le piattaforme più utilizzate per le conferenze e le comunicazioni video/web. Il servizio Cyber Protection consente di proteggere gli strumenti di collaborazione in uso.

La configurazione della protezione per Zoom, Cisco Webex Meetings, Citrix Workspace e Microsoft Teams è simile. L'esempio che segue mostra la configurazione della protezione per Zoom.

Per configurare la protezione di Zoom

1. Installare l'agente di protezione nel sistema in cui è installata l'applicazione di collaborazione.
2. Accedere alla console di Cyber Protect e applicare un piano di protezione in cui sia abilitato uno dei moduli seguenti:

© Acronis International GmbH, 2003-2024

- **Protezione antivirus e anti-malware** (con le impostazioni **Auto-protezione** e **Active Protection** abilitate) - se si dispone di una delle edizioni Cyber Protect.
- **Active Protection** (con l'impostazione **Auto-protezione** abilitata) - se si dispone di una delle edizioni Cyber Backup.

3. [Facoltativo] Per l'installazione automatica degli aggiornamenti, configurare il modulo **Gestione delle patch** nel piano di protezione.

Al termine, la protezione verrà estesa all'applicazione Zoom, incluse le seguenti attività:

- Installazione automatica degli aggiornamenti del client Zoom
- Protezione dei processi di Zoom dall'inserimento di codice
- Prevenzione delle operazioni sospette eseguite dai processi di Zoom
- Protezione dei file "host" dall'aggiunta dei domini correlati a Zoom

© Acronis International GmbH, 2003-2024

Comprensione del livello attuale di protezione

Monitoraggio

La scheda **Monitoraggio** fornisce informazioni importanti sul livello attuale di protezione e include le dashboard seguenti:

- **Panoramica**
- **Attività**
- **Avvisi**
- **Feed minacce** (per altre informazioni, consultare "Feed minacce" (pag. 309))

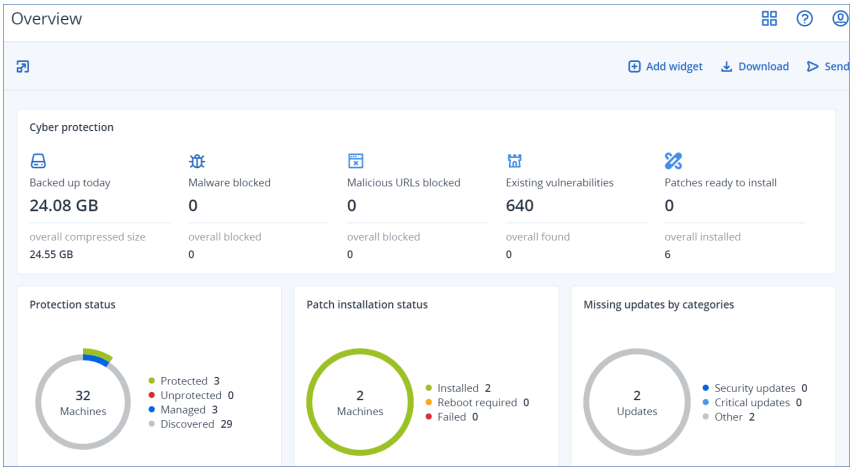
Pannello di controllo Panoramica

Il pannello di controllo **Panoramica** fornisce una serie di widget personalizzabili che offrono un'anteprima delle operazioni relative al servizio Cyber Protection. I widget di altri servizi saranno disponibili nelle release future.

I widget vengono aggiornati ogni cinque minuti. I widget presentano elementi cliccabili che consentono di indagare e risolvere i problemi. È possibile scaricare lo stato corrente del pannello di controllo in formato .pdf e/o .xlsx, oppure inviarlo tramite e-mail.

È possibile scegliere tra numerosi widget, presentati come tabelle, grafici a torta, a barre e mappe ad albero. È inoltre possibile aggiungere numerosi widget dello stesso tipo con filtri diversi.

I pulsanti **Download** e **Invia** in **Monitoraggio** > **Panoramica** non sono disponibili nelle edizioni standard del servizio Cyber Protection.



Per riorganizzare i widget nel pannello di controllo

Trascinare e rilasciare i widget facendo clic sui rispettivi nomi.

Per modificare un widget

© Acronis International GmbH, 2003-2024

Fare clic sull'icona a forma di matita accanto al nome del widget. La modifica del widget consente all'utente di rinominarlo, modificarne l'intervallo temporale e impostare i filtri e raggruppare le righe.

Per aggiungere un widget

Fare clic su **Aggiungi widget** e quindi eseguire una delle seguenti operazioni:

- Fare clic sul widget che si desidera aggiungere. Il widget verrà aggiunto con le impostazioni predefinite.
- Per modificare il widget prima di aggiungerlo, fare clic su Personalizza quando il widget è selezionato. Dopo aver modificato il widget, fare clic su **Fine**.

Per rimuovere un widget

Fare clic sul simbolo X accanto al nome del widget.

Dashboard Attività

La dashboard **Attività** fornisce una panoramica di tutte le attività passate e in corso. Per impostazione predefinita, il periodo di conservazione è di 90 giorni.

Per personalizzare la vista della dashboard **Attività**, fare clic sull'icona ingranaggio e quindi selezionare le colonne da visualizzare.

Per visualizzare il progresso dell'attività in tempo reale, selezionare la casella di controllo **Aggiorna automaticamente**. Tenere presente che un aggiornamento frequente di più attività può influire negativamente sulle prestazioni del server di gestione.

È possibile effettuare una ricerca delle attività in elenco secondo i seguenti criteri:

- **Nome periferica**
  Il sistema sul quale l'attività è in esecuzione.
- **Avviata da**
  L'account che ha avviato l'attività.

È inoltre possibile filtrare le attività con le seguenti proprietà:

- **Stato**
  Ad esempio Riuscita, Non riuscita, In corso, Annullata.
- **Tipo**
  Ad esempio Applicazione piano, Eliminazione backup, Installazione aggiornamenti software.
- **Orario**
  Ad esempio, Attività più recenti, Attività delle ultime 24 ore, Attività di un periodo specifico entro il periodo di conservazione predefinito.

Per visualizzare ulteriori dettagli su un'attività, selezionarla dall'elenco e quindi, nel riquadro **Dettagli attività**, fare clic su **Tutte le proprietà**. Per ulteriori informazioni sulle proprietà disponibili, consultare i riferimenti per le API Activity e Task nel Developer Network Portal.

© Acronis International GmbH, 2003-2024

Dashboard Avvisi

Il dashboard **Avvisi** visualizza tutti gli avvisi attuali. Gli avvisi in elenco sono avvisi critici o di errore, e in genere collegati ad attività come i backup non riusciti per qualsiasi ragione.

Per filtrare gli avvisi nel dashboard

1. Nell'elenco a discesa **Visualizza**, selezionare uno dei seguenti criteri:
   - **Gravità avviso**
   - **Categoria avviso**
   - **Tipo di avviso**
   - **Tipo di monitoraggio**
   - **Intervallo di date: da... a...**
   - **Workload**
   - **Piano**
   - **Cliente**
2. Se è stata selezionata l'opzione **Categoria avviso**, dall'elenco a discesa **Categoria** selezionare la categoria di avvisi da visualizzare.
3. Per visualizzare tutti gli avvisi senza filtrarli, fare clic su **Tutti i tipi di avviso**.

Ogni avviso consente di:

- Accedere al dispositivo a cui fa riferimento l'avviso facendo clic sul link **Dispositivi**.
- Leggere e provare a seguire alcune delle raccomandazioni indicate nella sezione **Risoluzione dei problemi** dell'avviso.
- Accedere alla documentazione pertinente e all'articolo della Knowledge Base facendo clic su **Cerca soluzione**. La funzionalità **Cerca soluzione** compila la richiesta con informazioni sull'avviso corrente, per assistere l'utente nel modo più efficace.

Per ordinare gli avvisi nel dashboard

Nella tabella degli avvisi, fare clic sul pulsante freccia accanto a uno dei seguenti nomi di colonna:

- **Gravità avviso**
- **Tipo di avviso**
- **Creazione**
- **Categoria avviso**
- **Workload**
- **Piano**

Se per l'account dell'utente è stato attivato il servizio Advanced Automation, è anche possibile creare un nuovo ticket del Service Desk direttamente dall'avviso.

© Acronis International GmbH, 2003-2024

Per creare un ticket del Service Desk

1. Nell'avviso pertinente, fare clic su **Crea un nuovo ticket**.

   In alternativa, quando si lavora nella modalità Visualizzazione tabella, selezionare un avviso e quindi **Crea un nuovo ticket** nel riquadro a destra.
2. Definire quanto segue:
   - Nella sezione dell'intestazione, selezionare la casella di controllo **Fatturabile** per fatturare al cliente il tempo registrato nel ticket. In aggiunta, selezionare la casella di controllo **Invia al cliente via e-mail** per inviare al cliente gli aggiornamenti dei ticket.
   - Nella sezione **Informazioni generali**, indicare un titolo per il ticket. Il campo è precompilato con un riepilogo dell'avviso, ma può essere modificato.
   - Nella sezione **Informazioni sul cliente**, i campi sono precompilati con le informazioni pertinenti estratte dall'avviso.
   - Nella sezione **Articolo o servizio di configurazione**, i campi sono precompilati con il dispositivo collegato all'avviso. Se necessario, è possibile riassegnare un dispositivo.
   - Nella sezione **Agente di supporto**, i campi sono precompilati con l'agente di supporto, la categoria e il gruppo di supporto predefiniti. Se necessario, è possibile riassegnare un altro agente.
   - Nella sezione **Aggiornamento ticket**, i campi sono precompilati con la descrizione e i dettagli dell'avviso. Il campo **Stato** è impostato su **Nuovo** per impostazione predefinita e può essere modificato.
   - Nelle sezioni **Allegati**, **Elementi fatturabili** e **Note interne**, aggiungere gli articoli pertinenti come necessario.
3. Fare clic su **Fine**. Una volta creato il ticket, all'avviso viene aggiunto un link al ticket.

   Se l'avviso viene chiuso, anche il ticket relativo verrà chiuso.

Nota
È possibile creare un solo ticket per avviso.

Tipi di avviso

Vengono generati i tipi di avviso seguenti:

- Avvisi di Backup
- Avvisi di Disaster recovery
- Avvisi di Protezione anti-malware
- Avvisi di Licensing
- Avvisi di Filtro URL
- Avvisi di EDR
- Avvisi di Controllo dispositivo
- Avvisi di Sistema

© Acronis International GmbH, 2003-2024

Avvisi di Backup

Avviso	Descrizione	Come risolvere l'avviso
Backup non riuscito	Viene generato un avviso quando il backup non è riuscito con un errore risolvibile durante l'esecuzione o se è stato interrotto a causa di un arresto del sistema.	Verificare il registro dell'operazione di backup difettosa: fare clic per selezionare il workload, fare clic su **Attività**, quindi trovare l'avviso nel registro. Il messaggio dovrebbe indirizzare alla causa principale del problema notificato dal software.
Backup completato con avvisi	Viene generato un avviso quando il backup viene completato con avvisi.	Verificare i registri delle conversioni in VM, delle repliche o dei piani di convalida. I problemi riscontrati durante queste operazioni generano avvisi del tipo "Attività non riuscita" o "Attività completata con avvisi".
Backup annullato	Viene generato un avviso ogni volta che un'attività di backup viene cancellata manualmente dall'utente.	È possibile avviare il backup manualmente facendo clic su Esegui ora o attendere l'esecuzione del backup alla prossima scadenza pianificata.
Backup annullato a causa di una finestra di backup chiusa	Viene generato un avviso quando l'attività di backup non viene eseguita perché non è rientrata nella finestra specificata nelle opzioni di backup.	Riconfigurare la pianificazione o modificare le opzioni del piano di backup in **Prestazioni e finestra di backup**. Espandere la sezione nel prodotto per ulteriori istruzioni.
Backup in attesa	Questo avviso viene generato ogni volta che si presenta un conflitto di pianificazione e due attività di backup vengono avviate in simultanea. In questo caso, la seconda attività di backup viene messa in coda fino al termine o all'arresto della prima.	Verificare che i backup vengano eseguiti nella finestra temporale prevista e secondo la propria pianificazione, ed evitare di creare conflitti di pianificazione dove possibile.
Il backup non risponde	Viene generato un avviso quando il backup in esecuzione non ha evidenziato alcun progresso per qualche tempo, e potrebbe essere bloccato.	Il problema potrebbe essere causato da un blocco. Seguire questo articolo per acquisire le informazioni necessarie per risolvere il problema.

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
Il backup non è stato avviato	Viene generato un avviso quando il backup pianificato non viene avviato per ragioni sconosciute.	Verificare che sia in uso la versione più recente del prodotto Acronis Backup. • Se il sistema dell'agente era disponibile durante l'orario di avvio del backup: 1. Modificare l'orario di avvio dell'attività di backup. 2. Se l'avviso viene visualizzato di nuovo, ricreare l'attività di backup. 3. Se anche l'attività di backup appena creata attiva l'avviso, contattare il supporto Acronis per assistenza. • Se l'agente era offline: 1. Non spegnere il sistema nell'orario del backup. 2. Se il sistema non era spento, verificare che Acronis Managed Machine Service sia in esecuzione: Start -> Cerca -> services.msc -> individuare Acronis Managed Machine Service. Contattare il supporto Acronis se è necessario ricevere assistenza.
Stato backup sconosciuto	Viene generato un avviso se l'agente di backup era offline all'ora in cui era stato pianificato il backup. Lo stato dei backup delle risorse sarà noto solo quando l'agente di backup sarà online.	1. Verificare se è previsto che l'agente sia offline (ad esempio, se il sistema è un notebook esterno alla rete del management server). 2. Se l'agente non deve essere offline, verificare che Acronis Managed Machine Service sia in esecuzione: Start -> Cerca -> services.msc -> individuare Acronis Managed Machine Service e controllarne lo stato. Avviare il servizio se è arrestato.
Backup mancante	Viene generato un avviso quando non è stato eseguito un backup completo per più di [giorni dall'ultimo backup] giorni.	

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
Backup danneggiato	Viene generato un avviso quando l'attività di convalida termina correttamente e mostra che il backup è danneggiato.	Seguire i passaggi indicati nell'articolo sulla risoluzione dei problemi dei backup danneggiati. Contattare il supporto Acronis se è necessario ricevere assistenza per l'identificazione della causa principale dei danni all'archivio.
La protezione continua dei dati non è riuscita	Viene generato un avviso se la protezione continua del backup non riesce.	Verificare le seguenti limitazioni: 1. La protezione continua dei dati è supportata solo per i file system NTFS e per i sistemi operativi seguenti: • Desktop: Windows 7 o versioni successive • Server: Windows Server 2008 R2 e versioni successive 2. La CDP non supporta **Acronis Secure Zone** come destinazione. 3. Non sono supportate le cartelle NFS montate su Windows. 4. Non è supportata la replica continua: se nel piano di protezione sono presenti due posizioni, le sezioni di CDP vengono create solo nella prima destinazione, e le modifiche verranno replicate nella seconda solo con il backup successivo. 5. Se le modifiche a una cartella locale protetta vengono applicate da un'origine di rete (ad esempio, quando gli utenti accedono alla cartella dalla rete), la CDP non le rileva. 6. Se le modifiche vengono apportate tramite un file, come nel caso di modifiche effettuate in un file di Excel, la CDP non le rileva. Affinché le modifiche vengano rilevate dalla CDP, è necessario salvarle e chiudere il file.
La configurazione degli host	Viene generato un avviso	Per evitare conflitti, è necessario

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
Hyper-V non è valida	quando sono presenti due o più agenti per Hyper-V installati negli host Hyper-V che presentano lo stesso nome host; ciò non è consentito a livello dello stesso account.	registrare gli Agenti per Hyper-V su unità figlio diverse di questo account.
Convalida non riuscita	Viene generato un avviso quando il processo di convalida del backup non viene completato.	Verificare il registro dell'operazione difettosa: fare clic per selezionare il sistema, quindi su **Attività**, e infine individuare l'avviso nel registro. Il messaggio dovrebbe indirizzare alla causa principale del problema notificato dal software.
Impossibile eseguire la migrazione dei backup nell'archivio nel cloud al nuovo formato	Viene generato un avviso quando non è possibile eseguire la migrazione dei backup nel cloud storage al nuovo formato.	La migrazione degli archivi di Acronis Cyber Backup Advanced è descritta qui. La migrazione degli archivi di Acronis Cyber Backup è descritta qui. Prima di contattare il supporto Acronis, acquisire i report indicati di seguito utilizzando lo strumento migrate_archives: **migrate_archives.exe --account=<Acronis Account> --password=<password> --subaccounts=All > report1.txt** **migrate_archives.exe --cmd=finishUpgrade --account=<Acronis Account> --password=<password> > report2.txt**
Password di crittografia mancante	Viene generato un avviso quando la chiave di crittografia del database non è corretta, è danneggiata o mancante.	Impossibile recuperare i backup crittografati se si perde o si dimentica la password. È necessario impostare questa password di crittografia in locale, nel dispositivo protetto. Non è possibile impostare la password di crittografia in un piano di protezione. Per ulteriori informazioni, consultare Impostare la password di crittografia.
Caricamento sospeso	Viene generato un avviso se un	

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
	controllo pianificato rileva che la Spedizione fisica dei dati all'archivio cloud per questo piano di backup non è stata caricata nello storage.	
Ripristino del backup non riuscito	Viene generato un avviso se l'operazione di ripristino non riesce quando si tenta di ripristinare backup di file o di sistema.	Determinare la data esatta in cui il backup non è riuscito e provare il ripristino con l'ultimo backup riuscito correttamente.

Avvisi di Disaster recovery

Avviso	Descrizione	Come risolvere l'avviso
La quota di storage è stata superata	Viene generato un avviso quando la quota variabile per lo storage di disaster recovery viene superata	Aumentare la quota o rimuovere alcuni archivi dal cloud storage.
La quota è stata raggiunta	Viene generato un avviso quando: • La quota variabile dei server cloud viene superata. • La quota variabile dei punti di calcolo viene superata. • La quota variabile degli indirizzi IP pubblici viene superata.	
Quota di archiviazione superata	Viene generato un avviso quando la quota fissa per lo storage di disaster recovery viene superata. Questo archivio è utilizzato dai server primari e di ripristino. Se il surplus per questa quota viene raggiunto, non sarà possibile creare server primari e di ripristino o aggiungere/estendere dischi ai server primari esistenti. Se il surplus per questa quota viene superato non sarà possibile avviare un failover o semplicemente avviare un server arrestato. I server in esecuzione non verranno arrestati.	
Quota superata	Viene generato un avviso quando:	Valutare l'acquisto di quote

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
	• La quota fissa dei server cloud viene superata. • La quota fissa dei punti di calcolo viene superata. • La quota fissa degli indirizzi IP pubblici viene superata.	aggiuntive per i dispositivi o disabilitare le attività di backup per i dispositivi che non è più necessario proteggere.
Errore di failover	Viene generato un avviso quando si verifica un problema di sistema dopo l'invio di un'azione di failover.	1. Nel server di ripristino, fare clic su **Modifica**. Per ulteriori informazioni, consultare Creazione di un server di ripristino. 2. Diminuire la CPU/RAM del server di ripristino. 3. Riprovare il failover.
Errore del test di failover	Viene generato un avviso quando si verifica un problema di sistema dopo l'invio di un'azione di test.	1. Nel server di ripristino, fare clic su **Modifica**. Per ulteriori informazioni, consultare Creazione di un server di ripristino. 2. Diminuire la CPU/RAM del server di ripristino. 3. Riprovare il failover. **Nota** Verificare che l'indirizzo IP specificato in Indirizzo IP in rete di produzione sia lo stesso specificato nella configurazione del server DHCP.
Errore di failback	Viene generato un avviso quando si verifica un problema di sistema dopo l'inizializzazione di un failback.	È possibile visualizzare la posizione errata negli elenchi di storage di backup: presenta un numero invece di un nome (in genere, il nome di una posizione corrisponde a uno dei nomi degli utenti finali esistenti) e non è stata creata dall'utente. Rimuovere la posizione errata: 1. Nella console di Cyber Protect, passare a Storage di backup. 2. Individuare la posizione e

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
		fare clic sull'icona a croce (x) per eliminarla. 3. Confermare la selezione facendo clic su Elimina. 4. Riprovare il failover.
Failback annullato	Viene generato un avviso quando il failback viene cancellato dall'utente.	Cancellazione manuale dell'avviso dalla console.
Errore di connessione VPN	Viene generato un avviso quando l'errore della connessione VPN si verifica per ragioni che non dipendono dalle azioni dell'utente. Il report sullo stato di un'appliance VPN è obsoleto.	Nel caso in cui si sia riscontrato un problema con il deployment o la connessione di un'appliance VPN Acronis, contattare il supporto Acronis. Con l'e-mail inviare le informazioni seguenti: • Screenshot dei messaggi di errore (se presenti) • Screenshot dell'interfaccia a riga di comando dell'appliance VPN Acronis • Nome data center e gruppo di Acronis Backup Cloud.
(VPN non raggiungibile) Il gateway di connessione non è raggiungibile	Viene generato un avviso quando il servizio DR non riesce a raggiungere il gateway di connessione. Il report sullo stato del gateway di connessione è obsoleto.	Nel caso in cui si sia riscontrato un problema con il deployment o la connessione di un'appliance VPN Acronis, contattare il supporto Acronis. Con l'e-mail inviare le informazioni seguenti: • Screenshot dei messaggi di errore (se presenti) • Screenshot dell'interfaccia a riga di comando dell'appliance VPN Acronis • Nome data center e gruppo di Acronis Backup Cloud
IP di riassegnazione del DR necessario	Viene generato un avviso se l'appliance VPN rileva modifiche alla rete.	Riassegnare l'indirizzo IP. Per ulteriori informazioni, consultare Nuova assegnazione di indirizzi IP.

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
Errore del gateway di connessione	Viene generato un avviso quando non è possibile distribuire il server VPN nel cloud.	Utilizzare lo strumento di verifica della connessione e controllare i risultati per evidenziare eventuali errori. Consentire il software Acronis tramite il controllo dell'applicazione dei firewall e del software anti-malware.
Creazione del server primario non riuscita	Viene generato un avviso quando il server primario non viene creato a causa di un errore.	
Creazione del server di ripristino non riuscita	Viene generato un avviso quando il server di ripristino non viene creato a causa di un errore.	Verificare che il server di ripristino soddisfi i Requisiti software.
Server primario eliminato	Viene generato un avviso quando il server primario viene eliminato.	
Errore di ripristino del server	Viene generato un avviso quando il server primario o il server di ripristino non vengono ripristinati.	Trovare i dettagli. Se il messaggio di errore è generico o poco chiaro, ad esempio riporta "Errore interno", passare a **Disaster Recovery → Server**, fare clic per selezionare i sistemi interessati e fare clic su **Attività**. Fare clic su un'attività, tenere premuto il tasto Ctrl e fare clic con il pulsante sinistro del mouse sull'attività. Viene visualizzata l'icona dei puntini di sospensione (...) accanto a ogni attività. Fare clic e selezionare **Info su questa attività**.
Backup non riuscito	Viene generato un avviso quando non riesce il backup del server cloud (primario o server in stato di failover in produzione).	1. Verificare la connessione della posizione di backup. 2. Controllare il dispositivo di storage di backup.
Limiti di rete superati	Viene generato un avviso quando viene raggiunto il numero massimo di reti cloud (5 reti cloud).	
Runbook non riuscito	Viene generato un avviso quando l'esecuzione del runbook non riesce.	Non incide sulla funzionalità del prodotto e può essere ignorato

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
		in sicurezza. Per ulteriori informazioni, consultare Creazione di un runbook.
Avviso relativo al runbook	Viene generato un avviso quando l'esecuzione del runbook viene completata con avvisi.	Non incide sulla funzionalità del prodotto e può essere ignorato in sicurezza. Per ulteriori informazioni, consultare Creazione di un runbook.
È necessaria l'interazione dell'utente del runbook	Viene generato un avviso quando il runbook è in attesa dell'interazione dell'utente.	Non incide sulla funzionalità del prodotto e può essere ignorato in sicurezza. Per ulteriori informazioni, consultare Creazione di un runbook.
Traffico Internet bloccato	Viene generato un avviso quando il traffico Internet viene bloccato dall'amministratore.	
Traffico Internet sbloccato	Viene generato un avviso quando il traffico Internet viene sbloccato dall'amministratore.	
Sovrapposizione delle reti locali	Viene generato un avviso quando vengono individuate reti locali identiche o sovrapposte.	
Quota del server insufficiente per il passaggio ad altro modello di licensing	Viene generato un avviso quando la quota dei server cloud non è sufficiente.	• Verificare che il tenant e l'utente dispongano di quote dei server di web hosting o di quote di server disponibili per un server fisico. • Verificare che il tenant e l'utente dispongano di quote dei server di web hosting o di quote di virtual machine disponibili per un server virtuale. Un server virtuale non può utilizzare quote dei server.
Elemento in offerta insufficiente per il passaggio ad altro modello di licensing	Viene generato un avviso quando l'elemento in offerta dello storage di disaster recovery viene disabilitato.	Per ulteriori informazioni, consultare Quote di disaster recovery.
Errore di passaggio ad altro modello di licensing	Viene generato un avviso quando l'aggiornamento del disaster	

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
	recovery ha riscontrato un errore.	
Punti di calcolo insufficienti per il passaggio ad altro modello di licensing	Viene generato un avviso quando non sono disponibili punti di calcolo.	Nel portale di gestione, controllare e aumentare la quota fissa per i punti di calcolo.
Elementi in offerta dei server insufficienti per il passaggio ad altro modello di licensing	Viene generato un avviso quando l'elemento in offerta dei server cloud è disabilitato.	
Creazione del server di ripristino tramite policy non riuscita	Viene generato un avviso quando si è verificato un errore durante la configurazione dell'infrastruttura di disaster recovery.	Creare manualmente il server di ripristino senza la proprietà Accesso a Internet. Per ulteriori informazioni, consultare Creazione di un server di ripristino
Il test automatico di failover del processore di backup è stato ripianificato	Viene generato un avviso quando l'esecuzione del test di failover automatizzato è stata ripianificata.	
Timeout del test automatico di failover del processore di backup raggiunto	Viene generato un avviso quando l'esecuzione del test di failover automatizzato è scaduta. **Nota** Ogni test di failover automatizzato eseguito consuma dei punti di calcolo ricaricabili.	
Errore generico del test di failover del processore di backup	Viene generato un avviso quando l'ultimo testo di failover automatizzato pianificato del server di ripristino non viene eseguito.	1. Avviare il test di failover del server di ripristino manualmente. Per ulteriori informazioni, consultare Esecuzione di un test di failover. 2. Attendere la successiva data pianificata di esecuzione del test di failover automatizzato
Errore di trasferimento dei dati di failback	Viene generato un avviso quando il trasferimento dei dati failback non riesce.	
Failback non riuscito	Viene generato un avviso quando si riscontra un errore nel failback.	È possibile visualizzare la posizione errata negli elenchi di storage di backup: presenta un numero invece di un nome (in

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
		genere, il nome di una posizione corrisponde a uno dei nomi degli utenti finali esistenti) e non è stata creata dall'utente. Rimuovere la posizione errata: 1. In Cyber Protection, passare allo storage di backup. 2. Individuare la posizione e fare clic sull'icona a croce (x) per eliminarla. 3. Confermare la selezione facendo clic su **Elimina**. Riprovare il failover.
Conferma del failback non riuscita	Viene generato un avviso quando la conferma del failback non riesce.	
Il sistema di failback è pronto per lo switchover	Viene generato un avviso quando il sistema è pronto per eseguire lo switchover.	
Switchover del failback terminato	Viene generato un avviso quando lo switchover è riuscito.	Cancellazione manuale dell'avviso dalla console.
Agente di destinazione del failback offline	Viene generato un avviso quando l'agente è offline.	

Avvisi di Protezione anti-malware

Avviso	Descrizione	Come risolvere l'avviso
È stata rilevata un'attività di connessione remota sospetta	Viene generato un avviso quando viene rilevato un ransomware proveniente da una connessione remota.	Cancellazione manuale dell'avviso dalla console.
È stata rilevata un'attività sospetta	Viene generato un avviso quando viene rilevato un ransomware nel workload.	Cancellazione manuale dell'avviso dalla console. per disattivare l'avviso. A seconda dell'opzione specificata nel piano di Active Protection, il processo pericoloso viene arrestato, le modifiche apportate dal processo vengono ripristinate o nessuna azione viene intrapresa ed è necessario risolvere il problema manualmente.

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
		Leggere i dettagli dell'avviso per individuare il processo che sta crittografando i file e i file interessati. Se si decide che il processo che crittografa i file è approvato (avviso falso-positivo), aggiungere questo processo ai processi affidabili: 1. Aprire il Piano di Active Protection. 2. Fare clic su **Modifica** per modificare le impostazioni. 3. In **Processi affidabili**, specificare i processi che non devono mai essere considerati ransomware. Specificare il percorso completo del processo eseguibile, iniziando con la lettera di unità. Per esempio: C:\Windows\Temp\er76s7sdkh.exe.
È stata rilevata un'attività di mining di criptovalute	Viene generato un avviso quando viene rilevato un cryptominer illecito nel workload	Cancellazione manuale dell'avviso dalla console.
Difesa del MBR: Attività sospetta rilevata e sospesa	Viene generato un avviso quando viene rilevato un ransomware nel workload (nello specifico, la partizione MBR/GPT è modificata dal ransomware).	Cancellazione manuale dell'avviso dalla console.
È stato specificato un percorso di rete non valido	Viene generato un avviso quando il percorso di ripristino fornito dall'amministratore non è un percorso alla cartella locale.	Specificare il percorso locale alla protezione della cartella di rete (percorso di ripristino). Cancellare manualmente l'avviso dalla console
Processo critico aggiunto come dannoso al piano di Active Protection	Viene generato un avviso quando un processo critico viene aggiunto come processo bloccato all'elenco delle Esclusioni dalla protezione.	Cancellazione manuale dell'avviso dalla console.
Impossibile applicare il criterio Active Protection	Viene generato un avviso quando l'applicazione di	Fare clic sul messaggio di errore per visualizzare il motivo per cui non è stato

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
	una policy di Active Protection non è riuscita.	possibile applicare la policy di Active Protection.
Secure Zone: Operazione non autorizzata rilevata e bloccata	Viene generato un avviso quando viene rilevato un ransomware nel workload (la partizione ASZ è modificata dal ransomware).	Cancellazione manuale dell'avviso dalla console.
Il servizio Active Protection non è in esecuzione	Viene generato un avviso quando il servizio Active Protection si è arrestato/non è in esecuzione.	Controllare il messaggio di errore per visualizzare il motivo per cui il servizio Active Protection non è in esecuzione.
Il servizio Active Protection non è disponibile	Viene generato un avviso quando il servizio Active Protection non è disponibile perché un driver non è compatibile o è mancante.	Controllare il registro degli eventi di Windows che riporta le interruzioni del servizio Acronis Active Protection (acronis_protection_ service.exe).
Conflitto con un'altra soluzione di sicurezza	Viene generato un avviso se Active Protection non è disponibile per il sistema ' {{resourceName}}' perché è stato rilevato un conflitto con un'altra soluzione di sicurezza. Per attivare Active Protection, disattivare o disinstallare la soluzione di sicurezza in conflitto.	**Soluzione 1**: Se si desidera utilizzare la protezione Acronis in tempo reale, disinstallare l'antivirus di terze parti dal sistema. **Soluzione 2**: Se si desidera utilizzare un antivirus di terze parti, disabilitare la protezione Acronis in tempo reale, il filtro degli URL e l'antivirus Windows Defender dal piano di protezione.
L'azione di quarantena non è riuscita	Viene generato un avviso quando l'anti-malware non è riuscito a mettere in quarantena un malware individuato.	Controllare il messaggio di errore per visualizzare il motivo per cui la quarantena non è riuscita.
Rilevato processo dannoso	Viene generato un avviso quando il motore comportamentale rileva un malware (tipo di processo). Il malware rilevato viene messo in quarantena.	Cancellazione manuale dell'avviso dalla console.
È stato rilevato un	Viene generato un avviso	Cancellazione manuale dell'avviso dalla

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
processo dannoso, ma non è stato inviato in quarantena	quando il motore comportamentale rileva un malware (tipo di processo). Il malware rilevato non viene messo in quarantena.	console.
Malware rilevato e bloccato (ODS)	Viene generato un avviso quando una scansione pianificata rileva un malware. Il malware rilevato viene messo in quarantena.	Cancellazione manuale dell'avviso dalla console.
Malware rilevato e bloccato (RTP)	Viene generato un avviso quando la protezione in tempo reale rileva un malware. Il malware rilevato viene messo in quarantena.	Cancellazione manuale dell'avviso dalla console.
Malware rilevato in un backup	Viene generato un avviso quando una scansione di backup reale rileva un malware.	Cancellazione manuale dell'avviso dalla console.
È stato rilevato un conflitto tra la Protezione anti-malware in tempo reale e un prodotto di sicurezza	Viene generato un avviso quando l'anti-malware non ha completato la registrazione nel Windows Security Center.	Disabilitare o disinstallare il prodotto di sicurezza di terze parti, o disabilitare la Protezione anti-malware in tempo reale nel piano di protezione.
Impossibile eseguire il modulo Microsoft Security Essentials	Viene generato un avviso quando non è possibile eseguire il modulo Microsoft Security Essentials.	Controllare il messaggio di errore per visualizzare il motivo per cui non è stato possibile eseguire il modulo Microsoft Security Essentials.
Protezione in tempo reale non disponibile perché risulta installato un software antivirus di terzi	Viene generato un avviso quando non è stato possibile attivare la protezione in tempo reale perché è ancora abilitata nell'antivirus di terze parti.	Disabilitare o disinstallare il prodotto di sicurezza di terze parti, o disabilitare la Protezione anti-malware in tempo reale nel piano di protezione.
Protezione in tempo reale non disponibile a causa di driver incompatibile o mancante	Viene generato un avviso quando la protezione in tempo reale non è disponibile a causa di driver incompatibile o mancante.	Controllare il messaggio di errore per visualizzare il motivo per cui Acronis non ha potuto installare il driver nel workload.

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
Il servizio Cyber Protection (o Active Protection) non risponde	Viene generato un avviso quando il servizio Cyber Protection risponde a un ping di controllo dell'integrità dalla console.	Cancellazione manuale dell'avviso dalla console.
Aggiornamento delle definizioni di sicurezza non riuscito	Viene generato un avviso quando l'aggiornamento delle definizioni di sicurezza non riesce.	Controllare il messaggio di errore per visualizzare il motivo per cui l'aggiornamento delle definizioni di sicurezza non è riuscito.
Protezione antimanomissione abilitata	Viene generato un avviso quando le impostazioni di Microsoft Defender non possono essere modificate perché la protezione antimanomissione è abilitata.	Disabilitare le impostazioni della protezione antimanomissione nel workload Windows.
Esecuzione del modulo di Windows Defender non riuscita	Viene generato un avviso quando l'esecuzione del modulo Windows Defender non riesce.	Controllare il messaggio di errore per visualizzare il motivo per cui non è stato possibile eseguire il modulo Windows Defender.
Windows Defender è bloccato da un software antivirus di terze parti	Viene generato un avviso quando Windows Defender è bloccato perché un antivirus di terze parti è installato nel sistema.	Disabilitare o disinstallare il prodotto di sicurezza di terze parti.
Conflitto tra criteri di gruppo	Viene generato un avviso quando le impostazioni di Microsoft Defender non possono essere modificate perché sono controllate da un criterio di gruppo.	Disabilitare le impostazioni del criterio di gruppo nel workload Windows.
Microsoft Security Essentials ha intrapreso un'azione per difendere questa macchina dal malware	Viene generato un avviso quando Microsoft Security Essential ha rilevato/messo in quarantena un malware.	Cancellazione manuale dell'avviso dalla console.
Microsoft Security Essentials ha rilevato un malware	Viene generato un avviso quando Microsoft Security Essentials ha rilevato un malware o altro software potenzialmente non	Cancellazione manuale dell'avviso dalla console.

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
	desiderato.	

Avvisi di Licensing

Avviso	Descrizione	Come risolvere l'avviso
Quota di archiviazione quasi raggiunta	Viene generato un avviso quando l'utilizzo scende al di sotto dell'80% (dopo un'attività di pulizia o di aggiornamento di una quota).	Valutare l'acquisto di ulteriore storage o liberare spazio su disco nel cloud storage.
Quota di archiviazione superata	Viene generato un avviso quando è utilizzato il 100% della quota di storage.	Acquistare altro spazio di storage. Per ulteriori informazioni su come eseguire questa operazione, verificare come acquistare altro cloud storage.
Quota del workload raggiunta	Viene generato un avviso quando l'utilizzo dell'elemento in offerta è > di 0 e l'utilizzo è > di quota, ma utilizzo <= quota + surplus della quota.	
Quota del workload superata	Viene generato un avviso quando l'utilizzo dell'elemento in offerta è > di quota + surplus della quota.	
Il workload non dispone della quota necessaria per l'applicazione di un piano di backup (la risorsa non dispone di una quota di servizio)	Viene generato un avviso quando: • La quota è stata rimossa manualmente: **Dispositivo** > **Dettagli** > **Quota di servizio**, quindi fare clic su **Modifica** e selezionare l'opzione **Nessuna quota**. • L'elemento in offerta della console di gestione è disabilitato. • Il valore di quota+surplus della quota della console di gestione dell'elemento in offerta è sceso al di sotto dell'utilizzo corrente.	
Impossibile proteggere un workload con quota assegnata	Viene generato un avviso quando l'elemento in offerta non è sufficiente, ed è necessario disporre di:	

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
	• un gruppo dinamico. • un piano di backup assegnato a tale gruppo. • è stata aggiunta una risorsa che rientra nel gruppo dinamico, ma presenta alcune qualità che impediscono di applicare a questa lo stesso piano di backup.	
Licenza in abbonamento scaduta	Viene generato un avviso quando il controllo quotidiano per la scadenza del contratto di licenza/di manutenzione invia una richiesta al server delle licenze e ottiene come risposta che la licenza è scaduta.	Una volta scaduto l'abbonamento, tutte le funzionalità del prodotto ad eccezione del ripristino restano bloccate fino al successivo rinnovo della sottoscrizione. I dati di cui è stato eseguito il backup sono accessibili per il ripristino. Acquistare una nuova licenza. **Nota** Se di recente è stato acquistato un nuovo abbonamento, ma si riceve ancora un messaggio che indica che l'abbonamento è scaduto, è necessario importare il nuovo abbonamento dall'Account Acronis: nella console di gestione, passare a Impostazioni -> Licenze e dare clic su sincronizza nell'angolo in alto a destra. Gli abbonamenti verranno sincronizzati.
La licenza abbonamento sta per scadere	Viene generato un avviso quando il controllo quotidiano per la scadenza del contratto di licenza/di manutenzione invia una richiesta al server delle licenze e ottiene come risposta che la licenza scade tra 30 giorni.	Valutare l'acquisto di un nuovo abbonamento.

© Acronis International GmbH, 2003-2024

Avvisi di Filtro URL

Avviso	Descrizione	Come risolvere l'avviso
L'URL dannoso è stato bloccato	Viene generato un avviso quando un URL dannoso viene bloccato dal filtro degli URL.	Controllare le impostazioni del filtro degli URL. Il filtro degli URL sta bloccando delle pagine che dovrebbero essere bloccate secondo le impostazioni definite in Filtro URL.
Un avviso URL dannoso è stato ignorato	Viene generato un avviso quando si è selezionato di procedere con l'URL dannoso bloccato dal filtro degli URL.	Controllare le impostazioni del filtro degli URL.
È stato rilevato un conflitto tra il Filtro URL e un prodotto di sicurezza	Viene generato un avviso quando non è possibile abilitare il filtro degli URL a causa di un conflitto con un altro prodotto di sicurezza.	Controllare le impostazioni del filtro degli URL.
L'URL del sito web è bloccato	Viene generato un avviso quando un URL soddisfa tutti i criteri specificati nella categoria bloccata relativa al filtro degli URL.	Controllare le impostazioni del filtro degli URL.

Avvisi di EDR

Avviso	Descrizione	Come risolvere l'avviso
È stato rilevato un problema	Viene generato un avviso quando si riscontra un problema o quando lo stato di un problema esistente viene aggiornato.	Questo avviso fornisce informazioni su un nuovo problema o su un problema esistente che è stato aggiornato. È possibile visualizzare l'avviso oppure chiuderlo. È anche possibile aprire il problema per ulteriori indagini, se necessario.
È stato rilevato un indicatore di compromissione	Viene generato un avviso quando il servizio di ricerca delle minacce di EDR rileva un nuovo indicatore di compromissione.	Questo avviso informa l'utente che su uno o più workload è stato rilevato un indicatore di compromissione. È possibile visualizzare l'avviso e quindi fare clic sul link nell'avviso per ulteriori dettagli sull'indicatore.
Impossibile isolare il workload	Viene generato un avviso quando	Intraprendere le azioni

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
dalla rete	l'utente attiva un'azione per isolare il sistema dalla rete, ma l'azione di isolamento non riesce.	necessarie.
Impossibile riconnettere il workload alla rete	Viene generato un avviso quando l'utente attiva un'azione per riconnettere il sistema dalla rete, ma l'azione non riesce.	Intraprendere le azioni necessarie.
Impostazioni di Windows Defender Firewall modificate	Viene generato un avviso quando le impostazioni del firewall sono state modificate su un sistema isolato.	Questo avviso informa l'utente dell'avvenuta modifica dei dettagli del firewall nel sistema isolato. È un messaggio esclusivamente informativo ed è possibile chiudere l'avviso dopo averlo visualizzato.

Avvisi di Controllo dispositivo

Avviso	Descrizione	Come risolvere l'avviso
Controllo dispositivo e Prevenzione della perdita di dati verranno eseguiti con funzionalità limitate (è stata rilevata una CPU non compatibile)	Viene generato un avviso quando l'agente DeviceLock si avvia in un sistema fisico con CPU che supporta la tecnologia CET.	Disabilitare l'opzione sui sistemi interessati per evitare gli avvisi.
La funzionalità Controllo dispositivo non è ancora supportata su macOS Ventura	Viene generato un avviso quando l'agente DeviceLock si avvia in un sistema macOS Ventura fisico, e un piano di protezione con Controllo dispositivo viene applicato all'agente. È applicabile solo alle versioni in cui è presente un problema di kernel panic causato da un driver DeviceLock.	
Trasferimento dei dati sensibili consentito	Viene generato un avviso quando viene consentito il trasferimento di dati sensibili.	
Trasferimento dei dati sensibili giustificato	Viene generato un avviso quando viene giustificato il trasferimento di dati sensibili.	
Trasferimento dei dati sensibili	Viene generato un avviso quando	

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
negato	viene bloccato il trasferimento di dati sensibili.	
Rivedere i risultati della modalità di osservazione Prevenzione della perdita di dati	Viene generato un avviso quando è il momento di rivedere i risultati della modalità Osservazione: • La licenza di Advanced DLP Pack non è applicata. • È passato un mese da quando la modalità Osservazione è stata abilitata in un qualsiasi Piano di protezione applicato ad almeno un workload. • È passato un mese da quando l'ultimo avviso simile è stato emesso ed è stato rilevato un qualche utilizzo di DLP in modalità Osservazione.	
È stato modificato l'identificatore di sicurezza dell'utente	Viene generato un avviso quando un SID viene aggiornato per un nome utente conosciuto. L'avviso può essere generato quando il sistema operativo viene reinstallato in un PC che non appartiene al dominio.	
L'accesso al dispositivo generico è bloccato	Viene generato un avviso quando vengono bloccate alcune azioni (operazioni di lettura/scrittura) sui dispositivi supportati.	
Impossibile connettersi a una risorsa SSL remota.	Il sistema genera un avviso quando l'accesso a una risorsa SSL remota è bloccato dalla prevenzione dell'handshake aggiuntiva utilizzata sulla risorsa.	Aggiungere la risorsa all'elenco degli elementi consentiti per gli host remoti.

Avvisi di Sistema

Avviso	Descrizione	Come risolvere l'avviso
Agente obsoleto	Viene generato un avviso quando la versione dell'agente è obsoleta.	Passare all'elenco degli Agenti e avviar l'aggiornamento dell'agente interessato.

© Acronis International GmbH, 2003-2024

Avviso	Descrizione	Come risolvere l'avviso
Aggiornamento automatico non riuscito	Viene generato un avviso quando l'aggiornamento automatico dell'agente non riesce.	Provare a eseguire l'aggiornamento manuale.
È necessario riavviare il dispositivo dopo aver installato un nuovo agente	Viene generato un avviso quando è necessario un riavvio dopo la riuscita di un'installazione da remoto.	Riavviare il workload.
Attività non riuscita	Viene generato un avviso quando un'attività non riesce.	Riavviare tutti i servizi Acronis sul sistema.
Attività completata con avvisi	Viene generato un avviso quando un'attività riesce con avvisi.	
L'attività non risponde	Viene generato un avviso quando un'attività in corso non risponde.	
Distribuzione piano di backup non riuscita	Viene generato un avviso quando il deployment del piano di protezione non riesce.	
Impossibile convertire il nome utente in SID	Viene generato un avviso quando la conversione del SID pianificata non riesce.	

Widget di avviso

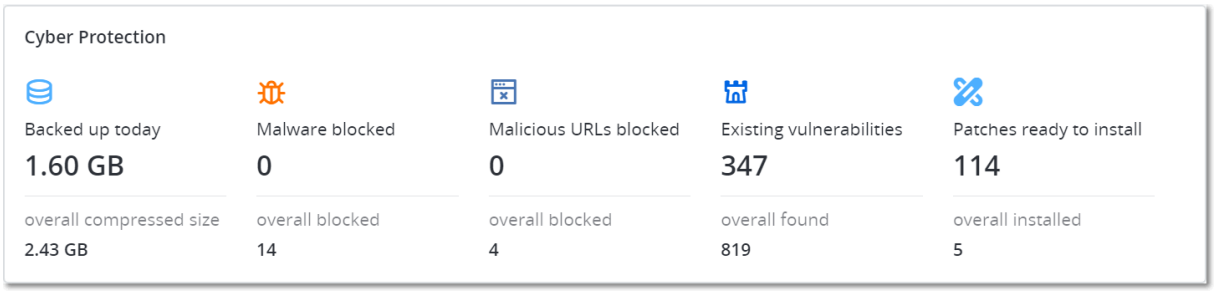
Nei widget degli avvisi è possibile visualizzare le seguenti informazioni sugli avvisi relativi al workload dell'utente:

Campo	Descrizione
Widget dei 5 avvisi più recenti	Un elenco dei cinque avvisi più recenti.
Riepilogo avvisi cronologici	Un widget grafico che, per ogni avviso, mostra la gravità, il tipo e l'intervallo temporale.
Riepilogo avvisi attivi	Un widget grafico che, per ogni avviso attivo, mostra la gravità, il tipo e la somma degli avvisi attivi.
Cronologia avvisi	Una visualizzazione in forma di tabella della cronologia degli avvisi.
Dettagli sugli avvisi attivi	Una visualizzazione in forma di tabella degli avvisi attivi.

© Acronis International GmbH, 2003-2024

Cyber Protection

Questo widget mostra informazioni generali su dimensione dei backup, malware bloccati, URL bloccati, vulnerabilità individuate e patch installate.



La riga superiore mostra le statistiche correnti:

- **Backup effettuato oggi** – la somma delle dimensioni dei punti di ripristino delle ultime 24 ore
- **Malware bloccati** – il numero di avvisi attualmente attivi relativi ai malware bloccati
- **URL bloccati** – il numero di avvisi attualmente attivi relativi agli URL bloccati
- **Vulnerabilità esistenti** – il numero di vulnerabilità attualmente esistenti
- **Patch pronte per l'installazione** – il numero di patch attualmente disponibili per l'installazione

La riga inferiore mostra le statistiche complessive:

- Dimensione compressa di tutti i backup
- Numero complessivo di malware bloccati in tutti i sistemi
- Numero complessivo di URL bloccati in tutti i sistemi
- Numero complessivo di vulnerabilità rilevate in tutti i sistemi
- Numero complessivo di patch/aggiornamenti installati in tutti i sistemi

Stato protezione

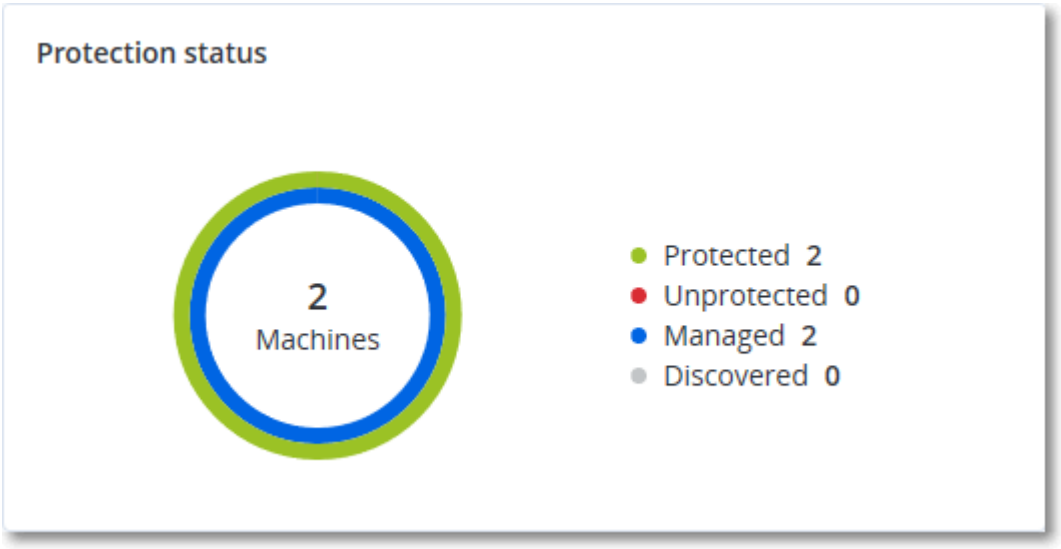
Questo widget mostra lo stato della protezione corrente di tutti i sistemi.

Un sistema può trovarsi in uno dei seguenti stati:

- **Protetto**: per tutti i sistemi con un piano di protezione applicato.
- **Non protetto**: per tutti i sistemi senza un piano di protezione applicato. Sono inclusi i sistemi individuati e quelli gestiti ai quali non è applicato un piano di protezione.
- **Gestito**: per tutti i sistemi con l'agente di protezione installato.
- **Individuato** : per tutti i sistemi senza l'agente di protezione installato.

Facendo clic sullo stato, si verrà reindirizzati all'elenco dei sistemi che presentano tale stato, per maggiori informazioni.

© Acronis International GmbH, 2003-2024



Macchine individuate

Questo widget mostra l'elenco dei sistemi rilevati durante l'intervallo di tempo specificato.

Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

Widget di Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) include sette widget, tutti accessibili dal dashboard **Panoramica**; tre di questi widget sono visualizzati per impostazione predefinita anche nella funzionalità EDR (consultare "Analisi riepilogativa dei problemi" (pag. 920)).

I sette widget disponibili sono:

- Distribuzione dei principali problemi per workload
- Stato minaccia (visualizzato in EDR)
- Cronologia gravità problema (visualizzato in EDR)

© Acronis International GmbH, 2003-2024

- MTTR dei problemi di sicurezza
- Burndown dei problemi di sicurezza
- Rilevamento per tattica (visualizzato in EDR)
- Stato della rete dei workload

Distribuzione dei principali problemi per workload

Questo widget mostra i primi cinque workload con il maggior numero di problemi (fare clic su **Mostra tutto** per essere reindirizzati all'elenco dei problemi filtrato in base alle impostazioni del widget).

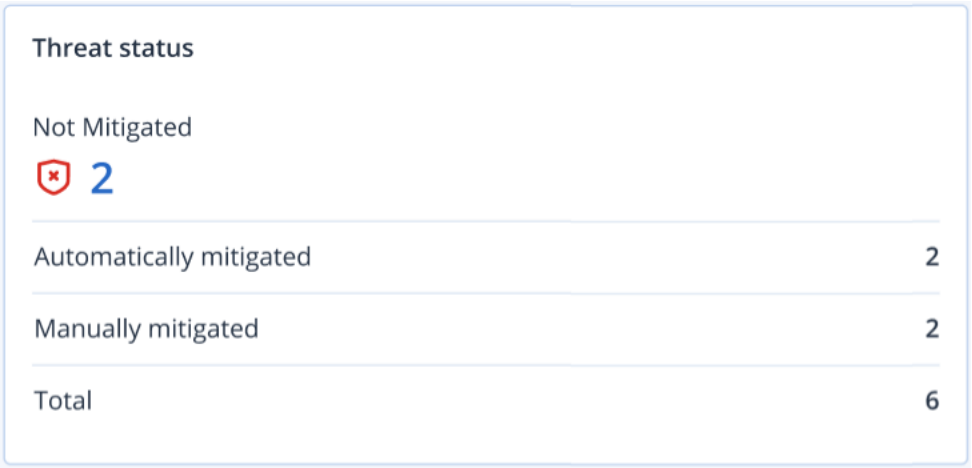
Passare il mouse su una riga del workload per visualizzare i dettagli dello stato corrente delle indagini sui problemi; i possibili stati dell'indagine sono **Non avviata**, **Indagine in corso**, **Chiusa** e **Falso positivo**. Fare quindi clic sul workload che si desidera analizzare ulteriormente; l'elenco dei problemi viene aggiornato in base alle impostazioni del widget.

Stato minaccia

Questo widget mostra lo stato corrente della minaccia per tutti i workload; evidenzia il numero attuale di problemi non mitigati che devono essere analizzati. Il widget indica anche il numero di problemi mitigati (manualmente e/o automaticamente dal sistema).

Fare clic sul numero accanto al problema **Non mitigati** per visualizzare nell'elenco dei problemi solo quelli non mitigati.

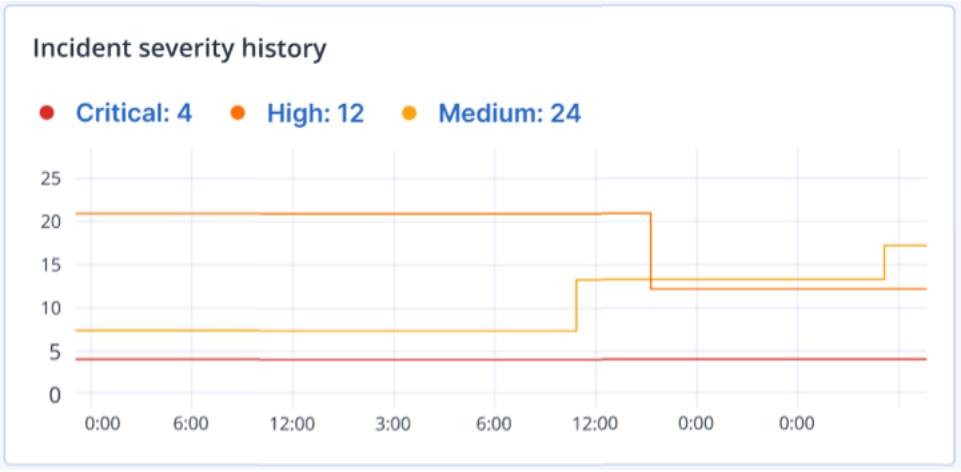
© Acronis International GmbH, 2003-2024



Cronologia gravità problema

Questo widget mostra l'evoluzione degli attacchi in base alla gravità e segnala possibili campagne di attacco. I picchi visualizzati possono indicare che l'organizzazione è sotto attacco.

Passare il mouse sul grafico per visualizzare una suddivisione della cronologia del problema in un punto specifico durante le 24 ore precedenti (periodo predefinito). Fare clic sul livello di gravità (**Critico**, **Alto** o **Medio**) per visualizzare l'elenco dei problemi correlati; l'utente viene reindirizzato all'elenco già filtrato con i problemi che corrispondono al livello di gravità selezionato.

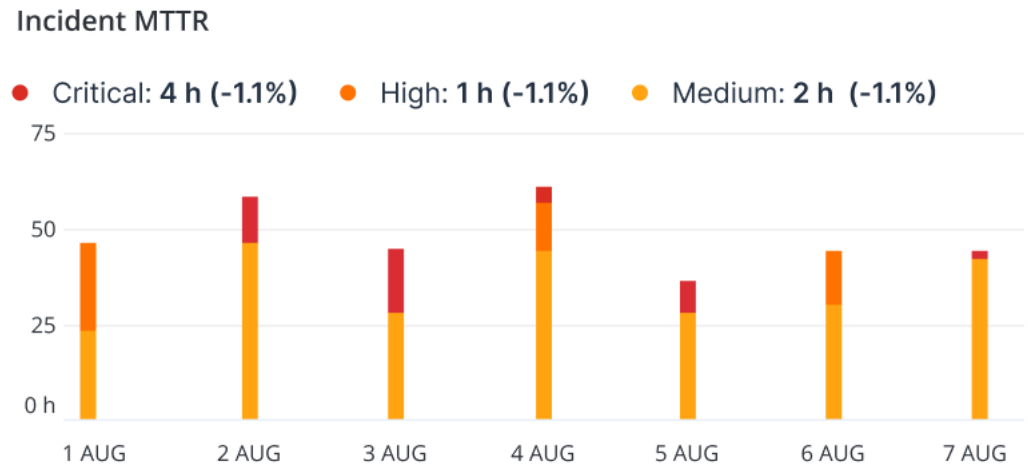


MTTR dei problemi di sicurezza

Questo widget mostra il tempo medio di risoluzione dei problemi di sicurezza. Indica la rapidità con la quale i problemi vengono analizzati e risolti.

Fare clic su una colonna per visualizzare in dettaglio i problemi in base al livello di gravità (**Critico**, **Alto** e **Medio**) e un'indicazione del tempo impiegato per risolverli in base ai diversi livelli di gravità. Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.

© Acronis International GmbH, 2003-2024

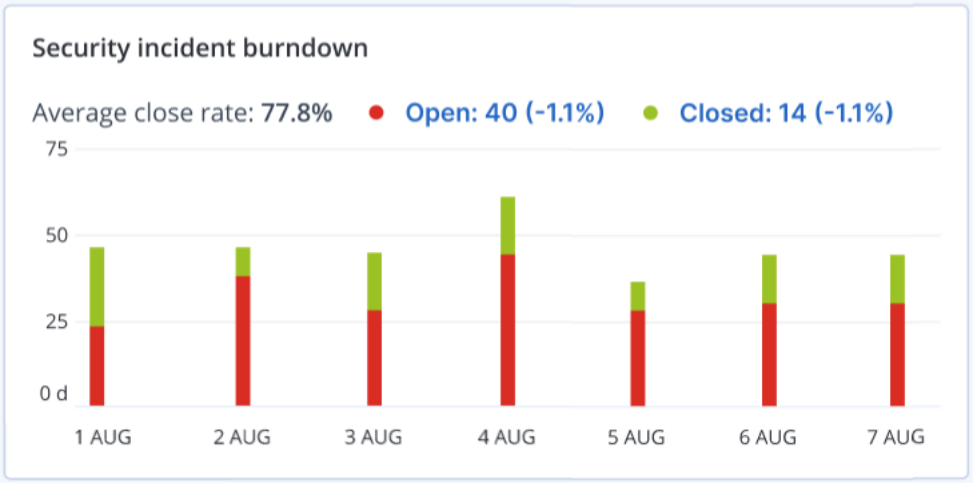


Burndown dei problemi di sicurezza

Questo widget indica il tasso di efficienza nella risoluzione dei problemi; il numero di problemi aperti viene misurato a fronte del numero di problemi chiusi in un determinato periodo di tempo.

Passare il mouse su una colonna per visualizzare in dettaglio i problemi chiusi o aperti per il giorno selezionato. Facendo clic sul valore Aperto, viene visualizzato l'elenco dei problemi filtrato su quelli attualmente aperti (con lo stato **Indagine in corso** o **Non avviata**). Se si fa clic sul valore Chiuso, viene visualizzato l'elenco dei problemi filtrato su quelli non più aperti (con lo stato **Chiuso** o **Falso positivo**).

Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.

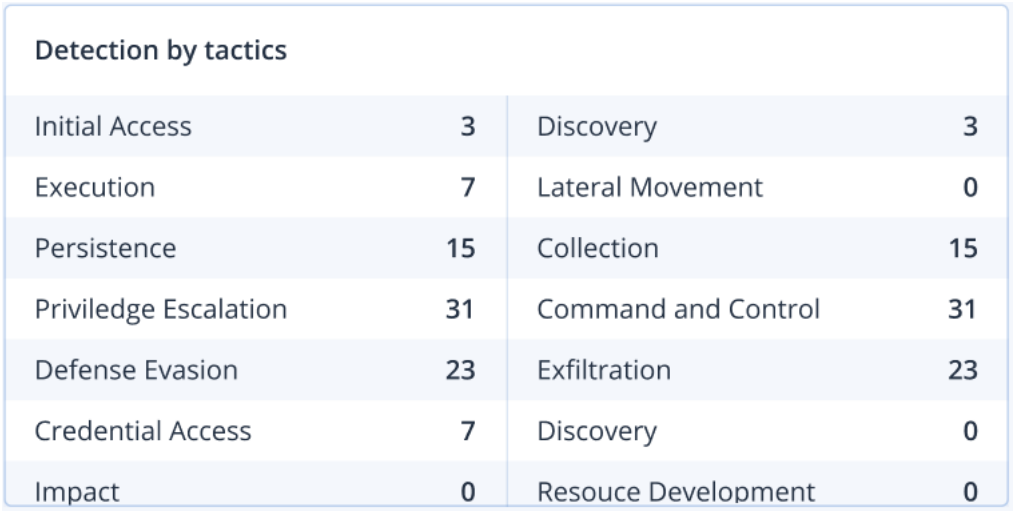


Rilevamento per tattica

Questo widget visualizza quante volte alcune tecniche di attacco specifiche sono state rilevate in problemi individuati in un periodo selezionato.

© Acronis International GmbH, 2003-2024

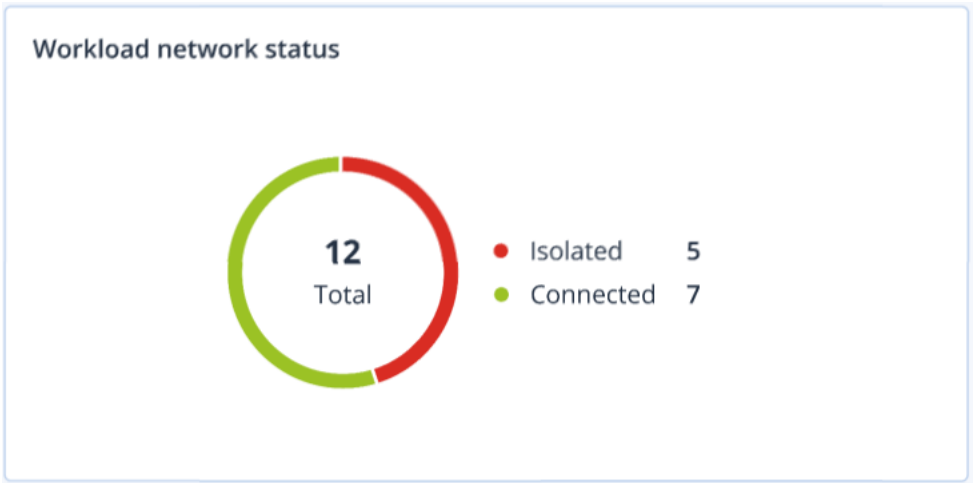
I valori in verde e rosso indicano se c'è stato un aumento o una diminuzione rispetto al periodo di tempo precedente. Nell'esempio seguente, gli attacchi di tipo Escalation dei privilegi e Comando e controllo hanno fatto registrare un aumento rispetto al periodo precedente; il dato potrebbe segnalare la necessità di analizzare il sistema di gestione delle credenziali migliorandone la sicurezza.



Stato della rete dei workload

Questo widget mostra lo stato corrente della rete dei workload e indica il numero di workload isolati e connessi.

Fare clic sul valore Isolato per visualizzare l'elenco Workload con agenti (nel menu **Workload** della console di Cyber Protect) filtrato per visualizzare i workload isolati. Fare clic sul valore Connesso per visualizzare l'elenco Workload con agenti filtrato sui workload connessi.



#CyberFit Score per sistema

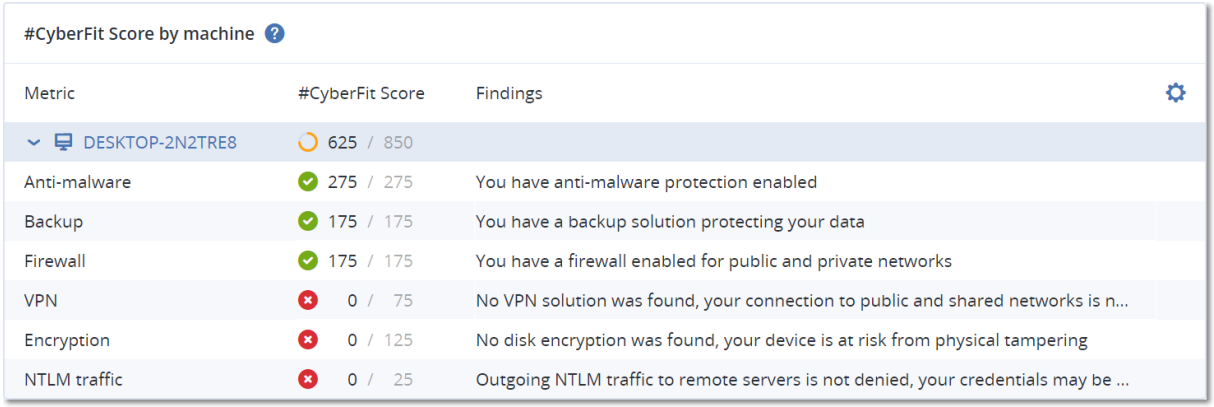
Questo widget mostra, per ogni sistema, il #CyberFit Score totale, i punteggi che lo compongono e i risultati ottenuti per ogni metrica valutata:

© Acronis International GmbH, 2003-2024

- Anti-malware
- Backup
- Firewall
- VPN
- Crittografia
- Traffico NTLM

Per migliorare il punteggio di ogni metrica è possibile visualizzare le raccomandazioni disponibili nel report.

Per ulteriori informazioni sul #CyberFit Score, consultare "#CyberFit Score dei sistemi".



Monitoraggio integrità del disco

Il monitoraggio dell'integrità del disco fornisce informazioni sullo stato corrente del disco e su quello prevedibile, così da prevenire perdite di dati che potrebbero essere correlate a un guasto del disco. La funzione supporta dischi HDD e SSD.

Limitazioni

- La previsione dell'integrità del disco è supportata solo per i sistemi che eseguono Windows.
- È possibile monitorare solo i dischi dei sistemi fisici. Non è possibile monitorare e mostrare nel widget dell'integrità del disco i dischi delle virtual machine.
- Non sono supportate le configurazioni RAID. I widget di integrità del disco non includono informazioni sui sistemi in cui è implementato RAID.
- Le unità SSD NVMe non sono supportate.

L'integrità del disco è rappresentata da uno dei seguenti stati:

- **OK**
  L'integrità del disco è compresa tra il 70 e il 100%.
- **Attenzione**
  L'integrità del disco è compresa tra il 30 e il 70%.

© Acronis International GmbH, 2003-2024

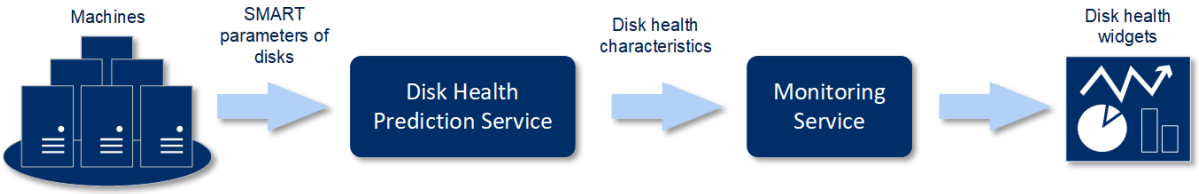
- **Critico**
  L'integrità del disco è compresa tra lo 0 e il 30%.
- **Calcolo dei dati del disco in corso**
  È in corso il calcolo dello stato corrente del disco e delle previsioni.

Come funziona

Il servizio Previsione dell'integrità del disco utilizza un modello di previsione basato su intelligenza artificiale.

1. L'agente di protezione acquisisce i parametri SMART dei dischi e invia i dati raccolti al servizio Previsione dell'integrità del disco:
   - SMART 5 – Conteggio dei settori riallocati.
   - SMART 9 – Ore di attività.
   - SMART 187 – Errori non correggibili segnalati.
   - SMART 188 – Timeout comando.
   - SMART 197 – Conteggio settori attualmente in sospeso.
   - SMART 198 – Conteggio settori non correggibili offline.
   - SMART 200 – Frequenza errori di scrittura.
2. Il servizio Previsione dell'integrità del disco elabora i parametri SMART ricevuti, effettua le previsioni e fornisce quindi le informazioni seguenti sull'integrità del disco:
   - Stato corrente di integrità del disco: OK, Attenzione, Critico.
   - Previsione dell'integrità del disco: negativa, stabile, positiva.
   - Probabilità della previsione dell'integrità del disco in percentuale.

   Il periodo di previsione è un mese.
3. Il Servizio di monitoraggio riceve queste caratteristiche e quindi mostra le informazioni pertinenti nei widget di integrità del disco nella console di Cyber Protect.



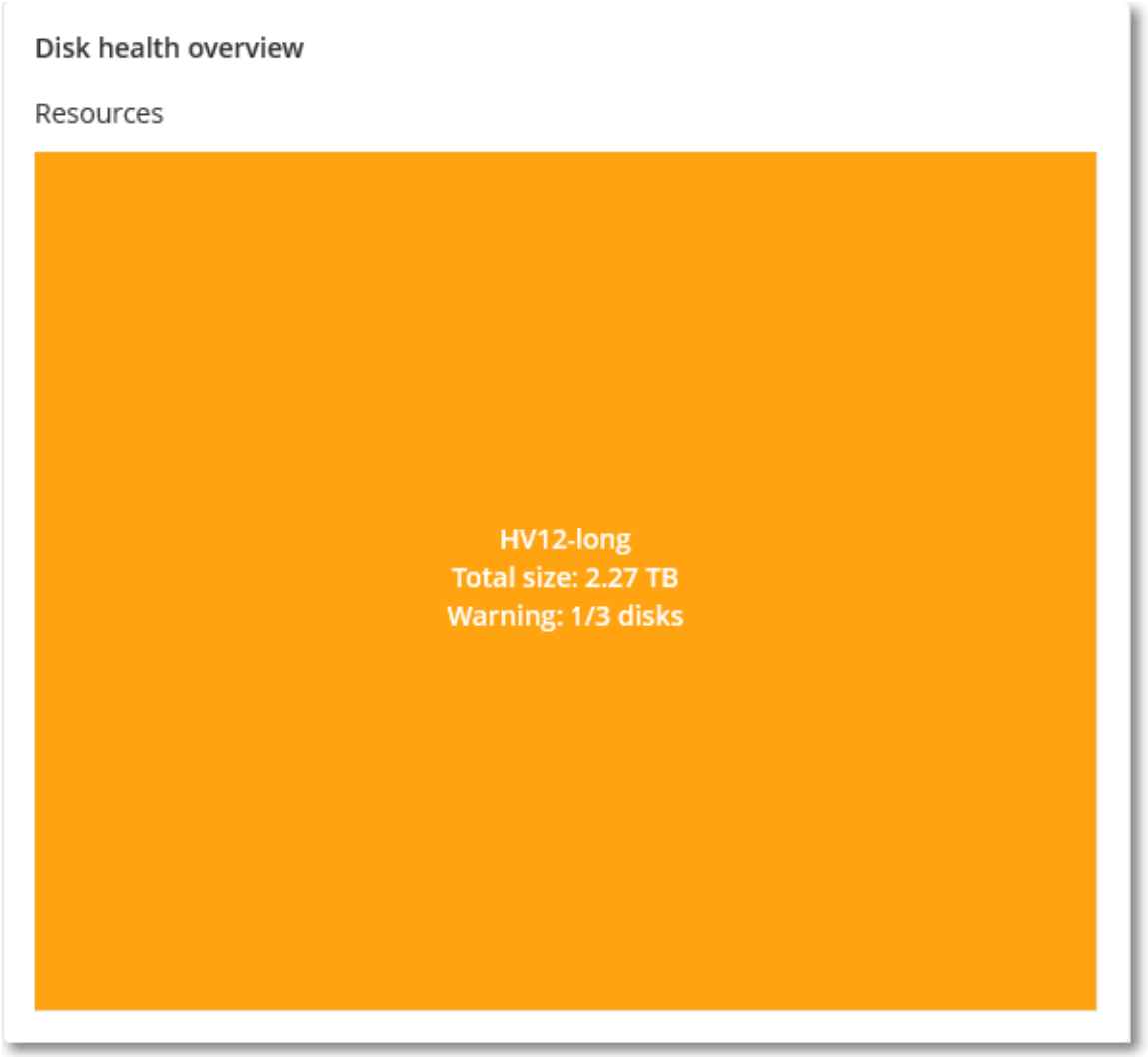
Widget di integrità del disco

I risultati del monitoraggio dell'integrità del disco vengono presentati nei widget seguenti, disponibili nella console di Cyber Protect.

- **Panoramica dell'integrità del disco** è un widget con struttura ad albero dotata di due livelli di dettaglio, visualizzabili eseguendo il drill down:
  - Livello del sistema
    Mostra informazioni di riepilogo sullo stato dell'integrità del disco di sistemi selezionati del

© Acronis International GmbH, 2003-2024

cliente. Vengono mostrati solo gli stati del disco critici. Gli altri stati vengono mostrati nei suggerimenti visualizzati quando si passa il mouse su uno specifico blocco. La dimensione del blocco del sistema dipende dalla dimensione totale di tutti i dischi del sistema. Il colore del blocco del sistema dipende dallo stato del disco con maggiore criticità individuato.

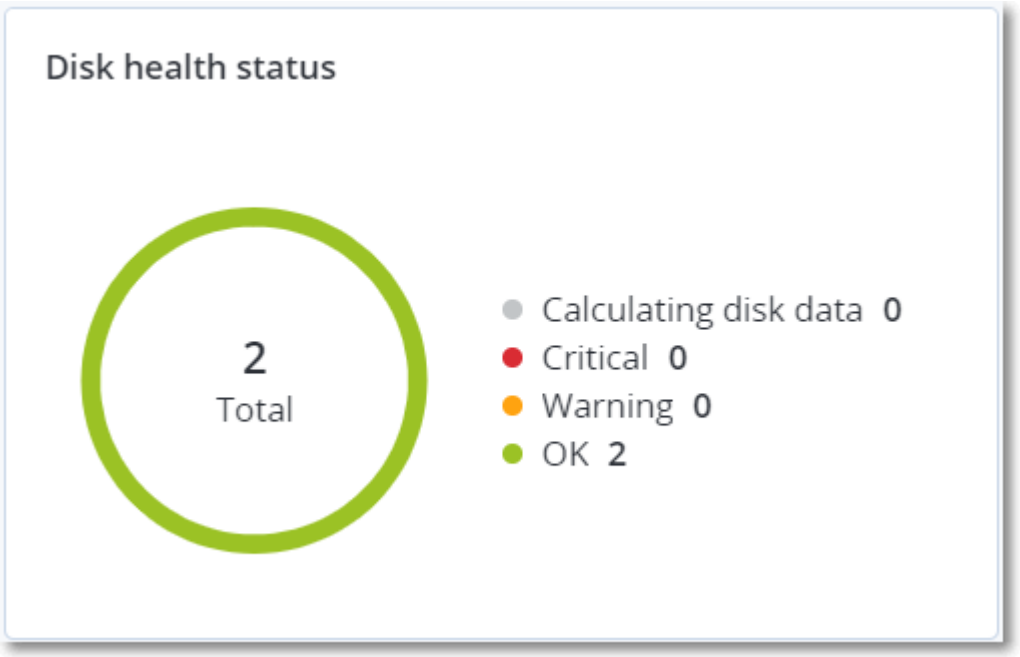


- Livello del disco
  Mostra lo stato corrente dell'integrità del disco di tutti i dischi del sistema selezionato. Ogni blocco disco mostra una delle seguenti previsioni di integrità del disco e la sua probabilità, espressa in percentuale:
  - Verrà danneggiato
  - Resterà stabile

© Acronis International GmbH, 2003-2024

- Verrà migliorato

- **Stato di integrità del disco** è un widget con grafico a torta che mostra il numero di dischi per ogni stato.



© Acronis International GmbH, 2003-2024

Avvisi di stato dell'integrità del disco

Il controllo dell'integrità del disco viene eseguito ogni 30 minuti, mentre l'avviso corrispondente viene generato una volta al giorno. Viene sempre generato un avviso quando lo stato di integrità del disco passa da **Attenzione** a **Critico**.

Nome avviso	Gravità	Stato integrità del disco	Descrizione
È possibile che il disco sia stato danneggiato	Attenzione	(30 – 70)	Il disco <nome disco> di questo sistema potrebbe subire un guasto nel prossimo futuro. Eseguire il backup dell'immagine completa del disco il più presto possibile, sostituirlo e quindi ripristinare l'immagine sul nuovo disco.
Il guasto del disco è imminente	Critico	(0 – 30)	Il disco <nome disco> in questo sistema è in condizioni critiche e potrebbe subire un danno nell'immediato futuro. Con queste condizioni il backup dell'immagine del disco non è consigliato, perché il lavoro aggiuntivo richiesto potrebbe causare il guasto del disco. Eseguire immediatamente il backup dei file più importanti presenti sul disco, e sostituirlo.

Mappa di protezione dati

Nota
Questa funzionalità è disponibile con il pacchetto Advanced Backup.

La funzione Mappa di protezione dati consente di individuare tutti i dati ritenuti importanti e di ottenere informazioni dettagliate su numero, dimensione, posizione, stato della protezione di tutti i file rilevanti, in una vista scalabile con mappa ad albero.

Ogni dimensione del blocco dipende dal numero/dimensione totale di tutti i file importanti che appartengono a un cliente/sistema.

I file possono presentare uno dei seguenti stati di protezione:

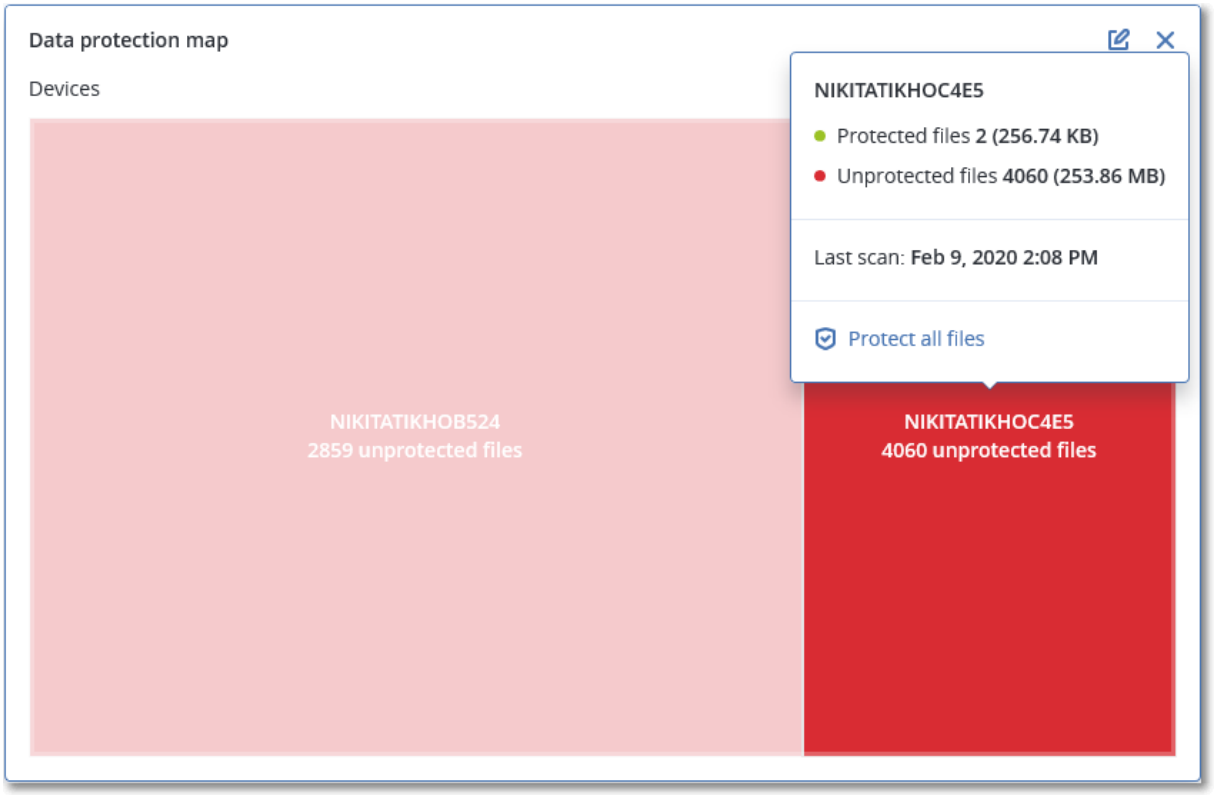
- **Critico** – è presente una percentuale compresa tra il 51 e il 100% di file non protetti con le estensioni specificate dall'utente di cui non viene eseguito il backup e di cui il backup non verrà eseguito con le impostazioni di backup esistenti per il sistema/la a posizione selezionati.
- **Basso** – è presente una percentuale compresa tra il 21 e il 50% di file non protetti con le estensioni specificate dall'utente di cui non viene eseguito il backup e di cui il backup non verrà eseguito con le impostazioni di backup esistenti per il sistema/la posizione selezionati.

© Acronis International GmbH, 2003-2024

- **Medio** – è presente una percentuale compresa tra l'1 e il 20% di file non protetti con le estensioni specificate dall'utente di cui non viene eseguito il backup e di cui il backup non verrà eseguito con le impostazioni di backup esistenti per il sistema/la posizione selezionati.
- **Alto** – tutti i file con le estensioni specificate dall'utente sono protetti (viene eseguito il backup) per il sistema/la posizione selezionati.

I risultati dell'analisi della protezione dati sono disponibili nel dashboard di monitoraggio nel widget Mappa della protezione dati, la cui struttura ad albero mostra i dettagli a livello di sistema.

- Livello del sistema – mostra informazioni di riepilogo sullo stato di protezione dei file importanti dei clienti selezionati.



Per proteggere file che non sono protetti, passare il mouse sul blocco e fare clic su **Proteggi tutti i file**. Nella finestra di dialogo sono reperibili informazioni sul numero di file non protetti e sulla loro posizione. Per proteggerli, fare clic su **Proteggi tutti i file**.

È inoltre possibile scaricare un rapporto dettagliato in formato CSV.

Widget di valutazione delle vulnerabilità

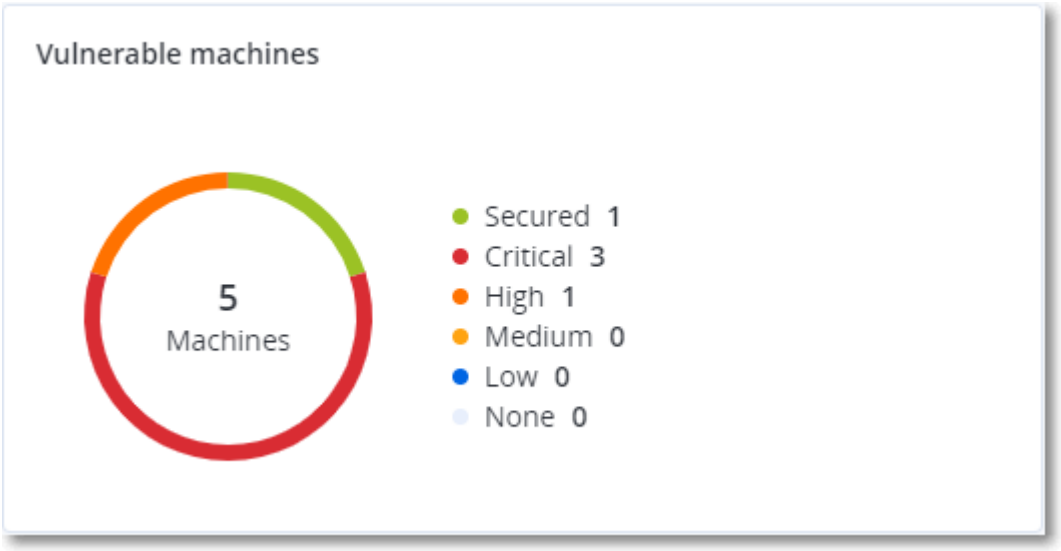
Sistemi vulnerabili

Questo widget mostra i sistemi vulnerabili ordinati in base alla gravità della vulnerabilità.

Conformemente al sistema CVSS (Common Vulnerability Scoring System) v3.0, la vulnerabilità individuata può presentare uno dei seguenti livelli di gravità:

© Acronis International GmbH, 2003-2024

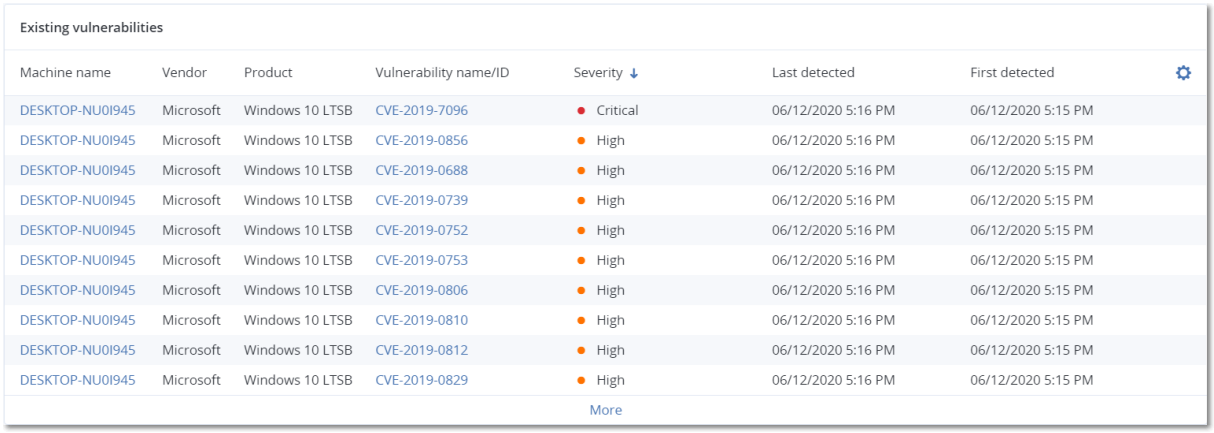
- Protetto: non sono state individuate vulnerabilità
- Critico: 9.0 - 10.0 CVSS
- Alto: 7.0 - 8.9 CVSS
- Medio: 4.0 - 6.9 CVSS
- Basso: 0.1 - 3.9 CVSS
- Nessuno: 0.0 CVSS



Vulnerabilità esistenti

Questo widget mostra le vulnerabilità attualmente esistenti sui sistemi. Nel widget **Vulnerabilità esistenti** sono presenti due colonne che mostrano gli indicatori data e ora:

- **Individuata per la prima volta** – la data e l'ora della prima individuazione della vulnerabilità nel sistema.
- **Individuata l'ultima volta** – la data e l'ora dell'ultima individuazione della vulnerabilità nel sistema.



© Acronis International GmbH, 2003-2024

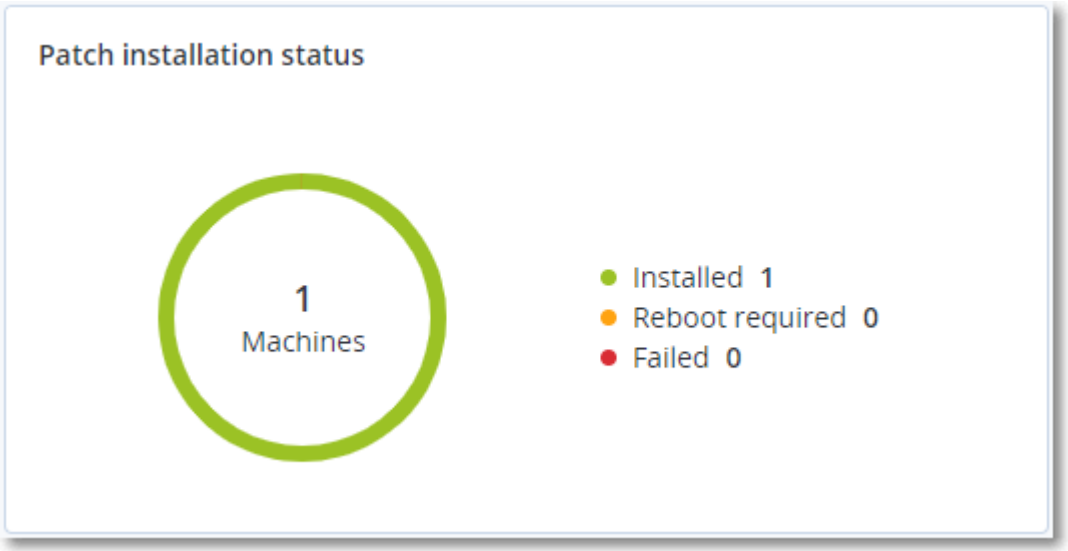
Widget di installazione patch

Sono disponibili quattro widget correlati alla funzionalità di gestione delle patch.

Stato di installazione patch

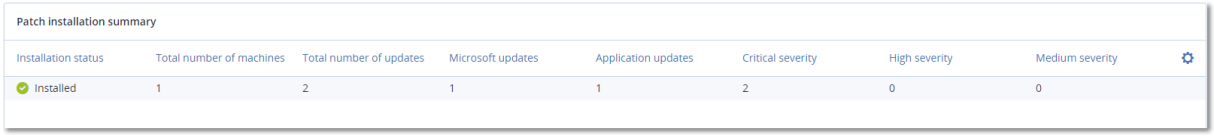
Questo widget mostra il numero di sistemi raggruppati in base allo stato di installazione delle patch.

- **Installate** – tutte le patch disponibili sono installate in un sistema
- **Riavvio necessario** – dopo l'installazione della patch, è richiesto il riavvio di un sistema
- **Non riuscita** – l'installazione di una patch non è riuscita in un sistema



Riepilogo di installazione patch

Questo widget mostra il riepilogo delle patch presenti nei sistemi, in base allo stato di installazione delle patch.



Cronologia di installazione patch

Questo widget mostra informazioni dettagliate sulle patch installate nei sistemi.

© Acronis International GmbH, 2003-2024

Patch installation history

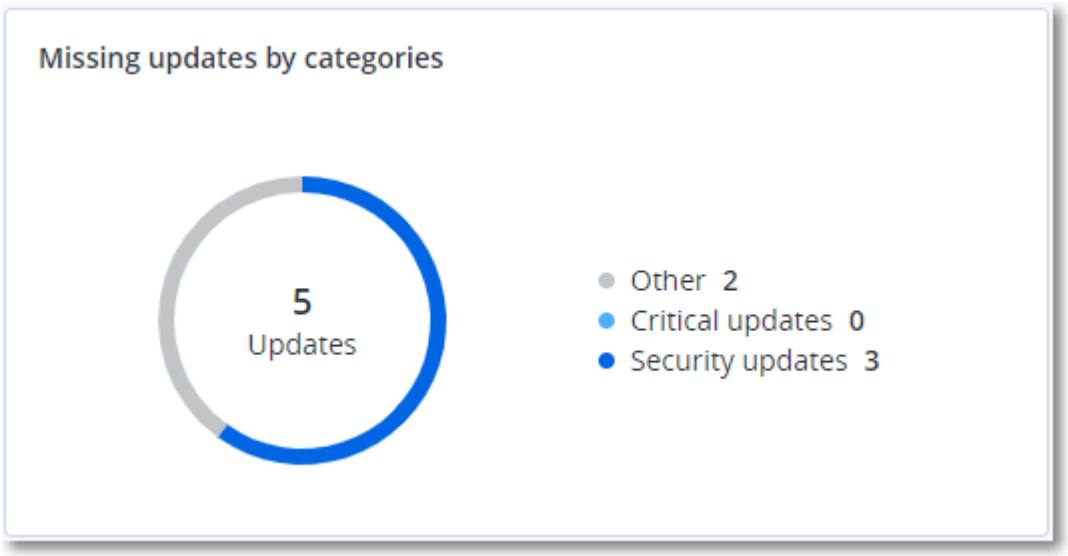
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020

More

Aggiornamenti non effettuati per categorie

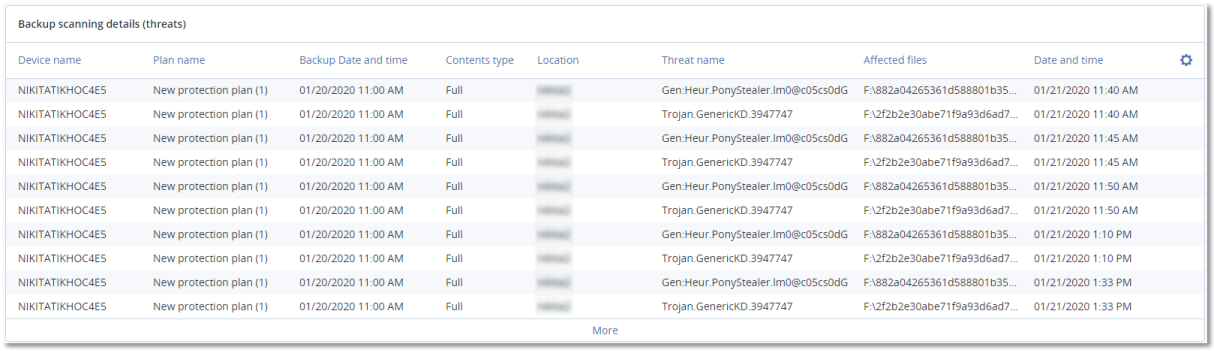
Questo widget mostra il numero di aggiornamenti non effettuati, per categoria. Vengono mostrate le seguenti categorie:

- Aggiornamenti di sicurezza
- Aggiornamenti critici
- Altro



Informazioni sulla scansione del backup

Questo widget mostra informazioni dettagliate sulle minacce individuate nei backup.



Backup scanning details (threats)

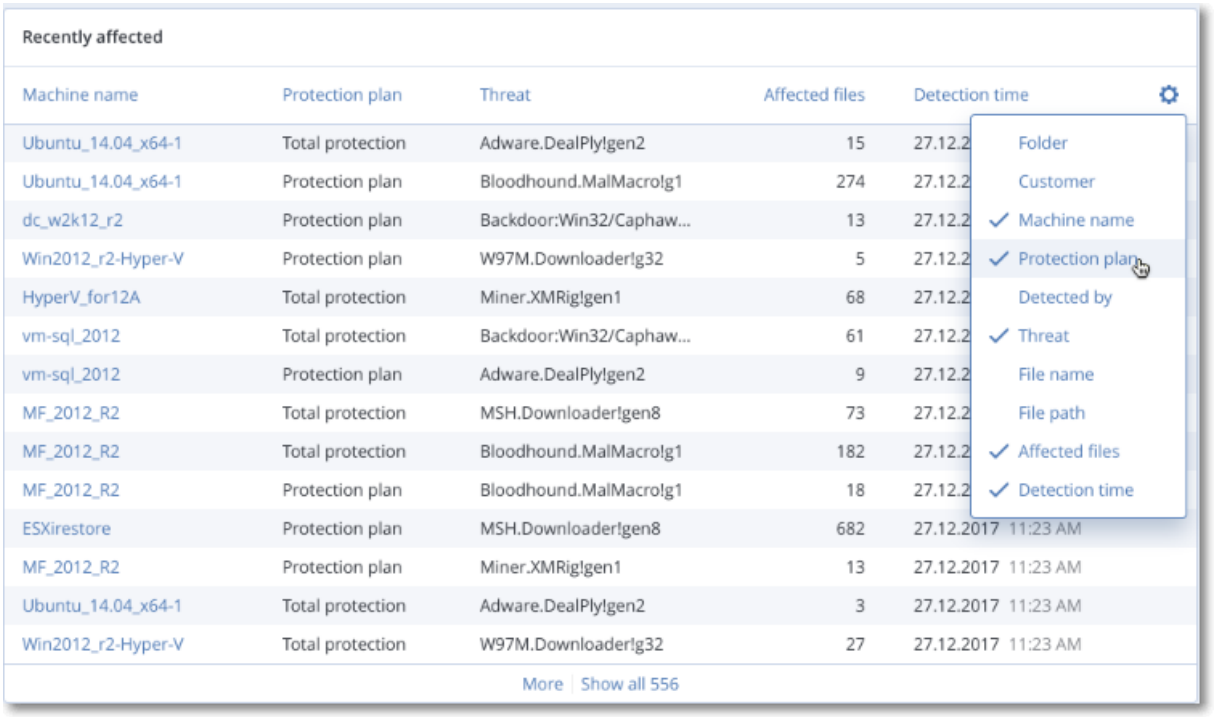
Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

© Acronis International GmbH, 2003-2024

Recentemente interessato

Questo widget mostra informazioni dettagliate sui workload recentemente interessati da minacce quali virus, malware e ramsomware. Lo strumento rende disponibili informazioni sulle minacce individuate, l'orario di individuazione e il numero di file infettati.



Download dei dati relativi ai workload recentemente interessati

È possibile scaricare i dati relativi ai workload recentemente interessati, generare un file CSV e inviarlo ai destinatari specificati.

Per scaricare i dati relativi ai workload recentemente interessati

1. Nel widget **Recentemente interessati** fare clic su **Scarica dati**.
2. Nel campo **Periodo di tempo**, inserire il numero di giorni per i quali scaricare i dati. Il numero massimo di giorni che è possibile inserire è 200.
3. Nel campo **Destinatari**, immettere gli indirizzi e-mail di tutte le persone che riceveranno un'e-mail con il link per scaricare il file CSV.
4. Fare clic su **Download**.

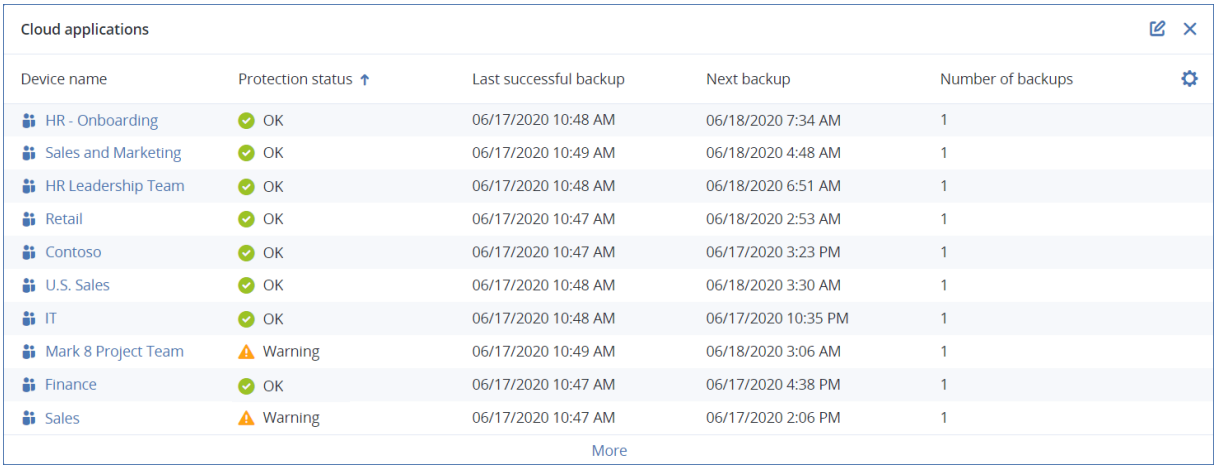
   Il sistema avvia la generazione del file CSV contenente i dati relativi ai workload interessati per il periodo di tempo specificato. Una volta completato il file CSV, il sistema invia un'e-mail ai destinatari. Ogni destinatario potrà quindi scaricare il file CSV.

Applicazioni cloud

Questo widget mostra informazioni dettagliate sulle risorse cloud-to-cloud.

© Acronis International GmbH, 2003-2024

- Utenti di Microsoft 365 (caselle di posta, OneDrive)
- Gruppi di Microsoft 365 (caselle di posta, sito del gruppo)
- Cartelle pubbliche di Microsoft 365
- Raccolte di siti di Microsoft 365
- Microsoft 365 Teams
- Utenti di Google Workspace (Gmail, Google Drive)
- Unità condivise di Google Workspace



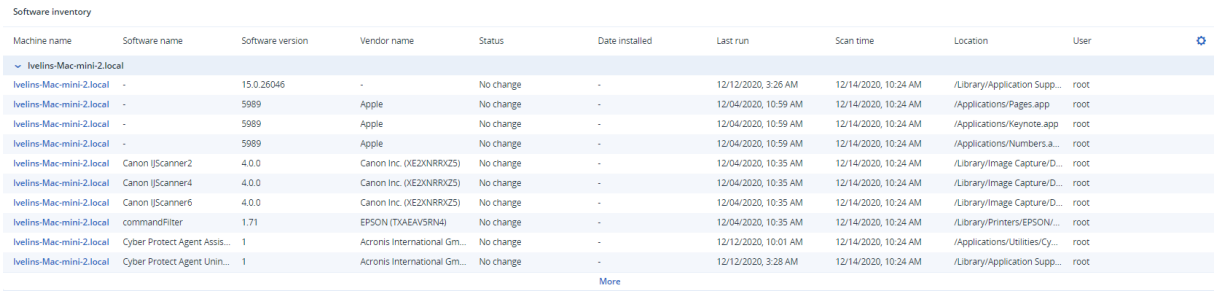
Nei seguenti widget sono disponibili ulteriori informazioni sulle risorse cloud-to-cloud:

- Attività
- Elenco attività
- 5 avvisi più recenti
- Cronologia avvisi
- Riepilogo avvisi attivi
- Riepilogo avvisi cronologici
- Dettagli sugli avvisi attivi
- Riepilogo posizioni

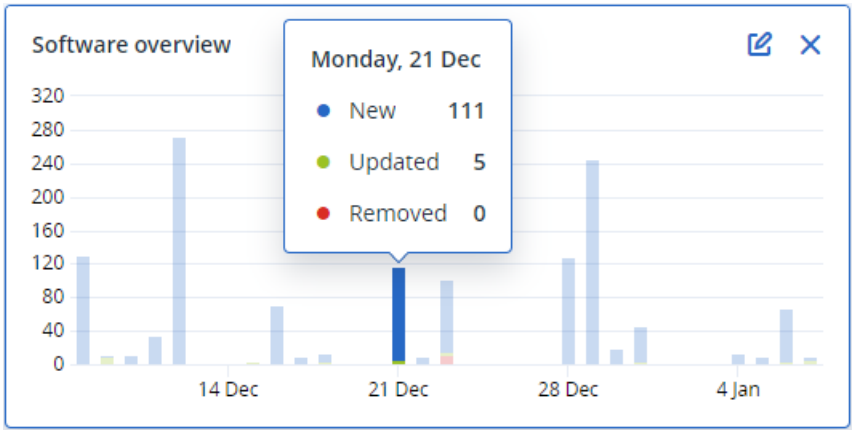
Widget Inventario software

Il widget di tabella **Inventario software** mostra informazioni dettagliate su tutti i componenti software installati nei sistemi Windows e macOS dell'organizzazione.

© Acronis International GmbH, 2003-2024



Il widget **Panoramica software** mostra il numero di applicazioni nuove, aggiornate ed eliminate sui sistemi Windows e macOS dell'organizzazione per il periodo di tempo specificato (7 giorni, 30 giorni o mese corrente).



Quando si passa il mouse su una determinata barra del grafico, viene visualizzato un suggerimento che mostra le informazioni seguenti:

Nuove - il numero di nuove applicazioni installate.

Aggiornate - il numero di applicazioni aggiornate.

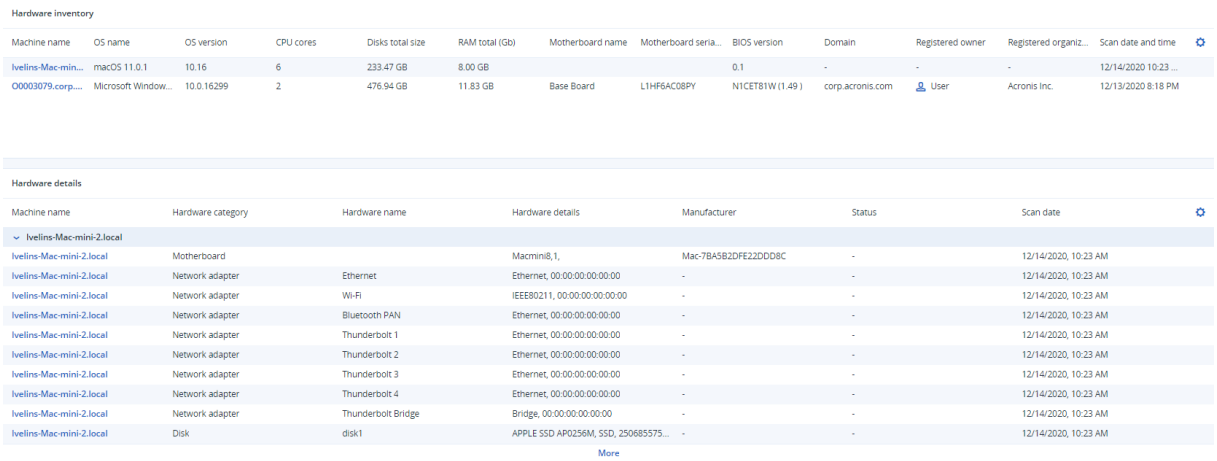
Rimosse - il numero di applicazioni rimosse.

Facendo clic sulla parte di barra relativa a un determinato stato, l'utente viene reindirizzato alla pagina **Gestione software** -> **Inventario software**. Le informazioni presenti nella pagina sono filtrate in base alla data e allo stato corrispondenti.

Widget Inventario hardware

I widget di tabella **Inventario hardware** e **Dettagli hardware** mostrano informazioni su tutti i componenti hardware installati sui dispositivi Windows e macOS fisici e virtuali dell'organizzazione.

© Acronis International GmbH, 2003-2024



Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-min...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp....	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1,	Mac-7BA5B2DFE22DDD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

More

Il widget di tabella **Modifiche hardware** mostra informazioni su tutti i componenti hardware aggiunti, eliminati e modificati sui sistemi Windows e macOS fisici e virtuali dell'organizzazione per il periodo di tempo specificato (7 giorni, 30 giorni o mese corrente).

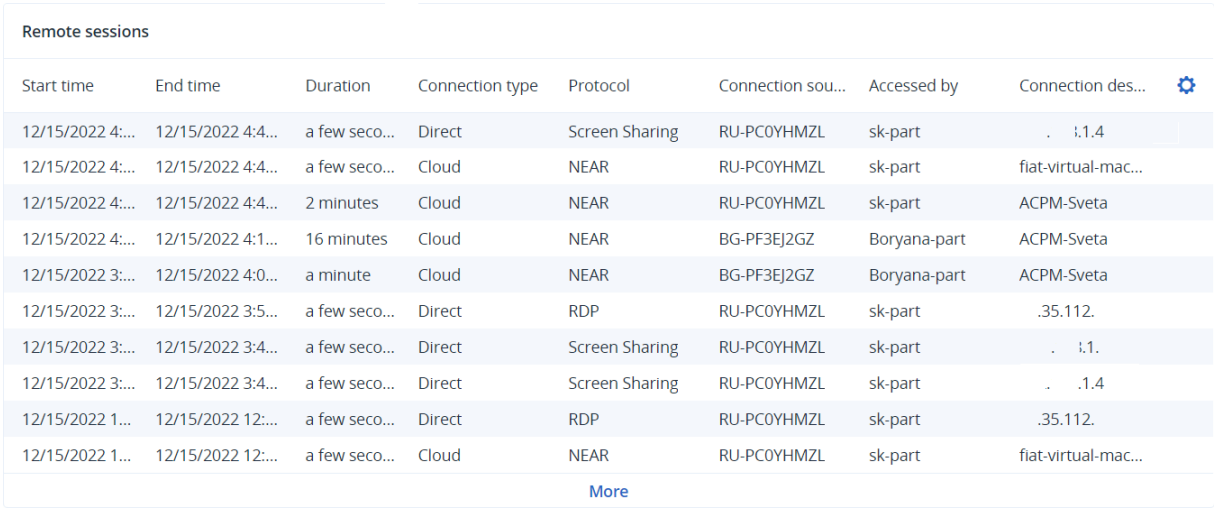
Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

Widget sessioni remote

Questo widget mostra informazioni dettagliate sulle sessioni di desktop remoto e trasferimento di file.



Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

© Acronis International GmbH, 2003-2024

Protezione intelligente

Feed minacce

Il centro operativo Acronis Cyber Protection (CPOC) genera avvisi di sicurezza che vengono inviati solo alle regioni geografiche associate. Tali avvisi di sicurezza forniscono informazioni su malware, vulnerabilità, calamità naturali, sanità pubblica e altri tipi di eventi globali che possono interessare la protezione dati. Il feed minacce fornisce informazioni su tutte le potenziali minacce e ne consente la prevenzione.

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Alcuni avvisi di sicurezza possono essere risolti seguendo un numero di azioni specifiche indicate dagli esperti della sicurezza. Altri avvisi vengono utilizzati solo per notificare le minacce imminenti, ma non contengono azioni correttive consigliate.

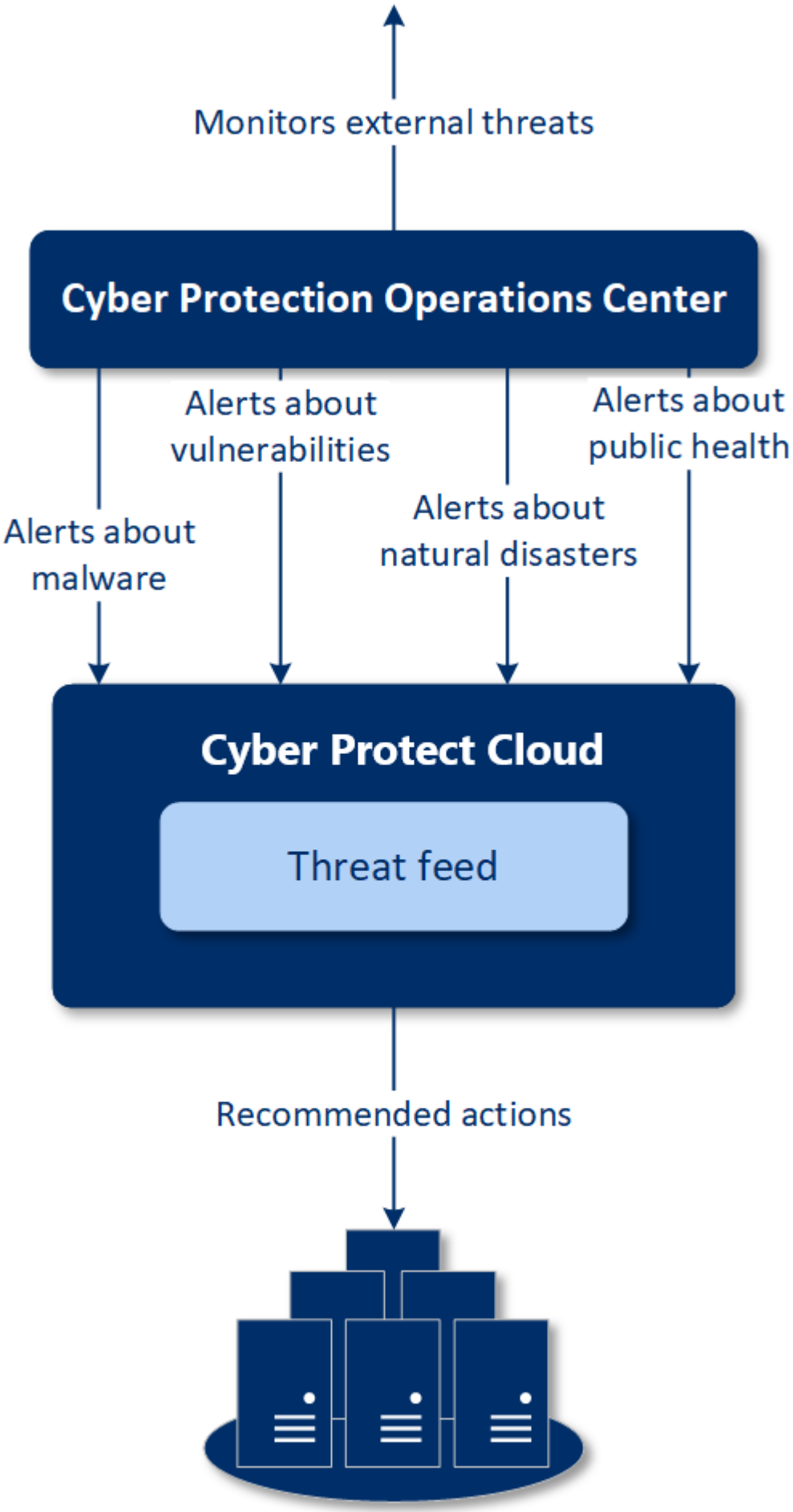
Nota
Gli avvisi malware vengono generati solo per i sistemi sui quali è installato l'agente per la protezione anti-malware.

Come funziona

Il centro operativo Acronis Cyber Protection monitora le minacce esterne e genera avvisi relativi a rischio di malware, vulnerabilità, calamità naturali e minacce alla salute pubblica. Questi avvisi possono essere visualizzati nella sezione **Feed minacce** della console di Cyber Protect. In base al tipo di avviso, è possibile eseguire le rispettive azioni correttive consigliate.

L'immagine seguente illustra il flusso di lavoro principale del feed delle minacce.

© Acronis International GmbH, 2003-2024



© Acronis International GmbH, 2003-2024

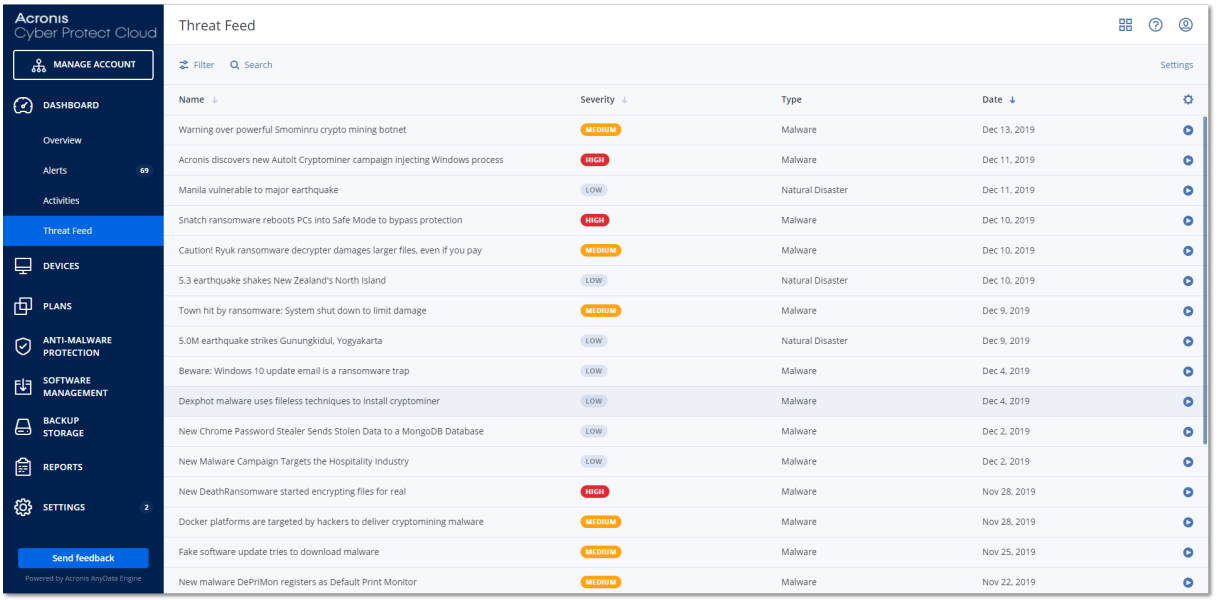
Per avviare le azioni correttive consigliate associate agli avvisi ricevuti dal centro operativo Acronis Cyber Protection, procedere come indicato di seguito:

1. Nella console di Cyber Protect, passare a **Monitoraggio** > **Feed minacce** per controllare la presenza di eventuali avvisi di sicurezza.
2. Selezionare un avviso nell'elenco e rivedere i dettagli forniti.
3. Fare clic su **Avvia** per lanciare la procedura guidata.
4. Abilitare le azioni da eseguire e i sistemi ai quali applicarle. Potrebbero essere suggerite le azioni indicate di seguito:
   - **Valutazione delle vulnerabilità** – per scansionare i sistemi in cerca di vulnerabilità
   - **Gestione patch** – per installare le patch sui sistemi selezionati
   - **Protezione anti-malware**: per una scansione completa dei sistemi protetti

     Nota
     Questa azione è disponibile solo per i sistemi sui quali è installato l'agente per la prevenzione anti-malware.

   - **Backup di sistemi protetti o non protetti** – per eseguire il backup di workload protetti o non protetti.
     Se non sono ancora presenti backup per il workload (in tutte le posizioni accessibili, cloud e locali), o se i backup esistenti sono crittografati, il sistema crea un backup completo con il formato di nome seguente:
     `%workload_name%-Remediation`
     Per impostazione predefinita, la destinazione del backup è lo storage Cyber Protect Cloud, ma è possibile configurare un'altra posizione prima di avviare l'operazione.
     Se esiste già un backup non crittografato, il sistema crea un backup incrementale nell'archivio esistente.
5. Fare clic su **Avvia**.
6. Nella pagina **Attività**, verificare che l'attività abbia avuto esito positivo.

© Acronis International GmbH, 2003-2024



Eliminazione di tutti gli avvisi

La pulizia automatica dei feed sulle minacce viene effettuata dopo i seguenti intervalli:

- Emergenza naturale - 1 settimana
- Vulnerabilità – 1 mese
- Malware – 1 mese
- Salute pubblica - 1 settimana

Mappa di protezione dati

La funzionalità Mappa di protezione dati consente di:

- Ottenere informazioni dettagliate sui dati archiviati (classificazione, posizioni, stato della protezione e informazioni aggiuntive) sui sistemi dell'utente.
- Individuare se i dati sono protetti o meno. I dati vengono considerati protetti se sono protetti con un backup (un piano di protezione con il modulo Backup abilitato).
- Eseguire azioni per la protezione dati.

Come funziona

1. Innanzitutto, creare un piano di protezione nel quale sia abilitato il modulo Mappa di protezione dati.
2. A questo punto, dopo l'esecuzione del piano e l'individuazione e l'analisi dei dati, nel widget Mappa di protezione dati viene mostrata una rappresentazione grafica della protezione dati.
3. È inoltre possibile passare a **Dispositivi** > **Mappa di protezione dati** e individuare le informazioni sui file non protetti di ogni dispositivo.
4. È possibile intraprendere azioni per proteggere i file non protetti individuati nei dispositivi.

© Acronis International GmbH, 2003-2024

Gestione dei file non protetti individuati

Per proteggere i file importanti individuati come non protetti, procedere come indicato di seguito:

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Mappa della protezione dati**.
   Nell'elenco dei dispositivi sono reperibili informazioni generiche sul numero di file non protetti, come la dimensione di tali file per ogni dispositivo, e sulla data dell'ultima individuazione.
   Per proteggere i file su uno specifico dispositivo, fare clic sull'icona dei puntini di sospensione e quindi su **Proteggi tutti i file**. Si viene reindirizzati all'elenco dei piani, dove è possibile creare un piano di protezione con il modulo Backup abilitato.
   Per eliminare un dispositivo specifico con file non protetti dall'elenco, fare clic su **Nascondi fino all'individuazione dati successiva**.
2. Per visualizzare informazioni più dettagliate sui file non protetti di uno specifico dispositivo, fare clic sul nome del dispositivo.
   Viene visualizzato il numero di file non protetti per estensione e per posizione. Nel campo di ricerca, specificare le estensioni associate ai file non protetti per i quali si desiderano informazioni.
3. Per proteggere tutti i file non protetti, fare clic su **Proteggi tutti i file**. Si viene reindirizzati all'elenco dei piani, dove è possibile creare un piano di protezione con il modulo Backup abilitato.

Per ottenere le informazioni sui file non protetti in forma di report, fare clic su **Scarica rapporto dettagliato in formato CSV**.

Impostazioni di Mappa di protezione dati

Per ulteriori informazioni su come creare un piano di protezione con il modulo Mappa di protezione dati, fare riferimento a "Creazione di un piano di protezione".

Per il modulo Mappa di protezione dati è possibile specificare le impostazioni seguenti.

Pianificazione

È possibile definire impostazioni diverse per creare la pianificazione in base alla quale verranno eseguite le attività del modulo Mappa di protezione dati.

Campo	Descrizione
Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito	Questa impostazione determina quando l'attività viene eseguita. Sono disponibili i seguenti valori: • **Pianificazione oraria**: questo è il valore predefinito. L'attività viene eseguita all'orario specificato. • **Quando l'utente accede al sistema**: per impostazione predefinita, l'accesso di qualsiasi utente determina l'avvio dell'attività. È possibile modificare questa impostazione in modo che solo un account utente specifico possa determinare l'attivazione dell'attività.

© Acronis International GmbH, 2003-2024

Campo	Descrizione
	• **Quando l'utente si disconnette dal sistema**: per impostazione predefinita, la disconnessione di qualsiasi utente determina l'avvio dell'attività. È possibile modificare questa impostazione in modo che solo un account utente specifico possa determinare l'attivazione dell'attività. **Nota** L'attività non verrà eseguita allo spegnimento del sistema. Nella configurazione della pianificazione, l'arresto del sistema e la disconnessione vanno considerate come azioni differenti. • **All'avvio del sistema** – L'attività viene eseguita all'avvio del sistema operativo. • **All'arresto del sistema** – L'attività viene eseguita all'arresto del sistema operativo.
Tipo di pianificazione	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria**. Sono disponibili i seguenti valori: • **Ogni mese** – Specificare il mese e le settimane o i giorni del mese in cui verrà eseguita l'attività. • **Ogni giorno**: questo è il valore predefinito. Specificare i giorni della settimana in cui verrà eseguita l'attività. • **Ogni ora** – Specificare i giorni della settimana, il numero di ripetizioni e l'intervallo temporale in cui verrà eseguita l'attività.
Ora di avvio	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria** Specificare l'ora esatta di avvio dell'attività.
Esegui entro un intervallo di date	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria**. Impostare un intervallo di validità della pianificazione configurata.
Specificare l'account utente il cui accesso al sistema operativo avvierà l'esecuzione dell'attività	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Quando l'utente accede al sistema**. Sono disponibili i seguenti valori: • **Tutti gli utenti**: utilizzare questa opzione per far sì che l'accesso di qualsiasi utente determini l'avvio dell'attività. • **L'utente seguente**: utilizzare questa opzione per far sì che solo

© Acronis International GmbH, 2003-2024

Campo	Descrizione
	l'accesso di uno specifico account utente determini l'avvio dell'attività.
Specificare l'account utente la cui disconnessione dal sistema operativo avvierà l'esecuzione dell'attività	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Quando l'utente si disconnette dal sistema**. Sono disponibili i seguenti valori: • **Tutti gli utenti**: utilizzare questa opzione per far sì che la disconnessione di qualsiasi utente determini l'avvio dell'attività. • **L'utente seguente**: utilizzare questa opzione per far sì che solo la disconnessione di uno specifico account utente determini l'avvio dell'attività.
Condizioni di avvio	Definisce tutte le condizioni che devono essere soddisfatte simultaneamente per avviare l'attività. Le condizioni di avvio per le scansioni anti-malware sono simili alle condizioni di avvio del modulo **Backup** descritte in "Condizioni di avvio". È possibile definire le seguenti condizioni di avvio aggiuntive: • **Ripartisci orari di avvio dell'attività all'interno di una finestra dell'orario** – Questa opzione consente di definire l'intervallo di tempo durante il quale deve essere eseguita l'attività in modo da evitare colli di bottiglia sulla rete. È possibile specificare il ritardo in ore o minuti. Se, ad esempio, l'orario di avvio predefinito è alle 10:00 e il ritardo è di 60 minuti, l'attività verrà avviata tra le 10:00 e le 11:00. • **Se la macchina è spenta, esegui le attività mancanti all'avvio della macchina** • **Impedisci la modalità di sospensione o ibernazione durante l'esecuzione dell'attività** – Questa opzione è valida solo per i sistemi che eseguono Windows. • **Se le condizioni di avvio non sono soddisfatte, esegui comunque l'attività dopo** – Specificare il periodo successivamente al quale l'attività verrà comunque avviata, indipendentemente dalle altre condizioni di avvio. **Nota** In Linux le condizioni di avvio non sono supportate.

Regole di estensione ed eccezione

Nella scheda **Estensioni**, è possibile definire l'elenco delle estensioni file che verranno considerate come importanti durante l'individuazione dei dati e per le quali verrà controllata la presenza di file non protetti. Per definire le estensioni, utilizzare i formati seguenti:

```
.html, .7z, .docx, .zip, .pptx, .xml
```


© Acronis International GmbH, 2003-2024

Nella scheda **Regole di eccezione**, è possibile definire di quali file e cartelle non verrà controllato lo stato di protezione durante l'individuazione dei dati.

- **File e cartelle nascosti** – se l'opzione è selezionata, i file e le cartelle nascoste specificate verranno escluse dall'analisi dei dati.
- **File e cartelle di sistema** – se l'opzione è selezionata, i file e le cartelle di sistema specificate verranno escluse dall'analisi dei dati.

Scheda Attività

La scheda **Attività** fornisce una panoramica delle attività degli ultimi 90 giorni.

Per filtrare le attività nel dashboard

1. Nel campo **Nome periferica**, specificare il sistema sul quale l'attività è in esecuzione.
2. Dall'elenco a discesa **Stato**, selezionare lo stato. Ad esempio Riuscita, Non riuscita, In corso, Annullata.
3. Dall'elenco a discesa **Azioni remote**, selezionare l'azione. Ad esempio Applicazione piano, Eliminazione backup, Installazione aggiornamenti software.
4. Nel campo **Più recente**, selezionare il periodo delle attività. Ad esempio, Attività più recenti, Attività delle ultime 24 ore o Attività di un periodo specifico entro i 90 giorni precedenti.
5. Se si accede alla scheda **Attività** come amministratore di partner, è possibile filtrare le attività per uno specifico cliente gestito.

Per personalizzare la vista della scheda **Attività**, fare clic sull'icona ingranaggio e quindi selezionare le colonne da visualizzare. Per visualizzare il progresso dell'attività in tempo reale, selezionare la casella di controllo **Aggiorna automaticamente**.

Per annullare un'attività in esecuzione, fare clic sul nome dell'attività e quindi, nella schermata **Dettagli** fare clic su **Annulla**.

È possibile effettuare una ricerca delle attività in elenco secondo i seguenti criteri:

- Nome periferica
  Il sistema sul quale l'attività è in esecuzione.
- Avviata da
  L'account che ha avviato l'attività.

Le attività di desktop remoto possono essere filtrate in base alle proprietà seguenti:

- Creazione piano
- Applicazione piano
- Revoca piano
- Eliminazione piano
- Connessione remota

© Acronis International GmbH, 2003-2024

    - Connessione desktop remoto in cloud tramite RDP
    - Connessione desktop remoto in cloud tramite NEAR
    - Connessione desktop remoto in cloud tramite Condivisione schermo di Apple
    - Connessione desktop remoto tramite client web
    - Connessione desktop remoto tramite Quick Assist
    - Connessione desktop remoto diretta tramite RDP
    - Connessione desktop remoto diretta tramite Condivisione schermo di Apple
    - Trasferimento di file
    - Trasferimento di file tramite Quick Assist
- Azione remota
    - Arresto di un workload
    - Riavvio di un workload
    - Disconnessione di un utente remoto nel workload
    - Svuotamento del cestino dell'utente nel workload
    - Sospensione di un workload

Cyber Protect Monitor

Cyber Protect Monitor visualizza le informazioni sullo stato di protezione del sistema nel quale è installato Agente per Windows o Agente per Mac, e consente agli utenti di configurare le impostazioni del server proxy e di crittografia del backup.

Quando l'Agente per File Sync & Share è installato sul sistema, Cyber Protect Monitor consente l'accesso al servizio File Sync & Share. La funzionalità File Sync & Share diventa accessibile dopo l'onboarding obbligatorio, durante il quale gli utenti accedono al proprio account File Sync & Share e selezionano una cartella di sincronizzazione personale. Per ulteriori informazioni sull'Agente per File Sync & Share, consultare il manuale dell'utente di Cyber Files Cloud.

Importante
Cyber Protect Monitor è accessibile agli utenti che potrebbero non disporre di diritti amministrativi per Cyber Protection o per il servizio File Sync & Share.

La tabella sottostante riassume le operazioni disponibili per gli utenti senza diritti amministrativi.

Agenti installati	Gli utenti possono	Gli utenti non possono
Agente per Windows o Agente per Mac	• Applicare il piano di protezione predefinito ai propri sistemi • Controllare lo stato di protezione dei propri sistemi • Ricevere notifiche di Active Protection	• Applicare piani di protezione personalizzati • Gestire piani di protezione che sono già applicati

© Acronis International GmbH, 2003-2024

Agenti installati	Gli utenti possono	Gli utenti non possono
	• Sospendere temporaneamente i backup dei propri sistemi • Configurare le impostazioni del server proxy • Modificare le impostazioni di crittografia del backup **Attenzione!** La modifica delle impostazioni di crittografia in Cyber Protect Monitor sovrascrive le impostazioni del piano di protezione e ha effetto su tutti i backup del sistema. Questa operazione può impedire il corretto funzionamento di alcuni piani di protezione. Per ulteriori informazioni, consultare "Crittografia" (pag. 449). Impossibile recuperare i backup crittografati se si perde o si dimentica la password.	
Agente per Windows e Agente per Sync & Share Agente per Mac e Agente per Sync & Share	• Sincronizzare contenuti tra la propria cartella di sincronizzazione locale e il proprio account File Sync & Share • Sospendere le operazioni di sincronizzazione • Modificare la cartella di sincronizzazione • Controllare i tipi di file che non possono essere sincronizzati	• Modificare i tipi di file che non possono essere sincronizzati

Configurazione delle impostazioni del server proxy in Cyber Protect Monitor

È possibile configurare le impostazioni del server proxy in Cyber Protect Monitor. La configurazione ha effetto su tutti gli agenti installati nel sistema.

Per configurare le impostazioni del server proxy

1. Aprire Cyber Protect Monitor e quindi fare clic sull'icona ingranaggio nell'angolo superiore destro.
2. Fare clic su **Impostazioni**, quindi su **Proxy**.
3. Abilitare l'opzione **Usa un server proxy**, quindi inserire l'indirizzo e la porta del server proxy.

© Acronis International GmbH, 2003-2024

4. [Se l'accesso al server proxy è protetto da password] Abilitare l'opzione **Password richiesta**, quindi inserire il nome utente e la password per accedere al server proxy.
5. Fare clic su **Salva**.
   Le impostazioni del server proxy vengono salvate nel file `http-proxy.yaml`.

Report

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Un report relativo alle operazioni può includere qualsiasi insieme di widget della dashboard. Tutti i widget mostrano le informazioni di riepilogo per l'intera azienda.

A seconda del tipo di widget, il report include i dati relativi a un intervallo di tempo o al momento in cui il report è stato esplorato o generato. Vedere "Dati inseriti nel report in base al tipo di widget" (pag. 322).

Tutti i widget cronologici mostrano i dati per lo stesso intervallo di tempo. È possibile modificare questo intervallo nelle impostazioni del report.

È possibile utilizzare i report predefiniti o crearne uno personalizzato.

È possibile scaricare un report o inviarlo via e-mail in formato Excel (XLSX) o PDF.

Il gruppo di report predefiniti dipende dall'edizione del servizio Cyber Protection in uso. I report predefiniti sono elencati di seguito:

Nome report	Descrizione
#CyberFit Score per sistema	Mostra il #CyberFit Score, basato sulla valutazione delle metriche di sicurezza e delle configurazioni per ogni sistema, nonché i miglioramenti consigliati.
Avvisi	Mostra gli avvisi generati durante un periodo di tempo specificato.
Informazioni sulla scansione del backup	Mostra informazioni dettagliate sulle minacce individuate nei backup.
Attività giornaliere	Mostra informazioni di riepilogo sulle attività eseguite durante un periodo di tempo specificato.
Mappa di protezione dati	Mostra informazioni dettagliate su numero, dimensione, posizione, stato della protezione di tutti i file importanti sui sistemi.
Minacce rilevate	Mostra informazioni relative ai sistemi interessati per numero di minacce bloccate e di sistemi integri e vulnerabili.
Macchine individuate	Mostra tutti i sistemi individuati nella rete dell'organizzazione.

© Acronis International GmbH, 2003-2024

Previsione dell'integrità del disco	Mostra le previsioni circa i guasti di HDD/SSD e lo stato attuale dei dischi.
Vulnerabilità esistenti	Mostra le vulnerabilità esistenti per i sistemi operativi e le applicazioni dell'organizzazione. Visualizza inoltre le informazioni sui sistemi interessati nella rete per ogni prodotto in elenco.
Inventario software	Mostra informazioni dettagliate sul software installato nei dispositivi dell'organizzazione.
Inventario hardware	Mostra informazioni dettagliate sull'hardware disponibile nei dispositivi dell'organizzazione.
Riepilogo di gestione patch	Mostra il numero di patch mancanti, patch installate e patch applicabili. È possibile esplorare i report per ottenere le informazioni sulle patch installate e/o mancanti e ulteriori dettagli su tutti i sistemi.
Riepilogo	Mostra informazioni di riepilogo sui dispositivi protetti per un periodo di tempo specificato.
Attività settimanali	Mostra informazioni di riepilogo sulle attività eseguite durante un periodo di tempo specificato.
Sessioni remote	Mostra informazioni dettagliate sulle sessioni di desktop remoto e trasferimento di file.

Azioni con i report

Per visualizzare un report, fare clic sul relativo nome.

Per aggiungere un nuovo report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report disponibili, fare clic su **Aggiungi report**.
3. [Per aggiungere un report predefinito] Fare clic sul nome del report predefinito.
4. [Per aggiungere un report personalizzato] Fare clic su **Personalizzato** e quindi aggiungere i widget al report.
5. [Facoltativo] Trascinare e rilasciare i widget per riorganizzarli.

Per modificare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report da modificare.
   È possibile:
   - Rinominare il report.
   - Modificare l'intervallo di tempo di tutti i widget nel report.
   - Specificare i destinatari del report e la data in cui il report verrà inviato. Sono disponibili i formati PDF e XLSX.

© Acronis International GmbH, 2003-2024

Per eliminare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report da eliminare.
3. Fare clic sull'icona dei puntini di sospensione, quindi fare clic su **Elimina**.
4. Confermare la selezione facendo clic su **Elimina**.

Per programmare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report da pianificare, quindi fare clic su **Impostazioni**.
3. Attivare il commutatore **Pianificato**.
   - Specificare gli indirizzi e-mail dei destinatari.
   - Selezionare il formato del report.

     Nota
     È possibile esportare fino a 1.000 voci in un file PDF e fino a 10.000 voci in un file XLSX. I timestamp nei file PDF e XLSX utilizzano l'ora locale del sistema.

   - Selezionare la lingua del report.
   - Configurare la pianificazione.
4. Fare clic su **Salva**.

Per scaricare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report, quindi fare clic su **Scarica**.
3. Selezionare il formato del report.

Per inviare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report, quindi fare clic su **Invia**.
3. Specificare gli indirizzi e-mail dei destinatari.
4. Selezionare il formato del report.
5. Fare clic su **Invia**.

Per esportare la struttura del report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report.
3. Fare clic sull'icona dei puntini di sospensione, quindi fare clic su **Esporta**.

La struttura del report viene salvata nel sistema come file JSON.

© Acronis International GmbH, 2003-2024

Per effettuare il dumping dei dati del report

Utilizzando questa opzione, è possibile esportare tutti i dati per un intervallo temporale del cliente, senza filtrarli, in un file CSV e inviare il file a un destinatario e-mail.

Nota
È possibile esportare fino a 150.000 voci in un file CSV. I timestamp nel file CSV utilizzano l'orario UTC (Coordinated Universal Time).

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report con i dati di cui eseguire il dump.
3. Fare clic sull'icona dei puntini di sospensione, quindi fare clic su **Dump dati**.
4. Specificare gli indirizzi e-mail dei destinatari.
5. In **Intervallo di tempo**, specificare l'intervallo temporale del cliente per il quale eseguire il dump dei dati.

   Nota
   La preparazione dei file CSV relativi a periodi più lunghi richiede più tempo.

6. Fare clic su **Invia**.

Dati inseriti nel report in base al tipo di widget

In base all'intervallo di dati che visualizzano, i widget nella dashboard sono di due tipi:

- Widget che visualizzano i dati correnti nel momento in cui il report viene sfogliato o generato.
- Widget che visualizzano dati cronologici.

Quando si configura un intervallo di dati nelle impostazioni del report, per eseguire il dump relativo a un determinato periodo, l'intervallo di tempo selezionato verrà applicato solo ai widget che visualizzano dati cronologici. Il parametro dell'intervallo di tempo non è applicabile ai widget che visualizzano i dati correnti nel momento in cui il report viene sfogliato.

La tabella seguente elenca i widget disponibili e i relativi intervalli di dati.

Nome widget	Dati visualizzati nel widget e nei report
#CyberFit Score per sistema	Correnti
5 avvisi più recenti	Correnti
Dettagli sugli avvisi attivi	Correnti
Riepilogo avvisi attivi	Correnti
Attività	Cronologici

© Acronis International GmbH, 2003-2024

Elenco attività	Cronologici
Cronologia avvisi	Cronologici
Statistiche delle tattiche di attacco	Cronologici
Informazioni sulla scansione del backup (minacce)	Cronologici
Stato backup	Cronologici - nelle colonne **Esecuzioni totali** e **Numero di esecuzioni riuscite** Correnti - in tutte le altre colonne
URL bloccati	Correnti
Applicazioni cloud	Correnti
Cyber protection	Correnti
Mappa di protezione dati	Cronologici
Dispositivi	Correnti
Macchine individuate	Correnti
Panoramica dell'integrità del disco	Correnti
Stato integrità del disco per dispositivi fisici	Correnti
Vulnerabilità esistenti	Cronologici
Modifiche hardware	Cronologici
Dettagli hardware	Correnti
Inventario hardware	Correnti
Riepilogo avvisi cronologici	Cronologici
Cronologia gravità problema	Cronologici
Riepilogo posizioni	Correnti
Aggiornamenti non effettuati per categorie	Correnti
Non protetto	Correnti
Cronologia di installazione patch	Cronologici
Stato di installazione patch	Cronologici
Riepilogo di installazione patch	Cronologici

© Acronis International GmbH, 2003-2024

Stato protezione	Correnti
Recentemente interessato	Cronologici
Sessioni remote	Cronologici
Burndown dei problemi di sicurezza	Cronologici
MTTR dei problemi di sicurezza	Cronologici
Inventario software	Correnti
Panoramica software	Cronologici
Stato minaccia	Correnti
Sistemi vulnerabili	Correnti
Stato della rete dei workload	Correnti

© Acronis International GmbH, 2003-2024

Gestione di workload nella console di Cyber Protect

Questa sezione descrive come gestire i workload nella console di Cyber Protect.

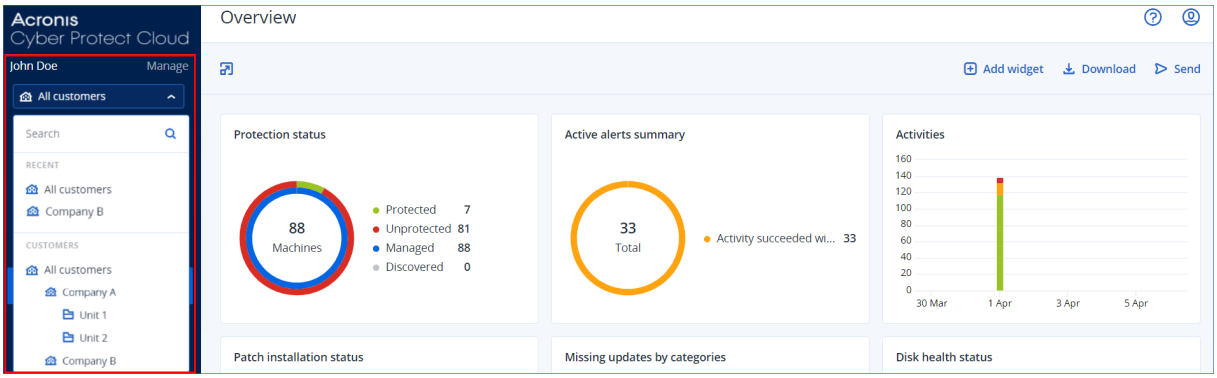
La console di Cyber Protect

Nella console di Cyber Protect è possibile gestire workload e piani, modificare le impostazioni di protezione, configurare i report o controllare l'archivio di backup.

La console consente di accedere ai servizi o alle funzionalità aggiuntive di Cyber Protect, quali File Sync & Share o Protezione antivirus e anti-malware, Gestione patch, Controllo dispositivo e Valutazione delle vulnerabilità. Il tipo e il numero di questi servizi e funzionalità varia in base alla licenza di Cyber Protection in uso.

Per controllare la dashboard con le informazioni più importanti sulla protezione, passare a **Monitoraggio** > **Panoramica**.

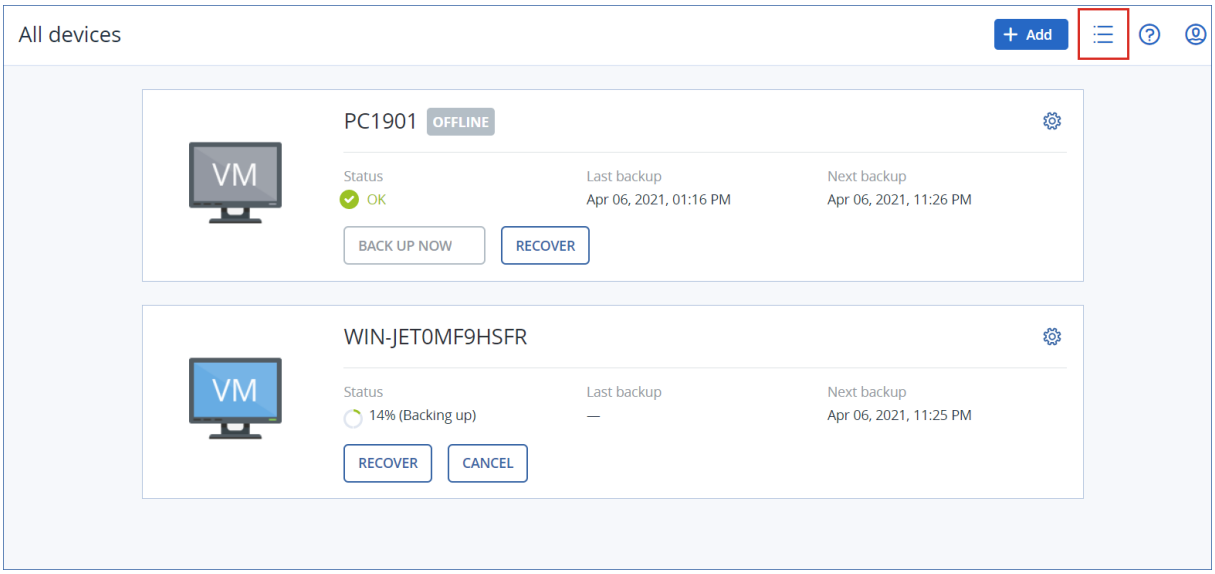
A seconda delle autorizzazioni di accesso disponibili, è possibile gestire la protezione per uno o per più tenant cliente o unità in un tenant. Per passare ad altri livelli gerarchici, utilizzare l'elenco a discesa nel menu di navigazione. Vengono visualizzati solo i livelli ai quali l'utente può accedere. Per passare al portale di gestione, fare clic su **Gestisci**.



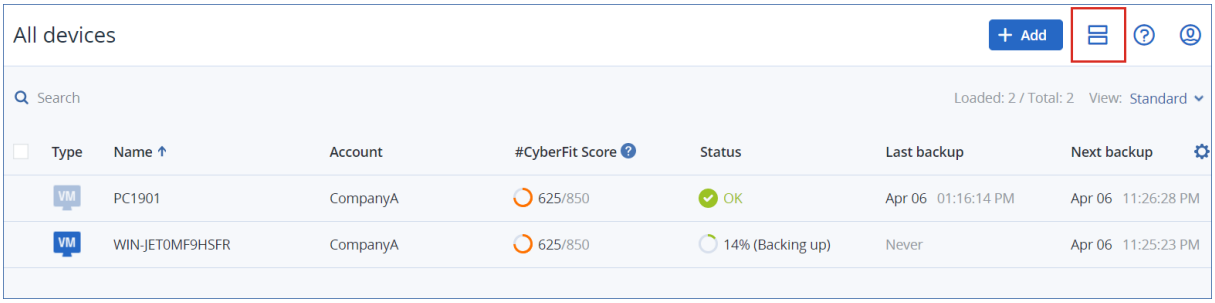
La sezione **Dispositivi** disponibile come semplice visualizzazione a tabella. Per passare da una visualizzazione all'altra, fare clic sull'icona corrispondente nell'angolo superiore destro.

La visualizzazione semplice mostra solo alcuni workload.

© Acronis International GmbH, 2003-2024



La visualizzazione tabella viene abilitata automaticamente quando il numero di workload diventa ampio.



Entrambe le visualizzazioni forniscono l'accesso alle stesse funzionalità e operazioni. Il presente documento descrive come accedere alle operazioni dalla visualizzazione tabella.

Quando un workload passa da online a offline o viceversa, la modifica dello stato nella console di Cyber Protect può richiede qualche minuto. Lo stato del workload viene controllato ogni minuto. Se l'agente installato sul sistema corrispondente non sta trasferendo dati e se non si ottiene risposta dopo cinque controlli consecutivi, il workload viene visualizzato come offline. Il workload viene di nuovo visualizzato come online quando risponde a un controllo di stato o avvia un trasferimento di dati.

Novità della console di Cyber Protect

Quando sono disponibili nuove funzionalità di Cyber Protect Cloud, all'accesso alla console di Cyber Protect viene visualizzata una finestra popup con una breve descrizione delle novità.

La descrizione delle nuove funzionalità è inoltre visualizzabile facendo clic sul link **Novità** nell'angolo in basso a sinistra della finestra della console di Cyber Protect.

Se non sono presenti nuove funzionalità, il collegamento alla pagina delle **Novità** non è visualizzato.

© Acronis International GmbH, 2003-2024

Utilizzo della console di Cyber Protect come amministratore di partner

Come amministratore del partner, è possibile utilizzare la console di Cyber Protect a livello del tenant partner (**Tutti i clienti**) o a livello del tenant cliente.

Livello del tenant partner (**Tutti i clienti**)

A livello del tenant partner (**Tutti i clienti**), è possibile eseguire le azioni seguenti:

- Gestire piani di scripting per i workload da tutti i tenant cliente gestiti.
  È possibile applicare lo stesso piano di scripting ai workload di diversi clienti e creare gruppi di dispositivi con workload di diversi clienti. Per ulteriori informazioni su come creare un gruppo di dispositivi statico o dinamico a livello del partner, consultare "Creazione di un gruppo di dispositivi statico a livello del partner" (pag. 330) e "Creazione di un gruppo di dispositivi dinamico a livello del partner" (pag. 330). Per ulteriori informazioni sugli script e sui piani di scripting, consultare "Cyber Scripting" (pag. 239).
- Creare piani di monitoraggio per i workload di tutti i tenant cliente gestiti.
- Creare piani di gestione remota per i workload da tutti i tenant cliente gestiti.
- Visualizza e gestisci i problemi di Endpoint Detection and Response (EDR) per tutti i tenant cliente da un'unica interfaccia di gestione, senza dover accedere alla schermata dei problemi di ogni singolo cliente.
- Eseguire l'individuazione automatica dei sistemi per tutti i tenant cliente gestiti.

Livello del tenant cliente

A questo livello si dispone degli stessi diritti di cui dispone l'amministratore dell'azienda per conto del quale si agisce.

Selezione di un livello tenant

È possibile selezionare il livello del tenant su cui lavorare nella console di Cyber Protect.

Prerequisiti

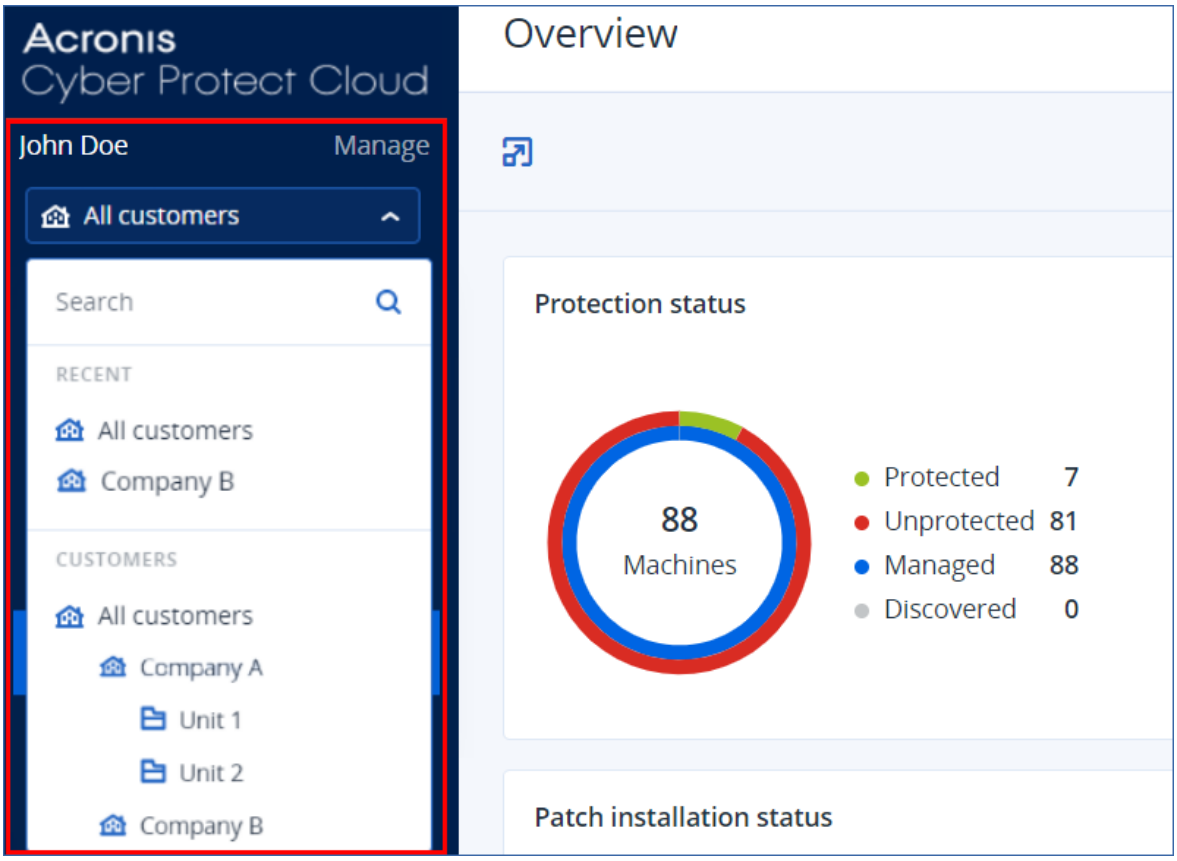
- Si dispone dei diritti di accesso sia alla console di Cyber Protect che al portale di gestione.
- È possibile gestire più di un tenant o unità.

Per selezionare un livello di tenant nella console di Cyber Protect

1. Nel menu di navigazione a sinistra, fare clic sulla freccia accanto al nome del tenant cliente.
2. Selezionare una delle seguenti opzioni:
   - Per lavorare al livello del partner, selezionare **Tutti i clienti**.

© Acronis International GmbH, 2003-2024

- Per lavorare al livello del cliente o dell'unità, selezionare il nome del cliente o dell'unità.



Livello del tenant partner nella console di Cyber Protect

Quando si utilizza la console di Cyber Protect al livello del tenant partner (**Tutti i clienti**) è disponibile una visualizzazione personalizzata.

Le schede **Avvisi** e **Attività** forniscono ulteriori filtri correlati al partner, mentre le schede **Dispositivi** e **Gestione** consentono l'accesso solo alle funzionalità o agli oggetti accessibili agli amministratori di partner.

Scheda Avvisi

Questa scheda consente di visualizzare gli avvisi di tutti i clienti gestiti, effettuare ricerche e filtrarli secondo i criteri seguenti:

- Dispositivo
- Cliente
- Piano

È possibile selezionare più elementi di ciascuno di questi criteri.

© Acronis International GmbH, 2003-2024

Scheda Attività

Questa scheda consente di visualizzare le attività di tutti i tenant gestiti o le attività di uno specifico tenant cliente.

È possibile filtrare le attività per cliente, stato, orario e tipo.

A questo livello, i seguenti tipi di attività sono preselezionati automaticamente:

- Applicazione piano
- Creazione del piano di protezione
- Piano di protezione
- Revoca piano
- Scripting

Scheda Dispositivi

Nella scheda **Macchine con agenti** sono visualizzati tutti i workload dei tenant cliente gestiti ed è possibile selezionare i workload di uno o più tenant. È anche possibile creare gruppi di dispositivi che contengono i workload di diversi tenant.

Importante
Quando si lavora a livello del partner (**Tutti i clienti**), è possibile eseguire un numero limitato di operazioni con i dispositivi. Ad esempio, non è possibile eseguire nessuna delle operazioni seguenti:

- Visualizzare e gestire i piani di protezione esistenti sui dispositivi dei clienti.
- Creare nuovi piani di protezione.
- Ripristinare i backup.
- Utilizzare la funzionalità di Disaster Recovery.
- Accedere alle funzionalità di Cyber Protection Desktop.

Per eseguire queste operazioni è necessario lavorare a livello del cliente.

Scheda Gestione software

Se è stata abilitata la scansione degli inventari software per i workload dei clienti, è possibile visualizzarne i risultati.

Visualizzazione di workload di clienti specifici

All'amministratore del partner è consentita la visualizzazione dei workload appartenenti ai tenant cliente gestiti.

Per visualizzare i workload di un cliente specifico

© Acronis International GmbH, 2003-2024

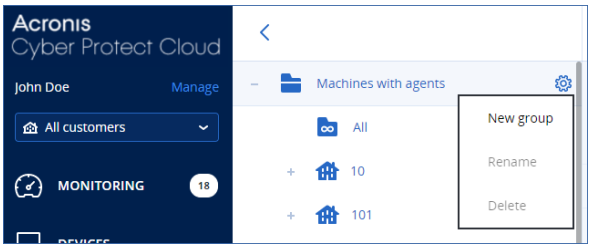
1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Nella struttura, fare clic su **Macchine con agenti** ed espandere l'elenco.
3. Fare clic sul nome del cliente di cui visualizzare e gestire i workload.

Creazione di un gruppo di dispositivi statico a livello del partner

È possibile creare gruppi di dispositivi statici a livello del partner (**Tutti i dispositivi**).

Per creare un gruppo di dispositivi statico al livello del partner

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Fare clic sull'icona ingranaggio accanto a **Macchine con agenti**, quindi su **Nuovo gruppo**.



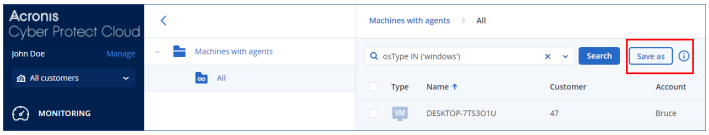
3. Specificare il nome del gruppo.
4. [Facoltativo] Aggiungere una descrizione.
5. Fare clic su **OK**.

Creazione di un gruppo di dispositivi dinamico a livello del partner

È possibile creare gruppi di dispositivi dinamici a livello del partner (**Tutti i dispositivi**).

Per creare un gruppo di dispositivi dinamico al livello del partner

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Nella struttura, fare clic su **Macchine con agenti** ed espandere l'elenco.
3. Fare clic su **Tutto**.
4. Nel campo di ricerca, specificare i criteri in base ai quali creare un gruppo di dispositivi dinamico, quindi fare clic su **Cerca**.
   Per ulteriori informazioni sui criteri di ricerca disponibili, consultare "Attributi di ricerca per i workload non cloud-to-cloud" (pag. 353) e "Attributi di ricerca per i workload cloud-to-cloud" (pag. 352).
5. Fare clic su **Salva come** e quindi specificare il nome del gruppo.



6. [Facoltativo] Aggiungere una descrizione.
7. Fare clic su **OK**.

© Acronis International GmbH, 2003-2024

Esecuzione dell'individuazione automatica dei sistemi a livello del tenant partner

È possibile eseguire l'individuazione automatica dei sistemi a livello del tenant partner (**Tutti i clienti**).

Prerequisiti

È necessario almeno un sistema con un agente di protezione installato nella rete locale o nel dominio di Active Directory del cliente.

Importante
È possibile utilizzare come agenti di individuazione solo quelli installati su sistemi Windows. Qualora negli ambienti del cliente non fossero presenti agenti di individuazione, non sarà possibile utilizzare l'opzione **Più dispositivi** nel riquadro **Aggiungi dispositivi**.

L'Individuazione automatica non è supportata per l'aggiunta dei controller di dominio, a causa delle autorizzazioni aggiuntive richieste per l'esecuzione del servizio agente.

L'installazione remota degli agenti è supportata solo per i sistemi che eseguono Windows (Windows XP non supportato). Per l'installazione remota su un sistema che esegue Windows Server 2012 R2, è necessario che in tale sistema sia installato l'aggiornamento Windows KB2999226.

Per eseguire l'individuazione automatica dei sistemi a livello del tenant partner

1. Nella console di Cyber Protect, selezionare **Tutti i clienti**.
2. Passare a **Dispositivi** > **Tutti i dispositivi**.
3. Fare clic su **Aggiungi**.
4. In **Più dispositivi**, fare clic su **Solo per Windows**. Si apre la finestra dell'Individuazione automatica guidata.
5. Selezionare un tenant cliente, quindi l'agente di individuazione che eseguirà la scansione per rilevare i sistemi.
6. Selezionare il metodo di individuazione:
   - **Cerca in Active Directory**. Verificare che il sistema con l'agente di individuazione sia membro del dominio di Active Directory.
   - **Scansiona rete locale**. Se l'agente di individuazione selezionato non è in grado di trovare alcun sistema, selezionarne un altro.
   - **Specifica manualmente o importa da file**. Definire manualmente i sistemi da aggiungere o importarli da un file di testo.
7. [Se è stato selezionato il metodo di individuazione da Active Directory] Selezionare come eseguire la ricerca dei sistemi:
   - **Nell'elenco delle unità organizzative**. Selezionare il gruppo di sistemi da aggiungere.

© Acronis International GmbH, 2003-2024

- **Per query in dialetto LDAP**. Utilizzare query in dialetto LDAP per selezionare i sistemi. **Base di ricerca** definisce l'ambito in cui eseguire la ricerca, mentre **Filtro** consente di specificare i criteri per la selezione del sistema.

8. A seconda del metodo di individuazione selezionato, procedere come segue:

Metodo di individuazione	Azione
Cerca in Active Directory	Dall'elenco dei sistemi individuati, selezionare i sistemi da aggiungere.
Scansiona rete locale	Dall'elenco dei sistemi individuati, selezionare i sistemi da aggiungere.

Specifica manualmente o importa da file	Specificare gli indirizzi IP o i nomi host del sistema, oppure importare l'elenco dei sistemi da un file di testo. Il file deve contenere gli indirizzi IP o i nomi host, uno per riga. Di seguito è riportato un esempio di file:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Dopo aver aggiunto manualmente gli indirizzi dei sistemi o averli importati da un file, l'agente tenta di eseguire il ping ai sistemi aggiunti e ne definisce la disponibilità.

9. Selezionare le azioni da eseguire dopo l'individuazione:

Opzione	Descrizione
Installa gli agenti e registra le macchine	È possibile selezionare quali componenti installare sui sistemi facendo clic su **Seleziona componenti**. Per ulteriori dettagli, consultare "Selezione dei componenti per l'installazione" (pag. 135).
Account di accesso per il servizio agente	Questa impostazione è disponibile nella schermata **Seleziona componenti**. L'impostazione definisce l'account con il quale verranno eseguiti i servizi. È possibile selezionare una delle opzioni seguenti: • **Usa gli account degli utenti del servizio** (impostazione predefinita per il servizio agente) Gli account degli utenti del servizio sono account di sistema Windows usati per eseguire i servizi. Questa impostazione è vantaggiosa perché i criteri di sicurezza del dominio non influiscono sui diritti utente di questi account. Per impostazione predefinita l'agente viene eseguito con l'account **Sistema locale**. • **Crea un nuovo account** Il nome account sarà l'Agent User dell'agente. • **Usa il seguente account**

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
	Se l'agente viene installato in un controller di dominio, il sistema chiede di specificare gli account esistenti (o lo stesso account) per l'agente. Per motivi di sicurezza, il sistema non crea automaticamente nuovi account su un controller di dominio. Se si sceglie l'opzione **Crea un nuovo account** o **Usa il seguente account**, verificare che i criteri di sicurezza del dominio non influiscano sui diritti degli account correlati. Se un account viene privato dei diritti utente assegnati durante l'installazione, il componente potrebbe non funzionare correttamente o non funzionare affatto.
Registra le macchine con agenti installati	Utilizzare questa opzione se l'agente è già installato sui sistemi e se è necessario solo registrarlo in Cyber Protection. Se non viene individuato nessun agente sui sistemi, questi verranno aggiunti come sistemi **Non gestiti**.
Aggiungi come macchine non gestite	Selezionando questa opzione, l'agente non viene installato sui sistemi. Sarà possibile visualizzare i sistemi nella console e installare o registrare l'agente in un secondo momento.
Riavviare la macchina, se necessario	Questa opzione viene visualizzata se è selezionata **Installa gli agenti e registra le macchine**. Selezionando questa opzione, il sistema viene riavviato il numero di volte necessario a completare l'installazione. Il riavvio del sistema può essere necessario in uno dei casi seguenti: • È stata completata l'installazione dei prerequisiti e il riavvio è richiesto per continuare l'installazione. • L'installazione è completa ma il riavvio è richiesto in quanto alcuni file vengono bloccati durante il processo. • L'installazione è completa ma il riavvio è richiesto per altro software installato in precedenza.
Non riavviare se l'utente ha effettuato l'accesso	Questa opzione viene visualizzata se è selezionata **Riavviare la macchina se necessario**. Se questa opzione è selezionata, il sistema non viene riavviato automaticamente se l'utente accede al sistema. Se, ad esempio, un utente sta lavorando quando l'installazione richiede il riavvio, il sistema non verrà riavviato. Se i prerequisiti sono stati installati ma il sistema non è stato riavviato perché un utente era collegato, per completare l'installazione è necessario riavviare il sistema, quindi avviare di nuovo l'installazione. Se l'agente è stato installato ma il sistema non è stato riavviato, è necessario riavviarlo.
Utente in cui registrare i sistemi	[Se sono presenti unità nell'organizzazione] Selezionare l'account utente dell'unità o delle unità secondarie per il quale registrare i sistemi. [Quando si esegue l'individuazione automatica a livello del tenant partner] Nell'elenco dei tenant cliente gestiti, espandere la struttura ad albero e selezionare l'account

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
	utente per il quale registrare i sistemi. [Quando si esegue l'individuazione automatica come amministratore del cliente] Se è stata selezionata l'opzione **Installa gli agenti e registra le macchine** o **Registra le macchine con agenti installati**, viene visualizzata anche un'opzione per applicare il piano di protezione ai sistemi. Se sono disponibili più piani di protezione, è possibile selezionare quale applicare.

10. Specificare le credenziali dell'utente che dispone dei diritti di amministratore per tutti i sistemi.

Importante
L'installazione remota degli agenti funziona senza alcuna preparazione solo se vengono specificate le credenziali dell'account di amministrazione integrato (il primo account creato quando è stato installato il sistema operativo). Per definire alcune credenziali di amministratore personalizzate, è necessario procedere con i passaggi preparatori descritti in "Prerequisiti" (pag. 331).

11. Viene controllata la connessione verso tutti i sistemi. Se la connessione ad alcuni sistemi non riesce, è possibile modificare le credenziali dei sistemi in questione.

Una volta avviata l'individuazione dei sistemi, l'attività corrispondente viene visualizzata in **Monitoraggio** > **Attività** > **Attività di individuazione dei sistemi**.

Supporto per ambienti multitenant

Il servizio Cyber Protection supporta gli ambienti multitenant, e prevede attività di amministrazione ai livelli seguenti:

- [Per service provider] Livello del tenant partner (**Tutti i clienti**)
  Questo livello è disponibile solo agli amministratori di partner che gestiscono tenant cliente.
- Livello del tenant cliente
  Questo livello è gestito dagli amministratori dell'azienda.
  Gli amministratori di partner possono lavorare anche a questo livello nei tenant cliente che gestiscono. A questo livello, gli amministratori di partner dispongono degli stessi diritti di cui dispone l'amministratore del cliente per conto del quale agiscono.
- Livello dell'unità
  Questo livello è gestito dagli amministratori dell'unità e dagli amministratori dell'azienda dal tenant cliente padre.
  Gli amministratori di partner che gestiscono il tenant cliente padre possono accedere anche al livello dell'unità. A questo livello, dispongono degli stessi diritti di cui dispongono gli amministratori del cliente per conto del quale agiscono.

Gli amministratori possono gestire oggetti nei propri tenant e nei rispettivi tenant figlio. Non possono visualizzare o accedere agli oggetti a un livello di amministrazione superiore, se presente.

© Acronis International GmbH, 2003-2024

Ad esempio, gli amministratori dell'azienda possono gestire i piani di protezione sia al livello del tenant cliente sia al livello dell'unità. Gli amministratori dell'unità possono gestire solo i propri piani di protezione al livello dell'unità. Non possono gestire nessun piano di protezione al livello del tenant cliente e non possono gestire i piani di protezione che vengono creati dall'amministratore del cliente al livello dell'unità.

Inoltre, gli amministratori di partner possono creare e applicare piani di scripting nei tenant cliente che gestiscono. In questi tenant, gli amministratori dell'azienda possono accedere esclusivamente in sola lettura ai piani di scripting che vengono applicati ai propri workload da un amministratore di partner. Gli amministratori dell'azienda possono, tuttavia, creare e applicare i propri piani di scripting o protezione.

Workload

Si definisce workload qualsiasi tipo di risorsa protetta, ad esempio un sistema fisico, una virtual machine, una casella di posta o un'istanza di database. Nella console di Cyber Protect, il workload viene visualizzato come oggetto al quale è possibile applicare un piano (piano di protezione, piano di backup, piano di scripting).

Alcuni workload richiedono l'installazione di un agente di protezione o la distribuzione di un'appliance virtuale. È possibile installare gli agenti utilizzando l'interfaccia utente grafica o l'interfaccia da riga di comando (installazione automatica). L'installazione automatica consente di automatizzare la procedura di installazione. Per ulteriori informazioni su come installare gli agenti di protezione, consultare "Installazione e deployment di agenti Cyber Protection" (pag. 59).

Un'appliance virtuale è una virtual machine già predisposta che contiene un agente di protezione. L'appliance virtuale consente di eseguire il backup di altre virtual machine nello stesso ambiente senza installare su di queste un agente di protezione (backup agentless). Le appliance virtuali sono disponibili nei formati specifici dell'hypervisor quali .ovf, .ova o .qcow. Per ulteriori informazioni sulle piattaforme di virtualizzazione che supportano il backup agentless, consultare "Piattaforme di virtualizzazione supportate" (pag. 32).

Importante
Gli agenti devono essere online almeno una volta ogni 30 giorni. In caso contrario, i rispettivi piani verranno revocati e i workload non saranno protetti.

La tabella seguente riepiloga i tipi di workload e i rispettivi agenti.

Tipo di workload	Agente	Esempi (elenco non esaustivo)
Macchine fisiche	In ogni sistema protetto è installato un agente di protezione.	Workstation Laptop Server

© Acronis International GmbH, 2003-2024

Tipo di workload	Agente	Esempi (elenco non esaustivo)
Macchine virtuali	A seconda della piattaforma di virtualizzazione, potrebbero essere disponibili i seguenti metodi di backup: • Backup con agente: in ogni sistema protetto è installato un agente di protezione. • Backup agentless: l'agente di protezione è installato solo sull'host hypervisor, su una virtual machine dedicata oppure distribuito come appliance virtuale. Questo agente esegue il backup di tutte le virtual machine dell'ambiente.	Macchina virtuale VMware Macchina virtuale Hyper-V Virtual machine basate su Kernel (KVM) gestite da oVirt
Workload di Microsoft 365 Business Workload di Google Workspace	Il backup dei workload viene eseguito da un agente cloud che non richiede installazione. Per utilizzare l'agente cloud, aggiungere l'organizzazione di Microsoft 365 o di Google Workspace alla console di Cyber Protect. È inoltre disponibile un agente locale per Office 365. Tale agente richiede l'installazione e può essere utilizzato per eseguire il backup delle caselle di posta di Exchange Online. Per ulteriori informazioni sulle differenze tra l'agente locale e quello cloud, consultare "Protezione dei dati di Microsoft 365" (pag. 608). .	Casella di posta di Microsoft 365 Microsoft 365 OneDrive Microsoft Teams Sito SharePoint Casella di posta Google Google Drive
Applicazioni	Il backup dei dati delle specifiche applicazioni viene eseguito da agenti dedicati, come l'Agente per SQL, l'Agente per Exchange, l'Agente per MySQL/MariaDB o l'Agente per Active Directory.	Database SQL Server Database MySQL/MariaDB Database Oracle Active Directory
Dispositivi mobili	Nei dispositivi protetti viene installata un'app mobile.	Dispositivi iOS o Android
Siti Web	Il backup dei siti web viene eseguito da un agente cloud che non richiede installazione.	Siti web accessibili tramite i protocolli SFTP o SSH

Per ulteriori informazioni sull'agente più adatto e sulla modalità di installazione, consultare "Di quale agente occorre disporre?" (pag. 62)

Aggiunta di workload alla console di Cyber Protect

Il primo passo per la protezione dei workload è la loro aggiunta alla console di Cyber Protect.

© Acronis International GmbH, 2003-2024

Nota
I tipi di workload che è possibile aggiungere variano in base alle quote di servizio dell'account. Se un tipo di workload specifico è mancante, risulta disabilitato nel pannello **Aggiungi dispositivi**.

Gli amministratori del Partner possono abilitare le quote di servizio necessarie nel portale di gestione. Per ulteriori informazioni, consultare "Informazioni per gli amministratori di Partner" (pag. 341).

Per aggiungere un workload

1. Accedere alla console di Cyber Protect.
2. Passare a **Dispositivi** > **Tutti i dispositivi**, quindi fare clic su **Aggiungi**.
   A sinistra viene aperto il pannello **Aggiungi dispositivi**.
3. Selezionare il canale di release.
4. Fare clic sul tipo di workload che si desidera aggiungere e quindi seguire le istruzioni per il workload specifico selezionato.

La tabella seguente riepiloga i tipi di workload e le azioni necessarie.

Workload da aggiungere	Azione richiesta	Procedura da seguire
Più sistemi Windows	Esecuzione dell'individuazione automatica nell'ambiente. Per eseguire l'individuazione automatica, è necessario almeno un sistema con un agente di protezione installato nella rete locale o nel dominio di Active Directory. Tale agente verrà utilizzato come agente di individuazione.	"Esecuzione dell'individuazione automatica e dell'individuazione manuale" (pag. 130)
Workstation Windows Server Windows	Installazione dell'Agente per Windows.	"Installazione degli agenti di protezione in Windows" (pag. 77) oppure "Installazione o disinstallazione automatica in Windows" (pag. 88)
Workstation macOs	Installazione dell'Agente per macOS.	"Installazione degli agenti di protezione in macOS" (pag. 82) oppure "Installazione e disinstallazione automatica in macOS" (pag. 112)
Server Linux	Installazione dell'Agente per Linux.	"Installazione degli agenti di protezione in Linux" (pag. 80)

© Acronis International GmbH, 2003-2024

Workload da aggiungere	Azione richiesta	Procedura da seguire
		oppure "Installazione o disinstallazione automatica in Linux" (pag. 106)
Dispositivi mobili (iOS, Android)	Installazione dell'app mobile.	"Protezione dei dispositivi mobili" (pag. 600)
Workload cloud-to-cloud		
Microsoft 365 Business	Aggiungere l'organizzazione Microsoft 365 alla console di Cyber Protect e utilizzare l'agente cloud per proteggere le caselle di posta di Exchange Online, i file di OneDrive, Microsoft Teams e i siti SharePoint. In alternativa, è possibile installare l'Agente per Office 365 locale. L'agente fornisce soltanto il backup per le caselle di posta di Exchange Online. Per ulteriori informazioni sulle differenze tra l'agente locale e quello cloud, fare riferimento a "Protezione dei dati di Microsoft 365" (pag. 608).	"Protezione dei dati di Microsoft 365" (pag. 608)
Google Workspace	Aggiungere l'organizzazione Google Workspace alla console di Cyber Protect e utilizzare l'agente cloud per proteggere le caselle di posta di Gmail e i file di Google Drive.	"Protezione dei dati di Google Workspace" (pag. 654)
Macchine virtuali		
VMware ESXi	Distribuzione dell'Agente per VMware (appliance virtuale) nell'ambiente.	"Distribuzione dell'Agente per VMware (Virtual Appliance)" (pag. 138)
	Installazione dell'Agente per VMware (Windows).	"Installazione degli agenti di protezione in Windows" (pag. 77) oppure "Installazione o disinstallazione automatica in Windows" (pag. 88)
Virtuozzo Hybrid Infrastructure	Distribuzione dell'Agente per Virtuozzo Hybrid Infrastructure	"Distribuzione dell'Agente per Virtuozzo Hybrid Infrastructure

© Acronis International GmbH, 2003-2024

Workload da aggiungere	Azione richiesta	Procedura da seguire
	(appliance virtuale) nell'ambiente.	(appliance virtuale)" (pag. 148)
Hyper-V	Installazione dell'Agente per Hyper-V.	"Installazione degli agenti di protezione in Windows" (pag. 77) oppure "Installazione o disinstallazione automatica in Windows" (pag. 88)
Virtuozzo	Installazione dell'Agente per Virtuozzo.	"Installazione degli agenti di protezione in Linux" (pag. 80) oppure "Installazione o disinstallazione automatica in Linux" (pag. 106)
KVM	Installazione dell'Agente per Windows.	"Installazione degli agenti di protezione in Windows" (pag. 77) oppure "Installazione o disinstallazione automatica in Windows" (pag. 88)
	Installazione dell'Agente per Linux.	"Installazione degli agenti di protezione in Linux" (pag. 80) oppure "Installazione o disinstallazione automatica in Linux" (pag. 106)
Red Hat Virtualization (oVirt)	Distribuzione dell'Agente per oVirt (appliance virtuale) nell'ambiente.	"Distribuzione dell'Agente per oVirt (Virtual Appliance)" (pag. 156)
Citrix XenServer	Installazione dell'Agente per Windows.	"Installazione degli agenti di protezione in Windows" (pag. 77) oppure "Installazione o disinstallazione automatica in Windows" (pag. 88)
	Installazione dell'Agente per Linux.	"Installazione degli agenti di protezione in Linux" (pag. 80) oppure "Installazione o disinstallazione automatica in Linux" (pag. 106)
Nutanix AHV	Installazione dell'Agente per Windows.	"Installazione degli agenti di

© Acronis International GmbH, 2003-2024

Workload da aggiungere	Azione richiesta	Procedura da seguire
		protezione in Windows" (pag. 77) oppure "Installazione o disinstallazione automatica in Windows" (pag. 88)
	Installazione dell'Agente per Linux.	"Installazione degli agenti di protezione in Linux" (pag. 80) oppure "Installazione o disinstallazione automatica in Linux" (pag. 106)
Oracle VM	Installazione dell'Agente per Windows.	"Installazione degli agenti di protezione in Windows" (pag. 77) oppure "Installazione o disinstallazione automatica in Windows" (pag. 88)
	Installazione dell'Agente per Linux.	"Installazione degli agenti di protezione in Linux" (pag. 80) oppure "Installazione o disinstallazione automatica in Linux" (pag. 106)
Scale Computing HC3	Distribuzione dell'Agente per Scale Computing HC3 (appliance virtuale) nell'ambiente.	"Distribuzione dell'Agente per Scale Computing HC3 (appliance virtuale)" (pag. 142)
Dispositivo di archiviazione collegato alla rete		
Synology	Distribuzione dell'Agente per Synology (appliance virtuale) nell'ambiente.	"Distribuzione dell'Agente per Synology" (pag. 163)
Applicazioni		
Microsoft SQL Server	Installazione dell'Agente per SQL.	"Installazione degli agenti di protezione in Windows" (pag. 77) oppure "Installazione o disinstallazione automatica in Windows" (pag. 88)
Microsoft Exchange Server	Installazione dell'Agente per Exchange.	
Microsoft Active Directory	Installazione dell'Agente per Active Directory.	
Database Oracle	Installazione dell'Agente per Oracle.	"Protezione per Oracle Database" (pag. 681)

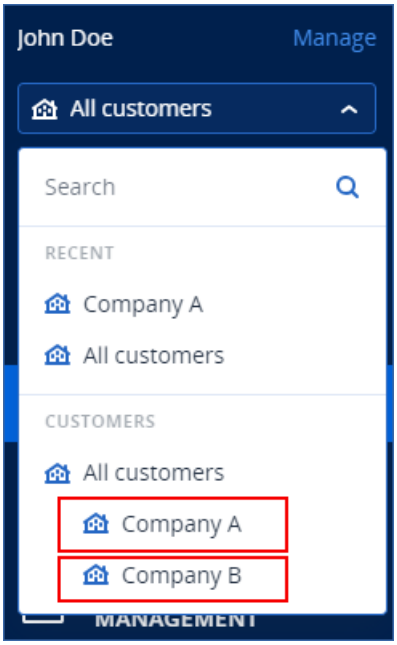
© Acronis International GmbH, 2003-2024

Workload da aggiungere	Azione richiesta	Procedura da seguire
Sito Web	Configurazione della connessione al sito web.	"Protezione di siti Web e di server di hosting" (pag. 689)

Per ulteriori informazioni sugli agenti di protezione disponibili e dove installarli, fare riferimento a "Di quale agente occorre disporre?" (pag. 62)

Informazioni per gli amministratori di Partner

- Un tipo di workload potrebbe essere mancante nel pannello **Aggiungi dispositivi** se una quota di servizio necessaria non è stata abilitata nel portale di gestione. Per altre informazioni sulle quote di servizio necessarie per i vari workload, fare riferimento a Abilitazione o disabilitazione degli elementi in offerta nella Guida per l'amministratore del Partner.
- L'amministratore del Partner non può aggiungere workload al livello **Tutti i clienti**. Per aggiungere un workload, selezionare un singolo tenant cliente.



Eliminazione di workload dalla console di Cyber Protect

È possibile rimuovere dalla console di Cyber Protect i workload che non è più necessario proteggere. La procedura varia in funzione del tipo di workload.

In alternativa, è possibile disinstallare l'agente nel workload protetto. Quando si disinstalla un agente, il workload protetto viene automaticamente rimosso dalla console di Cyber Protect.

© Acronis International GmbH, 2003-2024

Importante
Quando si rimuove un workload dalla console di Cyber Protect, tutti i piani applicati a tale workload vengono revocati. La rimozione di un workload non implica l'eliminazione dei piani o dei backup, né la disinstallazione dell'agente di protezione.

La tabella seguente riepiloga i tipi di workload e le azioni necessarie.

Workload da rimuovere	Azioni richieste	Procedura da seguire
Macchine fisiche e virtuali		
Sistemi fisici o virtuali nei quali è installato l'agente di protezione	1. Rimozione di workload dalla console di Cyber Protect. 2. [Facoltativo] Disinstallare l'agente di protezione.	"Per rimuovere un workload dalla console di Cyber Protect" (pag. 344) (Workload con agente di protezione)
Virtual machine il cui backup è eseguito al livello di hypervisor (backup agentless)	1. Nella console di Cyber Protect, rimuovere il sistema sul quale è installato l'agente di protezione. Tutte le virtual machine il cui backup è eseguito da questo agente verranno automaticamente rimosse dalla console. 2. [Facoltativo] Disinstallare l'agente di protezione.	"Per rimuovere un workload dalla console di Cyber Protect" (pag. 344) (Workload senza agente di protezione)
Workload cloud-to-cloud		
Workload di Microsoft 365 Business Workload di Google	Eliminare l'organizzazione Microsoft 365 o Google Workspace dalla console di Cyber	"Per rimuovere un workload dalla console di Cyber Protect" (pag. 344) (Workload cloud-to-cloud)

© Acronis International GmbH, 2003-2024

Workload da rimuovere	Azioni richieste	Procedura da seguire
Workspace	Protect. Tutte le risorse dell'organizzazione verranno automaticamente rimosse dalla console.	
Dispositivi mobili		
Dispositivi Android Dispositivi iOS	1. Rimuovere il dispositivo mobile dalla console di Cyber Protect. 2. [Facoltativo] Disinstallare l'app dal dispositivo mobile.	"Per rimuovere un workload dalla console di Cyber Protect" (pag. 344) (Dispositivo mobile)
Dispositivo di archiviazione collegato alla rete		
Synology	1. Rimozione di workload dalla console di Cyber Protect. 2. [Facoltativo] Disinstallare l'agente di protezione.	"Per rimuovere un workload dalla console di Cyber Protect" (pag. 344) (Workload con agente di protezione)
Applicazioni		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Database Oracle	1. Nella console di Cyber Protect, rimuovere il sistema sul quale è installato l'agente di protezione. Gli oggetti il cui backup è eseguito da questo agente verranno automaticamente rimossi dalla console. 2. [Facoltativo]	"Per rimuovere un workload dalla console di Cyber Protect" (pag. 344) (Workload senza agente di protezione)

© Acronis International GmbH, 2003-2024

Workload da rimuovere	Azioni richieste	Procedura da seguire
	Disinstallare l'agente di protezione.	
Siti Web	Rimuovere il sito web dalla console di Cyber Protect.	"Per rimuovere un workload dalla console di Cyber Protect" (pag. 344) (Sito web)

Per rimuovere un workload dalla console di Cyber Protect

Workload con agente di protezione

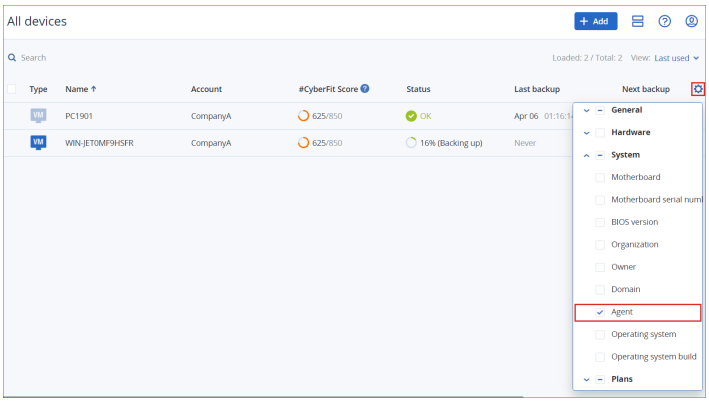
Questo tipo di workload può essere eliminato direttamente.

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare la casella di controllo accanto a uno o più workload da rimuovere.
3. Nel pannello **Azioni**, selezionare **Elimina**.
4. Confermare la selezione facendo clic su **Elimina**.
5. [Facoltativo] Disinstallare l'agente, come descritto in "Disinstallazione di agenti" (pag. 185).

Workload senza agente di protezione

Per rimuovere questo tipo di workload è necessario rimuovere il sistema nel quale è installato l'agente di protezione.

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Nell'angolo in alto a destra, fare clic sull'icona ingranaggio e selezionare la casella di controllo **Agente**.



Viene visualizzata la colonna **Agente**.

3. Nella colonna **Agente**, controllare il nome del sistema in cui è installato l'agente di protezione.
4. Nella console di Cyber Protect, selezionare la casella di controllo accanto al sistema nel quale è installato l'agente di protezione.

© Acronis International GmbH, 2003-2024

5. Nel pannello **Azioni**, selezionare **Elimina**.
6. Confermare la selezione facendo clic su **Elimina**.
7. [Facoltativo] Disinstallare l'agente, come descritto in "Disinstallazione di agenti" (pag. 185).

Workload cloud-to-cloud

Per rimuovere i workload il cui backup è eseguito da un agente cloud, rimuovere l'organizzazione Microsoft 365 o Google Workspace dalla console di Cyber Protect.

1. Nella console di Cyber Protect passare rispettivamente a **Dispositivi** > **Microsoft 365** oppure a **Dispositivi** > **Google Workspace**.
2. Fare clic sul nome dell'organizzazione Microsoft 365 o Google Workspace.
3. Nel pannello **Azioni**, selezionare **Elimina gruppo**.
4. Fare clic su **Elimina** per confermare l'azione.

Dispositivo mobile

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare la casella di controllo accanto al workload da rimuovere.
3. Nel pannello **Azioni**, selezionare **Elimina**.
4. Confermare la selezione facendo clic su **Elimina**.
5. [Facoltativo] Disinstallare l'app dal dispositivo mobile.

Sito Web

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare la casella di controllo accanto al workload da rimuovere.
3. Nel pannello **Azioni**, selezionare **Elimina**.
4. Confermare la selezione facendo clic su **Elimina**.

Gruppi dispositivi

I gruppi di dispositivi consentono di proteggere più workload simili con un piano di gruppo. Il piano viene applicato all'intero gruppo e non può essere revocato da un membro del gruppo.

Un workload può appartenere a più gruppi. Un workload incluso in un gruppo di dispositivi può essere protetto anche da piani individuali.

A un gruppo di dispositivi è possibile aggiungere solo workload dello stesso tipo. Ad esempio, in **Hyper-V** è possibile creare solo gruppi di virtual machine Hyper-V. In **Macchine con agenti**, è possibile creare soltanto gruppi di sistemi con agenti installati.

Non è possibile creare gruppi di dispositivi all'interno di gruppi di tipo **Tutti**, come il gruppo radice **Tutti i dispositivi**, o i gruppi integrati quali **Macchine con agenti** > **Tutti**, **Microsoft 365** > organizzazione dell'utente > **Utenti** > **Tutti gli utenti**.

© Acronis International GmbH, 2003-2024

Gruppi integrati e gruppi personalizzati

Gruppi integrati

Dopo essere stato registrato nella console di Cyber Protect, il workload viene visualizzato in uno dei gruppi radice integrati nella scheda **Dispositivi**, ad esempio **Macchine con agenti**, **Microsoft 365** o **Hyper-V**.

Tutti i workload non cloud-to-cloud registrati sono elencati anche nel gruppo radice **Tutti i dispositivi**. Un gruppo radice integrato distinto, che ha lo stesso nome del tenant, contiene tutti i workload non cloud-to-cloud e tutte le unità di questo tenant.

Non è possibile eliminare o modificare i gruppi radice o applicarvi dei piani.

Alcuni gruppi radice contengono uno o più livelli di sottogruppi integrati, ad esempio **Macchine con agenti** > **Tutti**, **Microsoft 365** > organizzazione dell'utente > **Team** > **Tutti i team**, **Google Workspace** > organizzazione dell'utente > **Unità condivise** > **Tutte le unità condivise**.

Non è possibile modificare o eliminare i sottogruppi integrati.

Gruppi personalizzati

Proteggere tutti i workload contenuti in un gruppo integrato non è sempre la scelta ottimale, in quanto il gruppo potrebbe includere workload che richiedono impostazioni della protezione diverse o una pianificazione della protezione differente.

In alcuni gruppi radice, ad esempio in **Macchine con agenti**, **Microsoft 365** o **Google Workspace**, è possibile creare sottogruppi personalizzati, che possono essere statici o dinamici.

È possibile modificare, rinominare o eliminare qualsiasi gruppo personalizzato.

Gruppi statici e gruppi dinamici

È possibile creare i seguenti tipi di gruppi personalizzati:

- Statico
- Dinamico

Gruppi statici

I gruppi statici contengono i workload aggiunti manualmente.

Il contenuto di un gruppo statico cambia soltanto quando un workload viene aggiunto o rimosso in modo esplicito.

Esempio: Viene creato un gruppo statico per il reparto contabilità aziendale, a cui si aggiungono manualmente i sistemi degli addetti contabili. Quando si applica un piano di gruppo, vengono protetti i sistemi inclusi nel gruppo. Se viene assunto un nuovo contabile, il sistema del nuovo addetto dovrà essere aggiunto manualmente al gruppo statico.

© Acronis International GmbH, 2003-2024

Gruppi dinamici

I gruppi dinamici contengono i workload che soddisfano criteri specifici. Questi criteri vengono definiti anticipatamente, creando una query di ricerca che include gli attributi (ad esempio, `osType`), i loro valori (ad esempio, `Windows`), e gli operatori di ricerca (ad esempio, `IN`).

In questo modo è possibile creare un gruppo dinamico per tutti i sistemi il cui sistema operativo è Windows o un gruppo dinamico che contiene tutti gli utenti dell'organizzazione Microsoft 365 il cui indirizzo e-mail inizia con `john`.

Tutti i workload che presentano gli attributi e i valori richiesti vengono automaticamente aggiunti al gruppo e qualsiasi workload che perda uno degli attributi o dei valori richiesti viene automaticamente rimosso dal gruppo.

Esempio 1: I nomi host dei sistemi che appartengono al reparto contabilità contengono la parola contabilità. Viene effettuata una ricerca dei sistemi che contengono la parola contabilità e i risultati della ricerca vengono quindi salvati come gruppo dinamico. A questo punto si applica un piano di protezione al gruppo. Se viene assunto un nuovo contabile, il nome del sistema del nuovo addetto conterrà la parola contabilità e il sistema verrà aggiunto automaticamente al gruppo dinamico non appena viene registrato nella console di Cyber Protect.

Esempio 2: Il reparto contabilità crea un'unità organizzativa (OU) Active Directory separata. L'unità organizzativa di contabilità viene specificata come attributo richiesto, e i risultati della ricerca vengono quindi salvati come gruppo dinamico. A questo punto si applica un piano di protezione al gruppo. Se viene assunto un nuovo contabile, il sistema del nuovo addetto verrà aggiunto al gruppo dinamico non appena viene aggiunto all'unità organizzativa di Active Directory e registrato nella console di Cyber Protect (indipendentemente da quale operazione avviene per prima).

Gruppi cloud-to-cloud e gruppi non cloud-to-cloud

I gruppi cloud-to-cloud contengono workload di Microsoft 365 o Google Workspace il cui backup è eseguito da un agente cloud.

I gruppi non cloud-to-cloud contengono tutti gli altri tipi di workload.

Piani supportati per gruppi di dispositivi

La tabella seguente riepiloga i piani che è possibile applicare a un gruppo di dispositivi.

Gruppo	Piani disponibili	Posizione del piano
Workload cloud-to-cloud (workload di Microsoft 365 e Google Workspace)	Piano di backup	**Gestione** > **Backup delle applicazioni cloud**
Workload non cloud-to-cloud	Piano di protezione	**Gestione** > **Piani di protezione**
	Piano di gestione	**Gestione** > **Piani di gestione remota**

© Acronis International GmbH, 2003-2024

Gruppo	Piani disponibili	Posizione del piano
	remota	
	Piano di scripting	**Gestione** > **Piani di scripting**

Le risorse cloud, ad esempio gli utenti di Microsoft 365 o Google Workspace, le condivisioni di OneDrive e Google Drive, Microsoft Teams o i gruppi di Azure AD vengono sincronizzate con la console di Cyber Protect subito dopo l'aggiunta di un'organizzazione di Microsoft 365 o Google Workspace alla console. Tutte le successive modifiche apportate a un'organizzazione vengono sincronizzate una volta al giorno.

Se è necessario sincronizzare subito una modifica, nella console di Cyber Protect passare rispettivamente a **Dispositivi** > **Microsoft 365** oppure a **Dispositivi** > **Google Workspace**, selezionare l'organizzazione richiesta e quindi fare clic su **Aggiorna**.

Creazione di un gruppo statico

È possibile creare un gruppo statico vuoto al quale aggiungere workload.

In alternativa, è possibile selezionare i workload e creare un nuovo gruppo statico con gli elementi selezionati.

Non è possibile creare gruppi di dispositivi all'interno di gruppi di tipo **Tutti**, come il gruppo radice **Tutti i dispositivi**, o i gruppi integrati quali **Macchine con agenti** > **Tutti**, **Microsoft 365** > organizzazione dell'utente > **Utenti** > **Tutti gli utenti**.

Per creare un gruppo statico

Nella finestra principale

1. Fare clic su **Dispositivi**, quindi selezionare il gruppo radice che contiene i workload per i quali creare il gruppo statico.
2. [Facoltativo] Per creare un gruppo nidificato, passare a un gruppo statico esistente.

   Nota
   Non è possibile creare gruppi statici nidificati per i workload cloud-to-cloud.

3. Fare clic su **+ Nuovo gruppo statico** al di sotto della struttura dei gruppi oppure fare clic su **Nuovo gruppo statico** nel pannello **Azioni**.
4. Specificare un nome per il nuovo gruppo.
5. [Facoltativo] Aggiungere un commento per il gruppo.
6. Fare clic su **OK**.

Nella struttura dei gruppi

1. Fare clic su **Dispositivi**, quindi selezionare il gruppo radice che contiene i workload per i quali creare il gruppo statico.

© Acronis International GmbH, 2003-2024

2. Fare clic sull'icona ingranaggio accanto al nome del gruppo in cui si desidera creare un nuovo gruppo statico.

   Nota
   Non è possibile creare gruppi statici nidificati per i workload cloud-to-cloud.

3. Fare clic su **Nuovo gruppo statico**.
4. Specificare un nome per il nuovo gruppo.
5. [Facoltativo] Aggiungere un commento per il gruppo.
6. Fare clic su **OK**.

Da una selezione

1. Fare clic su **Dispositivi**, quindi selezionare il gruppo radice che contiene i workload per i quali creare il gruppo statico.

   Nota
   Non è possibile creare gruppi di dispositivi all'interno di gruppi di tipo **Tutti**, come il gruppo radice **Tutti i dispositivi**, o i gruppi integrati quali **Macchine con agenti** > **Tutti**, **Microsoft 365** > organizzazione dell'utente > **Utenti** > **Tutti gli utenti**.

2. Selezionare le caselle di controllo accanto ai workload per i quali creare un nuovo gruppo, quindi fare clic su **Aggiungi al gruppo**.
3. Nella struttura delle cartelle, selezionare il livello padre del nuovo gruppo, quindi fare clic su **Nuovo gruppo statico**.

   Nota
   Non è possibile creare gruppi statici nidificati per i workload cloud-to-cloud.

4. Specificare un nome per il nuovo gruppo.
5. [Facoltativo] Aggiungere un commento per il gruppo.
6. Fare clic su **OK**.
   Il nuovo gruppo verrà visualizzato nella struttura della cartelle.
7. Fare clic su **Fine**.

Aggiunta di workload a un gruppo statico

È possibile selezionare prima il gruppo di destinazione e quindi aggiungere i workload a tale gruppo.

In alternativa, è possibile selezionare prima i workload e quindi aggiungerli a un gruppo.

Per aggiungere workload a un gruppo statico

Selezionando prima il gruppo di destinazione

© Acronis International GmbH, 2003-2024

1. Fare clic su **Dispositivi**, quindi individuare il gruppo di destinazione.
2. Selezionare il gruppo di destinazione, quindi fare clic su **Aggiungi periferiche**.
3. Nella struttura delle cartelle, scegliere il gruppo che contiene i workload necessari.
4. Selezionare le caselle di controllo accanto ai workload da aggiungere, quindi fare clic su **Aggiungi**.

Selezionando prima i workload

1. Fare clic su **Dispositivi**, quindi scegliere il gruppo radice che contiene i workload necessari.
2. Selezionare le caselle di controllo accanto ai workload da aggiungere, quindi fare clic su **Aggiungi al gruppo**.
3. Nella struttura delle cartelle, selezionare il gruppo di destinazione, quindi fare clic su **Fine**.

Creazione di un gruppo dinamico

È possibile creare un gruppo dinamico eseguendo una ricerca dei workload che presentano attributi specifici i cui valori vengono definiti nella query di ricerca. I risultati della ricerca vengono quindi salvati come gruppo dinamico.

Gli attributi supportati per la ricerca e la creazione di gruppi dinamici sono diversi per i workload cloud-to-cloud e per i workload non cloud-to-cloud. Per ulteriori informazioni sugli attributi supportati, consultare "Attributi di ricerca per i workload non cloud-to-cloud" (pag. 353) e "Attributi di ricerca per i workload cloud-to-cloud" (pag. 352).

I gruppi dinamici vengono creati nei rispettivi gruppi radice. Non sono supportati gruppi dinamici nidificati.

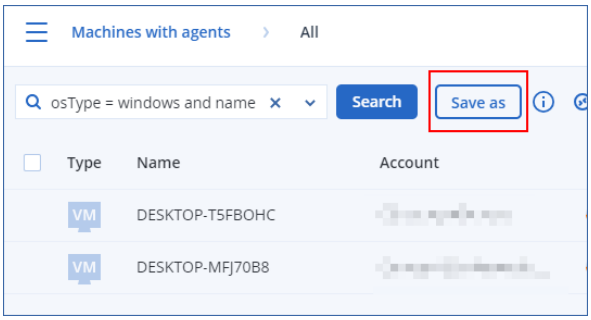
Non è possibile creare gruppi di dispositivi all'interno di gruppi di tipo **Tutti**, come il gruppo radice **Tutti i dispositivi**, o i gruppi integrati quali **Macchine con agenti** > **Tutti**, **Microsoft 365** > organizzazione dell'utente > **Utenti** > **Tutti gli utenti**.

Per creare un gruppo dinamico

Workload non cloud-to-cloud

1. Fare clic su **Dispositivi**, quindi selezionare il gruppo contenente i workload per i quali si intende creare un nuovo gruppo dinamico.
2. Eseguire la ricerca dei workload utilizzando gli attributi di ricerca e gli operatori supportati.
   In una singola query è possibile usare più attributi e operatori. Per ulteriori informazioni sugli attributi supportati, consultare "Attributi di ricerca per i workload non cloud-to-cloud" (pag. 353).
3. Fare clic su **Salva come** accanto al campo di ricerca.

© Acronis International GmbH, 2003-2024



Nota

Il pulsante **Salva come** non è disponibile se non è permessa la creazione di un gruppo dinamico in un livello specifico. Ad esempio, nel gruppo radice **Dispositivi** > **Tutti i dispositivi**.

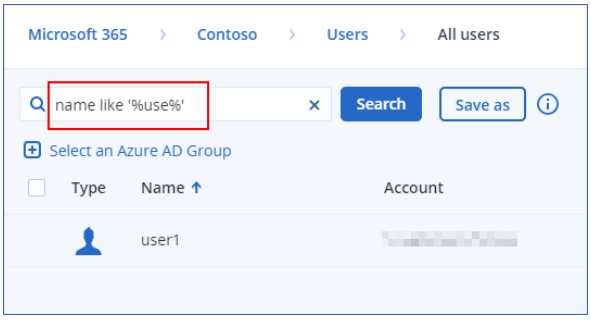
Selezionare un altro livello (ad esempio, **Dispositivi** > **Macchine con agenti** > **Tutti**), quindi ripetere i passaggi precedenti. Con questa ricerca è possibile creare un gruppo dinamico all'interno di **Macchine con agenti**, ma non all'interno di **Macchine con agenti** > **Tutti**.

4. Specificare un nome per il nuovo gruppo.
5. [Facoltativo] Nel campo **Commento**, aggiungere una descrizione per il nuovo gruppo.
6. Fare clic su **OK**.

Workload cloud-to-cloud

1. Fare clic su **Dispositivi**, quindi selezionare **Microsoft 365** o **Google Workspace**.
2. Selezionare il gruppo contenente i workload per i quali si intende creare un nuovo gruppo dinamico. Ad esempio, **Utenti** > **Tutti gli utenti**.
3. Eseguire la ricerca dei workload utilizzando gli attributi di ricerca e gli operatori supportati oppure selezionando gli utenti di Microsoft 365 da un gruppo Active Directory specifico.

   In una singola query è possibile usare più attributi e operatori. Per ulteriori informazioni sugli attributi supportati, consultare "Attributi di ricerca per i workload cloud-to-cloud" (pag. 352).



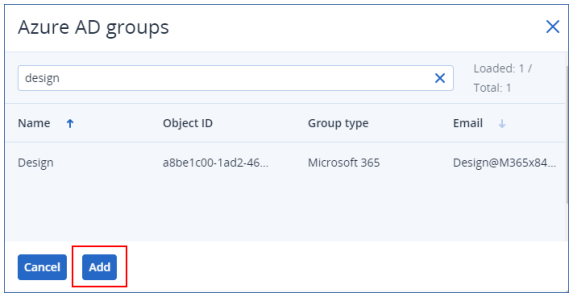
4. [Solo per **Microsoft 365** > **Utenti**] Per selezionare utenti da un gruppo Active Directory specifico, procedere come indicato di seguito:
   a. Passare a **Utenti** > **Tutti gli utenti**.
   b. Fare clic su **Selezionare un gruppo Azure AD**.

      Viene visualizzato un elenco di tutti i gruppi Active Directory dell'organizzazione.

© Acronis International GmbH, 2003-2024

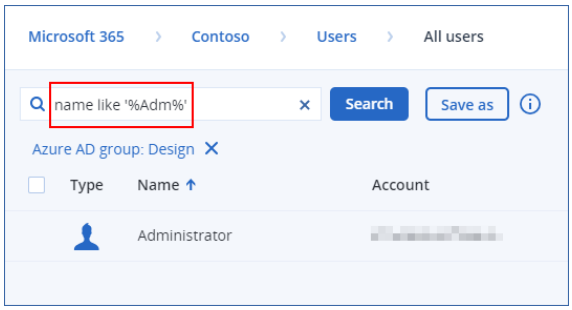
In questo elenco è possibile cercare un gruppo specifico oppure ordinare i gruppi in base al nome o all'indirizzo e-mail.

c. Selezionare il gruppo Active Directory desiderato, quindi fare clic su **Aggiungi**.



d. [Facoltativo] Per includere o escludere utenti specifici dal gruppo Active Directory selezionato, creare una query di ricerca utilizzando gli attributi di ricerca e gli operatori supportati.

In una singola query è possibile usare più attributi e operatori. Per ulteriori informazioni sugli attributi supportati, consultare "Attributi di ricerca per i workload cloud-to-cloud" (pag. 352).



5. Fare clic su **Salva come** accanto al campo di ricerca.

Nota

Il pulsante **Salva come** non è disponibile se non è permessa la creazione di un gruppo dinamico in un livello specifico. Ad esempio, in **Microsoft 365** > organizzazione dell'utente > **Utenti**.

Selezionare un altro livello (ad esempio, **Microsoft 365** > organizzazione dell'utente > **Utenti** > **Tutti**), quindi ripetere i passaggi precedenti. Con questa ricerca è possibile creare un gruppo dinamico all'interno di **Microsoft 365** > organizzazione dell'utente > **Utenti** >, ma non all'interno di **Utenti** > **Tutti**.

6. Specificare un nome per il nuovo gruppo.
7. [Facoltativo] Nel campo **Commento**, aggiungere una descrizione per il nuovo gruppo.
8. Fare clic su **OK**.

Attributi di ricerca per i workload cloud-to-cloud

La tabella seguente riepiloga gli attributi che è possibile utilizzare nelle query di ricerca per i workload di Microsoft 365 e Google Workspace.

Per vedere quali attributi è possibile utilizzare nelle query di ricerca per altri tipi di workload, fare riferimento a "Attributi di ricerca per i workload non cloud-to-cloud" (pag. 353).

© Acronis International GmbH, 2003-2024

Attributo	Significato	Può essere utilizzato in	Esempi di query di ricerca	Supportato per la creazione dei gruppi
`name`	Nome visualizzato di un workload di Microsoft 365 o Google Workspace	Tutte le risorse cloud-to-cloud	`name = 'My Name'` `name LIKE '*nam*'`	Sì

`email`	Indirizzo e-mail di un utente o di un gruppo di Microsoft 365 o di un utente di Google Workspace	Microsoft 365 > Gruppi
		Microsoft 365 > Utenti
		Google Workspace > Utenti
			`email = 'my_group_email@mycompany.com'`
			`email LIKE '*@company*'`
			`email NOT LIKE '*enterprise.com'`
				Sì

`siteName`	Nome di un sito associato a un gruppo di Microsoft 365	Microsoft 365 > Gruppi	`siteName = 'my_site'` `siteName LIKE '*company.com*support*'`	Sì
`url`	Indirizzo web di un gruppo di Microsoft 365 o di un sito SharePoint	Microsoft 365 > Gruppi Microsoft 365 > Raccolte di siti	`url = 'https://www.mycompany.com/'` `url LIKE '*www.mycompany.com*'`	Sì

Attributi di ricerca per i workload non cloud-to-cloud

La tabella seguente riepiloga gli attributi che è possibile utilizzare nelle query di ricerca per i workload non cloud-to-cloud.

Per vedere quali attributi è possibile utilizzare nelle query di ricerca per i workload cloud-to-cloud, fare riferimento a "Attributi di ricerca per i workload cloud-to-cloud" (pag. 352).

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
Informazioni generali			
`name`	Nome del workload, ad esempio: • Nome host per le	`name = 'en-00'`	Sì

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
	macchine fisiche • Nome per le macchine virtuali • Nome database • Indirizzo di posta elettronica per le caselle postali		
`id`	ID del dispositivo. Per visualizzare l'ID del dispositivo, in **Dispositivi**, selezionare il dispositivo, fare clic su **Dettagli** > **Tutte le proprietà**. L'ID è visualizzato nel campo `id`.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Sì
`resourceType`	Tipo di workload. Valori possibili: • `'machine'` • `'exchange'` • `'mssql_server'` • `'mssql_instance'` • `'mssql_database'` • `'mssql_database_folder'` • `'msexchange_database'` • `'msexchange_storage_group'` • `'msexchange_mailbox.msexchange'` • `'msexchange_mailbox.office365'` • `'mssql_aag_group'` • `'mssql_aag_database'` • `'virtual_machine.vmww'` • `'virtual_machine.vmwesx'` • `'virtual_host.vmwesx'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Sì

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
	• 'virtual_cluster.vmwesx' • 'virtual_appliance.vmwesx' • 'virtual_application.vmwesx' • 'virtual_resource_pool.vmwesx' • 'virtual_center.vmwesx' • 'datastore.vmwesx' • 'datastore_cluster.vmwesx' • 'virtual_network.vmwesx' • 'virtual_data_center.vmwesx' • 'virtual_machine.vmww' • 'virtual_cluster.mshyperv' • 'virtual_machine.mshyperv' • 'virtual_host.mshyperv' • 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_machine.parallelsw' • 'virtual_host.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm'		

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
	• `'virtual_machine.xen'` • `'bootable_media'`		
`chassis`	Tipo di chassis. Valori possibili: • `laptop` • `desktop` • `server` • `other` • `unknown`	`chassis = 'laptop'` `chassis IN ('laptop', 'desktop')`	Sì
`ip`	Indirizzo IP (solo per sistemi fisici).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Sì
`comment`	Commento per un dispositivo. È possibile specificarlo automaticamente o manualmente. Valore predefinito: • Per i sistemi fisici che eseguono Windows, la descrizione del sistema in Windows viene automaticamente copiata come commento. Questo valore viene sincronizzato ogni 15 minuti. • Il campo è vuoto per altri dispositivi.	`comment = 'important machine'` `commento = ''` (tutti i sistema senza un commento)	Sì

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi

	Nota
	La sincronizzazione automatica è disabilitata se nel campo del commento è presente del testo aggiunto manualmente. Per abilitare di nuovo la sincronizzazione, eliminare questo testo.
	
	Per aggiornare i commenti sincronizzati automaticamente per i workload, riavviare Managed Machine Service in **Servizi di Windows** o eseguire i comandi seguenti nel prompt dei comandi:
	`net stop mms`
	`net start mms`
	
	Per visualizzare il commento al dispositivo, in **Dispositivi** selezionare il dispositivo, fare clic su **Dettagli** e quindi individuare la sezione **Commento**.
	
	Per aggiungere o modificare un commento manualmente, fare clic su **Aggiungi** o su **Modifica**.
	
	Nei dispositivi nei quali è installato un agente di protezione, sono presenti due campi commento distinti:		

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
	• Commento per agente ◦ Per i sistemi fisici che eseguono Windows, la descrizione del sistema in Windows viene automaticamente copiata come commento. Questo valore viene sincronizzato ogni 15 minuti. ◦ Il campo è vuoto per altri dispositivi. **Nota** La sincronizzazione automatica è disabilitata se nel campo del commento è presente del testo aggiunto manualmente. Per abilitare di nuovo la sincronizzazione, eliminare questo testo. • Commento per dispositivo ◦ Se il commento per agente viene specificato automaticamente, viene copiato come un commento per dispositivo. I commenti per agente aggiunti manualmente non vengono copiati come commenti per dispositivo. ◦ I commenti per		

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
	dispositivo non vengono copiati come commenti per agente. In un dispositivo può essere specificato un solo commento o entrambi, oppure entrambi possono essere vuoti. Se entrambi i commenti sono specificati, il commento per dispositivo è prioritario. Per visualizzare un commento per agente, in **Impostazioni** > **Agenti**, selezionare il dispositivo con l'agente, fare clic su **Dettagli** e quindi individuare la sezione **Commento**. Per visualizzare il commento al dispositivo, in **Dispositivi** selezionare il dispositivo, fare clic su **Dettagli** e quindi individuare la sezione **Commento**. Per aggiungere o modificare un commento manualmente, fare clic su **Aggiungi** o su **Modifica**.		
`isOnline`	Disponibilità del workload. Valori possibili: • `true` • `false`	`isOnline = true`	No
`hasAsz`	Disponibilità di Secure Zone.	`hasAsz = true`	Sì

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
	Valori possibili: • `true` • `false`		

`tzOffset`	Offset del fuso orario rispetto all'orario UTC, in minuti.	`tzOffset = 120`
		`tzOffset > 120`
		`tzOffset < 120`
			Sì

CPU, memoria, dischi			
`cpuArch`	Architettura CPU. Valori possibili: • `'x64'` • `'x86'`	`cpuArch = 'x64'`	Sì
`cpuName`	Nome CPU.	`cpuName LIKE '%XEON%'`	Sì
`memorySize`	Dimensione della RAM in megabyte.	`memorySize < 1024`	Sì
`diskSize`	Dimensione dell'unità in gigabyte o megabyte (solo per sistemi fisici).	`diskSize < 300GB` `diskSize >= 3000000MB`	No
Sistema operativo			
`osName`	Nome del sistema operativo.	`osName LIKE '%Windows XP%'`	Sì
`osType`	Tipo di sistema operativo. Valori possibili: • `'windows'` • `'linux'` • `'macosx'`	`osType = 'windows'` `osType IN ('linux', 'macosx')`	Sì
`osArch`	Architettura del sistema operativo. Valori possibili: • `'x64'` • `'x86'`	`cpuArch = 'x86'`	Sì

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
`osProductType`	Tipo di prodotto del sistema operativo. Valori possibili: • `'dc'` Significa controller di dominio. **Nota** Quando il ruolo di controller di dominio è assegnato su un server Windows, `osProductType` cambia da `server` a `dc`. Questi sistemi non verranno inclusi nei risultati della ricerca per `osProductType='server'`. • `'server'` • `'workstation'`	`osProductType = 'server'`	Sì
`osSp`	Service Pack del sistema operativo.	`osSp = 1`	Sì
`osVersionMajor`	Versione principale del sistema operativo.	`osVersionMajor = 1`	Sì
`osVersionMinor`	Versione secondaria del sistema operativo.	`osVersionMinor > 1`	Sì
Agente			
`agentVersion`	Versione dell'agente di protezione installato.	`agentVersion LIKE '12.0.*'`	Sì
`hostId`	ID interno dell'agente di protezione. Per visualizzare l'ID dell'agente di protezione, in **Dispositivi**, selezionare il dispositivo, fare clic su **Dettagli** > **Tutte le proprietà**. Controllare il	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Sì

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
	valore `id` della proprietà `agent`.		
`virtualType`	Tipo di virtual machine. Valori possibili: • `'vmwesx'` Virtual machine VMware. • `'mshyperv'` Virtual machine Hyper-V. • `'pcs'` Virtual machine Virtuozzo. • `'hci'` Virtual machine Virtuozzo Hybrid Infrastructure. • `'scale'` Virtual machine Scale Computing HC3. • `'ovirt'` Virtual machine oVirt	`virtualType = 'vmwesx'`	Sì
`insideVm`	Macchina virtuale contenente un agente. Valori possibili: • `true` • `false`	`insideVm = true`	Sì
Posizione			
`tenant`	Il nome del tenant al quale appartiene il dispositivo.	`tenant = 'Unit 1'`	Sì
`tenantId`	L'identificatore del tenant al quale appartiene il dispositivo. Per visualizzare l'ID del tenant, in **Dispositivi**,	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Sì

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
	selezionare il dispositivo, fare clic su **Dettagli** > **Tutte le proprietà**. L'ID è visualizzato nel campo `ownerId`.		
`ou`	Dispositivi che appartengono all'unità organizzativa Active Directory specificata.	`ou IN ('RnD', 'Computers')`	Sì
Stato			
`state`	Stato dispositivo. Valori possibili: • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`	`state = 'backup'`	No
stato	Stato protezione. Valori possibili: • `ok` • `warning` • `error` • `critical` • `protected`	`status = 'ok'` `status IN ('error', 'warning')`	No

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
	• `notProtected`		
`protectedByPlan`	Dispositivi protetti da un piano di protezione con un ID indicato. Per visualizzare l'ID del piano, in **Gestione** > **Piani di protezione**, selezionare un piano, fare clic sulla barra nella colonna **Stato** e quindi selezionare il nome dello stato. Sarà creata una nuova ricerca con l'ID del piano.	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`okByPlan`	Dispositivi protetti da un piano di protezione con un ID indicato e con lo stato **OK**.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`errorByPlan`	Dispositivi protetti da un piano di protezione con un ID indicato e con lo stato **Errore**.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`warningByPlan`	Dispositivi protetti da un piano di protezione con un ID indicato e con lo stato **Attenzione**.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`runningByPlan`	Dispositivi protetti da un piano di protezione con un ID indicato e con lo stato **In esecuzione**.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`interactionByPlan`	Dispositivi protetti da un piano di protezione con un ID indicato e con lo stato **Interazione richiesta**.	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`lastBackupTime`*	Data e ora dell'ultimo backup riuscito. Il formato è `'YYYY-MM-DD HH:MM'`.	`lastBackupTime > '2023-03-11'` `lastBackupTime <= '2023-03-11 00:15'`	No

© Acronis International GmbH, 2003-2024

Attributo	Significato	Esempi di query di ricerca	Supportato per la creazione dei gruppi
		`lastBackupTime is null`	
`lastBackupTryTime*`	L'ora dell'ultimo backup tentato. Il formato è `'YYYY-MM-DD HH:MM'`.	`lastBackupTryTime >= '2023-03-11'`	No
`nextBackupTime*`	L'ora del backup successivo. Il formato è `'YYYY-MM-DD HH:MM'`.	`nextBackupTime >= '2023-08-11'`	No

`lastVAScanTime*`	Data e ora dell'ultima vulnerability assessment riuscita.
	Il formato è `'YYYY-MM-DD HH:MM'`.
		`lastVAScanTime > '2023-03-11'`
		`lastVAScanTime <= '2023-03-11 00:15'`
		`lastVAScanTime is null`
			Sì

`lastVAScanTryTime*`	L'ora dell'ultimo tentativo di vulnerability assessment. Il formato è `'YYYY-MM-DD HH:MM'`.	`lastVAScanTimeTryTime >= '2022-03-11'`	Sì
`nextVAScanTime*`	L'ora della vulnerability assessment successiva. Il formato è `'YYYY-MM-DD HH:MM'`.	`nextVAScanTime <= '2023-08-11'`	Sì
`network_status`	Stato di isolamento della rete per il servizio Endpoint Detection and Response (EDR). Valori possibili: • `connected` • `isolated`	`network_status= 'connected'`	Sì

© Acronis International GmbH, 2003-2024

Nota

Se il valore di ora e minuti viene ignorato, l'ora di avvio considerata corrisponderà a AAAA-MM-GG 00:00, e l'ora di fine a AAAA-MM-GG 23:59:59. Ad esempio, `lastBackupTime = 2023-01-20` significa che i risultati della ricerca includeranno tutti i backup dell'intervallo `lastBackupTime >= 2023-01-20 00:00` e `lastBackupTime <= 2023-01-20 23:59:59`.

Operatori di ricerca

La tabella seguente riepiloga gli operatori che è possibile utilizzare nelle query di ricerca.

In una singola query è possibile usare più operatori.

Operatore	Supportato da	Significato	Esempi
`AND`	Tutti i workload	Operatore logico di congiunzione	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Tutti i workload	Operatore logico di disgiunzione	`state = 'backup' OR state = 'interactionRequired'`
`NOT`	Tutti i workload	Operatore logico di negazione	`NOT(osProductType = 'workstation')`
`IN (<value1>,... <valueN>)`	Tutti i workload	Questo operatore controlla se un'espressione corrisponde a un qualsiasi valore in un elenco di valori.	`osType IN ('windows', 'linux')`
`NOT IN`	Tutti i workload	Questo operatore è l'inverso dell'operatore `IN`.	`NOT osType IN ('windows', 'linux')`

`LIKE 'wildcard pattern'`	Tutti i workload	Questo operatore controlla se un'espressione corrisponde al modello con carattere jolly.
		È possibile utilizzare i seguenti caratteri jolly:
		• * o % L'asterico e il segno di percentuale rappresentano zero, uno o caratteri
			`name LIKE 'en-00'`
			`name LIKE '*en-00'`
			`name LIKE '*en-00*'`
			`name LIKE 'en-00_'`

© Acronis International GmbH, 2003-2024

Operatore	Supportato da	Significato	Esempi
		multipli • _ Il trattino basso rappresenta un carattere singolo	

`NOT LIKE 'wildcard pattern'`	Tutti i workload	Questo operatore è l'inverso dell'operatore `LIKE`.
		È possibile utilizzare i seguenti caratteri jolly:
		• * o % L'asterico e il segno di percentuale rappresentano zero, uno o caratteri multipli
		• _ Il trattino basso rappresenta un carattere singolo
			`NOT name LIKE 'en-00'`
			`NOT name LIKE '*en-00'`
			`NOT name LIKE '*en-00*'`
			`NOT name LIKE 'en-00_'`

`RANGE (<starting_value>, <ending_value>)`	Tutti i workload	Questo operatore controlla se un'espressione è compresa in un intervallo di valori (inclusivo).
		Le query di ricerca con stringhe alfanumeriche utilizzano l'ordinamento ASCII ma non distinguono tra maiuscole e minuscole.
			`ip RANGE('10.250.176.1','10.250.176.50')`
			`name RANGE('a','d')`
			Questa query consente di filtrare tutti i nomi che iniziano con A, B e C, come `Alice`, `Bob`, `Claire`. Tuttavia, solo la singola lettera D soddisfa i requisiti, quindi i nomi con più lettere, come `Diana` o `Don` non verranno inclusi.
			Per ottenere lo stesso risultato, è possibile utilizzare anche la query seguente:
			`name >= 'a' AND name <= 'd'`

= o ==	Tutti i workload	Operatore *Uguale a*	`osProductType = 'server'`
!= o <>	Tutti i workload	Operatore *Diverso da*	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
<	Workload non cloud-to-cloud	Operatore *Minore di*	`memorySize < 1024`
>	Workload non cloud-to-	Operatore *Maggiore di*.	`diskSize > 300GB`

© Acronis International GmbH, 2003-2024

Operatore	Supportato da	Significato	Esempi
	cloud		
<=	Workload non cloud-to-cloud	Operatore *Minore o uguale a*	`lastBackupTime <= '2022-03-11 00:15'`
>=	Workload non cloud-to-cloud	Operatore *Maggiore o uguale a*	`nextBackupTime >= '2022-08-11'`

Modifica di un gruppo dinamico

È possibile modificare un gruppo dinamico modificando la query di ricerca che definisce il contenuto del gruppo.

Nei gruppi dinamici basati su Active Directory, è anche possibile modificare il gruppo Active Directory.

Per modificare un gruppo dinamico

Modificando la query di ricerca

1. Fare clic su **Dispositivi**, quindi passare al gruppo dinamico da modificare e selezionarlo.
2. Fare clic sull'icona ingranaggio accanto al nome del gruppo, quindi su **Modifica**. In alternativa, fare clic su **Modifica** nel pannello **Azioni**.
3. Modificare la query di ricerca modificando gli attributi di ricerca, i rispettivi valori o gli operatori di ricerca, quindi fare clic su **Cerca**.
4. Fare clic su **Salva** accanto al campo di ricerca.

Modificando il gruppo Active Directory

Nota
Questa procedura è applicabile ai gruppi dinamici basati su Active Directory. I gruppi dinamici basati su Active Directory sono disponibili solo in **Microsoft 365** > **Utenti**.

1. Fare clic su **Dispositivi**, passare a **Dispositivi** > **Microsoft 365** > organizzazione dell'utente > **Utenti**.
2. Selezionare il gruppo dinamico da modificare.
3. Fare clic sull'icona ingranaggio accanto al nome del gruppo, quindi su **Modifica**. In alternativa, fare clic su **Modifica** nel pannello **Azioni**.
4. Modificare il contenuto del gruppo in uno dei modi seguenti:
   - Modificare il gruppo Active Directory selezionato facendo clic sul relativo nome e quindi scegliendo un nuovo gruppo Active Directory dall'elenco visualizzato.

© Acronis International GmbH, 2003-2024

- Modificare la query di ricerca, quindi fare clic su **Cerca**.
  La query di ricerca si limita al gruppo Active Directory attualmente selezionato.

5. Fare clic su **Salva** accanto al campo di ricerca.

È possibile salvare le modifiche senza sovrascrivere il gruppo in uso. Per salvare la configurazione modificata come nuovo gruppo, fare clic sul pulsante freccia accanto al campo di ricerca, quindi su **Salva come**.

Eliminare un gruppo

Quando si elimina un gruppo di dispositivi, tutti i piani applicati a tale gruppo vengono revocati. I workload appartenenti al gruppo non saranno più protetti se non viene applicato loro un altro piano.

Per eliminare un gruppo di dispositivi

1. Fare clic su **Dispositivi**, quindi passare al gruppo da eliminare.
2. Fare clic sull'icona ingranaggio accanto al nome del gruppo, quindi su **Elimina**.
3. Confermare la selezione facendo clic su **Elimina**.

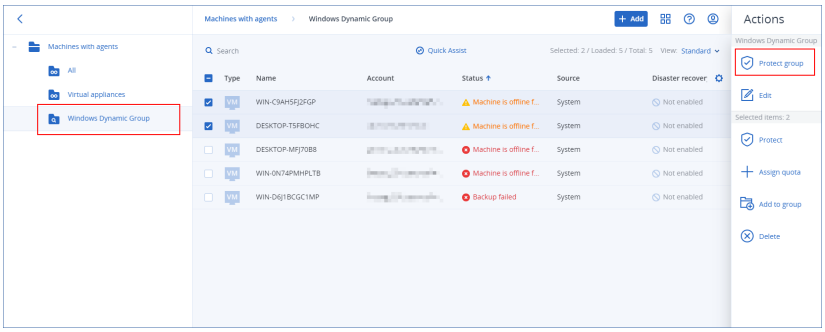
Applicazione di un piano a gruppo

È possibile applicare un piano a un gruppo selezionando prima il gruppo e quindi assegnando il piano a tale gruppo.

In alternativa, è possibile aprire un piano in modalità di modifica e quindi aggiungere un gruppo al piano.

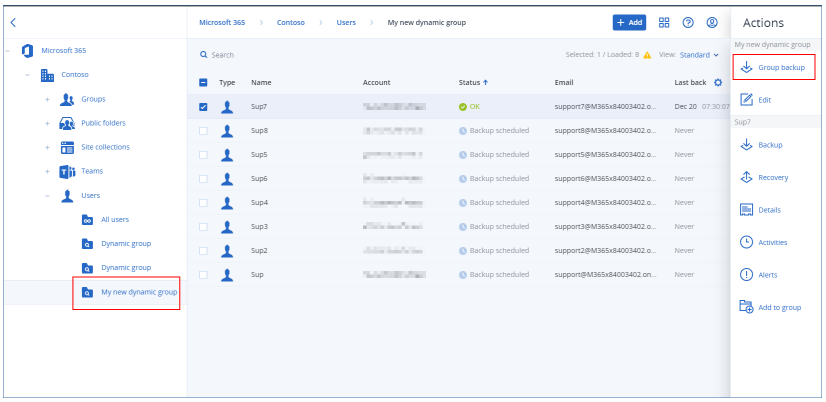
Per applicare un piano a un gruppo

1. Fare clic su **Dispositivi**, quindi passare al gruppo al quale applicare un piano.
2. [Per i workload non cloud-to-cloud] Fare clic su **Proteggi gruppo**.



   Viene visualizzato un elenco dei piani applicabili.
3. [Per i workload cloud-to-cloud] Fare clic su **Raggruppa backup**.

© Acronis International GmbH, 2003-2024



Viene visualizzato un elenco dei piani di backup applicabili.

4. [Per applicare un piano esistente] Selezionare il piano, quindi fare clic su **Applica**.
5. [Per creare un nuovo piano] Fare clic su **Crea piano**, selezionare il tipo di piano, quindi creare il nuovo piano.

   Per ulteriori informazioni sui tipi di piani disponibili e su come crearli, fare riferimento a "Piani supportati per gruppi di dispositivi" (pag. 347).

Nota
L'esecuzione dei piani di backup applicati a gruppi di dispositivi cloud-to-cloud è automaticamente pianificata una volta al giorno. Pertanto, non è possibile eseguire tali piani su richiesta facendo clic su **Esegui ora**.

Revocare un piano da un gruppo

È possibile revocare un piano da un gruppo selezionando per primo il gruppo e quindi revocando il piano da questo.

In alternativa, è possibile aprire il piano in modalità di modifica e quindi rimuovere il gruppo dal piano.

Per revocare un piano da un gruppo

1. Fare clic su **Dispositivi**, quindi passare al gruppo dal quale revocare un piano.
2. [Per i workload non cloud-to-cloud] Fare clic su **Proteggi gruppo**.
   Viene visualizzato un elenco dei piani applicati al gruppo selezionato.
3. [Per i workload cloud-to-cloud] Fare clic su **Raggruppa backup**.
   Viene visualizzato un elenco dei piani di backup applicati al gruppo selezionato.
4. Selezionare il piano da revocare.
5. [Per i workload non cloud-to-cloud] Fare clic sull'icona dei puntini di sospensione, quindi fare clic su **Revoca**.
6. [Per i workload cloud-to-cloud] Fare clic sull'icona ingranaggio, quindi fare clic su **Revoca**.

© Acronis International GmbH, 2003-2024

Lavorare con il modulo Controllo dispositivo

Come parte dei piani di protezione del servizio Cyber Protection, il modulo Controllo dispositivo[1] si avvale di un sottoinsieme delle funzioni dell'agente per la Prevenzione della perdita di dati[2] su ogni computer protetto, per rilevare e prevenire l'accesso non autorizzato ai dati e la loro trasmissione tramite i canali dei computer locali. Fornisce un controllo altamente granulare su un'ampia gamma di percorsi attraverso cui può avvenire la perdita di dati, incluso lo scambio di dati tramite supporti rimovibili, stampanti, dispositivi virtuali e reindirizzati, appunti di Windows.

Il modulo è disponibile per Cyber Protect Essentials, Cyber Protect Standard e per le edizioni di Cyber Protect Advanced concesse in licenza a workload.

Nota
Nei sistemi Windows, le funzionalità per il controllo dei dispositivi richiedono l'installazione dell'Agente per la Prevenzione della perdita di dati. Tale agente viene installato automaticamente per i workload protetti se il modulo **Controllo dispositivo** è abilitato nei rispettivi piani di protezione.

Il modulo Controllo dispositivo si avvale delle funzioni di prevenzione della perdita di dati[3] dell'agente per esercitare il controllo contestuale sull'accesso ai dati e sulle operazioni di trasferimento che avvengono sul computer protetto. Ne sono esempi l'accesso degli utenti a periferiche e porte, la stampa di documenti, operazioni di copia/incolla da appunti, operazioni di formattazione ed espulsione di supporti e sincronizzazioni con dispositivi mobili connessi in locale. L'agente per la Prevenzione della perdita di dati include una struttura per tutti i componenti della gestione e dell'amministrazione centralizzata del modulo Controllo dispositivo, e pertanto deve essere installato su ogni sistema da proteggere con tale modulo. L'agente consente, limita o nega le azioni dell'utente in base alle impostazioni del controllo dispositivo che riceve dal piano di protezione applicato al computer protetto.

---

[1]Componente di un piano di protezione, il modulo Controllo dispositivo si avvale di un sottoinsieme delle funzioni dell'agente di prevenzione della perdita di dati su ogni computer protetto, per rilevare e prevenire l'accesso non autorizzato ai dati e la loro trasmissione tramite i canali dei computer locali, quali, ad esempio, l'accesso degli utenti a periferiche e porte, la stampa di documenti, operazioni di copia/incolla da appunti, operazioni di formattazione ed espulsione di supporti e di sincronizzazione con dispositivi mobile connessi in locale. Il modulo Controllo dispositivo offre un controllo granulare e contestuale dei tipi di dispositivi e porte a cui gli utenti possono accedere sul computer protetto e sulle azioni che gli utenti possono intraprendere su tali dispositivi.
[2]Componente del sistema del cliente per la prevenzione della perdita di dati, che impedisce l'utilizzo non autorizzato del computer host per la trasmissione e l'archiviazione di dati sensibili, riservati o protetti applicando una combinazione di tecniche di analisi del contesto e dei contenuti e criteri per la prevenzione della perdita di dati gestiti a livello centralizzato. Cyber Protection offre un agente di prevenzione della perdita di dati ricco di funzionalità. Tuttavia, la funzionalità dell'agente in un computer protetto è limitata all'insieme di funzionalità di prevenzione della perdita di dati disponibile con le licenze di Cyber Protection, e dipende dal piano di protezione applicato a tale computer.
[3]Un sistema di tecnologie integrate e di misure organizzative intese a individuare e a prevenire la diffusione e/o l'accesso accidentale o intenzionale a dati riservati, protetti o sensibili da parte di entità non autorizzate interne o esterne all'organizzazione, o il trasferimento di tali dati in ambienti non attendibili.

© Acronis International GmbH, 2003-2024

Il modulo Controllo dispositivo controlla l'accesso a vari dispositivi periferici, che siano utilizzati direttamente sui computer protetti o che reindirizzati verso gli ambienti di virtualizzazione ospitati sui computer protetti. È in grado di riconoscere dispositivi reindirizzati verso Microsoft Remote Desktop Server, Citrix XenDesktop/XenApp/XenServer e VMware Horizon. Può inoltre controllare le operazioni di copia dei dati tra gli appunti del sistema operativo guest eseguito su VMware Workstation, VMware Player, Oracle VM VirtualBox o Windows Virtual PC, e gli appunti del sistema operativo host eseguito sul computer protetto.

Il modulo Controllo dispositivo può proteggere i computer che eseguono i sistemi operativi seguenti:

Controllo dispositivo

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

Nota
L'Agente per la Prevenzione della perdita di dati per macOS supporta solo processori x64. I processori Apple Silicon ARM non sono supportati.

Prevenzione della perdita di dati

- Microsoft Windows 7 Service Pack 1 e versioni successive
- Microsoft Windows Server 2008 R2 e versioni successive

Nota
L'Agente per la Prevenzione della perdita di dati potrebbe essere installato su sistemi macOS non supportati in quanto parte integrante dell'Agente per Mac. In questo caso, la console di Cyber Protect mostra che l'Agente per la Prevenzione della perdita di dati è installato nel sistema, ma la funzionalità di controllo del dispositivo e di prevenzione della perdita dei dati è disattivata. Controllo dispositivo funziona infatti solo sui sistemi macOS supportati dall'Agente per la Prevenzione della perdita di dati.

Limitazione all'uso dell'Agente per la Prevenzione della perdita di dati con Hyper-V

Non installare l'Agente per la Prevenzione della perdita di dati su host Hyper-V in cluster Hyper-V, in quanto potrebbe causare schermate blu, soprattutto nei cluster Hyper-V con volumi condivisi del cluster (CSV).

© Acronis International GmbH, 2003-2024

Se si utilizza una qualsiasi delle seguenti versioni di Agente per Hyper-V, è necessario rimuovere manualmente l'Agente per la Prevenzione della perdita di dati:

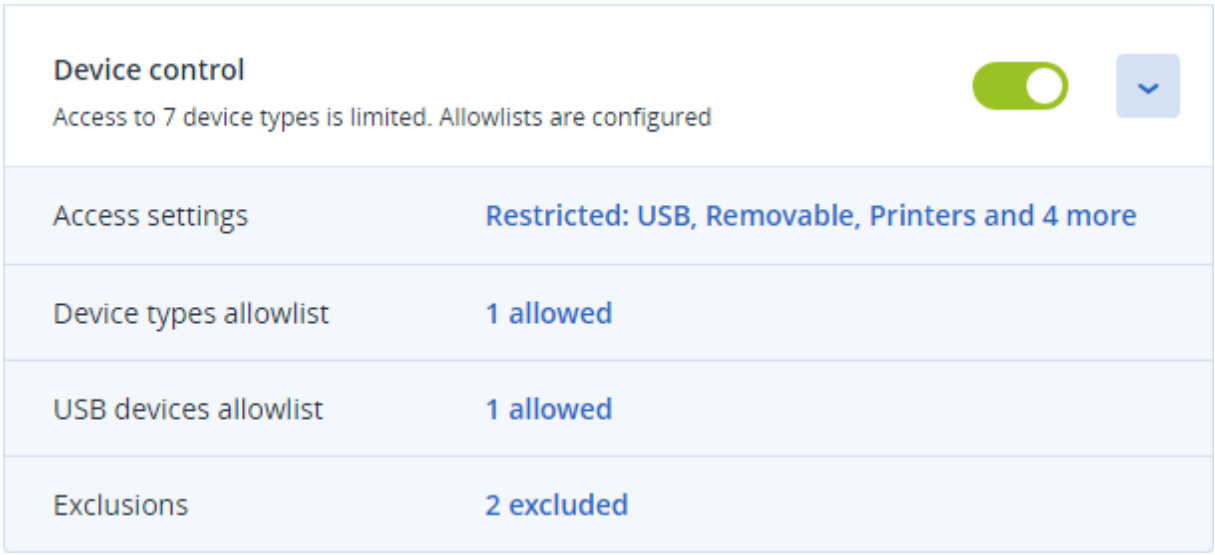
- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

Per rimuovere l'Agente per la Prevenzione della perdita di dati, nell'host Hyper-V eseguire manualmente il programma di installazione e deselezionare la casella di controllo dell'Agente da rimuovere o eseguire il comando seguente:

```
<installer_name> --remove-components=agentForDlp -quiet
```

È possibile abilitare e configurare il modulo per il controllo dei dispositivi nella sezione **Controllo dispositivo** del piano di protezione nella console di Cyber Protect. Per istruzioni, vedere i passaggi per abilitare o disabilitare il modulo Controllo dispositivo.

Nella sezione **Controllo dispositivo** viene visualizzato un riepilogo della configurazione del modulo:



- Impostazioni di accesso - Mostra un riepilogo dei tipi di dispositivo e delle porte con accesso limitato (non consentito o di sola lettura), se presenti. Altrimenti, indica che ogni tipo di dispositivo è consentito. Fare clic sul riepilogo per visualizzare o modificare le impostazioni di accesso (vedere i passaggi per visualizzare o modificare le impostazioni di accesso).
- Lista di tipi di dispositivi consentiti - Mostra quante sottoclassi di dispositivi sono consentite, escludendole dal controllo dell'accesso ai dispositivi, se presente. Altrimenti, indica che la lista di elementi consentiti è vuota. Fare clic sul riepilogo per visualizzare o modificare la selezione di sottoclassi di dispositivi consentiti (vedere i passaggi per escludere le sottoclassi di dispositivi dal controllo dell'accesso).

© Acronis International GmbH, 2003-2024

- Lista di dispositivi USB consentiti - Mostra quanti dispositivi/modelli di USB sono consentiti, escludendoli dal controllo dell'accesso ai dispositivi, se presente. Altrimenti, indica che la lista di elementi consentiti è vuota. Fare clic sul riepilogo per visualizzare o modificare la lista di dispositivi/modelli USB consentiti (vedere i passaggi per escludere i singoli dispositivi USB dal controllo dell'accesso).
- Esclusioni - Mostra quante esclusioni dal controllo dell'accesso sono state impostate per appunti Windows, acquisizioni di screenshot, stampanti e dispositivi mobili.

Utilizzo del modulo Controllo dispositivo

Questa sezione contiene istruzioni dettagliate per le attività di base concernenti l'utilizzo del modulo Controllo dispositivo.

Abilitare o disabilitare il controllo dispositivo

È possibile abilitare il controllo dispositivo durante la creazione di un piano di protezione. Un piano di protezione esistente può essere modificato per abilitare o disabilitare il controllo dispositivo.

Per abilitare o disabilitare il controllo dispositivo

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Eseguire una delle seguenti operazioni per aprire il riquadro del piano di protezione:
   - Se si desidera creare un nuovo piano di protezione, selezionare un sistema da proteggere, fare clic su **Proteggi**, quindi su **Crea piano**.
   - Se si desidera modificare un piano di protezione esistente, selezionare un sistema protetto, fare clic su **Proteggi**, fare clic sui puntini di sospensione (...) accanto al nome del piano di protezione, quindi su **Modifica**.
3. Nel riquadro del piano di protezione, passare alla sezione **Controllo dispositivo** e attivare o disattivare l'opzione **Controllo dispositivo**.
4. Eseguire una delle seguenti operazioni per applicare le modifiche:
   - Se si sta creando un piano di protezione, fare clic su **Crea**.
   - Se si sta modificando un piano di protezione, fare clic su **Salva**.

È inoltre possibile accedere al riquadro del piano di protezione dalla scheda Gestione. Questa funzionalità non è disponibile in tutte le edizioni del servizio Cyber Protection.

Abilitazione dell'utilizzo del modulo Controllo dispositivo su macOS

Le impostazioni di Controllo dispositivo di un piano di protezione diventano effettive solo dopo aver caricato il driver di controllo del dispositivo nel workload protetto. Questa sezione descrive come caricare il driver di controllo del dispositivo per abilitare l'utilizzo del modulo Controllo dispositivo su macOS. Questa operazione viene eseguita una sola volta e richiede privilegi di amministratore sul sistema endpoint.

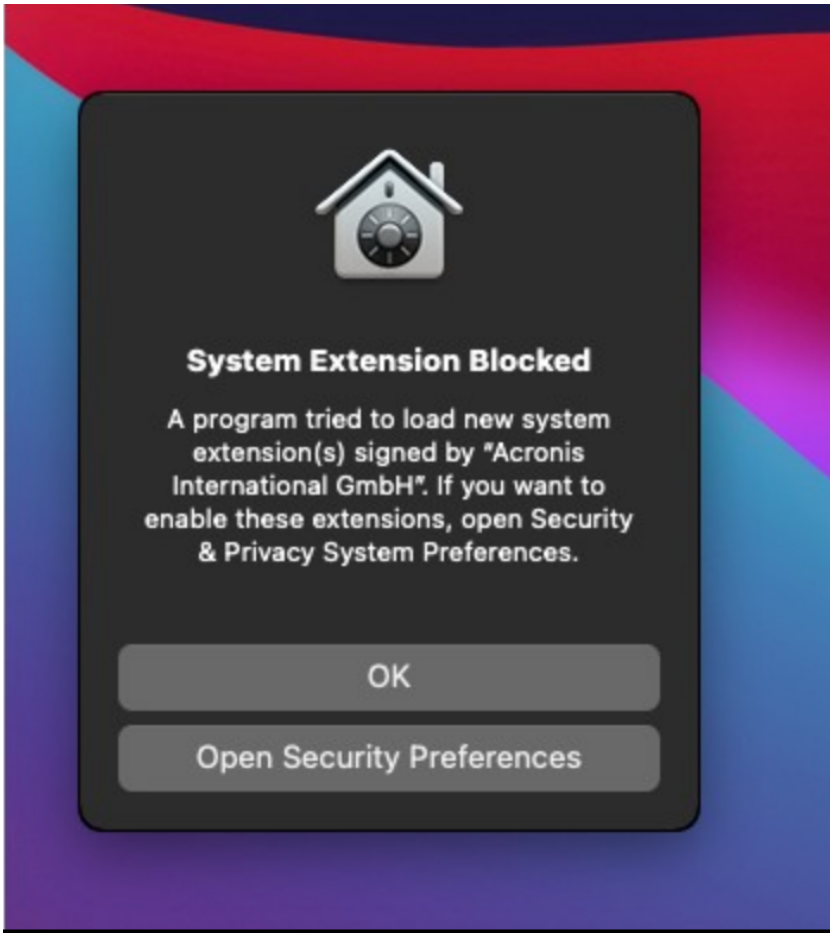
Versioni di macOS supportate:

© Acronis International GmbH, 2003-2024

- macOS 10.15 (Catalina) e versioni successive
- macOS 11.2.3 (Big Sur) e versioni successive
- macOS 12.2 (Monterey) e versioni successive
- macOS 13.2 (Ventura) e versioni successive

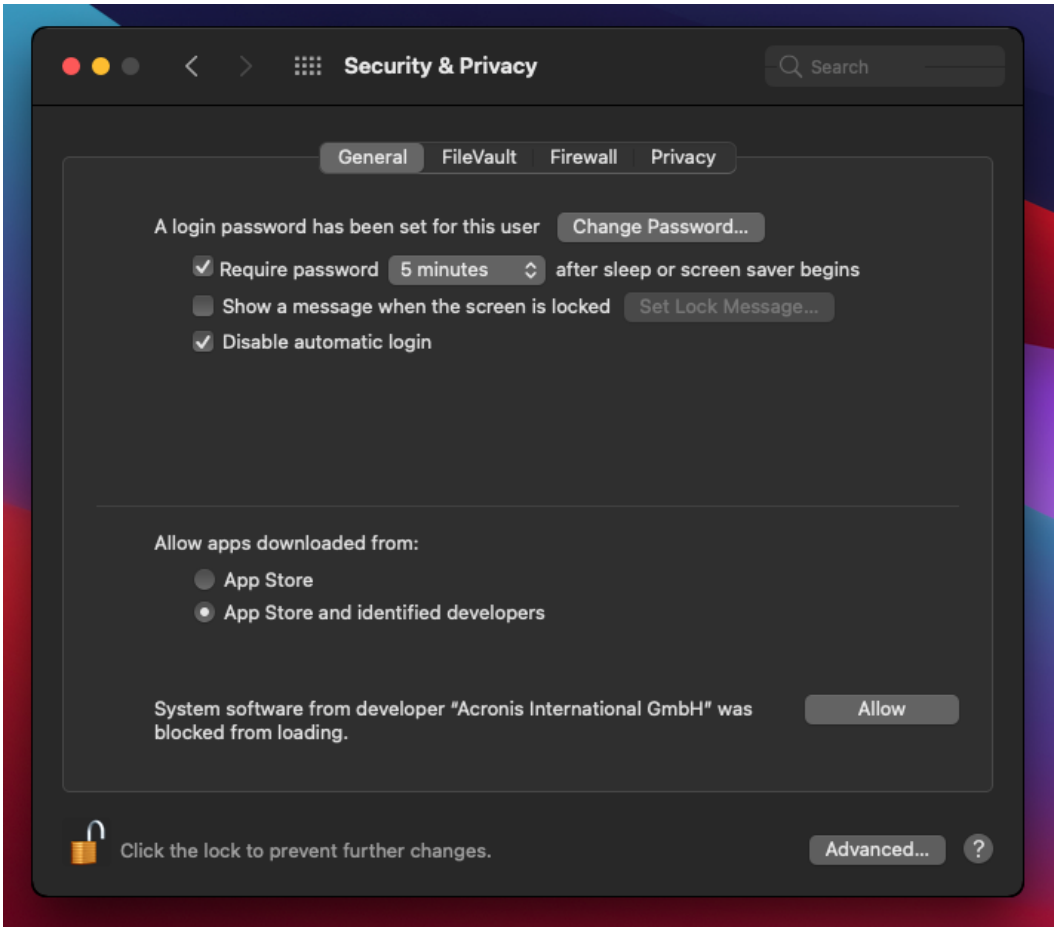
Per abilitare l'utilizzo del modulo Controllo dispositivo su macOS

1. Installare l'Agente per Mac sul sistema da proteggere.
2. Abilitare le impostazioni di controllo del dispositivo nel piano di protezione.
3. Applicare il piano di protezione.
4. Nel workload protetto viene visualizzato l'avviso di blocco dell'estensione di sistema. Aprire le **preferenze di sistema** relative alla sicurezza.



© Acronis International GmbH, 2003-2024

5. Nel riquadro **Sicurezza e Privacy** visualizzato, selezionare **App Store e sviluppatori identificati** e quindi fare clic su **Consenti**.



6. Nella finestra di dialogo visualizzata, fare clic su **Riavvia** per riavviare il workload e attivare le impostazioni di controllo del dispositivo.

Nota
Non è necessario ripetere questi passaggi se l'impostazione di controllo del dispositivo viene disabilitata e quindi abilitata di nuovo.

Visualizzare o modificare le impostazioni di accesso

Nel riquadro del piano di protezione, è possibile gestire le impostazioni di accesso per il modulo Controllo dispositivo. In questo modo è possibile consentire o negare l'accesso a dispositivi di determinati tipi, nonché abilitare o disabilitare le notifiche e gli avvisi.

Per visualizzare o modificare le impostazioni di accesso

1. Aprire il riquadro di un piano di protezione e abilitare il controllo dispositivo in tale piano (vedere i passaggi per abilitare o disabilitare il controllo dispositivo).
2. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare clic sul link accanto alle **Impostazioni di accesso**.

© Acronis International GmbH, 2003-2024

3. Nella pagina per la gestione delle impostazioni di accesso visualizzata, visualizzare o modificare le impostazioni di accesso come necessario.

Nota
Le impostazioni di accesso configurate in Controllo dispositivo potrebbero essere sovrascritte quando si utilizzano sia Controllo dispositivo che Advanced DLP per proteggere un workload. Consultare "Abilitazione di Advanced Data Loss Prevention nei piani di protezione" (pag. 896).

Abilitare o disabilitare le notifiche e gli avvisi di servizio del sistema operativo

Quando si gestiscono le impostazioni di accesso, è possibile abilitare o disabilitare le notifiche e gli avvisi di servizio del sistema operativo che segnalano i tentativi degli utenti di eseguire azioni non consentite.

Per abilitare o disabilitare le notifiche del sistema operativo

1. Seguire i passaggi per visualizzare o modificare le impostazioni di accesso.
2. Nella pagina per la gestione delle impostazioni di accesso, selezionare o deselezionare la casella di controllo **Mostra agli utenti finali una notifica del SO se tentano di utilizzare un tipo di dispositivo o porta bloccato**.

Per abilitare o disabilitare gli avvisi del servizio

1. Seguire i passaggi per visualizzare o modificare le impostazioni di accesso.
2. Nella pagina per la gestione delle impostazioni di accesso, selezionare o deselezionare la casella di controllo **Mostra avviso** del tipo di dispositivo desiderato.

La casella di controllo **Mostra avviso** è disponibile solo per i tipi di dispositivo con accesso limitato (di sola lettura o accesso negato), ad eccezione dell'acquisizione di screenshot.

Escludere sottoclassi di dispositivo dal controllo dell'accesso

Nel riquadro del piano di protezione, è possibile scegliere le sottoclassi di dispositivo da escludere dal controllo dell'accesso. Di conseguenza, l'accesso a tali dispositivi è consentito indipendentemente dalle impostazioni di accesso del modulo Controllo dispositivo.

Per escludere sottoclassi di dispositivo dal controllo dell'accesso

1. Aprire il riquadro di un piano di protezione e abilitare il controllo dispositivo in tale piano (vedere i passaggi per abilitare o disabilitare il controllo dispositivo).
2. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare clic sul link accanto alla **Lista di tipi di dispositivo consentiti**.
3. Nella pagina per la gestione delle liste di elementi consentiti visualizzata, visualizzare o modificare la selezione di sottoclassi di dispositivo da escludere dal controllo dell'accesso.

© Acronis International GmbH, 2003-2024

Escludere i singoli dispositivi USB dal controllo dell'accesso

Nel riquadro del piano di protezione, è possibile specificare singoli dispositivi USB o modelli di dispositivo USB da escludere dal controllo dell'accesso. Di conseguenza, l'accesso a tali dispositivi è consentito indipendentemente dalle impostazioni di accesso del modulo Controllo dispositivo.

Per escludere un dispositivo USB dal controllo dell'accesso

1. Aprire il riquadro di un piano di protezione e abilitare il controllo dispositivo in tale piano (vedere i passaggi per abilitare o disabilitare il controllo dispositivo).
2. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare clic sul link accanto alla **Lista di dispositivi USB consentiti**.
3. Nella pagina per la gestione delle liste di elementi consentiti visualizzata, fare clic su **Aggiungi dal database**.
4. Nella pagina per la selezione dei dispositivi USB visualizzata, selezionare il dispositivo desiderato tra quelli registrati nel Database dei dispositivi USB.
5. Fare clic sul pulsante **Aggiungi alla lista di elementi consentiti**.

Per bloccare l'esclusione di un dispositivo USB dal controllo dell'accesso

1. Aprire il riquadro di un piano di protezione e abilitare il controllo dispositivo in tale piano (vedere i passaggi per abilitare o disabilitare il controllo dispositivo).
2. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare clic sul link accanto alla **Lista di dispositivi USB consentiti**.
3. Nella pagina per la gestione delle liste di elementi consentiti visualizzata, fare clic sull'icona di eliminazione al termine dell'elemento che rappresenta il dispositivo USB desiderato.

Aggiungere o rimuovere i dispositivi USB dal database

Per escludere uno specifico dispositivo USB dal controllo dell'accesso, è necessario aggiungerlo al database dei dispositivi USB. Quindi sarà possibile aggiungere i dispositivi alla lista selezionandoli da tale database.

Le procedure seguenti sono valide per i piani di protezione nei quali è abilitata la funzionalità di controllo del dispositivo.

Per aggiungere i dispositivi USB al database

1. Aprire il piano di protezione di un dispositivo per la modifica:
   Fare clic sull'icona dei puntini di sospensione (...) accanto al nome del piano di protezione, quindi selezionare **Modifica**.

   Nota
   Nel piano deve essere abilitata la funzionalità di controllo del dispositivo per poter accedere alle impostazioni di Controllo dispositivo.

© Acronis International GmbH, 2003-2024

2. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare clic sul link accanto alla **Lista di dispositivi USB consentiti**.
3. Nella pagina della **Lista di dispositivi USB consentiti** visualizzata, fare clic su **Aggiungi dal database**.
4. Nella pagina di gestione del database dei dispositivi USB visualizzata, fare clic su **Aggiungi al database**.
5. Nella finestra di dialogo **Aggiungi dispositivo USB** visualizzata, selezionare il sistema al quale è connesso il dispositivo USB.
   Nell'elenco dei computer vengono mostrati solo i sistemi che sono online.
   L'elenco dei dispositivi USB viene visualizzato solo per i sistemi sui quali è installato l'agente per la prevenzione della perdita di dati.
   I dispositivi USB sono elencati nella visualizzazione ad albero. Il primo livello della visualizzazione rappresenta un modello di dispositivo. Il secondo livello rappresenta un dispositivo specifico di quel modello.
   Un'icona blu accanto alla descrizione del dispositivo indica che tale dispositivo è attualmente connesso al computer. Se il dispositivo non è connesso al computer, l'icona è inattiva (in grigio).
6. Selezionare le caselle di controllo dei dispositivi USB da aggiungere al database, quindi fare clic su **Aggiungi a database**.
   I dispositivi USB selezionati vengono aggiunti al data base.
7. Chiudere o salvare il piano di protezione.

Per aggiungere i dispositivi USB al database dal riquadro dei dettagli del computer

Nota
Questa procedura è valida solo per i dispositivi online sui quali è installato l'agente per la prevenzione della perdita di dati. Non è possibile visualizzare l'elenco dei dispositivi USB di un computer offline o nei quali non è installato l'agente per la prevenzione della perdita di dati.

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare un computer al quale non sia mai stato connesso il dispositivo USB desiderato, e nel menu a destra, fare clic su **Inventario**.
   Viene visualizzato il riquadro dei dettagli del computer.
3. Nel riquadro dei dettagli del computer, fare clic sulla scheda **Dispositivi USB**.
   Viene visualizzato l'elenco dei dispositivi USB noti presenti nel computer selezionato.
   I dispositivi USB sono elencati nella visualizzazione ad albero. Il primo livello della visualizzazione rappresenta un modello di dispositivo. Il secondo livello rappresenta un dispositivo specifico di quel modello.
   Un'icona blu accanto alla descrizione del dispositivo indica che tale dispositivo è attualmente connesso al computer. Se il dispositivo non è connesso al computer, l'icona è inattiva (in grigio).
4. Selezionare le caselle di controllo dei dispositivi USB da aggiungere al database, quindi fare clic su **Aggiungi a database**.

Per aggiungere i dispositivi USB al database dagli avvisi del servizio

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Monitoraggio** > **Avvisi**.
2. Individuare un avviso del controllo dispositivo che informa che è stato negato l'accesso al dispositivo USB.
3. Nella visualizzazione semplice dell'avviso, fare clic su **Consenti questo dispositivo USB**.
   In questo modo lo specifico dispositivo USB viene escluso dal controllo dell'accesso, e aggiunto al database per riferimento futuro.

Per aggiungere i dispositivi USB al database importando un elenco di dispositivi

È possibile importare nel database un file JSON con un elenco di dispositivi USB. Vedere "Importare un elenco di dispositivi USB nel database" (pag. 391).

Per eliminare i dispositivi USB dal database

1. Aprire il piano di protezione di un dispositivo per la modifica:
   Fare clic sull'icona dei puntini di sospensione (...) accanto al nome del piano di protezione, quindi selezionare **Modifica**.

   Nota
   Nel piano deve essere abilitata la funzionalità di controllo del dispositivo per poter accedere alle impostazioni di Controllo dispositivo.

2. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare sulla riga **Lista di dispositivi USB consentiti**.
3. Nella pagina per la gestione delle liste di elementi consentiti visualizzata, fare clic su **Aggiungi dal database**.
4. Nella pagina per la selezione dei dispositivi USB dal database, fare clic sui puntini di sospensione (...) alla fine dell'elemento della lista che rappresenta il dispositivo, fare clic su **Elimina** e confermare l'eliminazione.
   I dispositivi USB vengono eliminati dal database.
5. Chiudere o salvare il piano di protezione.

Visualizzare gli avvisi di Controllo dispositivo

È possibile configurare il modulo Controllo dispositivo affinché invii avvisi che informano sui tentativi utente non consentiti di utilizzare determinati tipi di dispositivo (vedere Abilitare o disabilitare le notifiche e gli avvisi di servizio del sistema operativo). Utilizzare i passaggi seguenti per visualizzare tali avvisi.

Per visualizzare gli avvisi di Controllo dispositivo

1. Nella console di Cyber Protect, passare a **Monitoraggio** > **Avvisi**.
2. Individuare gli avvisi con lo stato seguente:"L'accesso al dispositivo generico è bloccato".

Vedere Avvisi di Controllo dispositivo per ulteriori informazioni.

© Acronis International GmbH, 2003-2024

Impostazioni di accesso

Nella pagina **Impostazioni di accesso**, è possibile consentire o negare l'accesso a dispositivi di determinati tipi, nonché abilitare o disabilitare le notifiche del sistema operativo e gli avvisi di controllo dispositivo.

Nota
Le impostazioni di accesso configurate in Controllo dispositivo potrebbero essere sovrascritte quando si utilizzano sia Controllo dispositivo che Advanced DLP per proteggere un workload. Consultare "Abilitazione di Advanced Data Loss Prevention nei piani di protezione" (pag. 896).

Le impostazioni di accesso consentono di limitare l'accesso degli utenti ai seguenti tipi di dispositivi e porte:

- **Rimovibile** (controllo dell'accesso per tipo di dispositivo) - Dispositivi con qualsiasi interfaccia per la connessione a un computer (USB, FireWire, PCMCIA, IDE, SATA, SCSI, ecc.) che vengono riconosciuti dal sistema operativo come dispositivi di archiviazione rimovibili (ad esempio, pennette USB, lettori di schede, unità magneto-ottiche, ecc.). Il controllo dispositivo classifica tutti i dischi rigidi connessi tramite USB, FireWire e PMCIA come dispositivi rimovibili. Inoltre, classifica alcuni tipi di dischi rigidi (in genere con SATA e SCSI) come dispositivi rimovibili se questi supportano la funzionalità hot-plug e se non presentano un sistema operativo installato.

  È possibile consentire l'accesso completo, l'accesso di sola lettura, o negare l'accesso ai dispositivi rimovibili per controllare le operazioni di copia di dati da/verso qualsiasi dispositivo rimovibile su un computer protetto. I diritti di accesso non interessano i dispositivi crittografati con BitLocker o FileVault (solo file system HFS+).

  Questo tipo di dispositivo è supportato su Windows e su macOS.
- **Rimovibile crittografato** (controllo dell'accesso per tipo di dispositivo) - Dispositivi rimovibili crittografati con crittografia dell'unità BitLocker (su Windows) o FileVault (su macOS).

  macOS supporta soltanto unità rimovibili crittografate utilizzando il file system HFS+ (anche noto come HFS Plus o Mac OS Extended o HFS Extended). Le unità rimovibili crittografate mediante il file system APFS file sono considerate unità rimovibili.

  È possibile consentire l'accesso completo, l'accesso di sola lettura, o negare l'accesso ai dispositivi rimovibili crittografati per controllare le operazioni di copia di dati da/verso qualsiasi dispositivo rimovibile crittografato su un computer protetto. I diritti di accesso interessano solo i dispositivi crittografati con BitLocker o FileVault (solo file system HFS+).

  Questo tipo di dispositivo è supportato su Windows e su macOS.
- **Stampanti** (controllo dell'accesso per tipo di dispositivo) - Stampanti fisiche con qualsiasi tipo di interfaccia per la connessione a un computer (USB, LPT, Bluetooth, ecc.), nonché le stampanti a cui accede un computer sulla rete.

  È possibile consentire o negare l'accesso alle stampanti per controllare la stampa di documenti su qualsiasi stampante di un computer protetto.

© Acronis International GmbH, 2003-2024

Nota
Quando l'impostazione di accesso per le stampanti viene modificata in **Nega**, le applicazioni e i processi che accedono alle stampanti devono essere riavviati per applicare le impostazioni di accesso appena configurate. Per garantire che le impostazioni di accesso vengano applicate correttamente, riavviare i workload protetti.

Questo tipo di dispositivo è supportato solo su Windows.

- **Appunti** (controllo dell'accesso per tipo di dispositivo) - Appunti di Windows.
  È possibile consentire o negare l'accesso agli appunti per controllare le operazioni di copia/incolla di tramite gli appunti di Windows su un computer protetto.

Nota
Quando l'impostazione di accesso per gli appunti viene modificata in **Nega**, le applicazioni e i processi che accedono agli appunti devono essere riavviati per applicare le impostazioni di accesso appena configurate. Per garantire che le impostazioni di accesso vengano applicate correttamente, riavviare i workload protetti.

Questo tipo di dispositivo è supportato solo su Windows.

- **Acquisizione di screenshot** (controllo dell'acceso per tipo di dispositivo) - Abilita l'acquisizione di screenshot dell'intera schermata, della finestra attiva o di un'area selezionata dello schermo.
  È possibile consentire o negare l'accesso all'acquisizione di screenshot per controllare tale operazione su un computer protetto.

Nota
Quando l'impostazione di accesso per l'acquisizione di screenshot viene modificata in **Nega**, le applicazioni e i processi che accedono all'acquisizione di screenshot devono essere riavviati per applicare le impostazioni di accesso appena configurate. Per garantire che le impostazioni di accesso vengano applicate correttamente, riavviare i workload protetti.

Questo tipo di dispositivo è supportato solo su Windows.

- **Dispositivi mobili** (controllo dell'accesso per tipo di dispositivo) - Dispositivi (come gli smartphone Android, ecc.) che comunicano con un computer tramite Media Transfer Protocol (MTP), con qualsiasi interfaccia utilizzata per la connessione a un computer (USB, IP, Bluetooth).
  È possibile consentire l'accesso completo, l'accesso di sola lettura, o negare l'accesso ai dispositivi mobili per controllare le operazioni di copia di dati da/verso qualsiasi dispositivo mobile MTP su un computer protetto.

Nota
Quando l'impostazione di accesso per i dispositivi mobili viene modificata in **Sola lettura** o in **Nega**, le applicazioni e i processi che accedono ai dispositivi mobili devono essere riavviati per applicare le impostazioni di accesso appena configurate. Per garantire che le impostazioni di accesso vengano applicate correttamente, riavviare i workload protetti.

© Acronis International GmbH, 2003-2024

Questo tipo di dispositivo è supportato solo su Windows.

- **Bluetooth** (controllo dell'accesso per tipo di dispositivo) - Dispositivi Bluetooth interni ed esterni con qualsiasi interfaccia per la connessione a un computer (USB, PCMCIA, ecc.). Questa impostazione controlla l'utilizzo di dispositivi di questo tipo e non lo scambio di dati che avviene tramite tali dispositivi.

  È possibile consentire o negare l'accesso al Bluetooth per controllare l'utilizzo di qualsiasi dispositivo Bluetooth su un computer protetto.

  Nota
  Su macOS, i diritti di accesso al Bluetooth non interessano i dispositivi Bluetooth HID. L'accesso a questi dispositivi è sempre consentito per evitare che i dispositivi HID wireless (mouse e tastiere) siano disabilitati su hardware iMac e Mac Pro.

  Questo tipo di dispositivo è supportato su Windows e su macOS.
- **Unità ottiche** (controllo dell'accesso per tipo di dispositivo) - Unità CD/DVD/BD interne ed esterne (incluse unità di scrittura) con qualsiasi interfaccia per la connessione a un computer (IDE, SATA, USB, FireWire, PCMCIA, ecc.).

  È possibile consentire l'accesso completo, l'accesso di sola lettura, o negare l'accesso alle unità ottiche per controllare le operazioni di copia di dati da/verso qualsiasi unità ottica su un computer protetto.

  Questo tipo di dispositivo è supportato su Windows e su macOS.
- **Unità floppy** (controllo dell'accesso per tipo di dispositivo) - Unità floppy interne ed esterne con qualsiasi interfaccia per la connessione a un computer (IDE, SATA, USB, PCMCIA, ecc.). Alcuni modelli di unità floppy vengono riconosciuti dal sistema operativo come unità rimovibili; in questo caso anche il controllo del dispositivo identifica queste unità come dispositivi rimovibili.

  È possibile consentire l'accesso completo, l'accesso di sola lettura, o negare l'accesso alle unità floppy per controllare le operazioni di copia di dati da/verso qualsiasi unità floppy su un computer protetto.

  Questo tipo di dispositivo è supportato solo su Windows.
- **USB** (controllo dell'accesso per tipo di interfaccia) - Qualsiasi dispositivo connesso a una porta USB, ad eccezione degli hub.

  È possibile consentire l'accesso completo, l'accesso di sola lettura, o negare l'accesso alle porte USB per controllare le operazioni di copia di dati da/verso qualsiasi dispositivo connesso a una porta USB su un computer protetto.

  Questo tipo di dispositivo è supportato su Windows e su macOS.
- **FireWire** (controllo dell'accesso per interfaccia del dispositivo) - Qualsiasi dispositivo connesso a una porta FireWire (IEEE 1394), ad eccezione degli hub.

  È possibile consentire l'accesso completo, l'accesso di sola lettura, o negare l'accesso alle porte FireWire per controllare le operazioni di copia di dati da/verso qualsiasi dispositivo connesso a una porta FireWire su un computer protetto.

  Questo tipo di dispositivo è supportato su Windows e su macOS.

© Acronis International GmbH, 2003-2024

- **Dispositivi reindirizzati** (controllo dell'accesso per interfaccia del dispositivo) - Unità mappate (unità disco rigido, rimovibili e ottiche), dispositivi USB e appunti reindirizzati ad applicazioni virtuali/sessioni desktop.

  Il controllo dispositivo riconosce i dispositivi reindirizzati tramite i protocolli remoti Microsoft RDP, Citrix ICA, VMware PCoIP e HTML5/WebSockets negli ambienti di virtualizzazione Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer e VMware Horizon ospitati su computer Windows protetti. Può inoltre controllare le operazioni di copia dei dati tra gli appunti di Windows del sistema operativo guest eseguito su VMware Workstation, VMware Player, Oracle VM VirtualBox, o Windows Virtual PC, e gli appunti del sistema operativo host eseguito su un computer Windows protetto.

  Questo tipo di dispositivo è supportato solo su Windows.

  È possibile configurare l'accesso ai dispositivi reindirizzati come indicato di seguito:

  - **Unità mappate** - Consente l'accesso completo, l'accesso di sola lettura, o nega l'accesso per controllare le operazioni di copia di dati da/verso qualsiasi disco rigido, unità rimovibile o unità ottica reindirizzati alla sessione ospitata su un computer protetto.
  - **Appunti in entrata** - Consente o nega l'accesso per controllare le operazioni di copia di dati tramite gli appunti verso la sessione ospitata su un computer protetto.

    Nota
    Quando l'impostazione di accesso per gli appunti in entrata viene modificata in **Nega**, le applicazioni e i processi che accedono agli appunti devono essere riavviati per applicare le impostazioni di accesso appena configurate. Per garantire che le impostazioni di accesso vengano applicate correttamente, riavviare i workload protetti.

  - **Appunti in uscita** - Consente o nega l'accesso per controllare le operazioni di copia di dati tramite gli appunti dalla sessione ospitata su un computer protetto.

    Nota
    Quando l'impostazione di accesso per gli appunti in uscita viene modificata in **Nega**, le applicazioni e i processi che accedono agli appunti devono essere riavviati per applicare le impostazioni di accesso appena configurate. Per garantire che le impostazioni di accesso vengano applicate correttamente, riavviare i workload protetti.

  - **Porte USB** - Consente o nega l'accesso per controllare le operazioni di copia di dati da/verso dispositivi connessi a qualsiasi porta USB reindirizzata verso la sessione ospitata su un computer protetto.

Le impostazioni di Controllo dispositivo hanno lo stesso effetto su tutti gli utenti. Se, ad esempio, si nega l'accesso ai dispositivi rimovibili, si impedisce a qualsiasi utente di copiare dati da/verso tali dispositivo su un computer protetto. È possibile consentire selettivamente l'accesso a singoli dispositivi USB escludendo questi ultimi dal controllo dell'accesso (vedere Lista di tipi di dispositivo consentiti e Lista di dispositivi USB consentiti).

Quando si accede a un dispositivo controllato sia in base al tipo che in base all'interfaccia, l'impostazione di accesso al dispositivo in base a livello di interfaccia ha priorità. Se, ad esempio,

© Acronis International GmbH, 2003-2024

l'accesso alle porte USB non è consentito (interfaccia del dispositivo), non sarà consentito neanche l'accesso ai dispositivi mobili connessi a una porta USB, indipendentemente dal fatto che l'accesso ai dispositivi mobili sia negato o consentito (tipo di dispositivo). Per consentire l'accesso a tale dispositivo, è necessario consentire sia l'interfaccia sia il tipo.

Nota
Se il piano di protezione utilizzato su macOS contiene impostazioni per tipi di dispositivi supportati solo su Windows, tali impostazioni verranno ignorate su macOS.

Importante
Quando un dispositivo rimovibile, un dispositivo rimovibile crittografato, una stampante o un dispositivo Bluetooth sono connessi a una porta USB, l'autorizzazione all'accesso a tale dispositivo sovrascrive la negazione all'accesso impostata a livello di interfaccia USB. Se si autorizza tale tipo di dispositivo, l'accesso ad esso è consentito indipendentemente dal fatto che l'accesso alla porta USB sia negato.

Notifiche e avvisi di servizio del sistema operativo

È possibile configurare la funzionalità Controllo dispositivo affinché visualizzi le notifiche del sistema operativo agli utenti finali se questi tentano di utilizzare un tipo di dispositivo bloccato su computer protetti. Se, nell'impostazione di accesso, è selezionata la casella di controllo **Mostra agli utenti finali una notifica del SO se tentano di utilizzare un tipo di dispositivo o porta bloccato**, l'agente visualizza un messaggio a comparsa nell'area di notifica del computer protetto se si verifica uno dei seguenti eventi:

- Un tentativo negato di utilizzare un dispositivo su una porta USB o FireWire. Questa notifica viene visualizzata ogni volta che l'utente inserisce un dispositivo USB o FireWire che non è autorizzato a livello di interfaccia (ad esempio, quando non è autorizzato l'accesso alla porta USB) o a livello di tipo (ad esempio, quando non è autorizzato l'utilizzo di dispositivi rimovibili).La notifica segnala che all'utente non è consentito l'accesso al dispositivo/unità specificato.
- Un tentativo negato di copiare un oggetto dati (ad esempio un file) da un determinato dispositivo. Questa notifica viene visualizzata quando il sistema operativo non concede l'accesso in lettura ai seguenti dispositivi: unità floppy, unità ottiche, dispositivi rimovibili, dispositivi rimovibili crittografati, dispositivi mobili, unità mappate reindirizzate e dati in entrata reindirizzati dagli appunti. La notifica segnala che all'utente non è consentito ottenere l'oggetto dati specificato dal dispositivo specificato.

  La notifica di operazione in lettura non consentita viene visualizzata anche quando viene negato l'accesso in lettura/scrittura a funzionalità Bluetooth, porta FireWire, porta USB e porta USB reindirizzata.
- Un tentativo negato di copiare un oggetto dati (ad esempio un file) in un determinato dispositivo. Questa notifica viene visualizzata quando il sistema operativo non concede l'accesso in scrittura ai seguenti dispositivi: unità floppy, unità ottica, dispositivi rimovibili, dispositivi rimovibili crittografati, dispositivi mobili, appunti locali, acquisizioni di screenshot, stampanti, unità

© Acronis International GmbH, 2003-2024

mappate reindirizzate e dati in uscita reindirizzati dagli appunti. La notifica segnala che all'utente non è consentito inviare l'oggetto dati specificato al dispositivo specificato.

I tentativi degli utenti di accedere a tipi di dispositivo bloccati su computer protetti può generare avvisi che vengono registrati nella console di Cyber Protect. È possibile abilitare avvisi distinti per ogni tipo di dispositivo (escluse le acquisizioni di screenshot) o porta, selezionando la casella di controllo **Mostra avviso** nelle impostazioni di accesso. Se, ad esempio, l'accesso ai dispositivi rimovibili è limitato alla sola lettura, e se la casella di controllo **Mostra avviso** è selezionata per quel tipo di dispositivo, viene registrato un avviso ogni volta che un utente su un computer protetto tenta di copiare dati su un dispositivo rimovibile. Vedere Avvisi di Controllo dispositivo per ulteriori informazioni.

Vedere anche i passaggi per abilitare o disabilitare le notifiche e gli avvisi di servizio del sistema operativo.

Lista di tipi di dispositivo consentiti

Nella pagina **Lista di tipi di dispositivo consentiti**, è possibile scegliere le sottoclassi di dispositivo da escludere dal controllo dell'accesso ai dispositivi. Di conseguenza, l'accesso a tali dispositivi è consentito indipendentemente dalle impostazioni di accesso del modulo Controllo dispositivo.

Questa opzione è fornita per consentire l'accesso a dispositivi di determinati sottoclassi incluse in un tipo di dispositivo non consentito. L'opzione consente di negare l'accesso a tutti i dispositivi di un determinato tipo, ad esclusione di alcune sottoclassi di dispositivi di questo tipo. Può essere utile, ad esempio, quando è necessario negare l'accesso a tutte le porte USB consentendo al contempo l'utilizzo di una tastiera e di un mouse USB.

Durante la configurazione del modulo Controllo dispositivo, è possibile specificare quali sottoclassi di dispositivo escludere dal controllo dell'accesso ai dispositivi. Se un dispositivo appartiene a una sottoclasse esclusa, l'accesso a tale dispositivo è consentito indipendentemente dal fatto che il tipo di dispositivo o porta sia o meno consentito. È possibile escludere selettivamente le seguenti sottoclassi di dispositivo dal controllo dell'accesso ai dispositivi:

- **HID USB (mouse, tastiera, ecc.)** - Quando selezionata, questa opzione consente l'accesso a dispositivi HID (Human Interface Devices) come mouse, tastiera e così via, connessi a una porta USB anche se le porte USB sono negate. Per impostazione, questa voce è selezionata in modo che la negazione dell'accesso alla porta USB non disabili della tastiera o il mouse.
  Supportato su Windows e macOS.
- **Schede di rete USB e FireWire** - Quando selezionata, questa opzione consente l'accesso alle schede di rete connesse a una porta USB o FireWire (IEEE 1394), anche se le porte USB e/o FireWire sono negate.
  Supportato su Windows e macOS.
- **Scanner e dispositivi di acquisizione fermo immagine USB** - Quando selezionata, questa opzione consente l'accesso a scanner e dispositivi di acquisizione fermo immagine USB connessi a una porta USB anche se le porte USB sono negate.
  Supportato solo su Windows.

© Acronis International GmbH, 2003-2024

- **Dispositivi audio USB** - Quando selezionata, questa opzione consente l'accesso a dispositivi audio come cuffie e microfoni connessi a una porta USB anche se le porte USB sono negate.
  Supportato solo su Windows.
- **Fotocamere USB** - Quando selezionata, questa opzione consente l'accesso alle fotocamere web connesse a una porta USB anche se le porte USB sono negate.
  Supportato solo su Windows.
- **HID Bluetooth (mouse, tastiera, ecc.)** - Quando selezionata, questa opzione consente l'accesso a dispositivi HID (Human Interface Devices) come mouse, tastiera e così via, connessi tramite Bluetooth anche se il Bluetooth non è consentito.
  Supportato solo su Windows.
- **Copia/incolla negli appunti nell'applicazione** - Quando selezionata, questa opzione consente le operazioni di copia/incolla dei dati tramite gli appunti all'interno della stessa applicazione, anche se gli appunti non sono consentiti.
  Supportato solo su Windows.

Nota
Le impostazioni per le classi secondarie di dispositivi non supportati vengono ignorate se tali impostazioni sono configurate nel piano di protezione applicato.

Quando si inseriscono i tipi di dispositivo nella lista dei tipi di dispositivo consentiti, considerare quando segue:

- Nella lista dei tipi di dispositivo consentiti, è possibile consentire solo un'intera sottoclasse di dispositivo. Non è quindi possibile consentire uno specifico modello di dispositivo non consentendo anche tutti gli altri dispositivi della stessa sottoclasse. Ad esempio, escludendo le fotocamere USB dal controllo dell'accesso ai dispositivi, si consente l'utilizzo di qualsiasi fotocamera USB, indipendentemente dalla marca e dal modello. Per informazioni su come consentire singoli modelli o dispositivi, vedere Lista di dispositivi USB consentiti.
- I tipi di dispositivo possono essere selezionati solo da una lista chiusa di sottoclassi di dispositivi. Se il dispositivo da consentire appartiene a una sottoclasse diversa, non potrà essere consentito utilizzando la lista dei tipi di dispositivi consentiti. Ad esempio, non è possibile aggiungere alla lista dei dispositivi consentiti una sottoclasse di lettori di smartcard USB. Per consentire l'utilizzo di un lettore di smartcard USB quando le porte USB non sono consentite, seguire le istruzioni in Lista di dispositivi USB consentiti.
- La lista dei tipi di dispositivo funziona solo per i dispositivi che utilizzano driver Windows standard. Il modulo Controllo dispositivo potrebbe non riconoscere la sottoclasse di alcuni dispositivi USB con driver proprietari. Di conseguenza, non è possibile consentire l'accesso a tali dispositivi USB mediante la lista di tipi di dispositivi consentiti. In questo caso, è possibile consentire l'accesso per dispositivo o per modello (vedere Lista di dispositivi USB consentiti).

Lista di dispositivi USB consentiti

La lista di elementi consentiti è destinata a consentire l'impiego di determinati dispositivi USB indipendentemente da qualsiasi altra impostazione di controllo dei dispositivi. È possibile

© Acronis International GmbH, 2003-2024

aggiungere singoli dispositivi o modelli di dispositivo alla lista per disabilitare il controllo dell'accesso ai dispositivi desiderati. Se, ad esempio, si aggiunge alla lista un dispositivo mobile con un ID univoco, si consente l'utilizzo di quello specifico dispositivo anche se tutti gli altri dispositivi USB non sono consentiti.

Nella pagina della **Lista di dispositivi USB consentiti** page, è possibile specificare singoli dispositivi USB o modelli di dispositivo USB da escludere dal controllo dell'accesso. Di conseguenza, l'accesso a tali dispositivi è consentito indipendentemente dalle impostazioni di accesso del modulo Controllo dispositivo.

Esistono due modi per identificare i dispositivi nella lista:

- Modello di dispositivo - Identifica collettivamente tutti i dispositivi di un determinato modello. Ogni dispositivo viene identificato in base all'ID del vendor (VID) e all'ID del prodotto (PID), come nell'esempio USB\VID_0FCE&PID_E19E.

  Questa combinazione di VID e PID non identifica uno specifico dispositivo, ma tutti i dispositivi dello stesso modello. Aggiungendo un modello di dispositivo alla lista di elementi consentiti, si consente l'accesso a qualsiasi dispositivo di quel modello. In questo modo, ad esempio, si può consentire l'utilizzo di stampanti USB di un modello specifico.
- Dispositivo unico - Identifica un dispositivo specifico. Ogni dispositivo unico viene identificato in base all'ID del vendor (VID), all'ID del prodotto (PID) e al numero di serie, come nell'esempio USB\VID_0FCE&PID_E19E\D55E7FCA.

  Non a tutti i dispositivi USB è assegnato un numero di serie. È possibile aggiungere un dispositivo alla lista come dispositivo unico solo se al dispositivo è stato assegnato un numero di serie in fase di produzione, Ad esempio una pennetta USB dotata di un numero di serie univoco.

Per aggiungere un dispositivo alla lista dei dispositivi consentiti, è necessario prima aggiungerlo al Database dei dispositivi USB. Quindi sarà possibile aggiungere i dispositivi alla lista selezionandoli da tale database.

Questa lista di dispositivi consentiti è gestita da una pagina di configurazione distinta, denominata **Lista di dispositivi USB consentiti**. Ogni elemento della lista rappresenta un dispositivo o un modello di dispositivo ed è dotato dei campi seguenti:

- **Descrizione** - Il sistema operativo assegna una determinata descrizione quando esegue la connessione al dispositivo USB. È possibile modificare la descrizione del dispositivo nel database dei dispositivi USB (vedere Pagina di gestione del database dei dispositivi USB).
- **Tipo di dispositivo** - Viene visualizzato Unico se l'elemento della lista rappresenta un dispositivo unico, o Modello se rappresenta un modello di dispositivo.
- **Sola lettura** - Quando selezionata, l'opzione consente solo la ricezione dei dati dal dispositivo. Se il dispositivo non supporta l'accesso di sola lettura, l'accesso al dispositivo verrà bloccato. Deselezionare la casella di controllo per consentire l'accesso completo al dispositivo.
- **Reinizializza** - Quando selezionata, l'opzione fa sì che il dispositivo simuli la disconnessione/riconnessione all'accesso di un nuovo utente. Il funzionamento di alcuni dispositivi USB richiede la reinizializzazione; si consiglia pertanto di selezionare questa casella di controllo per tali dispositivi (mouse, tastiera ecc.). Si consiglia inoltre di deselezionarla per i

© Acronis International GmbH, 2003-2024

dispositivi di storage dei dati, ad esempio pennette USB, unità ottiche, dischi rigidi esterni.
Il modulo Controllo dispositivo potrebbe non essere in grado di reinizializzare alcuni dispositivi USB con driver proprietari. Se non è possibile accedere a questo tipo di dispositivo, è necessario disconnettere il dispositivo USB dalla porta USB e quindi reinserirlo.

Nota
Il campo **Reinizializza** è nascosto per impostazione predefinita. Per visualizzarla nella tabella, fare clic sull'icona ingranaggio nell'angolo in alto a destra della tabella e selezionare la casella di controllo **Reinizializza**.

Nota
I campi **Sola lettura** e **Reinizializza** non sono supportati su macOS. Se tali campi sono configurati nel piano di protezione applicato, verranno ignorati.

È possibile aggiungere o rimuovere i dispositivi/modelli dalla lista di elementi consentiti come indicato di seguito:

- Fare clic su **Aggiungi dal database** nella parte superiore della lista e quindi selezionare il dispositivo desiderato tra quelli registrati nel Database dei dispositivi USB. Il dispositivo selezionato viene aggiunto alla lista, dove sarà possibile configurarne le impostazioni e confermare le modifiche.
- Fare clic su **Consenti questo dispositivo USB** nell'avviso che informa che l'accesso al dispositivo USB non è consentito (vedere Avvisi di Controllo dispositivo). In questo modo il dispositivo viene aggiunto alla lista dei dispositivi consentiti e al database dei dispositivi USB.
- Fare clic per eliminare l'icona alla fine di un elemento della lista. In questo modo il dispositivo/modello associato all'icona viene eliminato dalla lista.

Database dei dispositivi USB

Il modulo Controllo dispositivo gestisce un database di dispositivi USB dal quale questi ultimi possono essere aggiunti all'elenco delle esclusioni (vedere Lista di dispositivi USB consentiti). È possibile registrare un dispositivo USB nel database in uno dei modi seguenti:

- Aggiungere un dispositivo sulla pagina visualizzata quando si aggiunge un dispositivo all'elenco delle esclusioni (vedere Pagina di gestione del database dei dispositivi USB).
- Aggiungere un dispositivo dalla scheda Dispositivi USB di un pannello Inventario di un computer nella console di Cyber Protect (vedere Lista dei dispositivi USB in un computer).
- Consentire il dispositivo da un avviso di accesso negato al dispositivo USB (vedere Avvisi di Consenti dispositivo).

Vedere anche Aggiungere o rimuovere i dispositivi USB dal database.

Pagina di gestione del database dei dispositivi USB

Quando si configura la lista dei dispositivi USB consentiti, si ha l'opzione di aggiungere un dispositivo dal database. Scegliendo questa opzione, viene visualizzata una pagina di gestione che

© Acronis International GmbH, 2003-2024

presenta una lista di dispositivi. Questa pagina elenca tutti i dispositivi registrati nel database, e consente di selezionare dispositivi da aggiungere alla lista dei consentiti e di eseguire le operazioni seguenti:

Registrare un dispositivo nel database

1. Fare clic su **Aggiungi al database** nella parte superiore della pagina.
2. Nella finestra di dialogo **Aggiungi dispositivo USB** visualizzata, selezionare il sistema al quale è connesso il dispositivo USB.
   Nell'elenco dei computer vengono mostrati solo i sistemi che sono online.
   L'elenco dei dispositivi USB viene visualizzato solo per i sistemi sui quali è installato l'agente per la prevenzione della perdita di dati.
   I dispositivi USB sono elencati nella visualizzazione ad albero. Il primo livello della visualizzazione rappresenta un modello di dispositivo. Il secondo livello rappresenta un dispositivo specifico di quel modello.
   Un'icona blu accanto alla descrizione del dispositivo indica che tale dispositivo è attualmente connesso al computer. Se il dispositivo non è connesso al computer, l'icona è inattiva (in grigio).
3. Selezionare la casella di controllo del dispositivo USB da registrare, quindi fare clic su **Aggiungi a database**.

Modificare la descrizione di un dispositivo

1. Nella pagina **Database dei dispositivi USB** fare clic sui puntini di sospensione (...) alla fine dell'elemento della lista che rappresenta il dispositivo, quindi fare clic su **Modifica**.
2. Apportare le modifiche alla descrizione nella finestra di dialogo visualizzata.

Rimuovere un dispositivo dal database

1. Fare clic sui puntini di sospensione (...) alla fine dell'elemento della lista che rappresenta il dispositivo.
2. Fare clic su **Elimina** e confermare l'operazione.

La lista nella pagina contiene le seguenti informazioni per ogni dispositivo:

- **Descrizione** - Un identificativo comprensibile per il dispositivo. È possibile modificare la descrizione come necessario.
- **Tipo di dispositivo** - Viene visualizzato Unico se l'elemento della lista rappresenta un dispositivo unico, o Modello se rappresenta un modello di dispositivo. Un dispositivo unico deve disporre di un numero di serie, di un ID vendor (VID) e di un ID prodotto (PID), mentre un modello di dispositivo è identificato tramite una combinazione di VID e PID.
- **ID vendor**, **ID prodotto ID**, **Numero di serie** - Nel loro complesso questi valori compongono l'ID del dispositivo nel formato USB\VID_<ID vendor>&PID_<ID prodotto>\<numero di serie>.
- **Account** -Indica il tenant a cui appartiene il dispositivo. Si tratta del tenant che contiene l'account utente che è stato usato per registrare il dispositivo nel database.

© Acronis International GmbH, 2003-2024

Nota
Questa colonna è nascosta per impostazione predefinita. Per visualizzarla nella tabella, fare clic sull'icona ingranaggio nell'angolo in alto a destra della tabella e selezionare **Account**.

La colonna più a sinistra è quella in cui selezionare i dispositivi da aggiungere alla lista dei dispositivi consentiti: Selezionare la casella di controllo di ogni dispositivo da aggiungere, quindi fare clic sul pulsante **Aggiungi alla lista di elementi consentiti**. Per selezionare o deselezionare tutte le caselle di controllo, fare clic sulla casella di controllo nell'intestazione della colonna.

È possibile fare una ricerca o filtrare la lista dei dispositivi:

- Fare clic su **Cerca** nella parte superiore della pagina e immettere una stringa di ricerca. La lista visualizza i dispositivi la cui descrizione corrisponde alla stringa digitata.
- Fare clic su **Filtra**, quindi configurare e applicare un filtro nella finestra di dialogo visualizzata. La lista è limitata ai dispositivi con il tipo, l'ID vendor, l'ID prodotto e l'account selezionati durante la configurazione del filtro. Per cancellare il filtro ad elencare tutti i dispositivi, fare clic su **Ripristina allo stato predefinito**.

Esportare la lista dei dispositivi USB nel database

È possibile esportare la lista dei dispositivi USB che vengono aggiunti al database.

1. Aprire il piano di protezione di un dispositivo per la modifica.
2. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare sulla riga **Lista di dispositivi USB consentiti**.
3. Nella pagina della lista di dispositivi USB consentiti, fare clic su **Aggiungi dal database**.
4. Nella pagina di gestione del database dei dispositivi USB visualizzata, fare clic su **Esporta**. Viene visualizzata la finestra di dialogo standard Sfoglia.
5. Selezionare la posizione in cui salvare il file, inserire un nuovo nome di file se necessario, quindi fare clic su **Salva**.

L'elenco dei dispositivi USB viene esportato in un file JSON.

È possibile modificare il file JSON risultante aggiungendo o rimuovendo dispositivi, e apportare modifiche di massa alle descrizioni dei dispositivi.

Importare un elenco di dispositivi USB nel database

Invece di aggiungere i dispositivi USB dalla console di Cyber Protect, è possibile importare una lista di dispositivi USB. L'elenco è un file in formato JSON.

Nota
È possibile importare i file JSON in un database che non contiene i dispositivi descritti nel file. Per importare un file modificato nel database dal quale è stato esportato, è necessario innanzitutto pulire il database perché non è possibile importare voci duplicate. Se si esporta la lista dei dispositivi USB, la si modifica e si tenta di importarla nello stesso database senza pulirla, l'importazione avrà esito negativo.

© Acronis International GmbH, 2003-2024

1. Aprire il piano di protezione di un dispositivo per la modifica.
2. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare sulla riga **Lista di dispositivi USB consentiti**.
3. Nella pagina della lista di dispositivi USB consentiti, fare clic su **Aggiungi dal database**.
4. Nella pagina di gestione del database dei dispositivi USB visualizzata, fare clic su **Importa**. Viene visualizzata la finestra di dialogo Importa dispositivi USB da file.
5. Utilizzare la funzione di trascinamento e rilascio per il file da importare, oppure individuarlo e selezionarlo.

La console di Cyber Protect verifica se la lista contiene voci duplicate che già esistono nel database, e le ignora. I dispositivi USB non individuati nel database vengono aggiunti al database.

Lista dei dispositivi USB in un computer

Il pannello Inventario di un computer nella console di Cyber Protect include la scheda **Dispositivi USB**. Se il computer è online ed è stato installato l'agente per la prevenzione della perdita di dati, la scheda **Dispositivi USB** elenca tutti i dispositivi USB che sono stati connessi a quel computer.

I dispositivi USB sono elencati nella visualizzazione ad albero. Il primo livello della visualizzazione rappresenta un modello di dispositivo. Il secondo livello rappresenta un dispositivo specifico di quel modello.

Per ogni dispositivo, la lista contiene le seguenti informazioni:

- **Descrizione** - Il sistema operativo assegna una determinata descrizione quando esegue la connessione al dispositivo USB. Questa descrizione può servire come identificativo comprensibile del dispositivo.
  Un'icona blu accanto alla descrizione del dispositivo indica che tale dispositivo è attualmente connesso al computer. Se il dispositivo non è connesso al computer, l'icona è inattiva (in grigio).
- **ID dispositivo** - Identificatore che indica il sistema operativo assegnato al dispositivo. L'identificatore ha il seguente formato: USB\VID_<ID vendor>&PID_<ID prodotto>\<numero di serie> dove <numero di serie> è facoltativo. Esempi: USB\VID_0FCE&PID_ADDE\D55E7FCA (dispositivo con numero di serie); USB\VID_0FCE&PID_ADDE (dispositivo senza numero di serie).

Per aggiungere dispositivi al database dei dispositivi USB, selezionare le caselle di controllo dei dispositivi USB desiderati, quindi fare clic su **Aggiungi a database**.

Esclusione di processi dal controllo dell'accesso

L'accesso agli appunti Windows, all'acquisizione di screenshot, alle stampanti e ai dispositivi mobili è controllato tramite l'esecuzione di hook aggiunti ai processi. Se nei processi non viene eseguito l'hook, l'accesso a tali dispositivi non verrà controllato.

Nota
L'esclusione di processi dal controllo dell'accesso non è supportata su MacOS. Se un elenco di processi esclusi è configurato nel piano di protezione applicato, verrà ignorato.

© Acronis International GmbH, 2003-2024

Nella pagina **Esclusioni** è possibile specificare un elenco di processi nei quali non viene eseguito l'hook. Ciò significa che i controlli dell'accesso agli appunti (locali e reindirizzati), alle acquisizione di screenshot, alle stampanti e ai dispositivi mobili non verranno applicati a tali processi.

Ad esempio, è stato applicato un piano di protezione che nega l'accesso alle stampanti e successivamente si avvia l'applicazione Microsoft Word. Il tentativo di avviare una stampa da questa applicazione verrà bloccato. Se si aggiunge il processo Microsoft Word all'elenco delle esclusioni, per questa applicazione non verrà eseguito l'hook. Di conseguenza, la stampa da Microsoft Word non sarà bloccata, mentre risulterà bloccata quella eseguita da altre applicazioni.

Per aggiungere processi alle esclusioni

1. Aprire il piano di protezione di un dispositivo per la modifica:
   Fare clic sull'icona dei puntini di sospensione (...) accanto al nome del piano di protezione, quindi selezionare **Modifica**.

   Nota
   Nel piano deve essere abilitata la funzionalità di controllo del dispositivo per poter accedere alle impostazioni di Controllo dispositivo.

2. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare clic sul link accanto alla riga **Esclusioni**.
3. Nella pagina **Esclusioni**, nella riga **Processi e cartelle**, fare clic su **+Aggiungi**.
4. Aggiungere i processi da escludere dal controllo degli accessi.
   Ad esempio, `C:\Cartella\Sottocartella\process.exe`.
   È possibile utilizzare caratteri jolly:
   - * sostituisce qualsiasi numero di caratteri.
   - ? sostituisce un carattere.

   Per esempio:

   ```
   C:\Cartella\*
   *\Cartella\Sottocartella?\*
   *\process.exe
   ```
5. Fare clic sul segno di spunta, quindi su **Fine**.
6. Nel piano di protezione, fare clic su **Salva**.
7. Riavviare il processo escluso per verificare la corretta rimozione degli hook.

I processi esclusi potranno accedere agli appunti, all'acquisizione di screenshot, alle stampanti e ai dispositivi mobili, indipendentemente dalle impostazioni di accesso di tali dispositivi.

Per rimuovere un processo dalle esclusioni

Aprire il piano di protezione di un dispositivo per la modifica:

Fare clic sull'icona dei puntini di sospensione (...) accanto al nome del piano di protezione, quindi selezionare **Modifica**.

© Acronis International GmbH, 2003-2024

Nota
Nel piano deve essere abilitata la funzionalità di controllo del dispositivo per poter accedere alle impostazioni di Controllo dispositivo.

1. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare clic sul link accanto alla riga **Esclusioni**.
2. Nella pagina **Esclusioni**, fare clic sull'icona del cestino accanto al processo da rimuovere dalle esclusioni.
3. Fare clic su **Fine**.
4. Nel piano di protezione, fare clic su **Salva**.
5. Riavviare il processo escluso per verificare la corretta aggiunta degli hook.

Le impostazioni di accesso provenienti dal piano di protezione verranno applicate ai processi rimossi dalle esclusioni.

Per modificare un processo nelle esclusioni

1. Aprire il piano di protezione di un dispositivo per la modifica:
   Fare clic sull'icona dei puntini di sospensione (...) accanto al nome del piano di protezione, quindi selezionare **Modifica**.

   Nota
   Nel piano deve essere abilitata la funzionalità di controllo del dispositivo per poter accedere alle impostazioni di Controllo dispositivo.

2. Fare clic sulla freccia accanto all'opzione **Controllo dispositivo** per espandere le impostazioni, quindi fare clic sul link accanto alla riga **Esclusioni**.
3. Nella pagina **Esclusioni**, fare clic sull'icona **Modifica** accanto al processo da modificare.
4. Applicare le modifiche e fare clic sul segno di spunta per confermare.
5. Fare clic su **Fine**.
6. Nel piano di protezione, fare clic su **Salva**.
7. Riavviare i processi interessati per verificare la corretta applicazione delle modifiche.

Avvisi di Controllo dispositivo

Il modulo Controllo dispositivo gestisce un registro eventi che tiene traccia dei tentativi degli utenti di accedere a tipi di dispositivi, porte o interfacce controllati. Alcuni eventi possono generare avvisi che vengono registrati nella console di Cyber Protect. Ad esempio, è possibile configurare il modulo Controllo dispositivo in modo che prevenga l'utilizzo di dispositivi rimovibili, con la registrazione di un avviso ogni volta che un utente cerca di copiare i dati da o verso un dispositivo di questo tipo.

Durante la configurazione del modulo Controllo dispositivo è possibile abilitare avvisi per la maggior parte degli elementi elencati in Tipo di dispositivo (ad eccezione delle acquisizioni di screenshot) o

© Acronis International GmbH, 2003-2024

Porte. Se gli avvisi sono abilitati, ogni tentativo dell'utente di eseguire un'operazione che non è consentita genera un avviso. Se, ad esempio, l'accesso ai dispositivi rimovibili è limitato alla sola lettura, e se la casella di controllo **Mostra avviso** è selezionata per quel tipo di dispositivo, viene generato un avviso ogni volta che un utente su un computer protetto tenta di copiare dati su un dispositivo rimovibile.

Per visualizzare gli avvisi nella console di Cyber Protect, passare a **Monitoraggio** > **Avvisi**. Per ogni avviso di controllo dispositivo, la console fornisce le seguenti informazioni sul rispettivo evento:

- **Tipo** - Attenzione.
- **Stato** - Visualizza "L'accesso al dispositivo generico è bloccato".
- **Messaggio** - Visualizza "L'accesso a '<tipo dispositivo o porta>' su '<nome computer>' è bloccato". Ad esempio, "Accesso a 'Rimovibile' su 'pc-contabilità' è bloccato".
- **Data e ora** - Data e ora in cui si è verificato l'evento.
- **Dispositivo** - Nome del computer sul quale si è verificato l'evento.
- **Nome del piano** - Il nome del piano di protezione che ha causato l'evento.
- **Origine** - Il tipo di dispositivo o porta coinvolti nell'evento. Ad esempio, nel caso di un tentativo utente non consentito di accedere a un dispositivo rimovibile, questo campo riporta Dispositivo rimovibile.
- **Azione** - L'operazione che ha causato l'evento. Ad esempio, nell'evento di un tentativo utente non consentito di copiare i dati in un dispositivo, questo campo riporta Scrittura. Per ulteriori informazioni, vedere Valori del campo Azione.
- **Nome** - Il nome dell'oggetto di destinazione dell'evento, ad esempio il file che l'utente ha tentato di copiare o il dispositivo che ha tentato di utilizzare. Non viene visualizzato se non è possibile identificare l'oggetto di destinazione.
- **Informazioni** - Informazioni aggiuntive sul dispositivo di destinazione dell'evento, ad esempio l'ID dei dispositivi USB. Non viene visualizzato se non sono disponibili ulteriori informazioni sul dispositivo di destinazione.
- **Utente** - Il nome dell'utente che ha causato l'evento.
- **Processo** - Il percorso completo al file eseguibile dell'applicazione che ha causato l'evento. In alcuni casi potrebbe essere visualizzato il nome del processo e non il percorso. Non viene visualizzato se le informazioni sul processo non sono disponibili.

Se un avviso è applicabile a un dispositivo USB (incluso i dispositivi rimovibili e i dispositivi rimovibili crittografati), l'amministratore potrà aggiungere il dispositivo direttamente alla lista degli elementi consentiti, evitando così che il modulo Controllo dispositivo limiti l'accesso a quello specifico dispositivo. L'opzione **Consenti questo dispositivo USB** lo aggiunge alla lista dei dispositivi USB consentiti nella configurazione del modulo Controllo dispositivo, e anche al database dei dispositivi USB per riferimento futuro.

Vedere anche i passaggi per visualizzare gli avvisi di Controllo dispositivo.

© Acronis International GmbH, 2003-2024

Valori del campo Azione

Il campo **Azione** degli avvisi può contenere i valori seguenti:

- **Lettura** - Consente di ottenere i dati dal dispositivo o dalla porta.
- **Scrittura** - Consente di inviare i dati al dispositivo o alla porta.
- **Formatta** - Accesso diretto (formattazione, controllo del disco, ecc.) al dispositivo. Se si tratta di una porta, il valore si applica al dispositivo connesso a tale porta.
- **Espelli** - Consente di rimuovere il dispositivo dal sistema o di espellere il supporto dal dispositivo. Se si tratta di una porta, il valore si applica al dispositivo connesso a tale porta.
- **Stampa** - Invia un documento alla stampante.
- **Copia audio** - Copia/incolla i dati audio tramite gli appunti locali.
- **Copia file** - Copia/incolla un file tramite gli appunti locali.
- **Copia immagine** - Copia/incolla un'immagine tramite gli appunti locali.
- **Copia testo** - Copia/incolla del testo tramite gli appunti locali.
- **Copia contenuto non identificato** - Copia/incolla altri tipi di dati tramite gli appunti locali.
- **Copia dati RTF (immagine)** - Copia/incolla un'immagine tramite gli appunti locali utilizzando il formato RTF.
- **Copia dati RTF (file)** - Copia/incolla un file tramite gli appunti locali utilizzando il formato RTF.
- **Copia dati RTF (testo, immagine)** - Copia/incolla un testo insieme a un'immagine tramite gli appunti locali utilizzando il formato RTF.
- **Copia dati RTF (testo, file)** - Copia/incolla del testo insieme a un file tramite gli appunti locali utilizzando il formato RTF.
- **Copia dati RTF (immagine, file)** - Copia/incolla un'immagine insieme a un file tramite gli appunti locali utilizzando il formato RTF.
- **Copia dati RTF (testo, immagine, file)** - Copia/incolla del testo insieme a un'immagine e a un file tramite gli appunti locali utilizzando il formato RTF.
- **Elimina** - Elimina i dati dal dispositivo (ad esempio, un dispositivo rimovibile, un dispositivo mobile, ecc.).
- **Accesso al dispositivo** - Consente l'accesso a dispositivi o porte (ad esempio, un dispositivo Bluetooth, una porta USB, ecc.).
- **Audio in entrata** - Copia/incolla dati audio dal computer client alla sessione in hosting tramite gli appunti reindirizzati.
- **File in entrata** - Copia/incolla un file dal computer client alla sessione in hosting tramite gli appunti reindirizzati.
- **Immagine in entrata** - Copia/incolla un'immagine dal computer client alla sessione in hosting tramite gli appunti reindirizzati.
- **Testo in entrata** - Copia/incolla un testo dal computer client alla sessione in hosting tramite gli appunti reindirizzati.

© Acronis International GmbH, 2003-2024

- **Contenuto non identificato in entrata** - Copia/incolla altri tipi di dati dal computer client alla sessione in hosting tramite gli appunti reindirizzati.
- **Dati RTF in entrata (immagine)** - Copia/incolla un'immagine dal computer client alla sessione in hosting tramite gli appunti reindirizzati in formato RTF.
- **Dati RTF in entrata (file)** - Copia/incolla un file dal computer client alla sessione in hosting tramite gli appunti reindirizzati in formato RTF.
- **Dati RTF in entrata (immagine, testo)** - Copia/incolla testo e un'immagine dal computer client alla sessione in hosting tramite gli appunti reindirizzati in formato RTF.
- **Dati RTF in entrata (testo, file)** - Copia/incolla del testo insieme a un file dal computer client alla sessione in hosting tramite gli appunti reindirizzati in formato RTF.
- **Dati RTF in entrata (immagine, file)** - Copia/incolla un'immagine insieme a un file dal computer client alla sessione in hosting tramite gli appunti reindirizzati in formato RTF.
- **Dati RTF in entrata (testo, immagine, file)** - Copia/incolla del testo insieme a un'immagine e a un file dal computer client alla sessione in hosting tramite gli appunti reindirizzati in formato RTF.
- **Inserisci** - Consente di connettere un dispositivo USB o un dispositivo FireWire.
- **Audio in uscita** - Copia/incolla dati audio dalla sessione in hosting al computer client tramite gli appunti reindirizzati.
- **File in uscita** - Copia/incolla un file dalla sessione in hosting al computer client tramite gli appunti reindirizzati.
- **Immagine in uscita** - Copia/incolla un'immagine dalla sessione in hosting al computer client tramite gli appunti reindirizzati.
- **Testo in uscita** - Copia/incolla del testo dalla sessione in hosting al computer client tramite gli appunti reindirizzati.
- **Contenuto non identificato in uscita** - Copia/incolla altri tipi di dati dalla sessione in hosting al computer client tramite gli appunti reindirizzati.
- **Dati RTF in uscita (immagine)** - Copia/incolla un'immagine dalla sessione in hosting al computer client tramite gli appunti reindirizzati in formato RTF.
- **Dati RTF in uscita (file)** - Copia/incolla un file dalla sessione in hosting al computer client tramite gli appunti reindirizzati in formato RTF.
- **Dati RTF in uscita (testo, immagine)** - Copia/incolla testo e insieme a un'immagine dalla sessione in hosting al computer client tramite gli appunti reindirizzati in formato RTF.
- **Dati RTF in uscita (testo, file)** - Copia/incolla del testo insieme a un file dalla sessione in hosting al computer client tramite gli appunti reindirizzati in formato RTF.
- **Dati RTF in uscita (immagine, file)** - Copia/incolla un'immagine insieme a un file dalla sessione in hosting al computer client tramite gli appunti reindirizzati in formato RTF.
- **Dati RTF in uscita (testo, immagine, file)** - Copia/incolla di testo insieme a un'immagine e a un file dalla sessione in hosting al computer client tramite gli appunti reindirizzati in formato RTF.
- **Rinomina** - Rinomina i file su un dispositivo (ad esempio, su dispositivi rimovibili, dispositivi mobili e altri).

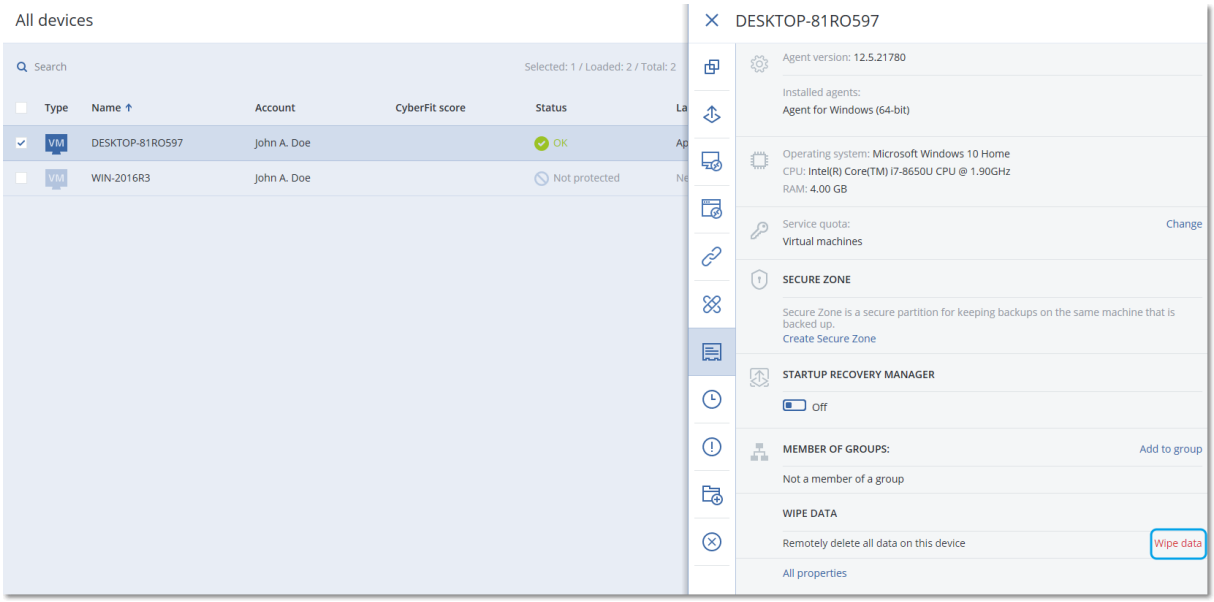
© Acronis International GmbH, 2003-2024

Cancellazione dei dati da un workload gestito

Nota
La funzionalità Cancellazione remota è disponibile solo con il pacchetto Advanced Security.

La cancellazione remota consente a un amministratore del servizio Cyber Protection e al proprietario di un sistema di eliminare i dati da una macchina gestita, ad esempio nel caso in cui venga smarrita o rubata. In questo modo si evita qualsiasi accesso non autorizzato alle informazioni sensibili.

La cancellazione remota è disponibile solo per i sistemi che eseguono Windows 10 e versioni successive. Per poter ricevere il comando di cancellazione, il sistema deve essere acceso e connesso a Internet.



Per cancellare i dati da un sistema

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare il sistema i cui dati si desidera cancellare.

   Nota
   È possibile cancellare i dati solo da un sistema alla volta.

3. Fare clic su **Dettagli**, quindi su **Cancella i dati**.
   Se il sistema selezionato non è online, l'opzione **Cancella i dati** non è accessibile.
4. Confermare la selezione.
5. Immettere le credenziali dell'amministratore locale del sistema, quindi fare clic su **Cancella i dati**.

© Acronis International GmbH, 2003-2024

Nota
È possibile controllare i dettagli relativi al processo di cancellazione e all'utente che lo esegue in **Monitoraggio** > **Attività**.

Visualizzazione di workload gestiti dalle integrazioni RMM

Nota
Questa funzionalità è disponibile solo se il servizio Advanced Automation è abilitato.

Quando una piattaforma RMM viene integrata come parte del servizio Advanced Automation, è possibile visualizzare e monitorare le informazioni dai dispositivi gestiti da tale piattaforma RMM. Queste informazioni sono disponibili nella console di Cyber Protect, nella sezione **Dispositivi**.

Per visualizzare i workload gestiti dalle integrazioni RMM

1. Passare a **Dispositivi > Tutti i dispositivi**.
2. (Facoltativo) Ordinare la colonna **Integrazione RMM** per individuare le integrazioni pertinenti.
3. Selezionare il workload pertinente.
4. Nel pannello **Azioni**, selezionare **Dettagli**.
5. Nel pannello visualizzato, a seconda del workload configurato, viene visualizzata una delle tre opzioni:
   - Se i servizi Acronis sono definiti per il workload senza integrazione RMM: Se il workload è configurato per operare solo con i servizi Acronis, non è visualizzata alcuna informazione sull'integrazione RMM.
   - Se per il workload sono configurati i servizi Acronis e un'integrazione RMM: Le informazioni sui servizi Acronis e sull'integrazione RMM sono disponibili nelle due schede **Panoramica** e **Integrazione RMM**. Fare clic su **Integrazione RMM** per visualizzare i dettagli sull'integrazione, incluso il nome e il tipo di workload (forniti dalla piattaforma RMM), la descrizione e la posizione. Vengono inoltre visualizzati tutti i componenti aggiuntivi dell'agente RMM, installati e abilitati.
   - Se il workload è configurato solo con un'integrazione RMM: Vengono visualizzati i dettagli dell'integrazione RMM, incluso il nome e il tipo di workload (forniti dalla piattaforma RMM), la descrizione e la posizione. Vengono inoltre visualizzati tutti i componenti aggiuntivi dell'agente RMM, installati e abilitati.

   Se il workload è configurato con l'integrazione RMM (sia insieme ai servizi Acronis sia solo con un'integrazione RMM), è possibile:
   - Avviare una connessione remota (disponibile per le integrazioni Datto RMM, N-able N-central, N-able RMM)
   - Esaminare gli add-on installati nel dispositivo RMM di terze parti (disponibile solo per l'integrazione N-able RMM)

© Acronis International GmbH, 2003-2024

- Accedere direttamente ai dettagli del dispositivo RMM di terze parti (disponibile per Datto RMM, N-able N-central, NinjaOne)

Workload CyberApp

I workload CyberApp sono creati dagli ISV (fornitori di software indipendente) e vengono visualizzati nella console di Cyber Protect dopo aver abilitato un'integrazione CyberApp. È necessario che siano soddisfatte le seguenti condizioni:

- Nella CyberApp deve essere abilitato il punto di estensione **Workload e azioni**.
- Nella CyberApp deve essere definito almeno un **Tipo di workload**.
- Il servizio di connettore in hosting presso l'ISV deve garantire che i workload CyberApp vengano aggiunti e aggiornati nella piattaforma Acronis.

Per ulteriori informazioni sul Vendor Portal e sulla creazione di CyberApp, consultare il Manuale dell'utente del Vendor Portal.

Workload aggregati

In un workload fisico possono essere installati contemporaneamente un agente Cyber Protect e uno o più agenti CyberApp. In questo caso, nella schermata **Tutti i dispositivi** lo stesso workload avrà più di una rappresentazione, ovvero viene visualizzato un record distinto per il workload Acronis e per ogni workload CyberApp. Se nel Vendor Portal o nella console di Cyber Protect è stata abilitata e configurata l'unione automatica dei workload, il sistema confronta gli indirizzi host e gli indirizzi MAC dei workload Acronis e dei workload CyberApp, e unisce tutte le rappresentazioni un unico workload aggregato. Nella console di Cyber Protect è anche possibile unire e annullare manualmente l'unione tra workload.

Lavorare con workload CyberApp

Oltre alle azioni standard integrate nella console di Cyber Protect, è possibile eseguire le operazioni che diventano disponibili dopo che i workload CyberApp vengono visualizzati nella console: unione manuale dei workload in un workload aggregato ed esecuzione delle azioni personalizzate configurate nella CyberApp.

Unisci

Prerequisiti

- Per il tenant sono disponibili workload di diverse origini.

È possibile unire manualmente un workload Acronis con uno o più workload CyberApp in un unico workload aggregato.

Per unire manualmente i workload in un workload aggregato

© Acronis International GmbH, 2003-2024

1. Nella schermata **Tutti i dispositivi**, selezionare i workload da unire.

   Nota
   L'azione di unione viene visualizzata se si selezionano workload di diverse origini, ad esempio un workload Acronis e un workload CyberApp.

2. Fare clic su **Unisci workload**.

Esecuzione di azioni personalizzate

Prerequisiti

- Per il tenant è abilitata un'integrazione CyberApp per la quale è stata definita l'opzione **Azioni workload**.

Le azioni personalizzate sono configurate nella CyberApp e diventano disponibili per il workload CyberApp corrispondente quando viene abilitata l'integrazione CyberApp per il tenant.

Per eseguire le azioni personalizzate

1. Nella schermata **Tutti i dispositivi**, fare clic sul workload.
2. Fare clic su **Azioni app integrate**.
3. Fare clic sull'azione.

Lavorare con workload aggregati

Oltre alle azioni standard integrate nella console di Cyber Protect, con i workload aggregati è possibile eseguire le operazioni seguenti: visualizzazione di dettagli, annullamento delle unioni dei workload di origine, esecuzione di azioni personalizzate configurate nelle CyberApp.

Visualizza dettagli

Prerequisiti

- Per il tenant è disponibile almeno un workload aggregato.

Per visualizzare i dettagli di un workload aggregato

1. Nella schermata **Tutti i dispositivi**, fare clic sul workload aggregato.
2. Fare clic su **Dettagli**.
   I dettagli del workload aggregato vengono separati in schede. Ogni scheda contiene i dettagli di ciascuna rappresentazione del workload.

Annulla unione

Prerequisiti

- Per il tenant è disponibile almeno un workload aggregato.

© Acronis International GmbH, 2003-2024

Dopo aver annullato l'unione di workload aggregato, questo non viene più visualizzato nell'elenco dei dispositivi. Nell'elenco viene invece visualizzata una voce distinta per ogni workload di origine che era stato unito nel workload aggregato.

Per annullare le unioni di un workload aggregato

1. Nella schermata **Tutti i dispositivi**, fare clic sul workload aggregato di cui si vuole annullare l'unione.
2. Fare clic su **Annulla unione dei workload di origine**.
3. Nella finestra di conferma, fare clic su **Annulla unione**.

Esecuzione di azioni personalizzate

Prerequisiti

- Per il tenant è abilitata almeno un'integrazione CyberApp per la quale è stata definita l'opzione **Azioni workload**.

Le azioni personalizzate sono configurate nelle CyberApp e diventano disponibili per il workload CyberApp corrispondente quando viene abilitata l'integrazione CyberApp per il tenant.

Per eseguire le azioni personalizzate

1. Nella schermata **Tutti i dispositivi**, fare clic sul workload.
2. Fare clic su **Azioni app integrate**.
3. A seconda delle azioni personalizzate disponibili, eseguire una delle seguenti operazioni.
   - Se per il workload aggregato è presente un workload CyberApp, fare clic sull'azione.
   - Se per il workload aggregato sono presenti più workload CyberApp, fare clic sul nome della CyberApp e quindi sull'azione.

Collegare workload a utenti specifici

Nota
Questa funzionalità è disponibile solo se il servizio Advanced Automation è abilitato.

Collegando un workload a un utente specifico è possibile collegare automaticamente il workload ai nuovi ticket del Service Desk creati o assegnati all'utente.

Per collegare un workload a un utente

1. Passare a **Dispositivi > Tutti i dispositivi**, quindi selezionare il workload pertinente.
2. Nel pannello **Azioni**, selezionare **Collega a un utente**.
3. Selezionare l'utente interessato.
   Se necessario, è anche possibile modificare l'utente selezionato dei workload collegati già esistenti.
4. Fare clic su **Fine**. L'utente selezionato viene visualizzato nella colonna **Utente collegato**.

© Acronis International GmbH, 2003-2024

Per annullare un collegamento di un workload da un utente

1. Passare a **Dispositivi > Tutti i dispositivi**, quindi selezionare il workload pertinente.
2. Nel pannello **Azioni**, selezionare **Collega a un utente**.
3. Fare clic su **Annulla collegamento a utente**.
4. Fare clic su **Fine**.

Trovare l'ultimo utente connesso

Affinché gli amministratori possano gestire i dispositivi, devono identificare l'utente connesso al dispositivo e l'orario di connessione. Queste informazioni sono visualizzate nel dashboard o nei dettagli dei workload.

È possibile abilitare o disabilitare la visualizzazione delle informazioni sull'ultimo accesso nei Piani di gestione remota.

Nel dashboard:

1. Fare clic su **Dispositivi**. Viene visualizzata la finestra **Tutti i dispositivi**.
2. Nella colonna **Ultimo accesso**, viene visualizzato il nome dell'ultimo utente connesso per ogni dispositivo.
3. Nella colonna **Ora ultimo accesso**, viene visualizzata l'ora in cui l'ultimo utente si è connesso, per ogni dispositivo.

Nei dettagli del dispositivo:

1. Fare clic su **Dispositivi**. Viene visualizzata la finestra **Tutti i dispositivi**.
2. Fare clic sul dispositivo per il quale verificare i dettagli.
3. Fare clic sull'icona dei **Dettagli**. Il nome dell'utente e la data e l'ora degli ultimi accessi per il dispositivo selezionato vengono visualizzati nella sezione **Ultimo accesso utenti il**.

Nota
Nella sezione **Ultimo accesso utenti il** verranno visualizzati un massimo di 5 diversi utenti che hanno fatto accesso al dispositivo.

Per mostrare o nascondere le colonne Ultimo accesso e Ora ultimo accesso nel dashboard

1. Fare clic su **Dispositivi**. Viene visualizzata la finestra **Tutti i dispositivi**.
2. Fare clic sull'icona a ingranaggio nell'angolo in alto a destra e procedere come segue nella sezione **Informazioni generali**:
   - Abilitare le colonne **Ultimo accesso** e **Ora ultimo accesso** se si desidera visualizzarle nel dashboard.
   - Disabilitare le colonne **Ultimo accesso** e **Ora ultimo accesso** se si desidera nasconderle nel dashboard.

© Acronis International GmbH, 2003-2024

Gestione del backup e del ripristino di workload e file

Questo modulo di backup consente l'esecuzione del backup e il ripristino di macchine, file e database fisici e virtuali nell'archivio locale o nel cloud.

Backup

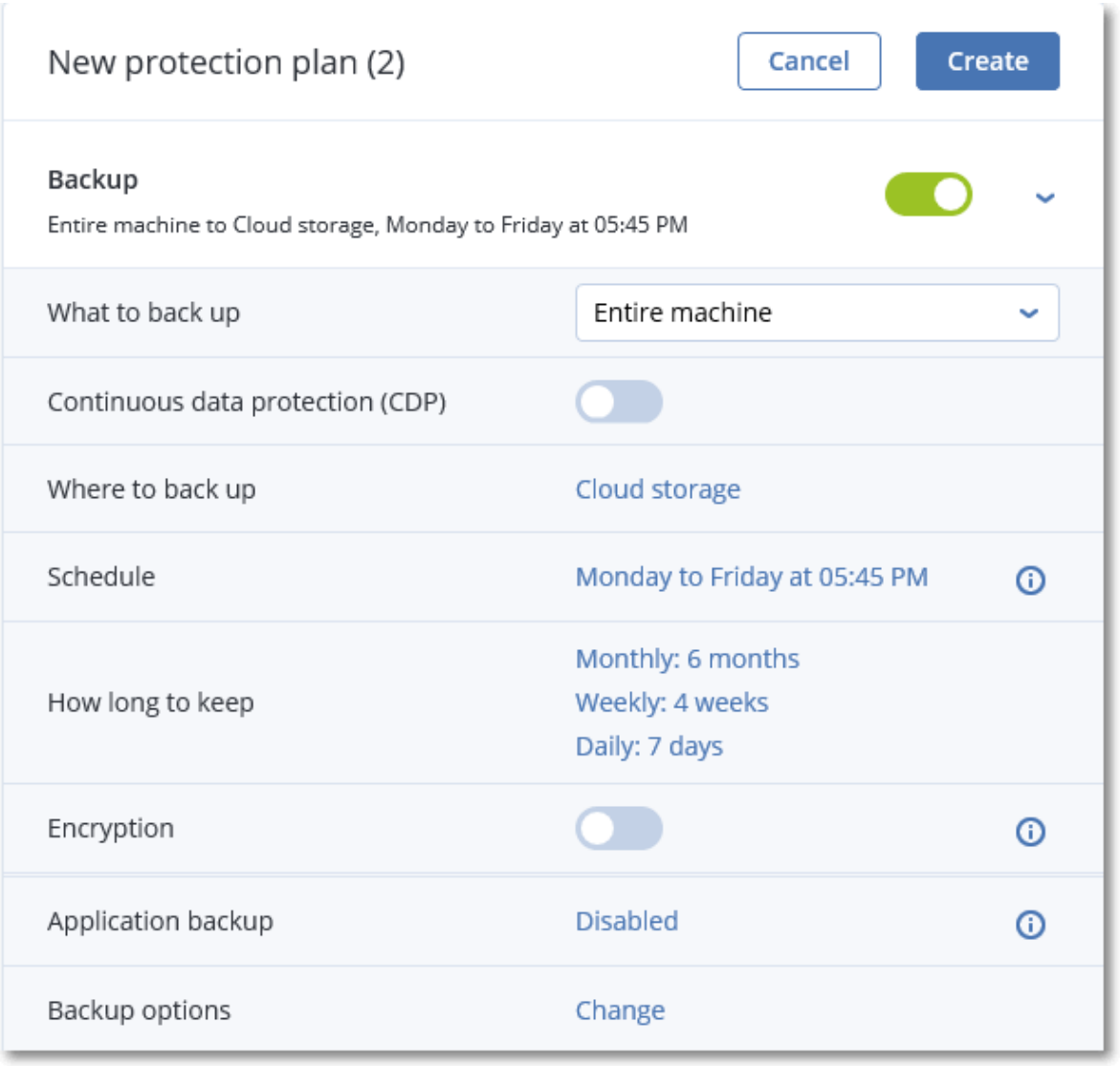
Un piano di protezione per il quale è abilitato il modulo Backup è un set di regole che specifica in che modo i dati indicati verranno protetti su un determinato sistema.

Un piano di protezione può essere applicato a più sistemi al momento della creazione o successivamente.

Per creare il primo piano di protezione con il modulo Backup abilitato

1. Selezionare i sistemi di cui si vuole eseguire il backup.
2. Fare clic su **Proteggi**.
   Vengono visualizzati i piani di protezione già applicati al sistema. Se al sistema non sono stati assegnati piani, verrà visualizzato il piano di protezione predefinito che è possibile applicare. È possibile regolare le impostazioni come necessario e applicare questo piano o crearne uno nuovo.
3. Per creare un nuovo piano, fare clic su **Crea piano**. Abilitare il modulo **Backup** ed espandere le impostazioni.

© Acronis International GmbH, 2003-2024

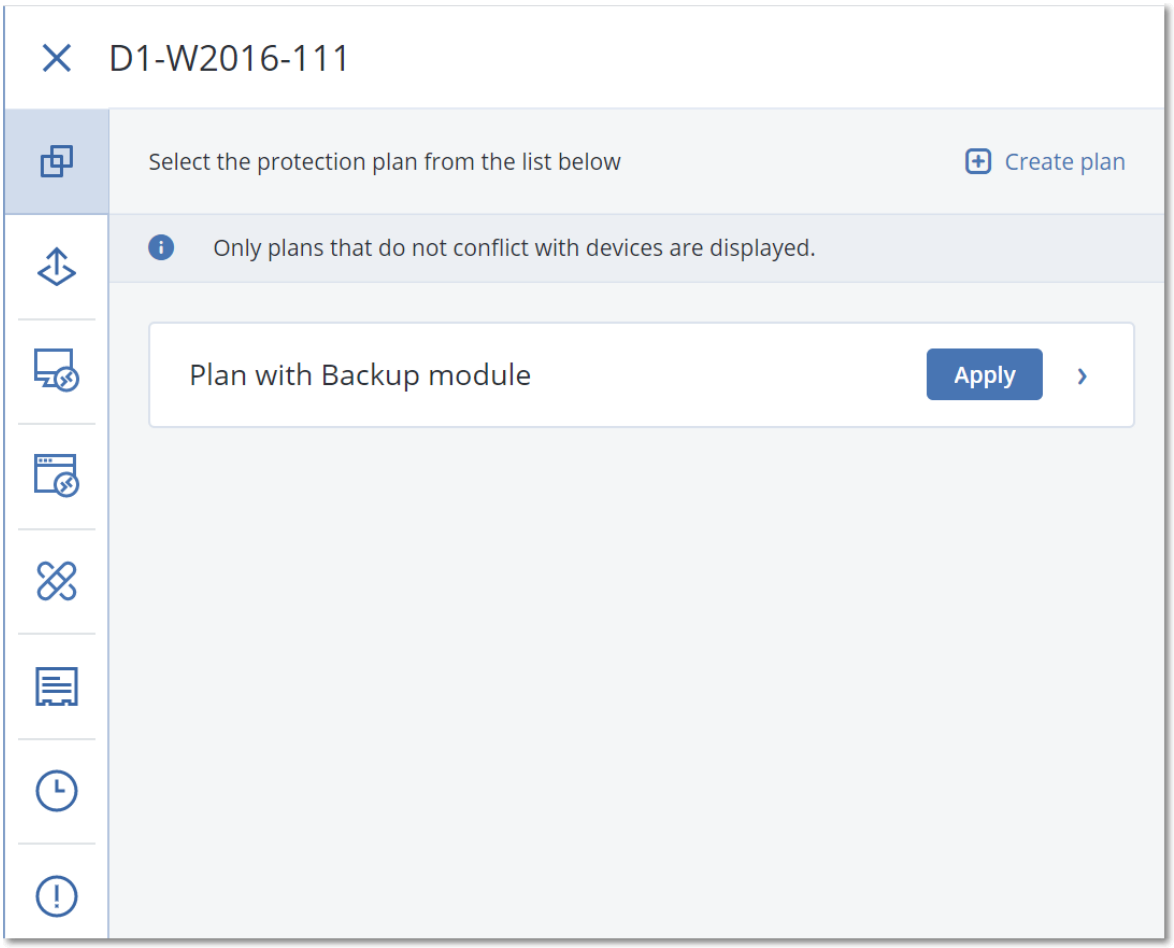


4. [Facoltativo] Per modificare il nome del piano di protezione, fare clic sul nome predefinito.
5. [Facoltativo] Per modificare i parametri del modulo Backup, fare clic sull'impostazione corrispondente nel riquadro del piano di protezione.
6. [Facoltativo] Per modificare le opzioni di backup, fare clic su **Modifica** accanto a **Opzioni di Backup**.
7. Fare clic su **Crea**.

Per applicare un piano di protezione esistente

1. Selezionare i sistemi di cui si vuole eseguire il backup.
2. Fare clic su **Proteggi**. Se ai sistemi selezionati è già applicato un piano di protezione comune, fare clic su **Aggiungi piano**.
   Il software mostra i piani di protezione creati in precedenza.

© Acronis International GmbH, 2003-2024



3. Selezionare un piano di protezione da applicare.
4. Fare clic su **Applica**.

Panoramica del piano di protezione

La seguente tabella riassume i parametri disponibili per il piano di protezione. Utilizzare la tabella per creare un piano di protezione adatto alle proprie esigenze.

COSA INCLUDERE NEL BACKUP	ELEMENTI DI CUI ESEGUIRE IL BACKUP Metodi di selezione	DOVE ESEGUIRE IL BACKUP	PIANIFICAZIONE Schemi di backup	TEMPO DI CONSERVAZIONE
Volumi/Dischi (macchine fisiche[1])	Selezione diretta Regole dei	Cloud Cartella locale	Sempre incrementale (a file singolo) Sempre completo	Per durata backup (regola singola/per set di backup)

[1]Una macchina il cui backup viene eseguito ad opera di un agente installato nel sistema operativo.

© Acronis International GmbH, 2003-2024

	criteri Filtri file	Cartella di rete NFS* Secure Zone**	Settimanale completo, Giornaliero incrementale Mensile completo, Settimanale differenziale, Giornaliero incrementale (GFS) Personalizzato (F-D-I)	Per numero di backup Per dimensione totale dei backup*** Conserva a tempo indefinito
Dischi/Volumi (macchine virtuali[1])	Regole dei criteri Filtri file	Cloud Cartella locale Cartella di rete NFS*		
File (solo macchine fisiche[2])	Selezione diretta Regole dei criteri Filtri file	Cloud Cartella locale Cartella di rete NFS* Secure Zone**	Sempre incrementale (a file singolo) Sempre completo Settimanale completo, Giornaliero incrementale Mensile completo, Settimanale differenziale, Giornaliero incrementale (GFS) Personalizzato (F-D-I)	
Configurazione ESXi	Selezione diretta	Cartella locale Cartella di rete NFS*		
Siti Web (file e database MySQL)	Selezione diretta	Cloud	—	

[1]Una virtual machine il cui backup viene eseguito a livello di hypervisor da un agente esterno, come l'Agente per VMware o l'Agente per Hyper-V. Dal punto di vista del backup, una virtual machine con un agente interno viene considerata come un sistema fisico.
[2]Una macchina il cui backup viene eseguito ad opera di un agente installato nel sistema operativo.

© Acronis International GmbH, 2003-2024

<table>
<tr><td colspan="2">Stato del sistema</td><td rowspan="3">Selezione diretta</td><td rowspan="3">Cloud
Cartella locale
Cartella di rete</td><td rowspan="3">Sempre completo
Settimanale completo, Giornaliero incrementale
Personalizzato (F-I)</td><td rowspan="6"></td></tr>
<tr><td colspan="2">Database SQL</td></tr>
<tr><td colspan="2">Database Exchange</td></tr>
<tr><td rowspan="5">Microsoft 365</td><td>Caselle postali
(Agente locale per Microsoft 365)</td><td>Selezione diretta</td><td>Cloud
Cartella locale
Cartella di rete</td><td>Sempre incrementale
Sempre incrementale (a file singolo) - solo per database SQL</td></tr>
<tr><td>Caselle postali
(Agente cloud per Microsoft 365)</td><td rowspan="3">Selezione diretta</td><td rowspan="4">Cloud</td><td rowspan="4">Fino a 6 backup al giorno</td></tr>
<tr><td>Cartelle pubbliche</td></tr>
<tr><td>Teams</td></tr>
<tr><td>File di OneDrive</td><td rowspan="2">Selezione diretta
Regole dei criteri</td></tr>
<tr><td>Google Workspace</td><td>Dati di SharePoint Online</td></tr>
<tr><td rowspan="3">Google Workspace</td><td>Caselle di posta di Gmail</td><td>Selezione diretta</td><td rowspan="3">Cloud</td><td rowspan="3">Fino a 6 backup al giorno</td></tr>
<tr><td>File di Google Drive</td><td>Selezione diretta</td></tr>
<tr><td>File di unità condivise</td><td>Regole dei criteri</td></tr>
</table>

* Il backup nelle condivisioni NFS non è disponibile in Windows.

** Non è possibile creare Secure Zone in un Mac.

*** La regola di conservazione **Per dimensione totale dei backup** non è disponibile con lo schema di backup **Sempre incrementale (a file singolo)** o quando il backup avviene nell'archiviazione cloud.

© Acronis International GmbH, 2003-2024

Selezione dei dati del backup

Selezione di un intero sistema

Il backup di un intero sistema è il backup di tutti i suoi dischi non rimovibili. Per ulteriori informazioni sul backup di disco, fare riferimento a "Selezione di dischi o volumi" (pag. 409).

Limitazioni

- Non sono supportati i backup del disco o volume per i volumi APFS crittografati e bloccati. Durante il backup di un intero sistema, questi volumi vengono ignorati.
- Per impostazione predefinita, la cartella radice di OneDrive viene esclusa dalle operazioni di backup. Se si sceglie di eseguire il backup di specifici file e cartelle di OneDrive, ne verrà eseguito il backup. I file non disponibili nel dispositivo avranno contenuti non validi nel set di backup.

Selezione di dischi o volumi

Un backup a livello di disco che contiene una copia di un disco o un volume in forma compressa. Da un backup del disco è possibile recuperare dischi, volumi, cartelle e file.

È possibile selezionare i dischi e i volumi di cui eseguire il backup per ogni workload del piano di protezione (selezione diretta) oppure configurare le regole dei criteri per più workload. Inoltre, configurando i filtri file è possibile escludere da un backup o includere in esso solo specifici file. Per ulteriori informazioni, consultare "Filtri file (Inclusioni/Esclusioni)" (pag. 468).

Per selezionare dischi o volumi

Selezione diretta

La seleziona diretta è disponibile solo per le macchine fisiche.

1. In **Cosa includere nel backup**, selezionare **Dischi/volumi**.
2. Fare clic su **Elementi di cui eseguire il backup**.
3. In **Seleziona elementi per il backup**, selezionare **Direttamente**.
4. Per ogni workload incluso nel piano di protezione, selezionare le caselle di controllo accanto ai dischi o i volumi di cui eseguire il backup.
5. Fare clic su **Fine**.

In base alle regole dei criteri

1. In **Cosa includere nel backup**, selezionare **Dischi/volumi**.
2. Fare clic su **Elementi di cui eseguire il backup**.
3. In **Seleziona elementi per il backup**, selezionare **Utilizzo regole del criterio**.

© Acronis International GmbH, 2003-2024

4. Selezionare una qualsiasi delle regole predefinite, digitare le proprie regole o applicare entrambe le opzioni.

   Per ulteriori informazioni sulle regole dei criteri disponibili, consultare "Regole dei criteri per dischi e volumi" (pag. 411).

   Le regole dei criteri verranno applicate a tutti i sistemi inclusi nel piano di protezione.

   Se non è possibile applicare a un workload nessuna delle regole specificate, il backup di tale workload non viene eseguito correttamente.
5. Fare clic su **Fine**.

Limitazioni

- Non sono supportati i backup del disco o volume per i volumi APFS crittografati e bloccati. Durante il backup di un intero sistema, questi volumi vengono ignorati.
- Per impostazione predefinita, la cartella radice di OneDrive viene esclusa dalle operazioni di backup. Se si sceglie di eseguire il backup di specifici file e cartelle di OneDrive, ne verrà eseguito il backup. I file non disponibili nel dispositivo avranno contenuti non validi nel set di backup.
- È possibile eseguire il backup di dischi connessi a un sistema fisico tramite il protocollo iSCSI. Si hanno tuttavia alcune limitazioni se si utilizza l'Agente per VMware o l'Agente per Hyper-V per il backup di dischi connessi con iSCSI. Per ulteriori informazioni, consultare "Limitazioni" (pag. 34).

Quali informazioni vengono memorizzate dal backup di un disco o un volume?

Il backup di un disco o di un volume archivia il **file system** di un disco o di un volume come unità intera e include tutte le informazioni necessarie per l'avvio del sistema operativo. Da questi backup è possibile ripristinare interi dischi o volumi, come pure singole cartelle o file.

Con l'opzione di backup **settore per settore (modalità raw)** abilitata, il backup di un disco archivia tutti i settori del disco. È possibile utilizzare il backup settore per settore per eseguire il backup di dischi con file system non riconosciuti o non supportati e altri formati di dati proprietari.

Windows

Un backup del volume archivia tutti i file e le cartelle del volume selezionato, indipendentemente dai relativi attributi (inclusi file nascosti e di sistema), il record di avvio, l'eventuale tabella di allocazione file (FAT), la radice e la traccia zero del disco rigido con il record di avvio principale (MBR).

Il backup di un disco archivia tutti i volumi del disco selezionato (inclusi volumi nascosti, ad esempio partizioni di manutenzione del fornitore) e la traccia zero con il record di avvio principale.

I seguenti elementi *non* sono inclusi nel backup di un disco o di un volume (oltre che in un backup dei file):

- Il file di scambio (pagefile.sys) e il file che include il contenuto della RAM quando la macchina va in ibernazione (hiberfil.sys). Dopo il ripristino, i file verranno creati nuovamente nella posizione appropriata con dimensione zero.

 © Acronis International GmbH, 2003-2024

- Se il backup viene eseguito nel sistema operativo (anziché nel supporto di avvio o i backup delle macchine virtuali a livello di hypervisor):
  - Archiviazione shadow di Windows. Il percorso è stabilito nel valore del Registro di sistema **VSS Default Provider** presente all'interno della chiave del Registro di sistema **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. Ciò significa che nei sistemi operativi a partire da Windows Vista, non viene eseguito il backup dei punti di ripristino di Windows.
  - Se l'opzione di backup **Servizio Copia Shadow del volume (VSS)** è abilitata, i file e le cartelle specificate nella chiave del Registro di sistema **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** .

Linux

Un backup del volume archivia tutti i file e le directory del volume selezionato, indipendentemente dai relativi attributi, un record di avvio e il superblocco del file system.

Il backup di un disco archivia tutti i volumi del disco e la traccia zero con il record di avvio principale.

Mac

Il backup di un disco o di un volume archivia tutti i file e le directory del disco o del volume selezionato, insieme alla descrizione del layout del volume.

Sono esclusi gli elementi seguenti:

- Metadati di sistema, come il journal del file system e l'indice Spotlight
- Il Cestino
- I backup di Time Machine

A livello fisico, i dischi e i volumi di un Mac vengono sottoposti a backup a livello di file. Il ripristino bare metal dai backup di dischi e volumi è possibile, tuttavia la modalità di backup settore per settore non è disponibile.

Regole dei criteri per dischi e volumi

Quando si selezionano dischi o volumi di cui eseguire il backup, è possibile utilizzare le regole dei criteri seguenti, in base al sistema operativo del workload protetto.

Windows

- `[All Volumes]` seleziona tutti i volumi del sistema.
- Lettera di unità (ad esempio `C:\`) seleziona il volume con la lettera di unità specificata.
- `[Fixed Volumes (physical machines)]` seleziona tutti i volumi di un sistema fisico, diversi dai supporti rimovibili. I volumi fissi includono volumi su periferiche SCSI, ATAPI, ATA, SSA, SAS e SATA e su array RAID.
- `[BOOT+SYSTEM]` seleziona i volumi di sistema e di avvio. Questa è la combinazione minima a partire dalla quale è possibile ripristinare un sistema operativo.

© Acronis International GmbH, 2003-2024

- `[Disk 1]` seleziona il primo disco del sistema, inclusi tutti i volumi sul disco. Per selezionare un altro disco, digitare il relativo numero.

Linux

- `[All volumes]` seleziona tutti i volumi montati nel sistema.
- `/dev/hda1` seleziona il primo volume sul primo disco rigido IDE.
- `/dev/sda1` seleziona il primo volume sul primo disco rigido SCSI.
- `/dev/md1` seleziona il primo disco rigido RAID software.
- Per selezionare altri volumi di base, specificare `/dev/xdyN`, dove:
  - "x" corrisponde al tipo di disco
  - "y" corrisponde al numero del disco (a per il primo disco, b per il secondo e così via)
  - "N" è il numero del volume.
- Per selezionare un volume logico, specificare il suo percorso così come appare dopo aver eseguito il comando `ls /dev/mapper` dall'account root.

  Per esempio:

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  Questo risultato mostra due volumi logici, `lv1` e `lv2`, che appartengono al gruppo di volume `vg_1`. Per eseguire il backup di questi volumi, specificare:

  `/dev/mapper/vg_1-lv1`
  `/dev/mapper/vg-l-lv2`

macOS

- `[All volumes]` seleziona tutti i volumi montati nel sistema.
- `[Disk 1]` seleziona il primo disco del sistema, inclusi tutti i volumi sul disco. Per selezionare un altro disco, specificare il numero corrispondente.

Selezione di file e cartelle

Utilizzare il backup a livello di file per proteggere solo dati specifici, ad esempio i file di un progetto in corso. I backup a livello di file hanno dimensioni inferiori ai backup del disco e consentono di risparmiare spazio di storage.

Importante
Non è possibile recuperare un sistema operativo da un backup a livello di file.

È possibile selezionare i file e le cartelle di cui eseguire il backup per ogni workload del piano di protezione (selezione diretta) oppure configurare le regole dei criteri per più workload. Inoltre, configurando i filtri è possibile escludere da un backup o includere in esso solo specifici file. Per ulteriori informazioni, consultare "Filtri file (Inclusioni/Esclusioni)" (pag. 468).

Per selezionare file o cartelle

 © Acronis International GmbH, 2003-2024

Selezione diretta

1. In **Cosa includere nel backup**, selezionare **File/cartelle**.
2. In **Elementi di cui eseguire il backup**, fare clic su **Specifica**.
3. In **Seleziona elementi per il backup**, selezionare **Direttamente**.
4. Specificare i file e le cartelle di cui eseguire il backup per ogni workload del piano di protezione.
   a. Fare clic su **Seleziona file e cartelle**.
   b. Fare clic su **Cartella locale** o **Cartella di rete**.
      Le cartelle di rete devono essere accessibili dal sistema selezionato.
      Quando si seleziona come origine la **Cartella di rete**, è possibile eseguire il backup dei dati da dispositivi di storage NAS, ad esempio i dispositivi NetApp. Sono supportati i dispositivi NAS di qualsiasi fornitore.
   c. Nella struttura ad albero, passare ai file o alle cartelle richieste.
      In alternativa, specificarne il percorso quindi fare clic sul pulsante freccia.
   d. [Per le cartelle condivise] Quando viene richiesto, specificare le credenziali di accesso alla cartella condivisa.
      L'esecuzione del backup di cartelle con accesso anonimo non è supportata.
   e. Selezionare i file e le cartelle desiderate.
   f. Fare clic su **Fine**.

In base alle regole dei criteri

1. In **Cosa includere nel backup**, selezionare **File/cartelle**.
2. In **Elementi di cui eseguire il backup**, fare clic su **Specifica**.
3. In **Seleziona elementi per il backup**, selezionare **Utilizzo regole del criterio**.
4. Selezionare una qualsiasi delle regole predefinite, digitare le proprie regole o applicare entrambe le opzioni.
   Per ulteriori informazioni sulle regole dei criteri disponibili, consultare "Regole dei criteri per file e cartelle" (pag. 414).
   Le regole dei criteri verranno applicate a tutti i sistemi inclusi nel piano di protezione.
   Se non è possibile applicare a un workload nessuna delle regole specificate, il backup di tale workload non viene eseguito correttamente.
5. Fare clic su **Fine**.

Limitazioni

- È possibile selezionare file e cartelle durante il backup di sistemi fisici o di virtual machine sui quali è installato un agente (backup con agente). Il backup a livello di file non è disponibile per le virtual machine il cui backup è eseguito in modalità agentless. Per ulteriori informazioni sulle differenze tra queste tipologie di backup, consultare "Backup con agente e agentless" (pag. 66).

© Acronis International GmbH, 2003-2024

- Per impostazione predefinita, la cartella radice di OneDrive viene esclusa dalle operazioni di backup. Se si sceglie di eseguire il backup di specifici file e cartelle di OneDrive, ne verrà eseguito il backup. I file non disponibili nel dispositivo avranno contenuti non validi nel set di backup.
- È possibile eseguire il backup di file e cartelle che si trovano su dischi connessi a un sistema fisico tramite il protocollo iSCSI. Si hanno tuttavia alcune limitazioni se si utilizza l'Agente per VMware o l'Agente per Hyper-V per il backup dei dati su dischi connessi con iSCSI.

Regole dei criteri per file e cartelle

Quando si selezionano file o cartelle di cui eseguire il backup, è possibile utilizzare le regole dei criteri seguenti, in base al sistema operativo del workload protetto.

Windows

- Percorso completo a un file o a una directory. Ad esempio, `D:\Lavoro\Testo.doc` oppure `C:\Windows`.
- Regole predefinite:
  - `[All Files]` seleziona tutti i file in tutti i volumi del sistema.
  - `[All Profiles Folder]` seleziona la cartella in cui sono collocati tutti i profili utente. Ad esempio, `C:\Utenti` o `C:\Documents and Settings`.
- Variabili d'ambiente:
  - `%ALLUSERSPROFILE%` seleziona la cartella in cui si trovano i dati comuni di tutti i profili utente. Ad esempio, `C:\ProgramData` o `C:\Documents and Settings\All Users`.
  - `%PROGRAMFILES%` seleziona la cartella `Programmi`. Ad esempio, `C:\Programmi`.
  - `%WINDIR%` seleziona la cartella `Windows`. Ad esempio, `C:\Windows`.

  È possibile utilizzare le variabili d'ambiente o una combinazione di variabili d'ambiente e testo. Ad esempio, per selezionare la cartella Java nella cartella Programmi del sistema, specificare: `%PROGRAMFILES%\Java`.

Linux

- Percorso completo per un file o una directory.

  Ad esempio, per eseguire il backup di `file.txt` sul volume `/dev/hda3` montato su `/home/usr/docs`, specificare `/dev/hda3/file.txt` o `/home/usr/docs/file.txt`.
- Regole predefinite:
  - `[All Profiles Folder]` seleziona `/home`. Per impostazione predefinita, in questa cartella sono archiviati tutti i profili utente.
  - `/home` seleziona la home directory degli utenti comuni.
  - `/root` seleziona la home directory dell'utente root.
  - `/usr` seleziona la directory per tutti i programmi correlati all'utente.
  - `/etc` seleziona la directory per i file di configurazione del sistema.

macOS

© Acronis International GmbH, 2003-2024

- Percorso completo per un file o una directory.

  Per esempio:
  - Per eseguire il backup del file `file.txt` nel desktop di un utente, specificare `/Users/<nome utente>/Desktop/file.txt`.
  - Per eseguire il backup delle cartelle `Desktop`, `Documenti` o `Download` di un utente, specificare rispettivamente `/Users/<nome utente>/Desktop`, `/Users/<nome utente>/Documenti` o `/Users/<nome utente>/Download`.
  - Per eseguire il backup delle home directory di tutti gli utenti che hanno un account in questo sistema, specificare `/Users`.
  - Per eseguire il backup della cartella in cui sono installate le applicazioni, specificare `/Applications`.
- Regole predefinite
  - `[All Profiles Folder]` seleziona `/Users`. Per impostazione predefinita, in questa cartella sono archiviati tutti i profili utente.

Selezione dello stato di sistema

Nota
Il backup dello stato del sistema è disponibile per i sistemi che eseguono Windows 7 e versioni successive nei quali è installato l'Agente per Windows. Il backup dello stato del sistema non è disponibile per le virtual machine il cui backup è eseguito al livello di hypervisor (backup agentless).

Per eseguire il backup dello stato del sistema, in **Cosa includere nel backup** selezionare **Stato del sistema**.

Un backup dello stato del sistema include i seguenti file:

- Configurazione di Attività pianificate
- Archivio metadati VSS
- Informazioni di configurazione del contatori delle prestazioni
- Servizio MSSearch
- Servizio trasferimento intelligente in background (BITS)
- Il registro
- Strumentazione gestione Windows (WMI)
- Data base di registrazione di Classe servizio componente

Selezione della configurazione ESXi

Il backup della configurazione di un host ESXi consente di ripristinare l'host ESXi da zero (bare metal). Il ripristino viene eseguito nel supporto di avvio.

© Acronis International GmbH, 2003-2024

Le macchine virtuali in esecuzione sull'host non sono incluse nel backup. Tali macchine possono essere sottoposte a backup e ripristinate separatamente.

Il backup della configurazione di un host ESXi include quanto segue:

- Il caricatore di avvio e le partizioni del banco di avvio dell'host.
- Lo stato dell'host (configurazione di networking e archivio virtuale, chiavi SSL, impostazioni di rete del server e informazioni dell'utente locale).
- Estensioni e patch installate o attivate temporaneamente nell'host.
- File di registro.

Prerequisiti

- SSH deve essere abilitato nel **Profilo di sicurezza** della configurazione host di ESXi.
- L'utente deve conoscere la password per l'account "radice" nell'host ESXi.

Limitazioni

- Il backup con configurazione ESXi non è supportato per gli host che eseguono VMware ESXi 7.0 e versioni successive.
- Non è possibile eseguire il backup di una configurazione ESXi nell'archivio nel cloud.

Per selezionare una configurazione di ESXi

1. Fare clic su **Dispositivi** > **Tutti i dispositivi**, quindi selezionare gli host ESXi di cui effettuare il backup.
2. Fare clic su **Proteggi**.
3. In **Cosa includere nel backup**, selezionare **Configurazione ESXi**.
4. In **Password radice di ESXi**, specificare una password per l'account "radice" su ogni host selezionato o applicare la stessa password a tutti gli host.

Protezione continua dei dati (CDP)

La funzionalità di Protezione continua dei dati (CDP) è parte del pacchetto Advanced Backup. Esegue il backup dei dati critici immediatamente dopo la modifica di tali dati, garantendo che nessuna modifica vada persa se il sistema subisce un guasto nel periodo che intercorre tra due backup pianificati. È possibile configurare la protezione continua dei dati per i seguenti dati:

- File o cartelle in posizioni specifiche
- File modificati con applicazioni specifiche

La protezione continua dei dati è supportata solo per i file system NTFS e per i sistemi operativi seguenti:

© Acronis International GmbH, 2003-2024

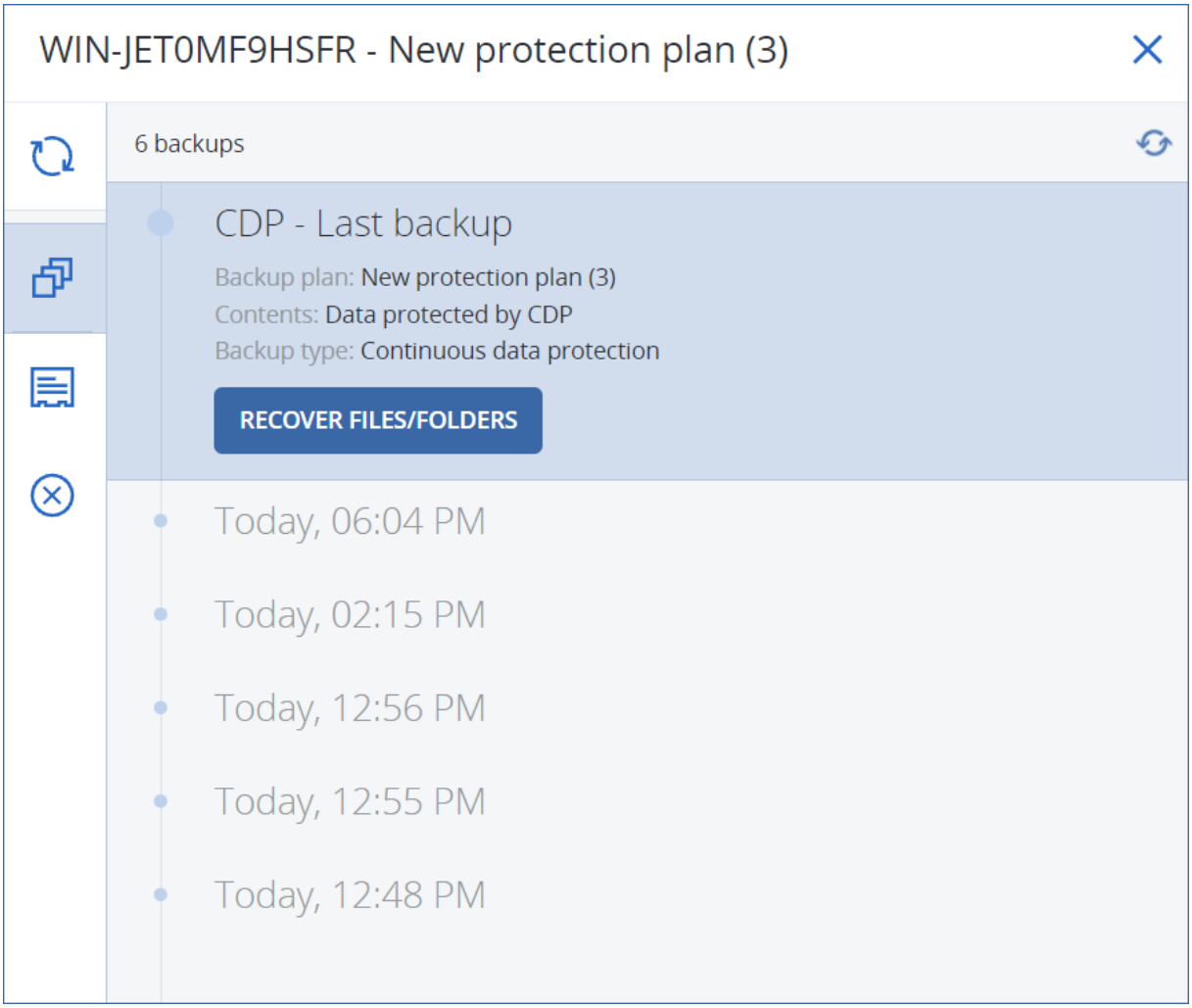
- Desktop: Windows 7 o versioni successive
- Server: Windows Server 2008 R2 e versioni successive

Sono supportate solo le cartelle locali. Non è possibile selezionare le cartelle di rete per la protezione continua dei dati.

La protezione continua dei dati non è compatibile con l'opzione **Backup dell'applicazione**.

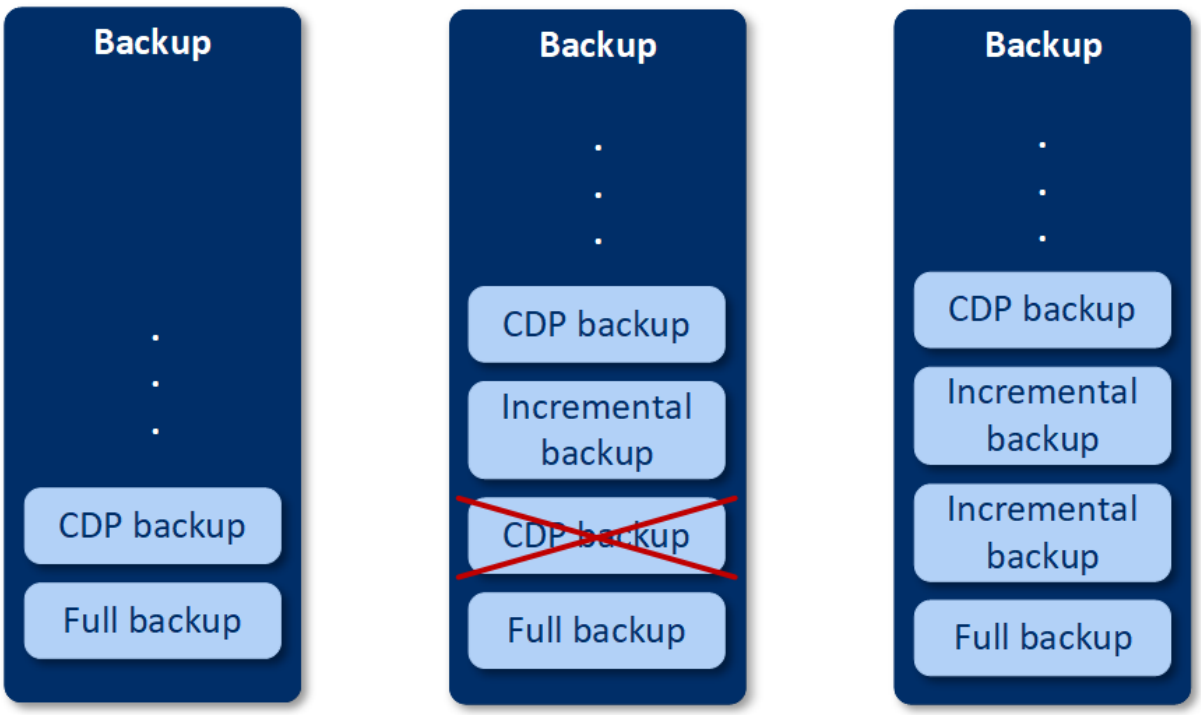
Come funziona

Le modifiche nei file e nelle cartelle monitorate con la protezione continua dei dati vengono salvate immediatamente in uno speciale backup CDP. In un set di backup è presente un solo backup CDP, ed è sempre il più recente.



Quando viene avviato un backup pianificato regolare, la protezione continua dei dati viene sospesa perché i dati più recenti devono essere inclusi nel backup pianificato. Al termine del backup pianificato, la protezione continua dei dati si riavvia, il backup CDP precedente viene eliminato e ne viene creato uno nuovo. Pertanto, il backup CDP sarà sempre il backup più recente del set di backup e conserverà soltanto lo stato più recente dei file o delle cartelle monitorate.

© Acronis International GmbH, 2003-2024



Se il sistema si arresta in modo anomalo durante un backup regolare, la protezione continua dei dati si riavvia automaticamente dopo il riavvio del sistema e crea un backup CDP sull'ultimo backup pianificato riuscito.

La protezione continua dei dati richiede la creazione di almeno un backup regolare prima del backup CDP. Per questa ragione, quando un piano di protezione con protezione continua dei dati viene eseguito per la prima volta, il sistema crea un backup completo e aggiunge immediatamente un backup CDP. Se si abilita l'opzione **Protezione continua dei dati** per un piano di protezione esistente, il backup CDP viene aggiunto al set di backup esistente.

Nota
La protezione continua dei dati è abilitata per impostazione predefinita nei piani di protezione creati nella scheda **Dispositivi**, se la funzionalità Advanced Backup è abilitata per l'utente e se non sono utilizzate altre funzionalità di Advanced Backup per i sistemi selezionati. Se già si dispone di un piano con protezione continua dei dati per un sistema selezionato, questa funzionalità non viene abilitata per impostazione predefinita per tale sistema nei nuovi piani creati.
La protezione continua dei dati non viene abilitata per impostazione predefinita nei piani creati per i gruppi di dispositivi.

Origini dati supportate

È possibile configurare la protezione continua dei dati per le origini dati seguenti:

- Intera macchina
- Dischi/volumi
- File/cartelle

© Acronis International GmbH, 2003-2024

Dopo aver selezionato l'origine dati nella sezione **Oggetto del backup** del piano di protezione, nella sezione **Elementi da proteggere continuativamente** selezionare i file, le cartelle o le applicazioni a sottoporre alla protezione continua dei dati. Per ulteriori informazioni su come configurare la protezione continua dei dati, fare riferimento a "Configurazione di un backup CDP" (pag. 419).

Destinazioni supportate

È possibile configurare la protezione continua dei dati per le destinazioni seguenti:

- Cartella locale
- Cartella di rete
- Archiviazione nel cloud
- Acronis Cyber Infrastructure
- Posizione definita da uno script

Nota
È possibile definire con un script solo le posizioni sopra elencate.

Configurazione di un backup CDP

È possibile configurare la Protezione continua dei dati nel modulo **Backup** di un piano di protezione. Per ulteriori informazioni su come creare un piano di protezione, fare riferimento a "Creazione di un piano di protezione" (pag. 218).

Per configurare le impostazioni di Protezione continua dei dati

1. Nel modulo **Backup** di un piano di protezione, abilitare l'opzione **Protezione continua dei dati (CDP)**.
   L'opzione è disponibile solo per le origini dati seguenti:
   - Intera macchina
   - Dischi/volumi
   - File/cartelle
2. In **Elementi da proteggere continuativamente**, configurare la protezione continua dei dati per **Applicazioni**, **File/cartelle** o entrambi.
   - Fare clic su **Applicazioni** per configurare il backup CDP per i file modificati da applicazioni specifiche.
     È possibile selezionare le applicazioni dalle categorie predefinite o aggiungere altre applicazioni specificando il percorso al file eseguibile dell'applicazione, ad esempio:
     - `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
     - `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`
   - Fare clic su **File/cartelle** per configurare il backup CDP per file in posizioni specifiche.

© Acronis International GmbH, 2003-2024

È possibile definire queste posizioni utilizzando le regole di selezione o selezionando direttamente i file e le cartelle.

- [Per tutti i sistemi] Per creare una regola di selezione utilizzare la casella di testo.

  È possibile utilizzare l'intero percorso ai file o percorsi con caratteri jolly (* e ?). L'asterisco sostituisce zero o più caratteri. Il punto di domanda sostituisce un singolo carattere.

  Importante
  Per creare il backup CDP di una cartella è necessario specificarne il contenuto utilizzando il carattere jolly asterisco:
  Percorso corretto: `D:\Data\*`
  Percorso non corretto: `D:\Data\`

- [Per sistemi online] Per selezionare direttamente file e cartelle:
  - In **Macchina da esplorare da** selezionare il sistema sul quale si trovano i file o le cartelle.
  - Fare clic su **Seleziona file e cartelle** per sfogliare il sistema selezionato.

    La selezione diretta consente di creare una regola di selezione. Se il piano di protezione viene applicato a più sistemi e la regola di selezione non è valida per un sistema, su tale sistema il piano verrà ignorato.

3. Nel riquadro del piano di protezione, fare clic su **Crea**.

A questo punto, il backup dei dati specificati verrà eseguito in modo continuativo negli intervalli tra i backup pianificati.

Selezione di una destinazione

Fare clic su **Dove eseguire il backup** e selezionare una delle seguenti opzioni:

- **Archiviazione nel cloud**

  I backup saranno archiviati nel datacenter sul cloud.
- **Cartelle locali**

  Se viene selezionato un solo sistema, passare a una cartella sul sistema in questione o digitare il percorso della cartella.

  Se sono selezionati più sistemi, digitare il percorso della cartella. I backup verranno archiviati in questa cartella su ciascuna delle macchine fisiche selezionate o sulla macchina in cui è installato l'agente per le macchine virtuali. Se la cartella non esiste, verrà creata.
- **Cartella di rete**

  Si tratta di una cartella condivisa mediante SMB/CIFS/DFS.

  Passare alla cartella condivisa richiesta o immettere il percorso nel seguente formato:
  - Per condivisioni SMB/CIFS: `\\<nome host>\<percorso>\` o `smb://<nome host>/<percorso>/`
  - Per condivisioni DFS: `\\<nome dominio DNS completo>\<root DFS>\<percorso>`

    Ad esempio, `\\esempio.azienda.com\condivisi\file`

© Acronis International GmbH, 2003-2024

Quindi, fare clic sul pulsante freccia. Se richiesto, specificare il nome utente e la password per la cartella condivisa. È possibile modificare queste credenziali in qualsiasi momento facendo clic sull'icona a forma di chiave accanto al nome della cartella.

L'esecuzione del backup in una cartella con accesso anonimo non è supportato.

- **Cloud pubblico**

  Questa opzione è parte del pacchetto Advanced Backup.

  Consente di configurare un backup diretto su uno storage compatibile nel cloud pubblico, senza che sia necessario distribuire componenti aggiuntivi (come Microsoft Azure o altre virtual machine come gateway). Selezionare e connettersi al cloud pubblico pertinente come necessario.

  Per ulteriori informazioni, consultare "Backup di workload su cloud pubblici" (pag. 548).

- **Cartella NFS** (disponibile per i sistemi che eseguono Linux o macOS)

  Verificare che il pacchetto nfs-utils sia installato nel server Linux in cui è installato l'Agente per Linux.

  Passare alla cartella NFS richiesta o immettere il percorso nel seguente formato:

  `nfs://<nome host>/<cartella esportata>:/<sottocartella>`

  Quindi, fare clic sul pulsante freccia.

  Nota
  Non è possibile eseguire il backup in una cartella NFS protetta da password.

- **Secure Zone** (disponibile se presente su ciascun sistema selezionato)

  Secure Zone è una partizione sicura su un disco del sistema sottoposto a backup. La partizione deve essere creata manualmente prima di configurare un backup. Per informazioni su come creare Secure Zone, nonché sui suoi limiti e vantaggi, fare riferimento a "Informazioni su Secure Zone" (pag. 422).

Opzione di archiviazione avanzata

Nota
Questa funzionalità è disponibile soltanto nell'edizione Advanced del servizio Cyber Protection.

Definita da uno script (disponibile per sistemi che eseguono Windows)

Consente di archiviare il backup di ogni sistema in una cartella definita da uno script. Il software supporta script scritti in JScript, VBScript o Python 3.5. Quando si distribuisce il piano di protezione, il software esegue lo script su ciascun sistema. L'output dello script per ogni sistema deve essere un percorso di cartella locale o di rete. Se la cartella non esiste, verrà creata (limitazioni: gli script scritti in Python non possono creare cartelle nelle condivisioni di rete). Nella scheda **Archivio di backup**, ogni cartella è visualizzata come una posizione di backup distinta.

In **Tipo di script**, selezionare il tipo di script (**JScript**, **VBScript** o **Python**) e quindi importare oppure copiare e incollare lo script. Per le cartelle di rete, specificare le credenziali di accesso con le autorizzazioni in lettura/scrittura.

Esempi:

© Acronis International GmbH, 2003-2024

- Il seguente script di JScript restituisce la posizione di backup di un sistema nel formato `\\bkpsrv\<nome sistema>`:

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  Di conseguenza, i backup di ciascun sistema verranno salvati in una cartella con lo stesso nome sul server **bkpsrv**.
- Il seguente script di JScript restituisce la posizione di backup in una cartella nel sistema in cui viene eseguito lo script:

  ```
  WScript.Echo("C:\\Backup");
  ```

  Di conseguenza, i backup di questo sistema verranno salvati nella cartella `C:\Backup` nello stesso sistema.

Nota
Il percorso alla posizione in questi script fa distinzione tra maiuscole e minuscole. Pertanto, `C:\Backup` e `C:\backup` vengono visualizzate come posizioni diverse nella console di Cyber Protect. Viene inoltre utilizzata la maiuscola per la lettera di unità.

Informazioni su Secure Zone

Secure Zone è una partizione sicura su un disco del sistema sottoposto a backup. Può archiviare backup di dischi o file del sistema interessato.

Qualora il disco presenti un difetto fisico, i backup posizionati in Secure Zone potrebbero essere perduti. È necessario pertanto che Secure Zone non sia l'unica posizione in cui un backup viene archiviato. In ambienti aziendali, Secure Zone può essere considerata una posizione intermedia in cui conservare i backup quando una posizione normalmente utilizzata non è temporaneamente disponibile o è connessa tramite un canale lento o saturo.

Perché utilizzare Secure Zone?

Secure Zone:

- Consente di ripristinare un disco nello stesso disco in cui risiede il backup.
- Costituisce un metodo pratico ed economico per proteggere i dati da malfunzionamenti software, attacchi di virus ed errori umani.
- Elimina la necessità di disporre di un supporto separato o di una connessione di rete per eseguire il backup o il ripristino dei dati. Questa caratteristica è particolarmente utile per gli utenti in roaming.
- Può fungere da destinazione primaria quando vengono utilizzate replicazioni di backup.

© Acronis International GmbH, 2003-2024

Limitazioni

- Non è possibile predisporre Secure Zone in un Mac.
- Secure Zone è una partizione su un disco di base. Non può essere predisposta su un disco dinamico o creata come volume logico (gestito da LVM).
- Secure Zone è formattata con il file system FAT32. Poiché FAT32 contempla un limite di dimensioni di file pari a 4 GB, i backup di dimensioni superiori vengono divisi quando sono salvati in Secure Zone. Ciò non influisce sulla procedura di ripristino e la velocità.

In che modo la creazione di Secure Zone trasforma il disco

- Secure Zone viene sempre creata alla fine del disco rigido.
- In mancanza di spazio o di spazio sufficiente non allocato alla fine del disco e nel caso in cui esista spazio non allocato tra i volumi, questi verranno spostati per aggiungere altro spazio non allocato alla fine del disco.
- Una volta raccolto tutto lo spazio non allocato, se questo non è sufficiente, il software sfrutterà lo spazio libero dai volumi selezionati, riducendone proporzionalmente le dimensioni.
- Lo spazio libero in un volume, tuttavia, dovrebbe consentire il funzionamento del sistema operativo e delle applicazioni, ad esempio per la creazione di file temporanei. Il software non ridurrà un volume in cui lo spazio libero sia o diventi inferiore al 25% della dimensione totale del volume. Solo quando tutti i volumi sul disco avranno il 25% di spazio libero o meno, il software proseguirà con la riduzione dei volumi in maniera proporzionale.

In base a quanto sopra indicato, appare evidente che l'impostazione della dimensione massima possibile di Secure Zone non è consigliabile. La conseguente assenza di spazio libero in un volume potrebbe causare instabilità del sistema operativo o delle applicazioni, che potrebbero perfino non avviarsi.

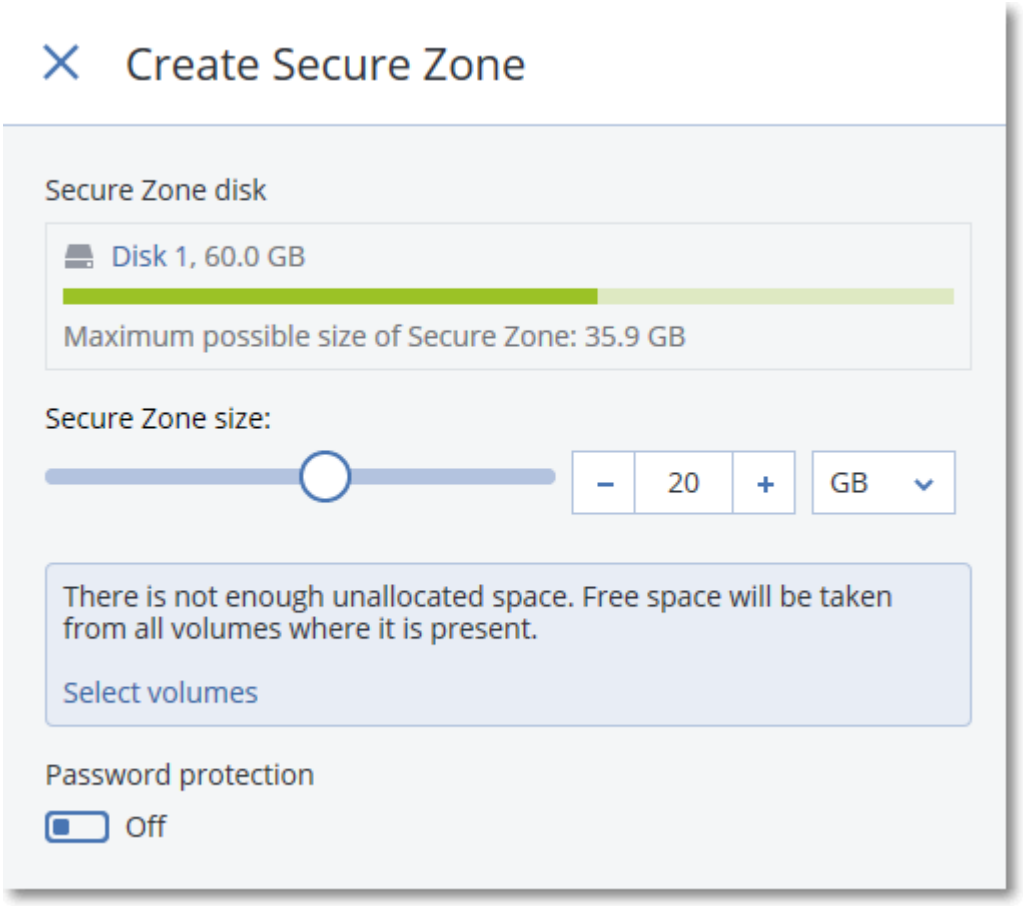
Importante
Lo spostamento o il ridimensionamento del volume da cui si è avviato il sistema richiede un riavvio.

Come creare Secure Zone

1. Selezionare il sistema in cui si desidera creare Secure Zone.
2. Fare clic su **Dettagli** > **Crea Secure Zone** .
3. Nel disco **Secure Zone**, fare clic su **Seleziona** e scegliere un disco rigido (se vi sono più dischi rigidi) in cui creare la zona.
   Il software calcola le dimensioni massime consentite di Secure Zone.
4. Immettere le dimensioni di Secure Zone o trascinare il dispositivo di scorrimento per selezionare una dimensione qualsiasi fra quella minima e quella massima.
   La dimensione minima è paria a circa 50 MB, a seconda della geometria del disco rigido. La dimensione massima è uguale allo spazio del disco non allocato a cui si aggiunge lo spazio libero totale su tutti i volumi di disco.

© Acronis International GmbH, 2003-2024

5. Se lo spazio non allocato non è sufficiente per le dimensioni specificate, il software sfrutterà lo spazio libero dai volumi esistenti. Per impostazione predefinita, sono selezionati tutti i volumi. Per escludere alcuni volumi, fare clic su **Seleziona volumi**. Altrimenti, ignorare questo passaggio.



6. [Facoltativo] Abilitare la **Protezione con password** e specificare una password.
   Sarà richiesta la password per accedere ai backup che si trovano in Secure Zone. Per eseguire backup in Secure Zone non è necessaria la password, tranne se il backup è eseguito in un supporto di avvio.
7. Fare clic su **Crea**.
   Il software visualizza il layout di partizione previsto. Fare clic su **OK**.
8. Attendere che il software crei Secure Zone.

Ora è possibile scegliere Secure Zone in **Dove eseguire il backup** quando si crea un piano di protezione.

Come eliminare Secure Zone

1. Selezionare un sistema con Secure Zone.
2. Fare clic su **Dettagli**.
3. Fare clic sull'icona ingranaggio accanto a **Secure Zone** , quindi scegliere **Elimina**.

© Acronis International GmbH, 2003-2024

4. [Facoltativo] Specificare i volumi a cui verrà aggiunto lo spazio liberato della zona. Per impostazione predefinita, sono selezionati tutti i volumi.
   Lo spazio verrà distribuito in modo equo tra i volumi selezionati. Se non si seleziona alcun volume, lo spazio liberato diventerà non allocato.
   Il ridimensionamento del volume da cui si è avviato il sistema richiede un riavvio.
5. Fare clic su **Elimina**.

Di conseguenza, Secure Zone verrà eliminata assieme a tutti i backup conservati al suo interno.

Pianificazione del backup

È possibile configurare un backup affinché venga eseguito a un orario specifico, a intervalli specifici o in seguito a un evento specifico.

I backup pianificati delle risorse non cloud-to-cloud vengono eseguiti in base alle impostazioni del fuso orario del workload nel quale è installato l'agente di protezione. Ad esempio, se si applica lo stesso piano di protezione a workload con impostazioni del fuso orario differenti, i backup si avvieranno in base al fuso orario locale di ogni workload.

La pianificazione di un backup prevede le azioni seguenti:

- Selezione di uno schema di backup
- Configurazione dell'orario o selezione dell'evento che attiva il backup
- Configurazione delle impostazioni facoltative e delle condizioni di avvio

Schemi di backup

Lo schema di backup è la parte della pianificazione di un piano di protezione che definisce quale tipo di backup (completo, differenziale o incrementale) viene creato e quando. È possibile scegliere uno schema di backup predefinito o crearne uno personalizzato.

I tipi e gli schemi di backup disponibili dipendono dalla posizione e dall'origine del backup. Ad esempio, il backup differenziale non è disponibile quando si esegue il backup di dati SQL o di Exchange o dello stato del sistema. Lo schema di backup **Sempre incrementale (a file singolo)** non è supportato per i dispositivi a nastro.

Schema di backup	Descrizione	Elementi configurabili
Sempre incrementale (a file singolo)	Il primo backup è completo; l'operazione può richiedere molto tempo. I backup successivi sono incrementali e richiedono meno tempo.	• Tipo di pianificazione: mensile, settimanale, giornaliera, oraria

© Acronis International GmbH, 2003-2024

Schema di backup	Descrizione	Elementi configurabili
	I backup utilizzano il formato di backup a file singolo[1]*. Per impostazione predefinita, i backup vengono eseguiti giornalmente dal lunedì al venerdì. Si consiglia di utilizzare questo schema quando si archiviano i backup nel cloud storage, perché i backup incrementali sono più veloci e generano meno traffico di rete.	• Condizione che attiva il backup: orario o evento • Ora di inizio • Condizioni di avvio • Opzioni aggiuntive
Sempre completo	Tutti i backup nel set di backup sono completi. Per impostazione predefinita, i backup vengono eseguiti giornalmente dal lunedì al venerdì.	• Tipo di pianificazione: mensile, settimanale, giornaliera, oraria • Condizione che attiva il backup: orario o evento • Ora di inizio • Condizioni di avvio • Opzioni aggiuntive
Settimanale completo, giornaliero incrementale	Una volta alla settimana viene creato un backup completo, tutti gli altri backup sono incrementali. Il primo backup è completo e gli altri backup durante la settimana sono incrementali; il ciclo quindi si ripete. Per selezionare il giorno della settimana in cui viene creato il backup completo settimanale, nel piano di protezione fare clic sull'icona ingranaggio, quindi passare a **Opzioni di backup** > **Backup settimanale**. Per impostazione predefinita, i backup vengono eseguiti giornalmente dal lunedì al venerdì.	• Condizione che attiva il backup: orario o evento • Ora di inizio • Condizioni di avvio • Opzioni aggiuntive
Mensile completo, Settimanale differenziale, Giornaliero incrementale (GFS)	Per impostazione predefinita, i backup incrementali vengono eseguiti ogni giorno dal lunedì al venerdì. I backup differenziali vengono eseguiti ogni sabato. I backup completi vengono eseguiti il primo giorno di ogni mese.	• Modificare la pianificazione esistente per tipo di backup: ◦ Tipo di

[1]Un nuovo formato di backup, in cui i backup incrementali completi e successivi vengono salvati su un unico file .tibx. Questo formato consente di sfruttare la velocità del metodo di backup incrementale, evitando tuttavia il suo principale svantaggio ovvero la difficoltà di eliminazione dei backup obsoleti. Il software contrassegna i blocchi utilizzati dai backup obsoleti come "liberi" e li utilizza per scrivere i nuovi backup. Ne consegue una pulizia estremamente rapida, con un consumo minimo delle risorse. Il formato di backup a file singolo non è disponibile quando si esegue il backup in posizioni che non supportano le modalità di lettura e scrittura con accesso casuale.

© Acronis International GmbH, 2003-2024

Schema di backup	Descrizione	Elementi configurabili
	Nota Questo è uno schema personalizzato predefinito. Nel piano di protezione, viene visualizzato come **Personalizzato**.	pianificazione: mensile, settimanale, giornaliera, oraria ◦ Condizione che attiva il backup: orario o evento ◦ Ora di inizio ◦ Condizioni di avvio ◦ Opzioni aggiuntive • Aggiungere nuove pianificazioni per tipo di backup
Personalizzato	È necessario selezionare i tipi di backup (completo, differenziale e incrementale) e configurare una pianificazione distinta per ogni tipo*.	• Modificare la pianificazione esistente per tipo di backup: ◦ Tipo di pianificazione: mensile, settimanale, giornaliera, oraria ◦ Condizione che attiva il backup: orario o evento ◦ Ora di inizio ◦ Condizioni di avvio ◦ Opzioni aggiuntive • Aggiungere nuove pianificazioni per tipo di backup

* Dopo aver creato un piano di protezione, non è possibile passare dallo schema **Sempre incrementale (a file singolo)** ad altri schemi di backup e viceversa. **Sempre incrementale (a file singolo)** è un formato con un singolo file, mentre il resto degli schemi hanno un formato composto da più file. Per passare da un formato all'altro, creare un nuovo piano di protezione.

Tipi di backup

Sono disponibili i seguenti tipi di backup:

- Completo: un backup completo contiene tutti i dati di origine. Si tratta di un backup autosufficiente. Per recuperare i dati, non è necessario accedere ad altri backup.

© Acronis International GmbH, 2003-2024

Nota
Il primo backup creato da qualunque piano di protezione è un backup completo.

- Incrementale: in un backup incrementale vengono archiviate le modifiche apportate ai dati rispetto all'ultimo backup, indipendentemente dal fatto che quest'ultimo backup sia completo, differenziale o incrementale. Per recuperare i dati, è necessaria l'intera catena di backup da cui dipende il backup incrementale, risalendo fino al backup completo iniziale.
- Differenziale: in un backup differenziale vengono archiviate le modifiche apportate ai dati rispetto all'ultimo backup completo. Per recuperare i dati, è necessario disporre sia del backup differenziale che del corrispondente backup completo da cui dipende il backup differenziale.

Esecuzione di un backup da una pianificazione

Per eseguire automaticamente un backup a un'ora specifica o in seguito a un evento specifico, è necessario abilitare un pianificazione nel piano di protezione.

Per abilitare una pianificazione

1. In un piano di protezione, espandere il modulo **Backup**.
2. Fare clic su **Pianificazione**.
3. Abilitare l'interruttore della pianificazione.
4. Selezionare lo schema di backup.
5. Configurare la pianificazione come necessario, quindi fare clic su **Fine**.
   Per ulteriori informazioni sulle opzioni di pianificazione disponibili, consultare "Pianificazione per eventi" (pag. 431) e "Pianificazione oraria" (pag. 429).
6. [Facoltativo] Configurare le condizioni di avvio o altre opzioni di pianificazione.
7. Salvare il piano di protezione.

L'operazione di backup si avvia ogni volta che le condizioni pianificate vengono soddisfatte.

Per disabilitare una pianificazione

1. In un piano di protezione, espandere il modulo **Backup**.
2. Fare clic su **Pianificazione**.
3. Disabilitare l'interruttore della pianificazione.
4. Salvare il piano di protezione.

L'operazione di backup potrà essere avviata solo manualmente.

Nota
Se la pianificazione è disabilitata, le regole di conservazione non vengono applicate automaticamente. Per applicare le regole, eseguire il backup manualmente.

© Acronis International GmbH, 2003-2024

Pianificazione oraria

La tabella seguente riepiloga le opzioni di pianificazione basate sull'orario. La disponibilità di queste opzioni dipende dallo schema di backup. Per ulteriori informazioni, consultare "Schemi di backup" (pag. 425).

Opzione	Descrizione	Esempi
Ogni mese	Selezionare i mesi, i giorni del mese o i giorni della settimana, quindi indicare l'ora di avvio del backup.	Esegui il backup il 1 gennaio e il 3 febbraio alle 12:00. Esegui il backup il primo giorno di ogni mese alle 10:00. Esegui il backup il 1 marzo, il 5 marzo, il 1 aprile e il 5 aprile alle 09:00. Esegui il backup il secondo e il terzo venerdì di ogni mese alle 11:00. Esegui il backup l'ultimo mercoledì del mese alle 10:30.
Ogni settimana	Selezionare i giorni della settimana, quindi indicare l'ora di avvio del backup.	Esegui il backup da lunedì a venerdì alle 10:00. Esegui il backup il lunedì alle 11:00. Esegui il backup il martedì e il sabato alle 08:00.
Ogni giorno	Selezionare i giorni (ogni giorno o solo nel fine settimana), quindi indicare l'ora di avvio del backup.	Esegui il backup ogni giorno alle 11:45. Esegui il backup da lunedì a venerdì alle 09:30.
Ogni ora	Selezionare i giorni della settimana, quindi indicare un intervallo orario tra due backup consecutivi e l'intervallo di tempo entro il quale deve essere eseguito il backup. Quando si configura l'intervallo in minuti, è possibile selezionare un intervallo suggerito tra 10 e 60 minuti, oppure specificarne uno personalizzato, ad esempio 45 o 75 minuti.	Esegui il backup ogni ora tra le 08:00 e le 18:00, da lunedì a venerdì. Esegui il backup ogni 3 ore tra le 01:00 e le 18:00, il sabato e la domenica.

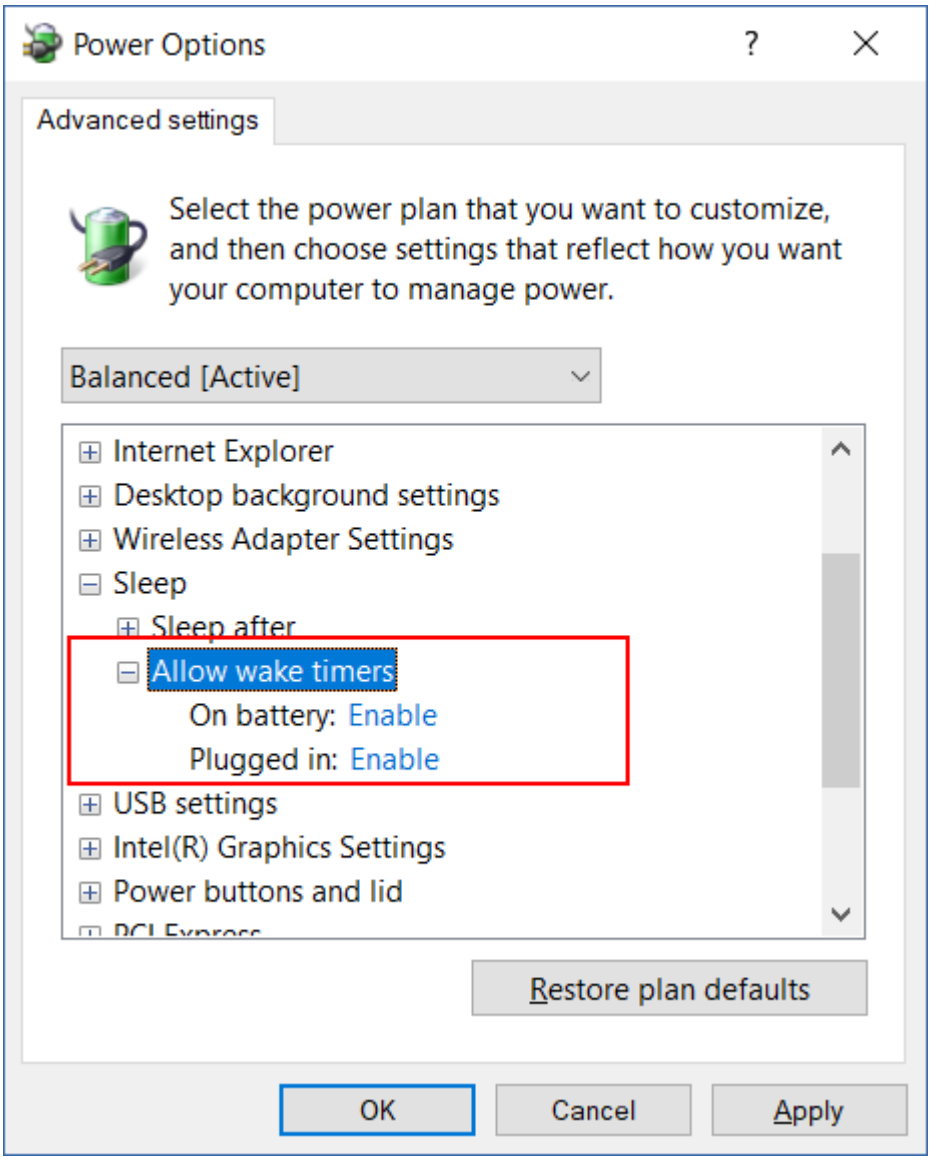
Opzioni aggiuntive

Quando si pianifica un backup in base alla data e all'ora, sono disponibili le opzioni di pianificazione aggiuntive seguenti.

© Acronis International GmbH, 2003-2024

Per accedere a queste opzioni, nel pannello **Pianificazione**, fare clic su **Mostra altro**.

- **Se la macchina è spenta, esegui le attività mancanti all'avvio della macchina**
  Impostazione predefinita: Disabilitata.
- **Impedisci la modalità di sospensione o ibernazione durante il backup**
  Questa opzione è applicabile solo ai sistemi che eseguono Windows.
  Impostazione predefinita: Abilitata.
- **Riattiva dalla modalità di sospensione o ibernazione per avviare un backup pianificato**
  Questa opzione è applicabile solo ai sistemi che eseguono Windows nei cui profili di risparmio energetico è abilitata l'opzione **Consenti timer di riattivazione**.



  Questa opzione non utilizza la funzionalità Wake-on-LAN e non è applicabile ai sistemi spenti.
  Impostazione predefinita: Disabilitata.

© Acronis International GmbH, 2003-2024

Pianificazione per eventi

Per configurare l'esecuzione di un backup in concomitanza con un evento specifico, selezionare una delle seguenti opzioni.

Opzione	Descrizione	Esempi
A un tempo stabilito dall'ultimo backup	Il backup si avvia dopo il periodo specificato successivo all'ultimo backup completato correttamente. **Nota** Questa opzione dipende da come è stato completato il backup precedente. Se il backup non è riuscito, quello successivo non si avvia automaticamente. In questo caso, è necessario eseguire il backup manualmente e verificare che venga completato correttamente, per poi ripristinare la pianificazione.	Esegui il backup un giorno dopo l'ultimo backup completato correttamente. Esegui il backup quattro ore dopo l'ultimo backup completato correttamente.
Quando un utente accede al sistema	Il backup si avvia quando un utente accede al sistema. È possibile configurare questa opzione per qualsiasi accesso o per l'accesso di un utente specifico. **Nota** L'accesso con un profilo utente temporaneo non avvia il backup.	Esegui il backup all'accesso dell'utente John Doe.
Quando un utente si disconnette dal sistema	Il backup si avvia quando un utente si disconnette dal sistema. È possibile configurare questa opzione per qualsiasi disconnessione o per la disconnessione di un utente specifico. **Nota** La disconnessione da un profilo utente temporaneo non avvia il backup. L'arresto di un sistema non avvia il backup.	Esegui il backup quando qualsiasi utente si disconnette.
All'avvio del sistema	Il backup viene eseguito all'avvio del sistema protetto.	Esegui il backup quando un utente avvia il sistema.
All'arresto del	Il backup viene eseguito all'arresto del	Esegui il backup quando un utente

© Acronis International GmbH, 2003-2024

Opzione	Descrizione	Esempi
sistema	sistema protetto.	arresta il sistema.
All'evento Registro eventi di Windows	Il backup viene eseguito quando si verifica l'evento Windows specificato.	Esegui il backup quando l'7 di tipo errore e l'origine disco vengono registrati nel registro di sistema di Windows.

La disponibilità di queste opzioni dipende dall'origine del backup e dal sistema operativo dei workload protetti. La tabella seguente riepiloga le opzioni disponibili per Windows, Linux e macOS.

Evento	Origine del backup (Cosa includere nel backup)					
	Intera macchina, Dischi/volumi o File/cartelle (sistemi fisici)	**Intera macchina o Dischi/Volumi (virtual machine)**	**Configurazione ESXi**	**Caselle di posta di Microsoft 365**	**Database e caselle di posta di Exchange**	**Database SQL**
A un tempo stabilito dall'ultimo backup	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Quando un utente accede al sistema	Windows	N/D	N/D	N/D	N/D	N/D
Quando un utente si disconnette dal sistema	Windows	N/D	N/D	N/D	N/D	N/D
All'avvio del sistema	Windows, Linux, macOS	N/D	N/D	N/D	N/D	N/D
All'arresto del sistema	Windows	N/D	N/D	N/D	N/D	N/D
All'evento Registro eventi di Windows	Windows	N/D	N/D	Windows	Windows	Windows

© Acronis International GmbH, 2003-2024

All'evento Registro eventi di Windows

È possibile eseguire automaticamente un backup quando un evento specifico viene registrato in un registro eventi di Windows, ad esempio il registro applicazioni, il registro di sicurezza o il registro di sistema.

Nota
È possibile sfogliare gli eventi e visualizzarne le proprietà in **Gestione computer** > **Visualizzatore eventi** di Windows. Per aprire il registro di sicurezza, è necessario disporre dei diritti di amministratore.

Parametri evento

La tabella seguente riepiloga i parametri che è necessario specificare durante la configurazione dell'opzione **All'evento Registro eventi di Windows**.

Parametro	Descrizione
Nome registro	Il nome del registro. Selezionare il nome di un registro standard (Applicazione, Sicurezza o Sistema) dall'elenco o specificare un altro nome di registro, ad esempio Sessioni di Microsoft Office
Origine evento	L'origine evento indica il programma o la componente di sistema che ha causato l'evento, ad esempio, disco. Qualsiasi origine evento che contiene la stringa di testo specificata attiverà il backup pianificato. L'opzione non distingue tra maiuscole e minuscole. Se, ad esempio, si specifica la stringa `service`, entrambe le origini evento Service Control Manager e Time-Service attiveranno il backup.
Tipo di evento	Tipo di evento: Errore, Attenzione, Informazione, Audit riuscito o Audit fallito.
ID evento	L'ID dell'evento identifica un tipo di evento specifico nell'ambito di un'origine evento. Ad esempio, un evento Errore con origine evento disco e ID Evento 7 si verifica quando Windows rileva un blocco danneggiato in un disco, mentre un evento Errore con origine evento disco e ID Evento 15 si verifica quando un disco non è ancora pronto per l'accesso.

Esempio: Backup di emergenza in caso di blocchi danneggiati sul disco rigido

Uno o più blocchi danneggiati su un'unità disco rigido possono indicare un guasto imminente. Per questo motivo, è possibile creare un backup quando viene rilevato un blocco danneggiato.

© Acronis International GmbH, 2003-2024

Se Windows rileva un blocco danneggiato in un disco, nel registro di sistema viene registrato un evento di errore con origine evento disco e numero di evento 7. Nel piano di protezione, configurare la pianificazione seguente:

- Pianifica: All'evento Registro eventi di Windows
- Nome registro: Sistema
- Origine evento: disco
- Tipo di evento: Errore
- ID evento: 7

Importante
Per garantire che il backup venga completato malgrado i blocchi danneggiati, in **Opzioni di backup** passare a **Gestione degli errori** e selezionare la casella di controllo **Ignora settori danneggiati**.

Condizioni di avvio

Affinché un backup venga eseguito solo se sono soddisfatte alcune condizioni specifiche, configurare una o più condizioni di avvio. Se si configurano più condizioni, è necessario che tutte vengano soddisfatte contemporaneamente affinché il backup si avvii. È possibile specificare un periodo dopo il quale i backup verranno eseguiti, indipendentemente dal fatto che le condizioni siano state soddisfatte. Per ulteriori informazioni su questa opzione di backup, consultare "Condizioni di avvio dell'attività" (pag. 498).

Le condizioni di avvio non sono applicabili quando si avvia un backup manualmente.

Nella tabella seguente sono elencate le condizioni di avvio disponibili per vari dati su Windows, Linux e macOS.

Condizione di avvio	Origine del backup (Cosa includere nel backup)					
	Intera macchina, Dischi/volumi o File/cartelle (sistemi fisici)	**Intera macchina o Dischi/volumi (virtual machine)**	**Configurazione ESXi**	**Caselle di posta di Microsoft 365**	**Database e caselle di posta di Exchange**	**Database SQL**
L'utente è inattivo	Windows	N/D	N/D	N/D	N/D	N/D
Host della posizione di backup disponibile	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Utenti	Windows	N/D	N/D	N/D	N/D	N/D

© Acronis International GmbH, 2003-2024

Condizione di avvio	Origine del backup (Cosa includere nel backup)					
	Intera macchina, Dischi/volumi o File/cartelle (sistemi fisici)	**Intera macchina o Dischi/volumi (virtual machine)**	**Configurazione ESXi**	**Caselle di posta di Microsoft 365**	**Database e caselle di posta di Exchange**	**Database SQL**
disconnessi						
Rientra nell'intervallo di tempo	Windows, Linux, macOS	Windows, Linux	N/D	N/D	N/D	N/D
Risparmia carica della batteria	Windows	N/D	N/D	N/D	N/D	N/D
Non avviare se è attiva una connessione a consumo	Windows	N/D	N/D	N/D	N/D	N/D
Non avviare se è attiva la connessione alle reti Wi-Fi seguenti	Windows	N/D	N/D	N/D	N/D	N/D
Controlla gli indirizzi IP del dispositivo	Windows	N/D	N/D	N/D	N/D	N/D

L'utente è inattivo

"L’utente è inattivo" indica che uno screen saver è in esecuzione nella macchina o che la macchina è bloccata.

Esempio

Esegui il backup ogni giorno alle 21:00, preferibilmente quando l'utente è inattivo. Se l'utente è ancora attivo alle 23:00, esegui comunque il backup.

- Pianifica: **Ogni giorno**, **Esegui ogni giorno**. Ora avvio: **21:00**.
- Condizione: **L’utente è inattivo**.

© Acronis International GmbH, 2003-2024

- Condizioni di avvio del backup: **Attendi quando le condizioni sono soddisfatte**, **Esegui comunque l'attività dopo 2** ore.

Di conseguenza:

- Se l'utente è inattivo prima delle 21:00, il backup viene avviato alle 21:00.
- Se l'utente diventa inattivo tra le 21:00 e le 23:00, il backup viene avviato immediatamente.
- Se l'utente è ancora attivo alle 23:00, il backup viene avviato alle 23:00.

Host della posizione di backup disponibile

"Host della posizione di backup disponibile" indica che il sistema che ospita la posizione del backup è disponibile in rete.

Questa condizione è applicabile alle cartelle di rete, al cloud storage e alle posizioni gestite da un nodo di storage.

Questa condizione non riguarda la disponibilità della posizione in sé, ma solo della disponibilità dell'host. Ad esempio, se l'host è disponibile, ma la cartella di rete in esso contenuta non è condivisa o le credenziali della cartella non sono più valide, la condizione viene comunque considerata soddisfatta.

Esempio

I backup vengono eseguiti in una cartella di rete ogni giorno feriale alle 21:00. Se il sistema che ospita la cartella non è disponibile in quel momento (ad esempio, a causa di operazioni di manutenzione), è possibile ignorare il backup e attendere l'avvio pianificato nel giorno feriale successivo.

- Pianifica: **Ogni giorno**, **Esegui da lunedì a venerdì**. Ora avvio: **21:00**.
- Condizione: **Host della posizione di backup disponibile**
- Condizioni di avvio del backup: **Ignora il backup pianificato**.

Di conseguenza:

- Se alle 21:00 l'host è disponibile, il backup inizia immediatamente.
- Se alle 21:00 l'host non è disponibile, il backup inizia il giorno feriale successivo (se l'host è disponibile all'orario indicato).
- Se l'host non è mai disponibile nei giorni lavorativi alle 21:00, il backup non viene mai avviato.

Utenti disconnessi

Utilizzare questa condizione di avvio per posticipare un backup fino a quando tutti gli utenti si disconnettono da un sistema Windows.

© Acronis International GmbH, 2003-2024

Esempio

Si esegue il backup alle 20:00 ogni venerdì, preferibilmente quando tutti gli utenti sono disconnessi. Se uno degli utenti è ancora connesso alle 23:00, il backup viene comunque eseguito.

- Pianifica: **Ogni settimana**, il venerdì. Ora avvio: **20:00**.
- Condizione: **Utenti disconnessi**.
- Condizioni di avvio del backup: **Attendi quando le condizioni sono soddisfatte**, **Avvia comunque il backup dopo 3** ore.

Di conseguenza:

- Se tutti gli utenti sono disconnessi alle 20:00, il backup viene avviato alle 20:00.
- Se l'ultimo utente si disconnette tra le 20:00 e le 23:00, il backup viene avviato immediatamente.
- Se sono ancora presenti utenti connessi alle 23:00, il backup viene avviato alle 23:00.

Rientra nell'intervallo di tempo

Utilizzare questa condizione di avvio per limitare l'avvio del backup a un intervallo di tempo specificato.

Esempio

Una società esegue il backup di server e dati utente su diverse posizioni nella stessa NAS (Network Attached Storage).

La giornata di lavoro inizia alle 8:00 e termina alle 17:00. I dati utente devono essere sottoposti a backup non appena l'utente si disconnette, ma non prima delle 16:30.

Tutti i giorni alle 23:00 viene eseguito il backup di tutti i server della società. Pertanto, i dati di tutti gli utenti devono essere preferibilmente sottoposti a backup prima delle 23:00, al fine di rendere disponibile la larghezza di banda della rete per i backup dei server.

Si presume che il backup dei dati degli utenti non richieda più di un'ora, per cui l'ultimo backup ha inizio alle 22:00. Se un utente è ancora connesso durante l'intervallo di tempo specificato, oppure se si disconnette in qualsiasi altro momento, il backup dei relativi dati viene ignorato.

- Evento: **Quando un utente si disconnette dal sistema**. Specificare l'account utente: **Tutti gli utenti**.
- Condizione: **Rientra nell'intervallo di tempo** dalle **16:30** alle **22:00**.
- Condizioni di avvio del backup: **Ignora il backup pianificato**.

Di conseguenza:

- Se l'utente si disconnette tra le 16:30 e le 22:00, il backup viene avviato immediatamente.
- Se l'utente si disconnette in qualsiasi altro momento, il backup viene ignorato.

© Acronis International GmbH, 2003-2024

Risparmia carica della batteria

Utilizzare questa condizione di avvio per impedire l'esecuzione del backup se il sistema (ad esempio un portatile o tablet) non è collegato a una fonte di alimentazione. A seconda del valore impostato per l'opzione di backup Condizioni di avvio del backup, il backup ignorato viene avviato o meno dopo il collegamento del sistema a una fonte di alimentazione.

Sono disponibili le seguenti opzioni:

- **Non avviare se è attiva l'alimentazione con batteria**
  Il backup viene avviato solo se il sistema è collegato a una fonte di alimentazione.
- **Avvia se è attiva l'alimentazione con batteria e il livello della batteria è superiore a**
  Il backup viene avviato se il sistema è collegato a una fonte di alimentazione o se il livello della batteria è superiore al valore specificato.

Esempio

Il backup dei dati viene eseguito ogni giorno feriale alle 21:00. Se il sistema non è collegato a una fonte di alimentazione, è possibile ignorare il backup per risparmiare la carica della batteria e attendere che il sistema venga collegato a una fonte di alimentazione.

- Pianifica: **Ogni giorno**, **Esegui da lunedì a venerdì**. Ora avvio: **21:00**.
- Condizione: **Risparmia carica della batteria**, **Non avviare se è attiva l'alimentazione con batteria**.
- Condizioni di avvio del backup: **Attendi fino a quando le condizioni sono soddisfatte**.

Di conseguenza:

- Se alle 21:00 il sistema è collegato a una fonte di alimentazione, il backup viene avviato immediatamente.
- Se alle 21:00 il sistema è collegato alla batteria, il backup viene avviato non appena il sistema è collegato a una fonte di alimentazione.

Non avviare se è attiva una connessione a consumo

Utilizzare questa condizione di avvio per impedire l'esecuzione di un backup (incluso il backup su disco locale) se il sistema è connesso a Internet tramite una connessione impostata come "a consumo" in Windows. Per ulteriori informazioni sulle connessioni a consumo in Windows, fare riferimento a https://support.microsoft.com/it-it/help/17452/windows-metered-internet-connections-faq.

La condizione di avvio aggiuntiva **Non avviare se è attiva la connessione alle reti Wi-Fi seguenti** viene abilitata automaticamente quando si abilita la condizione **Non avviare se è attiva una connessione a consumo**. Questa misura aggiuntiva impedisce l'esecuzione dei backup su hotspot mobile. Per impostazione predefinita sono specificati i seguenti nomi di rete: android, telefono, mobile e modem.

© Acronis International GmbH, 2003-2024

Per eliminare questi nomi dall'elenco, fare clic sul segno X. Per aggiungere un nuovo nome, digitarlo nel campo vuoto.

Esempio

Il backup dei dati viene eseguito ogni giorno feriale alle 21:00. Se il sistema è connesso a Internet tramite una connessione a consumo, è possibile ignorare il backup per risparmiare traffico di rete e attendere l'avvio del backup pianificato per il giorno feriale successivo.

- Pianifica: **Ogni giorno**, **Esegui da lunedì a venerdì**. Ora avvio: **21:00**.
- Condizione: **Non avviare se è attiva una connessione a consumo**.
- Condizioni di avvio del backup: **Ignora il backup pianificato**.

Di conseguenza:

- Se alle 21:00 il sistema non è connesso a Internet tramite una connessione a consumo, il backup viene avviato immediatamente.
- Se alle 21:00 il sistema è connesso a Internet tramite una connessione a consumo, il backup viene avviato il giorno feriale successivo.
- Se alle 21:00 dei giorni feriali il sistema è sempre connesso a Internet tramite una connessione a consumo, il backup non viene mai avviato.

Non avviare se è attiva la connessione alle reti Wi-Fi seguenti

Utilizzare questo condizione di avvio per impedire l'esecuzione di un backup (incluso il backup su disco locale) se il sistema è connesso a una qualsiasi delle reti wireless specificate (ad esempio, per limitare l'esecuzione dei backup tramite un hotspot mobile).

È possibile specificare i nomi delle reti Wi-Fi, anche noti come identificatori del set di servizi (SSID). La limitazione si applica a tutte le reti che contengono nel proprio nome il nome specificato come stringa secondaria, senza distinzione tra maiuscole e minuscole. Se, ad esempio, si specifica `phone` come nome della rete, il backup non si avvia quando il sistema è connesso a una qualsiasi delle reti seguenti: `John's iPhone`, `phone_wifi` oppure `my_PHONE_wifi`.

La condizione di avvio **Non avviare se è attiva la connessione alle reti Wi-Fi seguenti** viene abilitata automaticamente quando si abilita la condizione **Non avviare se è attiva una connessione a consumo**. Per impostazione predefinita sono specificati i seguenti nomi di rete: android, `telefono`, `mobile` e modem.

Per eliminare questi nomi dall'elenco, fare clic sul segno X. Per aggiungere un nuovo nome, digitarlo nel campo vuoto.

Esempio

Il backup dei dati viene eseguito ogni giorno feriale alle 21:00. Se il sistema è connesso a Internet tramite hotspot mobile, è possibile ignorare il backup e attendere l'avvio del backup pianificato per il giorno feriale successivo.

© Acronis International GmbH, 2003-2024

- Pianifica: **Ogni giorno**, **Esegui da lunedì a venerdì**. Ora avvio: **21:00**.
- Condizione: **Non avviare se è attiva la connessione alle reti seguenti**, **Nome rete**: `<SSID della rete hotspot>`
- Condizioni di avvio del backup: **Ignora il backup pianificato**.

Di conseguenza:

- Se alle 21:00 il sistema non è connesso alla rete specificata, il backup viene avviato immediatamente.
- Se alle 21:00 il sistema non è connesso alla rete specificata, il backup viene avviato il giorno feriale successivo.
- Se alle 21:00 dei giorni feriali il sistema è sempre connesso alla rete specificata, il backup non viene mai avviato.

Controlla gli indirizzi IP del dispositivo

Utilizzare questa condizione di avvio per impedire l'esecuzione di un backup (incluso il backup su disco locale) se uno qualsiasi degli indirizzi IP del sistema rientra o non rientra nell'intervallo di indirizzi IP specificato. In questo modo, ad esempio, è possibile evitare carichi di transito di dati di grandi dimensioni durante il backup di sistemi i cui utenti sono a grande distanza, o evitare l'esecuzione dei backup su una connessione VPN (Virtual Private Network).

Sono disponibili le seguenti opzioni:

- **Avvia se è fuori dall'intervallo IP**
- **Avvia se rientra nell'intervallo IP**

Per ogni opzione è possibile specificare più intervalli. Sono supportati solo indirizzi IPv4.

Esempio

Il backup dei dati viene eseguito ogni giorno feriale alle 21:00. Se il sistema è connesso alla rete aziendale tramite un tunnel VPN, è possibile ignorare il backup.

- Pianifica: **Ogni giorno**, **Esegui da lunedì a venerdì**. Inizia alle **21:00**.
- Condizione: **Controlla gli indirizzi IP del dispositivo**, **Avvia se è fuori dall'intervallo IP**, **Da**: `<inizio dell'intervallo di indirizzi IP VPN>`, **A**: `<fine dell'intervallo di indirizzi IP VPN>`.
- Condizioni di avvio del backup: **Attendi fino a quando le condizioni sono soddisfatte**.

Di conseguenza:

- Se alle 21:00 l'indirizzo IP del sistema non rientra nell'intervallo specificato, il backup viene avviato immediatamente.
- Se alle 21:00 l'indirizzo IP del sistema rientra nell'intervallo specificato, il backup viene avviato non appena il sistema ottiene un indirizzo IP non VPN.
- Se alle 21:00 dei giorni feriali l'indirizzo IP del sistema è sempre nell'indirizzo specificato, il backup non viene mai avviato.

© Acronis International GmbH, 2003-2024

Ulteriori opzioni di pianificazione

È possibile configurare i backup affinché vengano eseguiti solo se sono soddisfatte alcune condizioni specifiche, solo durante un periodo specificato o con un ritardo specificato rispetto alla pianificazione.

Per configurare le condizioni di avvio

1. In un piano di protezione, espandere il modulo **Backup**.
2. Fare clic su **Pianificazione**.
3. Nel pannello **Pianificazione**, fare clic su **Mostra altro**.
4. Selezionare le caselle di controllo accanto alle condizioni di avvio da includere, quindi fare clic su **Fine**.
   Per ulteriori informazioni sulle condizioni di avvio disponibili e su come configurarle, consultare "Condizioni di avvio" (pag. 434).
5. Salvare il piano di protezione.

Per configurare un intervallo di tempo

1. In un piano di protezione, espandere il modulo **Backup**.
2. Fare clic su **Pianificazione**.
3. Selezionare la casella di controllo **Esegui il piano in un intervallo di date**.
4. Specificare il periodo in base alle esigenze e quindi fare clic su **Fine**.
5. Salvare il piano di protezione.

L'operazione di backup viene eseguita solo durante il periodo specificato.

Per configurare un ritardo

Per evitare un carico eccessivo sulla rete quando si esegue il backup di più workload su una posizione di rete, come opzione di backup è configurato un lieve ritardo casuale. È possibile abilitare o modificare questa impostazione.

1. In un piano di protezione, espandere il modulo **Backup**.
2. Fare clic su **Opzioni di backup**, quindi selezionare **Programmazione**.
   Il valore di ritardo per ciascun workload viene selezionato in maniera casuale in un intervallo compreso tra zero e il valore massimo specificato dall'utente. Per impostazione predefinita il valore massimo è 30 minuti.
   Per ulteriori informazioni su questa opzione di backup, consultare "Programmazione" (pag. 496)
   Il valore di ritardo per ciascun workload viene calcolato quando il piano di protezione viene applicato al workload e rimane invariato fino a quando non si modifica il valore di ritardo massimo.

© Acronis International GmbH, 2003-2024

3. Specificare il periodo in base alle esigenze e quindi fare clic su **Fine**.
4. Salvare il piano di protezione.

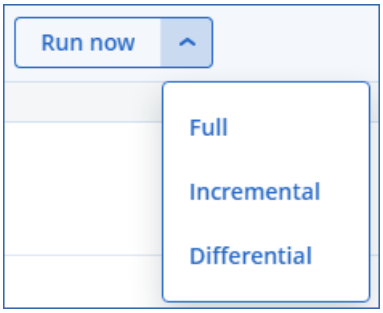
Esecuzione manuale di un backup

È possibile eseguire manualmente i backup pianificati e non pianificati.

Per eseguire un backup manualmente

1. Nella console di Cyber Protect, passare a **Dispositivi**.
2. Selezionare il workload di cui eseguire il backup, quindi fare clic su **Proteggi**.
3. Selezionare il piano di protezione che deve creare il backup.
   Se al workload non è applicato alcun piano di protezione, applicare un piano esistente o crearne uno nuovo.
   Per ulteriori informazioni su come creare un piano di protezione, consultare "Creazione di un piano di protezione" (pag. 218).
4. [Per creare il tipo di backup predefinito] Nel piano di protezione, fare clic sull'icona **Esegui ora**.

   In alternativa, nel piano di protezione espandere il modulo **Backup**, quindi fare clic sul pulsante **Esegui ora**.
5. [Per creare un tipo di backup specifico] Nel piano di protezione, espandere il modulo **Backup**, fare clic sulla freccia accanto al pulsante **Esegui ora**, quindi selezionare il tipo di backup.



Nota
La selezione del tipo non è disponibile per gli schemi di backup che utilizzano un solo metodo di backup, ad esempio **Sempre incrementale (a file singolo)** o **Sempre completo**.

L'operazione di backup si avvia. È possibile controllarne il progresso e i risultati nella scheda **Dispositivi**, nella colonna **Stato**.

© Acronis International GmbH, 2003-2024

Regole di conservazione

Per eliminare automaticamente i backup meno recenti, configurare le regole di conservazione dei backup nel piano di protezione.

Tali regole possono essere basate su una qualsiasi delle proprietà del backup seguenti:

- Numero
- Età
- Dimensione

Le regole di conservazione e le relative opzioni disponibili dipendono dallo schema di backup. Le regole sono pertinenti anche per gli agenti, i workload e i backup cloud-to-cloud. Per ulteriori informazioni, consultare "Regole di conservazione in base allo schema di backup" (pag. 444).

È possibile disabilitare la pulizia automatica dei backup meno recenti selezionando l'opzione **Conserva i backup all'infinito** durante la configurazione delle regole di conservazione. Questa scelta può tuttavia incrementare l'utilizzo dello storage, e pertanto sarà necessario eliminare manualmente i backup meno recenti e non necessari.

Suggerimenti importanti

- Le regole di conservazione fanno parte del piano di protezione. Se si revoca o elimina un piano, le regole di conservazione nel piano non vengono più applicate. Per ulteriori informazioni su come eliminare i backup che non sono più necessari, consultare "Eliminazione di backup" (pag. 542).
- Se, in base allo schema e al formato di backup, ciascun backup viene archiviato come file separato, non è possibile eliminare un backup dal quale dipendono altri backup incrementali o differenziali. Tale backup viene eliminato in base alle regole di conservazione applicate ai backup dipendenti. Questa configurazione può causare un aumento del consumo di storage, perché l'eliminazione di alcuni backup viene posticipata. Inoltre, la durata, il numero o le dimensioni dei backup possono superare i valori specificati. Per ulteriori informazioni su come modificare questo comportamento, consultare "Consolidamento backup" (pag. 456).
- Per impostazione predefinita, il backup più recente creato da un piano di protezione non viene mai eliminato. Tuttavia, se si configura una regola di conservazione che prevede la pulizia dei backup prima di avviare una nuova operazione di backup, e se il numero di backup da conservare è impostato su zero, verrà eliminato anche il backup più recente.

  Attenzione!
  Se questa regola di conservazione viene applicata a un set di backup con un solo backup, e l'operazione di backup non riesce, non sarà possibile recuperare i dati perché il backup esistente viene eliminato prima della creazione del nuovo backup.

© Acronis International GmbH, 2003-2024

Regole di conservazione in base allo schema di backup

Le regole di conservazione e le relative impostazioni disponibili dipendono dallo schema di backup utilizzato nel piano di protezione. Per ulteriori informazioni sugli schemi di backup, consultare "Schemi di backup" (pag. 425).

La tabella seguente riepiloga le regole di conservazione e le relative impostazioni disponibili.

Schema di backup	Pianificazione	Regole di conservazione e impostazioni disponibili
Sempre incrementale (a file singolo)	Ogni mese Ogni settimana Ogni giorno Ogni ora Backup attivati da eventi	Per numero di backup Per durata backup (impostazioni distinte per backup mensili, settimanali, giornalieri e orari) Conserva i backup per un periodo illimitato
Sempre completo	Ogni mese Ogni settimana Ogni giorno Ogni ora Backup attivati da eventi	Per numero di backup Per durata backup (impostazioni distinte per backup mensili, settimanali, giornalieri e orari) Per dimensione totale dei backup Conserva i backup per un periodo illimitato
Settimanale completo, giornaliero incrementale	Ogni giorno Backup attivati da eventi	Per numero di backup Per durata backup (impostazioni distinte per backup mensili e giornalieri) Per dimensione totale dei backup Conserva i backup per un periodo illimitato
Mensile completo, settimanale differenziale, giornaliero incrementale	Ogni mese Ogni settimana Ogni giorno Ogni ora Backup attivati da eventi	Per numero di backup Per durata backup (impostazioni distinte per backup completi, differenziali e incrementali) Per dimensione totale dei backup Conserva i backup per un periodo illimitato
Personalizzato	Ogni mese Ogni settimana Ogni giorno Ogni ora Backup attivati da eventi	Per numero di backup Per durata backup (impostazioni distinte per backup completi, differenziali e incrementali) Per dimensione totale dei backup Conserva i backup per un periodo illimitato

© Acronis International GmbH, 2003-2024

Perché sono presenti backup mensili con uno schema orario?

A seconda dello schema di backup, è possibile configurare l'opzione **Per durata backup** per uno dei seguenti backup:

- mensile, settimanale, giornaliero e orario.

  Queste impostazioni sono disponibili per tutti gli schemi di backup non personalizzati, e sono basati sull'ora. Tutti questi backup (mensile, settimanale, giornaliero e orario) sono disponibili anche se si configura un'esecuzione a ogni ora. Vedere l'esempio seguente.

Backup	Descrizione
Ogni mese	Un backup mensile è il primo backup di ogni mese.
Ogni settimana	Un backup settimanale è il primo backup del giorno della settimana selezionato nell'opzione Backup settimanale. Questo giorno viene considerato come inizio della settimana dalle regole di conservazione. Se il backup settimanale è anche il primo backup del mese, viene considerato mensile. In questo caso, il backup settimanale viene creato nel giorno selezionato della settimana successiva.
Ogni giorno	Un backup giornaliero è il primo backup del giorno, a meno che tale backup non rientri nella definizione di backup mensile o settimanale. In questo caso, il backup giornaliero viene creato il giorno successivo.
Ogni ora	Un backup orario, o eseguito ogni ora, è il primo backup dell'ora, a meno che tale backup non rientri nella definizione di backup mensile, settimanale o giornaliero. In questo caso, il backup orario viene creato all'ora successiva.

- Backup completi, differenziali e incrementali.

  Queste impostazioni sono disponibili per lo schema di backup **Personalizzato**, e sono basati sul metodo di backup. Lo schema **Mensile completo, Settimanale differenziale, Giornaliero incrementale** è uno schema personalizzato predefinito.

Esempio

Si utilizza lo schema di backup **Sempre incrementale (a file singolo)** con l'impostazione predefinita per i backup orari:

- Pianificazione in base all'ora.
- I backup vengono eseguiti ogni ora: da lunedì a venerdì, ogni ora, dalle 08:00 alle 18:00.
- L'opzione **Backup settimanale** è impostata su lunedì.

Nella sezione **Tempo di conservazione** del piano di protezione, è possibile applicare le regole di conservazione ai backup mensili, settimanali, giornalieri e orari.

La tabella seguente riepiloga i tipi di backup che vengono creati in un periodo di 8 giorni.

© Acronis International GmbH, 2003-2024

Data	Giorno della settimana	Descrizione
1 luglio	Lunedì	Il primo backup di ogni mese è mensile, quindi il primo backup di oggi è un backup mensile. Gli altri backup eseguiti nella giornata sono backup orari. In questa settimana, il primo backup è considerato un backup mensile. Per questa ragione non sono presenti backup settimanali. Il primo backup della prossima settimana sarà un backup settimanale.
2 luglio	Martedì	Il primo backup è giornaliero, gli altri backup eseguiti nella giornata sono orari.
3 luglio	Mercoledì	Il primo backup è giornaliero, gli altri backup eseguiti nella giornata sono orari.
4 luglio	Giovedì	Il primo backup è giornaliero, gli altri backup eseguiti nella giornata sono orari.
5 luglio	Venerdì	Il primo backup è giornaliero, gli altri backup eseguiti nella giornata sono orari.
6 luglio	Sabato	Il primo backup è giornaliero, gli altri backup eseguiti nella giornata sono orari.
7 luglio	Domenica	Il primo backup è giornaliero, gli altri backup eseguiti nella giornata sono orari.
8 luglio	Lunedì	Il primo backup è settimanale, gli altri backup eseguiti nella giornata sono orari.

Configurazione delle regole di conservazione

Le regole di conservazione fanno parte del piano di protezione; la loro disponibilità e le opzioni dipendono dallo schema di backup. Per ulteriori informazioni, consultare "Regole di conservazione in base allo schema di backup" (pag. 444).

Per configurare le regole di conservazione

1. In un piano di protezione, espandere il modulo **Backup**.
2. Fare clic su **Numero da conservare**.
3. Selezionare una delle seguenti opzioni:
   - **Per numero di backup**
   - **Per durata backup**

     Sono disponibili impostazioni distinte per backup mensili, settimanali, giornalieri e orari. Il valore massimo per tutte le tipologie è 9999.

     È inoltre possibile utilizzare un'unica impostazione per tutti i backup.

© Acronis International GmbH, 2003-2024

- **Per dimensione totale dei backup**

  Questa impostazione non è disponibile con lo schema di backup **Sempre incrementale (a file singolo)**.
- **Conserva i backup per un periodo illimitato**

4. [Se non è stata selezionata l'opzione **Conserva i backup per un periodo illimitato**] Configurare i valori per l'opzione selezionata.
5. [Se non è stata selezionata l'opzione **Conserva i backup per un periodo illimitato**] Selezionare quando vengono applicate le regole di conservazione.
   - Dopo il backup
   - Prima del backup

     Questa opzione non è disponibile quando si effettua il backup di cluster di Microsoft SQL Server o di Microsoft Exchange Server.
6. Fare clic su **Fine**.
7. Salvare il piano di protezione.

Replica

Con la replica, ogni nuovo backup viene copiato automaticamente in una posizione di replica. I backup nella posizione di replica non dipendono dai backup nella posizione di origine e viceversa.

Viene replicato solo l'ultimo backup nella posizione di origine. Tuttavia, se i backup precedenti non vengono replicati (ad esempio a causa di un problema di connessione di rete), l'operazione di replica includerà tutti i backup creati dopo l'ultima replica riuscita.

Se un'operazione di replica viene interrotta, i dati elaborati verranno utilizzati dall'operazione di replica successiva.

Nota
Questo argomento descrive la replica come parte di un piano di protezione. È anche possibile creare un piano di replica del backup distinto. Per ulteriori informazioni, consultare "Replica di backup" (pag. 202).

Esempi di utilizzo

- Garantire un ripristino affidabile

  Archiviare i backup sia in loco (per il ripristino immediato) che fuori sede (per garantire che i backup rimangano al sicuro anche in caso di problemi di archiviazione o catastrofi naturali che interessino la posizione primaria).
- Utilizzo del cloud storage per proteggere i dati da una catastrofe naturale

  Replicare i backup all'interno dell'archivio nel cloud trasferendo soltanto le modifiche dei dati.
- Conservazione solo degli ultimi punti di ripristino

  Configurare le regole di conservazione per eliminare i backup più vecchi da un archivio ad elevata velocità per risparmiare sui costi di archiviazione.

© Acronis International GmbH, 2003-2024

Posizioni supportate

Posizione	Come posizione di origine	Come posizione di replica
Cartella locale	+	+
Cartella di rete	+	+
Archiviazione nel cloud	-	+
Secure Zone	+	–
Cloud pubblico	+	+

Per attivare la replica

1. In un piano di protezione, espandere il modulo **Backup**, quindi fare clic su **Aggiungi posizione**.

   Nota
   L'opzione **Aggiungi posizione** non è disponibile quando si seleziona il cloud storage in **Dove eseguire il backup**.

2. Dall'elenco delle posizioni disponibili, selezionare la posizione di replica.
   In base al numero di posizioni aggiunte alla replica, la posizione verrà visualizzata nel piano di protezione come **2a posizione**, **3a posizione**, **4a posizione** o **5a posizione**.
3. [Facoltativo] Fare clic sull'icona ingranaggio per configurare le opzioni per la posizione di replica.
   - **Prestazioni e finestra di backup** - Imposta la finestra di backup per la posizione scelta, come descritto in "Prestazioni e finestra di backup" (pag. 486). Queste impostazioni definiscono le prestazioni della replica.
   - **Rimuovi posizione** - Elimina la posizione di replica attualmente selezionata.
   - [Solo per il cloud storage] **Consegna fisica dei dati** - Salva il backup iniziale in un dispositivo di storage rimovibile e lo invia per il caricamento nel cloud storage invece di replicarlo su Internet.
     Questa opzione è adatta alle posizioni con una connessione di rete lenta o quando è necessario risparmiare larghezza di banda in caso di trasferimenti di file di grandi dimensioni. L'abilitazione di questa opzione non richiede ulteriori quote del servizio Cyber Protect, ma è necessario disporre di una quota del servizio Consegna fisica dei dati per creare un ordine di consegna e tenerne traccia. Consultare "Consegna fisica dei dati" (pag. 490).

     Nota
     Questa opzione è supportata con la versione dell'agente di protezione dalla release C21.06 o successive.

4. [Facoltativo] Nella sezione della posizione di replica, alla riga **Numero da conservare**, configurare le regole di conservazione per quella posizione, come descritto in "Regole di conservazione" (pag. 443).

© Acronis International GmbH, 2003-2024

5. [Facoltativo] Ripetere i passaggi da 1 a 4 per aggiungere altre posizioni di replica.
   È possibile configurare fino a quattro posizioni di replica (**2a posizione**, **3a posizione**, **4a posizione** e **5a posizione**). Se si seleziona **cloud storage**, non è possibile aggiungere altre posizioni di replica.

Importante
Se si abilitano backup e replica nello stesso piano di protezione, verificare che la replica venga completata prima del successivo backup pianificato. Se la replica è ancora in corso, il sistema non avvia il backup pianificato; ad esempio, un backup pianificato eseguito ogni 24 ore non viene avviato se il completamento della replica dura 26 ore.

Per evitare questa dipendenza, utilizzare un piano distinto per la replica di backup. Per ulteriori informazioni su questo specifico piano, consultare "Replica di backup" (pag. 202).

Crittografia

L'algoritmo crittografico Advanced Encryption Standard (AES) opera in modalità Galois/Counter (GCM) e utilizza una chiave a 256 bit generata casualmente. La chiave di crittografia viene quindi crittografata con l'algoritmo AES-256 utilizzando l'hash SHA-2 (a 256 bit) della password come chiave. La password stessa non viene memorizzata né sul disco né nei backup, e l'hash della password viene utilizzato per la verifica.

Con questa sicurezza a due livelli, i dati di backup sono protetti dagli accessi non autorizzati, ma non è possibile ripristinare una password perduta.

Nota
L'utilizzo dell'algoritmo AES-256 insieme a una password complessa garantisce una crittografia quantum resistant, che protegge dagli attacchi crittoanalitici basati sull'elaborazione quantistica.

Si raccomanda di crittografare tutti i backup archiviati nell'archivio nel cloud, soprattutto se l'azienda è soggetta a conformità normativa.

È possibile configurare la crittografia nei modi seguenti:

- Nel piano di protezione
- Come proprietà del sistema, utilizzando Cyber Protect Monitor o l'interfaccia a riga di comando

Configurazione della crittografia nel piano di protezione

In un piano di protezione, la crittografia è abilitata per impostazione predefinita e viene utilizzato l'algoritmo AES-256.

Con una password complessa, l'algoritmo AES-256 fornisce la crittografia quantum resistant.

Per gli account in modalità Conformità non è possibile configurare la crittografia nel piano di protezione. Per ulteriori informazioni su come configurare la crittografia sul dispositivo protetto, consultare "Configurazione della crittografia come proprietà del sistema" (pag. 450).

© Acronis International GmbH, 2003-2024

Per configurare la crittografia

1. In un piano di protezione, espandere il modulo **Backup**.
2. In **Crittografia**, fare clic su **Specificare una password**.
3. Specificare la password per la crittografia e confermarla.
4. Fare clic su **OK**.

Attenzione!
Impossibile recuperare i backup crittografati se si perde o si dimentica la password.

Non è possibile modificare le impostazioni di crittografia dopo aver applicato il piano di protezione. Per utilizzare impostazioni di crittografia diverse, creare un nuovo piano.

Configurazione della crittografia come proprietà del sistema

È possibile configurare la crittografia di backup come proprietà del sistema. In questo caso, la crittografia di backup non viene configurata nel piano di protezione, ma nel workload protetto. La crittografia come proprietà del sistema utilizza l'algoritmo AES con una chiave a 256 bit (AES-256).

Nota
L'utilizzo dell'algoritmo AES-256 insieme a una password complessa garantisce una crittografia quantum resistant, che protegge dagli attacchi crittoanalitici basati sull'elaborazione quantistica.

La configurazione della crittografia come proprietà del sistema influisce sui piani di protezione nel seguente modo:

- **Piani di protezione già applicati al sistema.** Se le impostazioni di crittografia in un piano di protezione sono diverse, il backup non andrà a buon fine.
- **Piani di protezione che verranno applicati al sistema in un secondo momento.** Le impostazioni di crittografia salvate sul sistema prevalgono su quelle definite nel piano di protezione. Tutti i backup saranno crittografati, anche se la crittografia è disabilitata nelle impostazioni del modulo Backup.

Per gli account in modalità Conformità, è disponibile solo la crittografia come proprietà del sistema.

Se è presente più di un Agente per VMware connesso allo stesso vCenter Server, e si configura la crittografia come proprietà del sistema, è necessario utilizzare la stessa password di crittografia su tutti i sistemi con Agente per VMware, a causa del bilanciamento del carico tra gli agenti.

È possibile configurare la crittografia come proprietà del sistema nei seguenti modi:

- Dalla riga di comando
- In Cyber Protect Monitor (disponibile per Windows e macOS)

Per configurare la crittografia

Dalla riga di comando

© Acronis International GmbH, 2003-2024

1. Accedere come amministratore (in Windows) o come utente root (in Linux).
2. Nella riga di comando eseguire il comando seguente:
   - Per Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
     <encryption_password>
     ```

     Per impostazione predefinita, il percorso di installazione è `%ProgramFiles%\BackupClient`.
   - Per Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   - Per un'appliance virtuale:

     ```
      /./sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   Attenzione!
   Impossibile recuperare i backup crittografati se si perde o si dimentica la password.

In Cyber Protect Monitor

1. Accedere come amministratore.
2. Fare clic sull'icona Cyber Protect Monitor nella barra delle notifiche (in Windows) o nella barra dei menu (in macOS).
3. Fare clic sull'icona ingranaggio, quindi su **Impostazioni** > **Crittografia**.
4. Selezionare **Impostare una password per questo sistema**. Specificare e confermare la password di crittografia.
5. Fare clic su **Salva**.

Attenzione!
Impossibile recuperare i backup crittografati se si perde o si dimentica la password.

Per reimpostare le impostazioni di crittografia

1. Accedere come amministratore (in Windows) o come utente root (in Linux).
2. Nella riga di comando eseguire il comando seguente:
   - Per Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
     ```

     Per impostazione predefinita, il percorso di installazione è `%ProgramFiles%\BackupClient`.
   - Per Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --reset
     ```


© Acronis International GmbH, 2003-2024

- Per un'appliance virtuale:

```
/./sbin/acropsh -m manage_creds --reset
```

Importante
Se si reimposta la crittografia come proprietà del sistema o si modifica la password di crittografia dopo che un piano di protezione ha creato un backup, l'operazione di backup successiva non avrà esito positivo. Per continuare a eseguire il backup del workload, creare un nuovo piano di protezione.

Autenticazione

Nota
Questa funzionalità è disponibile con il pacchetto Advanced Backup.

L'autenticazione consente di dimostrare l'autenticità del file e l'assenza di modifiche dal momento del backup. L'utilizzo di questa funzionalità è consigliato per proteggere i file dei documenti legali o qualsiasi altro file che richieda una prova di autenticità.

L'autenticazione è disponibile solo per i backup dei file. I file dotati di firma digitale vengono ignorati perché la loro autenticazione non è necessaria.

L'autenticazione *non* è disponibile:

- Se il formato del backup è impostato su **Versione 11**.
- Se la destinazione del backup è Secure Zone.

Come utilizzare l'autenticazione

Per abilitare l'autenticazione di tutti i file selezionati per il backup, ad eccezione dei file dotati di firma digitale, selezionare l'opzione **Autenticazione** quando si crea un piano di protezione.

Durante la configurazione del ripristino, i file sottoposti ad autenticazione vengono contrassegnati con un'icona speciale ed è quindi possibile verificare l'autenticità dei file.

Come funziona

Durante l'esecuzione di un backup, l'agente elabora i codici hash dei file sottoposti a backup, crea un albero hash basato sulla struttura della cartella, salva l'albero nel backup e quindi invia la root dell'albero hash al servizio di autenticazione. Il servizio di autenticazione salva la root dell'albero hash nel database blockchain Ethereum per garantire che questo valore non venga modificato.

Durante la verifica dell'autenticità del file, l'agente elabora l'hash del file ed esegue il confronto con l'hash archiviato nell'albero hash all'interno del backup. Se gli hash non corrispondono, il file non è considerato autentico. Altrimenti, l'autenticità del file è garantita dall'albero hash.

© Acronis International GmbH, 2003-2024

Per verificare che lo stesso albero hash non sia stato compromesso, l'agente invia la root dell'albero hash al servizio di autenticazione, che lo confronta con quello archiviato nel database blockchain. Se gli hash corrispondono, viene garantita l'autenticità del file selezionato. In caso contrario, il software visualizza un messaggio che segnala la non autenticità del file.

Opzioni di backup predefinite

I valori predefiniti delle opzioni di backup esistono a livello di azienda, unità e utente. Quando un'unità o un account utente viene creato all'interno di un'azienda o di un'unità, eredita le impostazioni predefinite fissate per tale azienda od unità.

Gli amministratori dell'azienda e dell'unità, nonché ogni utente privo di diritti di amministratore, possono modificare un valore dell'opzione rispetto a quello predefinito. Una volta avvenuto il cambio, il nuovo valore sarà utilizzato come impostazione predefinita al rispettivo livello in tutti i piani di protezione.

Quando viene creato un piano di protezione, è possibile sovrascrivere un valore predefinito con un valore personalizzato, che diventerà specifico per il piano in uso.

Per cambiare un'opzione di valore predefinito

1. Eseguire una delle seguenti operazioni:
   - Per modificare il valore predefinito per l'azienda, accedere alla console di Cyber Protect come amministratore aziendale.
   - Per modificare il valore predefinito per l'unità, accedere alla console di Cyber Protect come amministratore dell'unità.
   - Per modificare il valore predefinito per l'utente, accedere alla console di Cyber Protect usando un account privo di diritti di amministratore.
2. Fare clic su **Impostazioni** > **Impostazioni di sistema**.
3. Espandere la sezione **Opzioni di backup predefinite**.
4. Selezionare l'opzione e apportare le modifiche necessarie.
5. Fare clic su **Salva**.

Opzioni di backup

Per modificare le opzioni di backup di un piano di protezione, nel modulo **Backup**, nel campo **Opzioni di backup**, fare clic su **Modifica**.

Disponibilità delle opzioni di backup

La serie di opzioni di backup disponibili dipende dai seguenti fattori:

- L'ambiente in cui opera l'agente (Windows, Linux, macOS).
- Il tipo di dati sottoposti a backup (disco, file, macchine virtuali, dati di applicazioni).

© Acronis International GmbH, 2003-2024

- La destinazione di backup (archivio nel cloud, cartella locale o di rete).

La tabella seguente riepiloga la disponibilità delle opzioni di backup.

	Backup a livello di disco			Backup a livello di file			Macchine virtuali			SQL e Exchange
	Windows	**Linux**	**macOS**	**Windows**	**Linux**	**macOS**	**ESXi**	**Hyper-V**	**Virtuozzo**	**Windows**
Avvisi	+	+	+	+	+	+	+	+	+	+
Consolidamento backup	+	+	+	+	+	+	+	+	+	-
Nome file di backup	+	+	+	+	+	+	+	+	+	+
Formato backup	+	+	+	+	+	+	+	+	+	+
Convalida del backup	+	+	+	+	+	+	+	+	+	+
Changed block tracking (CBT)	+	-	-	-	-	-	+	+	-	-
Modalità backup cluster	-	-	-	-	-	-	-	-	-	+
Livello di compressione	+	+	+	+	+	+	+	+	+	+
Gestione degli errori										
Riprova se si verifica un errore	+	+	+	+	+	+	+	+	+	+
Non visualizzare i messaggi e le finestre di dialogo durante l'elaborazione (modalità nascosta)	+	+	+	+	+	+	+	+	+	+
Ignora settori danneggiati	+	-	+	+	-	+	+	+	+	-
Riprova se si verifica un errore durante la creazione dello	-	-	-	-	-	-	+	+	+	-

© Acronis International GmbH, 2003-2024

snapshot MV										
Backup incrementale/differenziale veloce	+	+	+	-	-	-	-	-	-	-
Istantanea di backup a livello di file	-	-	-	+	+	+	-	-	-	-
Filtri file	+	+	+	+	+	+	+	+	+	-
Dati forensi	+	-	-	-	-	-	-	-	-	-
Troncamento registro	-	-	-	-	-	-	+	+	-	Solo per SQL
Creazione snapshot LVM	-	+	-	-	-	-	-	-	-	-
Punti di montaggio	-	-	-	+	-	-	-	-	-	-
Snapshot multivolume	+	+	-	+	+	-	-	-	-	-
One-click Recovery	+	+	-	-	-	-	-	-	-	-
Prestazioni e finestra di backup	+	+	+	+	+	+	+	+	+	+
Consegna fisica dei dati	+	+	+	+	+	+	+	+	+	-
Comandi pre/post	+	+	+	+	+	+	+	+	+	+
Comandi prima/dopo la cattura dei dati	+	+	+	+	+	+	-	-	-	+
Programmazione										
Ripartisci orari di avvio all'interno di una finestra dell'orario	+	+	+	+	+	+	+	+	+	+
Limita il numero di backup eseguiti simultaneamente	-	-	-	-	-	-	+	+	+	-
Backup settore per settore	+	+	-	-	-	-	+	+	+	-

© Acronis International GmbH, 2003-2024

Suddivisione	+	+	+	+	+	+	+	+	+	+
Gestione fallimento dell'attività	+	+	+	+	+	+	+	+	+	+
Condizioni di avvio dell'attività	+	+	-	+	+	-	+	+	+	+
Servizio Copia Shadow del volume (VSS)	+	-	-	+	-	-	-	+	-	+
Servizio Copia Shadow del volume per macchine virtuali	-	-	-	-	-	-	+	+	-	-
Backup settimanale	+	+	+	+	+	+	+	+	+	+
Registro eventi di Windows	+	-	-	+	-	-	+	+	-	+

Avvisi

Non ci sono backup completati per un numero specifico di giorni consecutivi

L'impostazione predefinita è: **Disabilitata**.

Questa opzione determina se viene generato un avviso nel caso in cui non vengano eseguiti correttamente i backup previsti dal piano di protezione per un determinato periodo di tempo. Oltre ai backup non riusciti, il software conta i backup che non sono stati eseguiti nei tempi previsti dalla pianificazione (backup mancati).

Gli avvisi, generati per ogni sistema, vengono visualizzati nella scheda **Avvisi**.

È possibile specificare dopo quanti giorni consecutivi senza backup viene generato un avviso.

Consolidamento backup

Questo opzione definisce se consolidare i backup durante la pulizia oppure eliminare le intere catene di backup.

L'impostazione predefinita è: **Disabilitata**.

Il consolidamento è il processo di accorpamento di due o più backup successivi in un unico backup.

Se questa opzione è abilitata, un backup destinato a essere eliminato durante la pulizia viene consolidato con il successivo dependent backup (incrementale o differenziale).

© Acronis International GmbH, 2003-2024

In caso contrario, il backup viene conservato finché tutti i dependent backup non diventano soggetti a eliminazione. Ciò consente di evitare l'operazione di consolidamento, che potrebbe richiedere molto tempo, ma richiede spazio aggiuntivo per l'archiviazione dei backup di cui viene posticipata l'eliminazione. L'età o il numero dei backup può superare i valori specificati nelle regole di conservazione.

Importante
Va tenuto presente che il consolidamento è solo un metodo di eliminazione, non un'alternativa ad essa. Il backup risultante non conterrà i dati che erano presenti nel backup eliminato e che non erano presenti in quello incrementale o differenziale conservato.

Questa opzione *non* è effettiva se una delle seguenti affermazioni è vera:

- La destinazione di backup è l'archivio nel cloud.
- Lo schema di backup è configurato su **Sempre incrementale (a file singolo)**.
- La formattazione di backup è configurata su **Versione 12**.

I backup archiviati nell'archivio nel cloud, nonché i backup di singoli file (nei formati delle versioni 11 e 12), sono sempre consolidati poiché la loro struttura interna garantisce un consolidamento facile e veloce.

Se viene utilizzato il formato versione 12 e se sono presenti più catene di backup (e ogni catena è archiviata in un file .tibx distinto), il consolidamento funziona solo sull'ultima catena. Ogni altra catena viene completamente eliminata eccetto la prima, che verrà compressa alla dimensione minima necessaria a conservare le meta informazioni (~12 KB). Tali informazioni sono necessarie per garantire la coerenza dei dati durante le operazioni di lettura e scrittura simultanee. I backup inclusi in tali catene non saranno visualizzabili nell'interfaccia utente dal momento in cui si applica la regola di conservazione, sebbene continuino ad esistere fisicamente fino all'eliminazione dell'intera catena.

In tutti gli altri casi, i backup la cui eliminazione è rimandata vengono contrassegnati con l'icona a forma di cestino ( ) nell'interfaccia utente. Se si elimina questo tipo di backup facendo clic sul simbolo X, viene eseguito il consolidamento.

Nome file di backup

Questa opzione definisce i nomi dei file di backup creati dal piano di protezione o dal piano di backup delle applicazioni cloud.

I nomi dei file di backup creati dai piani di protezione sono visualizzabili in un file manager quando si sfoglia la posizione del backup.

Che cos'è un file di backup?

Ogni piano di protezione crea uno o più file nella posizione di backup, in base a quale schema di backup e quale formato di backup vengono usati. La tabella seguente elenca i file che possono

© Acronis International GmbH, 2003-2024

essere creati per sistema o casella di posta.

	Sempre incrementale (a file singolo)	Altri schemi di backup
Formato di backup **Versione 11**	Un file TIB e un file di metadati XML	Più file TIB e un file di metadati XML
Formato di backup **Versione 12**	Un file TIBX per catena di backup (backup completo o differenziale, e tutti i backup incrementali che dipendono da esso). Se la dimensione di un file archiviato in una cartella locale o di rete (SMB) supera i 200 GB, il file viene suddiviso in file da 200 GB per impostazione predefinita.	

Tutti i file hanno lo stesso nome, con o senza l'aggiunta di un marcatore temporale o di una sequenza di numeri. È possibile definire questo nome (indicato come nome file di backup) quando si crea o si modifica un piano di protezione o un piano di backup delle applicazioni cloud.

Nota
L'indicatore data e ora è aggiunto al nome del file di backup solo nel formato di backup della versione 11.

Dopo aver modificato il nome di un file di backup in un piano di protezione o in un piano di backup delle applicazioni cloud, il backup successivo sarà un backup completo.

Se si specifica un nome di un file di un backup presente dello stesso sistema, viene creato un backup completo, incrementale o differenziale, in base a quanto previsto dal piano.

Nota
Se si spostano i file di backup (.tibx) dallo storage originale, non devono essere rinominati. I file rinominati verranno visualizzati come danneggiati e non saranno utilizzabili per recuperare i dati.

È possibile impostare i nomi dei file di backup per le posizioni che non è possibile sfogliare con un file manager (come il cloud storage). In questo caso, nella scheda **Archivio di backup** vengono visualizzati i nomi personalizzati.

Dove posso vedere i nomi dei file di backup?

Per i piani di protezione, nella scheda **Archivio di backup** selezionare la posizione e quindi l'archivio di backup.

- Il nome del file di backup predefinito è visualizzato nel pannello **Dettagli**.
- Se si imposta un nome di un file di backup non predefinito, sarà visualizzato direttamente nella scheda **Archivio di backup**, colonna **Nome**.

Per i piani di backup delle applicazioni cloud, nella scheda **Archivio di backup** selezionare la posizione, l'archivio di backup e quindi fare clic sull'icona ingranaggio.

© Acronis International GmbH, 2003-2024

Limitazioni per i nomi del file di backup

- Il nome di un file di backup non deve terminare con una cifra.

  Nel nome di un file di backup predefinito, per evitare che il nome termini con una cifra, viene aggiunta la lettera "A". Quando si crea un nome personalizzato, assicurarsi sempre che non termini con una cifra. Quando si usano delle variabili, il nome non deve terminare con una variabile, poiché potrebbe terminare con una cifra.
- Il nome di un file di backup non può contenere i simboli seguenti: **()&?*$<>":\|/#**, terminazioni di riga (**\n**), e tabulazioni (**\t**).

Nota
Scegliere nomi dei file di backup intuitivi. In questo modo è più facile distinguere i backup quando si sfoglia la posizione del backup con un file manager.

Nome file di backup predefinito

Il nome del file di backup predefinito per i backup di sistemi fisici e di virtual machine completi, dischi/volumi, file/cartelle, database di Microsoft SQL Server, database di Microsoft Exchange Server e configurazione ESXi è `[Machine Name]-[Plan ID]-[Unique ID]A`.

Il nome predefinito per i backup delle caselle di posta di Exchange e di Microsoft 365 creati da un Agente per Microsoft 365 locale è `[Mailbox ID]_mailbox_[Plan ID]A`.

Il nome predefinito per i backup di Microsoft Azure ha il prefisso `[Mailbox ID]_`. Tale prefisso non può essere rimosso.

Il nome predefinito per i backup delle applicazioni cloud creati dagli agenti cloud è `[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`.

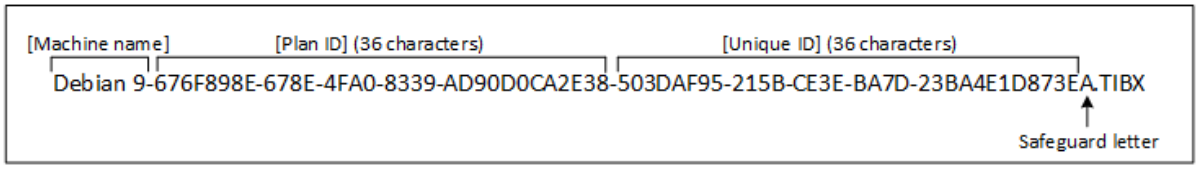
Il nome predefinito è costituito dalle seguenti variabili:

- `[Machine Name]`: questa variabile è sostituita dal nome del sistema (lo stesso nome visualizzato nella console di Cyber Protect).
- `[Plan ID]`, `[Plan Id]`: queste variabili sono sostituite da un identificatore univoco del piano di protezione. Questo valore non cambia se il piano viene rinominato.
- `[Unique ID]`: questa variabile è sostituita da un identificatore univoco del sistema selezionato. Questo valore non cambia se il sistema viene rinominato.
- `[Mailbox ID]`: questa variabile è sostituita dal nome principale dell'utente della casella di posta (UPN).
- `[Resource Name]`: questa variabile è sostituita dal nome dell'origine dei dati cloud, come il nome principale dell'utente della casella di posta (UPN), l'URL del sito SharePoint o il nome dell'unità condivisa.
- `[Resource Type]`: questa variabile è sostituita dal tipo di origine dei dati cloud, ad esempio `mailbox`, `O365Mailbox`, `O365PublicFolder`, `OneDrive`, `SharePoint`, `GDrive`.

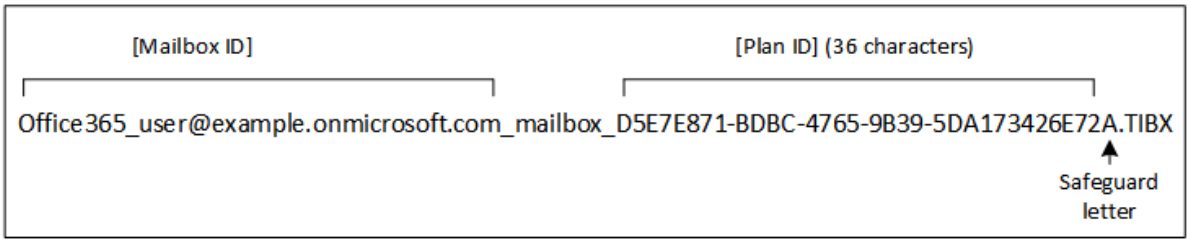
© Acronis International GmbH, 2003-2024

- `[Resource ID]`: questa variabile è sostituita da un identificatore univoco dell'origine dei dati cloud. Il valore non cambia se l'origine dei dati cloud viene rinominata.
- La `"A"` è una lettera di salvaguardia aggiunta per evitare che il nome termini con una cifra.

Il diagramma sottostante mostra il nome del file di backup predefinito.



Il diagramma sottostante mostra il nome predefinito del file di backup per i backup delle caselle di posta di Microsoft 365 eseguiti da un agente locale.



Nomi senza variabili

Se si modifica il nome del file di backup in `MyBackup`, i file di backup avranno l'aspetto dei file seguenti. Entrambi gli esempi presuppongono backup incrementali giornalieri pianificati alle 14:40, con inizio dal 13 settembre 2016.

Per il formato della versione 12 con lo schema di backup **Sempre incrementale (a file singolo)**:

```
MyBackup.tibx
```

Per il formato della versione 12 con altri schemi di backup:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Utilizzo delle variabili

Oltre alle variabili utilizzate per impostazione predefinita, è possibile utilizzare le variabili seguenti:

- La variabile `[Plan name]`, che viene sostituita dal nome del piano di protezione.
- La variabile `[Virtualization Server Type]`, che viene sostituita da "vmwesx" se il backup delle macchine virtuali viene eseguito dall'Agente per VMware o da "mshyperv" se il backup delle macchine virtuali viene eseguito dall'Agente per Hyper-V.

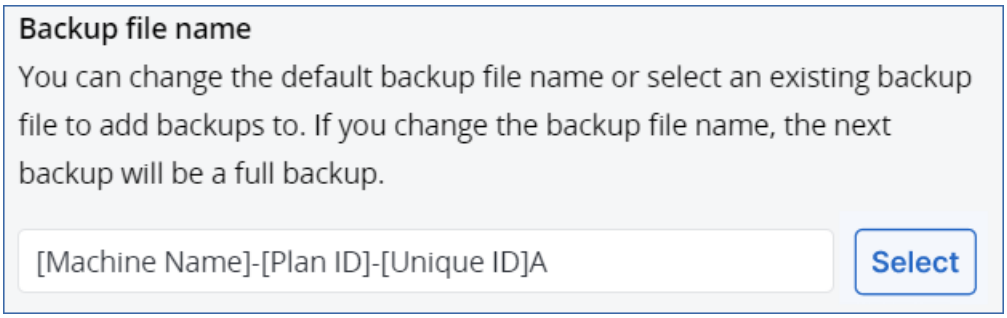
© Acronis International GmbH, 2003-2024

Se vengono selezionati diversi sistemi o caselle di posta per il backup, il nome del file di backup deve contenere le variabili `[Machine Name]`, `[Unique ID]`, `[Mailbox ID]`, `[Resource Name]` o `[Resource Id]`.

Creazione di backup in un archivio di backup esistente

È possibile configurare i backup di un workload in modo che vengano aggiunti a un archivio di backup esistente.

Questa opzione può essere utile, ad esempio, quando un piano di protezione è applicato a un solo sistema ed è necessario rimuovere tale sistema dalla console di Cyber Protect o disinstallare l'agente insieme alle relative impostazioni di configurazione. Dopo aver di nuovo aggiunto il sistema o reinstallato l'agente, è possibile impostare il piano di protezione in modo che continui a eseguire i backup nell'archivio originale.



Per configurare i backup di un workload in modo che vengano aggiunti a un archivio di backup esistente

Workload non cloud-to-cloud

1. Nella schermata **Tutti i dispositivi**, fare clic sul workload, quindi su **Proteggi**.
2. Nelle impostazioni del piano di protezione, estendere il modulo **Backup**.
3. Fare clic su **Opzioni di backup**, quindi su **Modifica**.
4. Nella scheda **Nome file di backup**, fare clic su **Seleziona**.
   Il pulsante **Seleziona** mostra i backup nella posizione selezionata nella sezione **Dove eseguire il backup** del piano di protezione.

   Nota
   Il pulsante **Seleziona** è disponibile solo per i piani di protezione creati e applicati a un singolo workload.

5. Selezionare un archivio, quindi fare clic su **Fine**.
6. Fare clic su **Fine**, quindi su **Applica**.

Workload cloud-to-cloud

1. Nella scheda **Gestione** > **Backup delle applicazioni cloud**, selezionare il piano.
2. Fare clic su **Modifica**, quindi sull'icona ingranaggio accanto al nome del piano.

© Acronis International GmbH, 2003-2024

3. Nella scheda **Nome file di backup**, fare clic su **Seleziona**.

   Nota
   Il pulsante **Seleziona** è disponibile solo per i piani di backup che sono stati creati e applicati a un singolo workload.

4. Selezionare un archivio di backup, quindi fare clic su **Fine**.
5. Fare clic su **Fine**, quindi su **Salva modifiche**.

Formato backup

L'opzione **Formato backup** definisce il formato dei backup creati dal piano di protezione. Questa opzione è disponibile solo per i piani di protezione che già utilizzano la versione 11 del formato di backup. In questo caso è possibile modificare il formato di backup alla versione 12. Dopo essere passati al formato di backup della versione 12, l'opzione non sarà più disponibile.

- **Versione 11**
  Il formato precedente, mantenuto per la retrocompatibilità.

  Nota
  Non è possibile eseguire il backup di un gruppo di disponibilità database (DAG) utilizzando il formato di backup della versione 11. Il backup dei gruppi DAG è supportato solo con il formato della versione 12.

- **Versione 12**
  Il formato di backup introdotto in Acronis Backup 12 per ottenere backup e ripristini più rapidi. Ogni catena di backup (backup completo o differenziale, e tutti i backup incrementali che ne dipendono) viene salvata in un singolo file TIBX.

Formato e file di backup

Per le posizioni di backup che è possibile sfogliare con un file manager (come le cartelle locali o di rete), il formato del backup determina il numero di file e la loro estensione. La tabella seguente elenca i file che possono essere creati per sistema o casella di posta.

	Sempre incrementale (a file singolo)	**Altri schemi di backup**
Formato di backup **Versione 11**	Un file TIB e un file di metadati XML	Più file TIB e un file di metadati XML
Formato di backup **Versione 12**	Un file TIBX per catena di backup (backup completo o differenziale, e tutti i backup incrementali che dipendono da esso). Se la dimensione di un file archiviato in una cartella locale o di rete (SMB) supera i 200 GB, il file viene suddiviso in file da 200 GB per impostazione predefinita.	

© Acronis International GmbH, 2003-2024

Modifica del formato di backup alla versione 12 (TIBX)

Se si modifica il formato di backup dalla versione 11 (formato TIB) alla versione 12 (formato TIBX):

- Il backup successivo sarà completo.
- Per le posizioni di backup che è possibile sfogliare con un file manager (come le cartelle locali o di rete), viene creato un file TIBX. Il nuovo file riprenderà il nome del file originale con l'aggiunta del suffisso **_v12A**.
- Le regole di conservazione e la replica vengono applicate solo ai nuovi backup.
- I backup precedenti non verranno eliminati e rimarranno disponibili nella scheda **Archivio di backup**. È possibile eliminarli manualmente.
- I precedenti backup nel cloud non consumano la quota di **Archiviazione nel cloud**.
- Consumano tuttavia la quota di **Backup locale** fino a quando non vengono eliminati manualmente.

Deduplicazione negli archivi

Il formato di backup TIBX della versione 12 supporta la deduplicazione negli archivi, che fornisce i seguenti vantaggi:

- Dimensione del backup significativamente ridotta, con deduplicazione integrata a livello di blocco per qualsiasi tipologia di dati
- Gestione efficiente dei collegamenti reali, per garantire che non siano presenti archivi duplicati
- Suddivisione in blocchi basata su hash

Nota
La deduplicazione negli archivi è abilitata per impostazione predefinita in tutti i backup con formato TIBX. Non è necessario attivarla nelle opzioni di backup e non è possibile disattivarla.

Compatibilità del formato del backup tra diverse versioni del prodotto

Per informazioni sulla compatibilità del formato del backup, vedere Compatibilità dell'archivio di backup tra diverse versioni del prodotto (1689).

Convalida del backup

La convalida è un'operazione che consente di verificare la possibilità di ripristino dei dati da un backup. Quando questa opzione è abilitata, immediatamente dopo la creazione ogni backup creato dal piano di protezione viene convalidato tramite il metodo di verifica checksum. Questa operazione viene eseguita dall'agente di protezione.

L'impostazione predefinita è: **Disabilitata**.

Per ulteriori informazioni sulla convalida tramite verifica checksum, fare riferimento a "Verifica checksum" (pag. 209).

© Acronis International GmbH, 2003-2024

Nota
A seconda delle impostazioni selezionate dal service provider, la convalida potrebbe non essere disponibile quando si esegue il backup nell'archivio nel cloud. La convalida non è disponibile neanche per le posizioni di backup nei cloud pubblici.

Changed block tracking (CBT)

Questa opzione ha effetto solo per i backup seguenti:

- Backup del disco di virtual machine
- Backup del disco di sistemi fisici che eseguono Windows
- Backup di database Microsoft SQL Server
- Backup di database Microsoft Exchange Server

L'impostazione predefinita è: **Abilitata**.

L'opzione consente di stabilire se utilizzare Changed Block Tracking (CBT) quando si esegue un backup incrementale o differenziale.

La tecnologia CBT accelera il processo di backup. Le modifiche al disco o al database sono continuamente monitorate a livello di blocco. Quando viene avviato un backup, le modifiche possono essere immediatamente salvate nel backup.

Modalità backup cluster

Nota
Questa funzionalità è disponibile con il pacchetto Advanced Backup.

Queste opzioni sono effettive per il backup a livello di database di Microsoft SQL Server e Microsoft Exchange Server.

Queste opzioni sono effettive solo se il cluster stesso (Gruppi di Disponibilità Always On (AAG) di Microsoft SQL Server o Gruppo di Disponibilità Database (DAG) di Microsoft Exchange Server) è selezionato per il backup, invece dei singoli nodi o dei database all'interno di esso. Se si selezionano dei singoli elementi all’interno del cluster, il backup non sarà compatibile con il cluster e sarà eseguito il backup solo delle copie selezionate degli elementi.

Microsoft SQL Server

Questa opzione determina la modalità di backup per i gruppi di disponibilità Always On (AAG) di SQL Server. Affinché questa opzione sia effettiva, l'Agente per SQL deve essere installato su tutti i nodi AAG. Per ulteriori informazioni sull’esecuzione del backup dei gruppi di disponibilità Always On, fare riferimento a “Protezione dei gruppi di disponibilità Always On (AAG)".

L'impostazione predefinita è: **Copia secondaria, se possibile.**

È possibile selezionare uno dei casi seguenti:

© Acronis International GmbH, 2003-2024

- **Copia secondaria, se possibile**

  Se tutte le copie secondarie non sono in linea, viene eseguito il backup della copia primaria. Il backup della copia primaria potrebbe rallentare l'operatività del SQL Server, ma i dati del backup saranno nello stato più recente.
- **Copia secondaria**

  Se tutte le copie secondarie non sono in linea, il backup non ha esito positivo. Il backup delle copie secondarie non ha impatto sulle prestazioni del server SQL e consente di estendere la finestra del backup. Tuttavia, le copie passive potrebbero contenere informazioni non aggiornate, poiché tali copie spesso sono impostate per l'aggiornamento asincrono (lagged).
- **Copia primaria**

  Se la copia primaria non è in linea, il backup non ha esito positivo. Il backup della copia primaria potrebbe rallentare l'operatività del server SQL, ma i dati del backup saranno nello stato più recente.

A prescindere dal valore di questa opzione, per garantire la consistenza del database, il software ignora i database che *non* si trovano nello stato **SINCRONIZZATO** o **IN SINCRONIZZAZIONE** quando il backup si avvia. Se tutti i database sono ignorati, il backup non ha esito positivo.

Microsoft Exchange Server

Questa opzione determina la modalità di backup per i gruppi di disponibilità database (DAG) di Exchange Server. Affinché questa opzione sia effettiva, l'Agente per Exchange deve essere installato su tutti i nodi DAG. Per ulteriori informazioni sull'esecuzione del backup dei gruppi di disponibilità database, fare riferimento a "Protezione dei gruppi di disponibilità dei database (DAG)".

L'impostazione predefinita è: **Copia passiva se possibile.**

È possibile selezionare uno dei casi seguenti:

- **Copia passiva se possibile**

  Se tutte le copie passive non sono in linea, viene eseguito il backup della copia attiva. Il backup della copia attiva primaria potrebbe rallentare l'operatività del server Exchange, ma i dati saranno copiati nello stato più recente.
- **Copia passiva**

  Se tutte le copie passive non sono in linea, il backup non ha esito positivo. Il backup delle copie passive non ha impatto sulle prestazioni del server di Exchange e consente di estendere la finestra del backup. Tuttavia, le copie passive potrebbero contenere informazioni non aggiornate, poiché tali copie spesso sono impostate per l'aggiornamento asincrono (lagged).
- **Copia attiva**

  Se la copia attiva non è in linea, il backup non ha esito positivo. Il backup della copia attiva primaria potrebbe rallentare l'operatività del server Exchange, ma i dati saranno copiati nello stato più recente.

A prescindere dal valore di questa opzione, per garantire la consistenza del database, il software ignora i database che *non* si trovano nello stato **INTEGRO** o **ATTIVO** quando il backup si avvia. Se tutti i database sono ignorati, il backup non ha esito positivo.

© Acronis International GmbH, 2003-2024

Livello di compressione

Nota
Questa opzione non è disponibile per i backup cloud-to-cloud. La compressione per questi backup è abilitata per impostazione predefinita con un livello fisso che corrisponde al livello **Normale** indicato di seguito.

Questa opzione definisce il livello di compressione applicato ai dati inclusi nel backup. I livelli disponibili sono: **Nessuno**, **Normale**, **Alto**, **Massimo**.

L'impostazione predefinita è: **Normale**.

Un livello di compressione più elevato indica che il processo di backup richiede più tempo, ma il backup risultante occupa meno spazio. Attualmente, i livelli **Alto** e **Massimo** funzionano in modo simile.

Il livello ottimale della compressione dei dati dipende dal tipo di dati inclusi nel backup. Ad esempio, anche la comprensione massima non riduce significativamente le dimensioni del backup, se quest'ultimo contiene essenzialmente file compressi quali .jpg, .pdf o .mp3. La compressione di determinati formati, quali .doc o .xls, verrà tuttavia eseguita correttamente.

Gestione degli errori

Queste opzioni permettono di specificare come trattare gli errori che si potrebbero verificare durante il backup.

Riprova se si verifica un errore

L'impostazione predefinita è: **Abilitata. Numero di tentativi: 10. Intervallo tra i tentativi: 30 secondi.**

Quando si verifica un errore recuperabile, il programma riprova ad eseguire l'operazione non riuscita. È possibile impostare l'intervallo di tempo e il numero dei tentativi. I tentativi avranno termine appena l'operazione è stata completata correttamente oppure quando viene eseguito il numero specificato dei tentativi, a seconda dell'evento che si verifica prima.

Per esempio, se la destinazione di backup sulla rete diventa non disponibile o non raggiungibile durante l'esecuzione di un backup, il software tenterà di raggiungere la destinazione ogni 30 secondi ma non più di 30 volte. I tentativi saranno interrotti appena si ristabilisce la connessione oppure quando viene eseguito il numero specificato dei tentativi, a seconda dell'evento che si verifica prima.

Se, tuttavia la destinazione di backup non è disponibile all'avvio del backup, verranno eseguiti solo 10 tentativi.

© Acronis International GmbH, 2003-2024

Non visualizzare i messaggi e le finestre di dialogo durante l'elaborazione (modalità nascosta)

L'impostazione predefinita è: **Abilitata**.

Con la modalità nascosta abilitata, il programma gestirà automaticamente le situazioni che richiedono l'intervento dell'utente (eccetto per la gestione dei settori difettosi, che è definita come opzione separata). Se un'operazione non può continuare in assenza di un'interazione dell'utente, non sarà portata a termine. I dettagli dell'operazione, inclusi eventuali errori, potranno essere visualizzati nel registro dell'operazione.

Ignora settori danneggiati

L'impostazione predefinita è: **Disabilitata**.

Quando l'opzione è disabilitata, ogni volta che il programma riscontra un settore danneggiato, all'attività di backup verrà assegnato lo stato **Richiesta interazione**. Per realizzare un backup delle informazioni valide presenti su un disco difettoso, abilitare l'opzione per ignorare i settori corrotti. Il resto dei dati verrà copiato con un backup e sarà possibile montare il disco finale ed estrarre i file validi su un altro disco.

Nota
In Linux non è consentito ignorare i settori danneggiati. È possibile eseguire il backup di sistemi Linux con settori danneggiati in modalità offline, utilizzando il generatore di supporti di avvio nella versione in locale di Cyber Protect. Per utilizzare il generatore in locale è richiesta una licenza separata. Contattare il supporto per richiedere assistenza.

Riprova se si verifica un errore durante la creazione dello snapshot MV

L'impostazione predefinita è: **Abilitata. Numero di tentativi: 3. Intervallo tra i tentativi: 5 minuti.**

Quando si verifica un errore durante la creazione di uno snapshot di macchina virtuale, il programma riprova ad eseguire l'operazione non riuscita. È possibile impostare l'intervallo di tempo e il numero dei tentativi. I tentativi avranno termine appena l'operazione è stata completata correttamente OPPURE quando viene eseguito il numero specificato dei tentativi, a seconda dell'evento che si verifica prima.

Backup incrementale/differenziale veloce

Questa opzione è disponibile quando per entrambi il backup a livello di disco.

Questa opzione non è disponibile (sempre disabilitata) per i volumi formattati con i file system JFS, ReiserFS3, ReiserFS4, ReFS o XFS.

L'impostazione predefinita è: **Abilitata**.

© Acronis International GmbH, 2003-2024

Nel backup incrementale o differenziale sono acquisite solo le modifiche dei dati. Per accelerare la procedura di backup, il programma determina se il file sia cambiato o no sotto il profilo della dimensione e della data/ora dell'ultima modifica. Se si disattiva questa funzione, il programma confronterà l'intero contenuto del file con quello memorizzato nel backup.

Filtri file (Inclusioni/Esclusioni)

Utilizzare i filtri file per includere solo specifiche cartelle o file in un backup o per escludere da un backup solo file e cartelle specifiche.

Se non diversamente specificato, i filtri file sono disponibili per i backup dell'intero sistema, i backup del disco e i backup a livello di file.

I filtri dei file non sono disponibili con i file system XFS, JFS, exFAT e ReiserFS4. Per ulteriori informazioni, consultare "File system supportati" (pag. 54).

I filtri file non applicabili ai dischi dinamici (volumi LVM o LDM) delle virtual machine il cui backup viene eseguito in modalità agentless, ad esempio da Agente per VMware, Agente per Hyper-V o Agente per Scale Computing.

Per attivare i filtri file

1. In un piano di protezione, espandere il modulo **Backup**.
2. In **Opzioni di backup**, fare clic su **Modifica**.
3. Selezionare **Filtri file (Inclusioni/Esclusioni)**.
4. Utilizzare una qualsiasi delle opzioni descritte qui di seguito.

Filtri di inclusione ed esclusione

Sono disponibili due filtri: un filtro di inclusione e un filtro di esclusione.

- **Includi solo i file che corrispondono ai seguenti criteri**

  Se si specifica `C:\File.exe` nel filtro di inclusione, verrà eseguito solo il backup di questo file, anche se si seleziona il backup dell'intera macchina.

  Nota
  Questo filtro non è supportato per i backup a livello di file il formato del backup e nella **Versione 11** e se la destinazione di backup non è il cloud storage.

- **Escludi i file che corrispondono ai seguenti criteri**

  Se si specifica `C:\File.exe` nel filtro di esclusione, questo file verrà ignorato nel corso del backup, anche se si seleziona il backup dell'intera macchina.

È possibile utilizzare entrambi i filtri contemporaneamente. Il filtro di esclusione prevale sul filtro di inclusione: ciò significa che se si specifica `C:\File.exe` in entrambi i campi, questo file verrà ignorato nel corso del backup.

© Acronis International GmbH, 2003-2024

Criteri di selezione

Come criteri di filtro è possibile utilizzare nomi di file e cartelle, percorsi completi a file e cartelle e maschere con simboli jolly.

I criteri dei filtri non danno distinzione tra maiuscole o minuscole. Ad esempio, se si specifica `C:\Temp`, si selezioneranno anche `C:\TEMP` e `C:\temp`.

- Nome

  Specificare il nome del file o della cartella, ad esempio `Document.txt`. Verranno selezionati tutti i file e le cartelle con quel nome.
- Percorso completo

  Specificare il percorso completo del file o della cartella, iniziando con la lettera di unità (quando si esegue il backup di Windows) o con la directory root (quando si esegue il backup in Linux o macOS). In Windows, Linux e macOS è possibile utilizzare le barre, come in `C:/Temp/File.tmp`. In Windows, è possibile utilizzare anche la barra rovesciata, come in `C:\Temp\File.tmp`.

  Importante

  Se il sistema operativo della macchina di cui è stato eseguito il backup non viene rilevato correttamente durante il backup del disco, il percorso intero ai filtri file non funzionerà. Per i filtri di esclusione viene visualizzato un avviso. In presenza di un filtro di inclusione, il backup non avrà esito positivo.

  Per esempio, un percorso completo al file è: `C:\Temp\File.tmp`. Un filtro con percorso completo, che include la lettera di unità o la directory radice, ad esempio `C:\Temp\File.tmp` o `C:\Temp\*` avrà come esito un avviso o un errore.

  Un filtro che non include la lettera di unità o la root directory (ad esempio `Temp\*` o `Temp\File.tmp`) o un filtro che inizia con un asterisco (ad esempio `*C:\`) non avrà come esito un avviso o un errore. Tuttavia, se il sistema operativo del sistema di cui è stato eseguito il backup non viene rilevato correttamente, questi filtri non funzioneranno.

- Maschera

  È possibile utilizzare i seguenti caratteri jolly per i nomi e i percorsi completi: asterisco (*), doppio asterisco (**), punto interrogativo (?).

  L'asterisco (*) sostituisce lo zero o più caratteri. Ad esempio, il criterio di filtro **Doc*.txt** corrisponde a file come `Doc.txt` e `Documento.txt`.

  Il doppio asterisco (**) sostituisce lo zero o più caratteri, inclusa la barra. Ad esempio, ****/Docs/**.txt** corrisponde a tutti i file con estensione txt in tutte le sottocartelle di tutte le cartelle denominate `Docs`. Il doppio asterisco (**) può essere utilizzato solo per i backup nel formato Versione 12.

  Il punto interrogativo (?) sostituisce un solo carattere. Ad esempio, **Doc?.txt** corrisponde ai file `Doc1.txt` e `Docs.txt`, ma non ai file `Doc.txt` o `Doc11.txt`.

© Acronis International GmbH, 2003-2024

Istantanea di backup a livello di file

Questa opzione ha effetto solo per backup a livello di file

Questa opzione definisce se eseguire il backup di file uno per uno o creare uno snapshot di dati.

Nota
I file memorizzati nelle condivisioni di rete vengono sempre sottoposti a backup uno alla volta.

L'impostazione predefinita è:

- Se per il backup sono selezionate solo macchine che eseguono Linux: **Non creare uno snapshot.**
- Altrimenti: **Crea uno snapshot se possibile.**

È possibile selezionare una delle seguenti opzioni:

- **Crea uno snapshot se possibile**
  Esegui direttamente il backup dei file se non è possibile creare uno snapshot.
- **Crea sempre un'istantanea**
  Lo snapshot abilita il backup di tutti i file, inclusi quelli aperti per l'accesso esclusivo. I file saranno inseriti nel backup nello stesso punto temporale. Scegliere questa impostazione solo se questi fattori sono critici, cioè se non ha senso eseguire il backup dei file senza uno snapshot. Se non è possibile creare uno snapshot, il backup fallirà.
- **Non creare uno snapshot**
  Esegui sempre il backup dei file direttamente. Il tentativo di eseguire backup dei file aperti con accesso esclusivo provocherà un errore di lettura. I file nel backup potrebbero non essere cronologicamente coerenti.

Dati forensi

Virus, malware e ransomware possono contenere azioni dannose e causare il furto o la modifica dei dati. Su queste attività è possibile effettuare delle indagini, a condizione che siano fornite delle prove digitali. Tuttavia, alcune prove digitali, come i file o le tracce di attività, possono essere state cancellate, oppure il sistema sul quale è avvenuta l'attività potrebbe diventare non disponibile.

I backup con dati forensi consentono agli investigatori di analizzare aree del disco che in genere non sono incluse in un normale backup di disco. L'opzione di backup **Dati forensi** consente di raccogliere le seguenti prove digitali, che possono essere utilizzate in indagini forensi: snapshot dello spazio su disco non utilizzato, dump di memoria e snapshot dei processi in esecuzione.

I backup con dati forensi vengono autenticati automaticamente.

L'opzione **Dati forensi** è disponibile solo per i backup dell'intero sistema di sistemi Windows con i sistemi operativi seguenti:

© Acronis International GmbH, 2003-2024

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

I backup con dati forensi non sono disponibili per i sistemi seguenti:

- Sistemi connessi alla rete tramite VPN che non hanno accesso diretto a Internet
- Sistemi con dischi crittografati da BitLocker

Nota
Non è possibile modificare le impostazioni relative ai dati forensi dopo aver applicato al sistema un piano di protezione con il modulo **Backup** abilitato. Per utilizzare impostazioni diverse relative ai dati forensi, creare un nuovo piano di protezione.

È possibile archiviare i backup con dati forensi nelle posizioni seguenti:

- Archiviazione nel cloud
- Cartella locale

  Nota
  La posizione nella cartella locale è supportata solo per i dischi rigidi esterni connessi tramite USB. I dischi dinamici locali non sono supportati come posizione per i backup con dati forensi.

- Cartella di rete

Processo di backup con dati forensi

Durante la creazione di backup con dati forensi, il sistema esegue quanto indicato di seguito:

1. Acquisisce il dump della memoria raw e l'elenco dei processi in esecuzione.
2. Riavvia automaticamente un sistema con il supporto di avvio.
3. Crea il backup che include sia lo spazio occupato che quello non allocato.
4. Autentica i dischi di cui è stato eseguito il backup.
5. Sia riavvia con il sistema operativo live e continua l'esecuzione del piano (ad esempio eseguendo la replica, la conservazione, la convalida e altre attività).

Per configurare la raccolta di dati forensi

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**. In alternativa, è possibile creare il piano di protezione dalla scheda **Gestione**.
2. Selezionare il dispositivo e fare clic su **Proteggi**.
3. Nel piano di protezione, attivare il modulo **Backup**.
4. In **Cosa includere nel backup**, selezionare **Intera macchina**.
5. In **Opzioni di backup**, fare clic su **Modifica**.
6. Individuare l'opzione **Dati forensi**.

© Acronis International GmbH, 2003-2024

7. Abilitare **Raccogli dati forensi**. Il sistema acquisisce automaticamente un dump di memoria e crea uno snapshot dei processi in esecuzione.

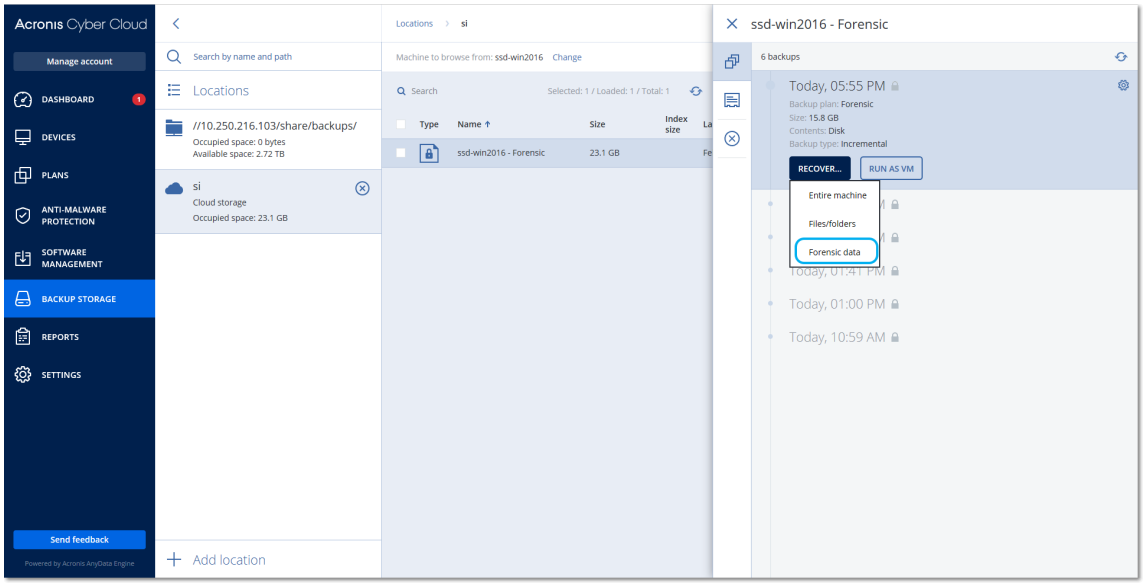
   Nota
   Il dump della memoria completa può contenere dati sensibili, ad esempio password.

8. Specificare la posizione.
9. Fare clic su **Esegui ora** per eseguire un backup con dati forensi subito o attendere la creazione del backup in base alla pianificazione.
10. Passare a **Monitoraggio** > **Attività** e verificare che la creazione del backup con dati forensi sia riuscita.

A questo punto, i backup includeranno i dati forensi che sarà possibile acquisire e analizzare. I backup con dati forensi vengono contrassegnati e possono essere filtrati tra gli altri backup in **Archivio di backup** > **Posizioni** utilizzando l'opzione **Solo con dati forensi**.

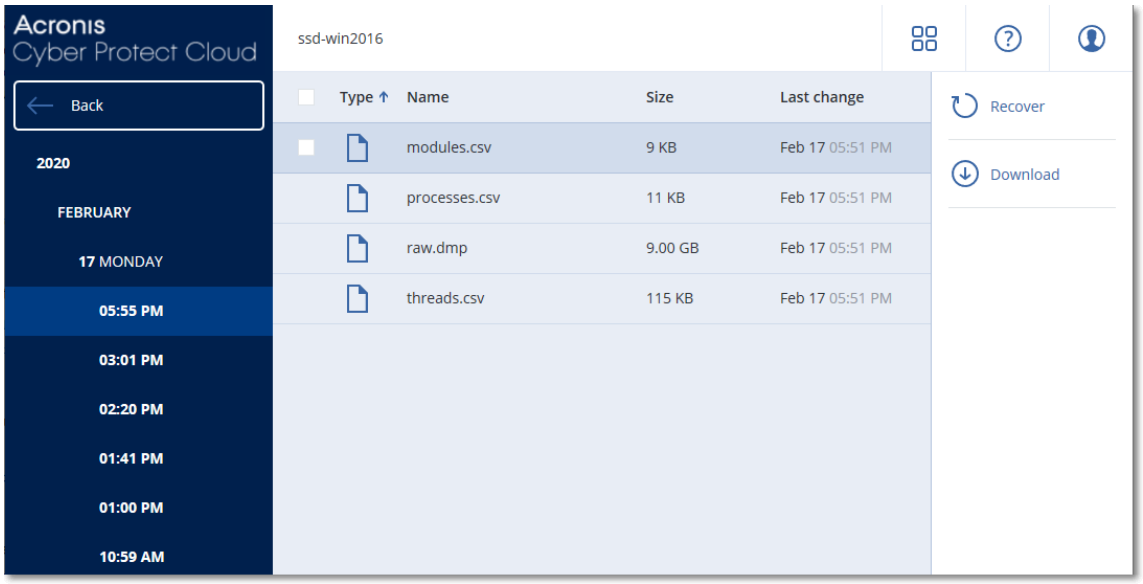
Come ottenere i dati forensi da un backup

1. Nella console di Cyber Protect, passare a **Archivio di backup** e selezionare la posizione con i backup che includono dati forensi.
2. Selezionare il backup con dati forensi e fare clic su **Mostra backup**.
3. Fare clic su **Ripristina** per il backup con dati forensi.
   - Per ottenere solo i dati forensi, fare clic su **Dati forensi**.



   Il sistema visualizza una cartella con i dati forensi. Selezionare un file dump di memoria o qualsiasi altro file con dati forensi e fare clic su **Scarica**.

© Acronis International GmbH, 2003-2024



- Per ripristinare un intero backup forense, fare clic su **Intera macchina**. Il sistema recupera il backup senza la modalità di avvio. Ciò consente di controllare che il disco non abbia subìto modifiche.

È possibile utilizzare il dump di memoria fornito con diversi software per dati forensi di terze parti, come Volatility Framework, disponibile all'indirizzo https://www.volatilityfoundation.org/, che consente ulteriori analisi della memoria.

Autenticazione dei backup con dati forensi

Per garantire che un backup con dati forensi corrisponda esattamente all'immagine eseguita e che non sia stato danneggiato, il modulo Backup offre la funzione di autenticazione di questo tipo di backup.

Come funziona

L'autenticazione consente di dimostrare l'autenticità di un disco con dati forensi e l'assenza di modifiche dal momento dell'esecuzione del backup.

Durante l'esecuzione di un backup, l'agente elabora i codici hash dei dischi sottoposti a backup, crea un albero hash, lo salva nel backup e quindi invia la root dell'albero hash al servizio di autenticazione. Il servizio di autenticazione salva la root dell’albero hash nel database blockchain Ethereum per garantire che questo valore non venga modificato.

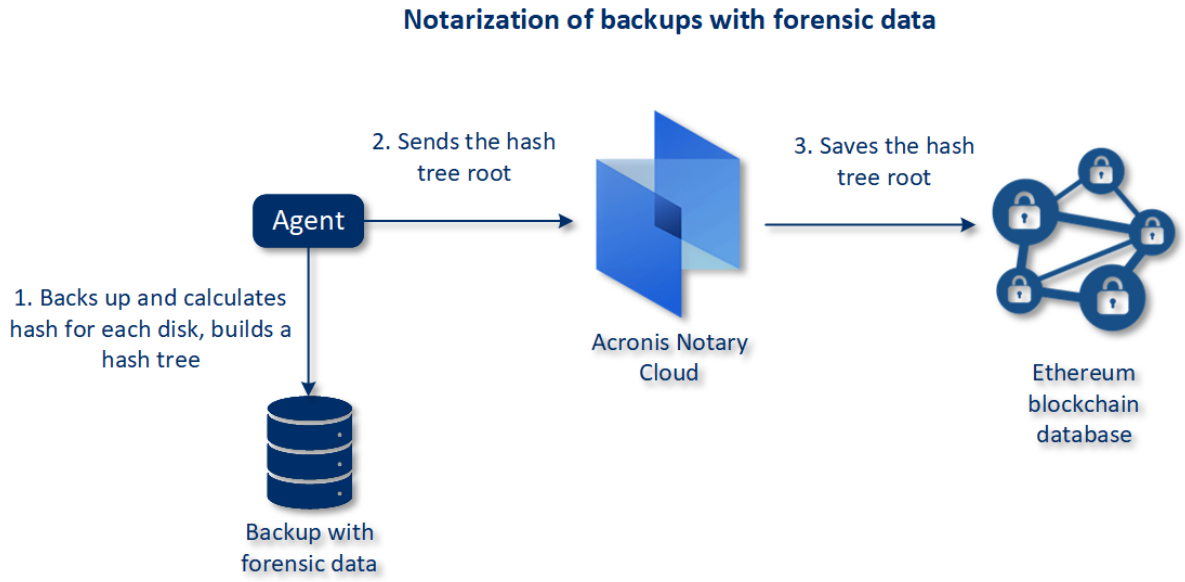
Durante la verifica dell'autenticità del disco con dati forensi, l'agente elabora l'hash del file ed esegue il confronto con l'hash archiviato nell'albero hash all'interno del backup. Se gli hash non corrispondono, il disco non è considerato autentico. Altrimenti, l'autenticità del disco è garantita dall'albero hash.

Per verificare che lo stesso albero hash non sia stato compromesso, l’agente invia la root dell’albero hash al servizio di autenticazione, che lo confronta con quello archiviato nel database blockchain. Se

© Acronis International GmbH, 2003-2024

gli hash corrispondono, viene garantita l'autenticità del disco selezionato. In caso contrario, il software visualizza un messaggio che segnala la non autenticità del disco.

Lo schema seguente mostra in breve il processo di autenticazione dei backup con dati forensi.



Per verificare manualmente il backup del disco autenticato, è possibile acquisire il relativo certificato e seguire la procedura di verifica indicata nel certificato stesso utilizzando lo strumento tibxread.

Acquisizione dei certificato per i backup con dati forensi

Per acquisire il certificato per un backup con dati forensi dalla console, attenersi alla procedura seguente:

1. Aprire **Archivio di backup** e selezionare il backup con dati forensi.
2. Ripristinare l'intero sistema.
3. Il sistema si apre nella visualizzazione **Mappatura disco**.
4. Fare clic sull'icona **Ottieni certificato** relativa al disco.
5. Il sistema genera il certificato e apre una nuova finestra nel browser con il certificato. Al di sotto del certificato sono visibili le istruzioni per la verifica manuale del backup del disco autenticato.

Strumento "tibxread" per l'acquisizione dei dati di cui è stato eseguito il backup

Cyber Protection offre uno strumento chiamato `tibxread` che consente il controllo manuale dell'integrità del disco di cui è stato eseguito il backup. Tale strumento permette di ottenere i dati di un backup e di elaborare l'hash del disco specificato. Lo strumento viene installato automaticamente insieme ai seguenti componenti: Agente per Windows, Agente per Linux e Agente per Mac.

© Acronis International GmbH, 2003-2024

Il percorso di installazione corrisponde alla stessa cartella dell'agente (ad esempio, `C:\Program Files\BackupClient\BackupAndRecovery`).

Le posizioni supportate sono:

- Il disco locale
- La cartella di rete (CIFS/SMB) alla quale è possibile accedere senza le credenziali.
  Nel caso in cui la cartella di rete sia protetta con password, è possibile montare la cartella di rete nella cartella locale utilizzando gli strumenti in dotazione con il sistema operativo e quindi utilizzare la cartella locale come origine per lo strumento.
- L'archivio nel cloud
  È necessario fornire URL, porta e certificato. L'URL e la porta possono essere ottenuti dal registro di sistema di Windows o dai file di configurazione nei sistemi Linux/Mac.
  Per Windows:

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<tenant_login>\FesUri
  ```

  Per Linux:

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  Per macOS:

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  Il certificato è reperibile nelle posizioni seguenti:
  Per Windows:

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```

  Per Linux:

  ```
  /var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

  Per macOS:

  ```
  /Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

Lo strumento include i comandi seguenti:

- `list backups`
- `list content`
- `get content`
- `calculate hash`

© Acronis International GmbH, 2003-2024

list backups

Elenca i punti di ripristino in un backup.

RIEPILOGO:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Opzioni

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Modello di output:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <data> <indicatoredataora>
```

<guid> – il GUID di un backup.

<data> – una data di creazione del backup. Il formato del valore è "GG.MM.AAAA HH24:MM:SS". È indicato nel fuso orario locale per impostazione predefinita (è possibile modificarlo usando l'opzione --utc).

Esempio di output:

```
GUID   Date   Date timestamp
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

Elenca il contenuto di un punto di ripristino.

RIEPILOGO:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

Opzioni

```
--loc=URI
--arc=BACKUP_NAME
```


© Acronis International GmbH, 2003-2024

```
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

Modello di output:

```
Disk     Size   Notarization status
-------- ------ --------------------
<numero> <dimensione> <stato_autenticazione>
```

<numero> – identificatore del disco.

<dimensione> – dimensione espressa in byte.

<stato_autenticazione> – sono possibili gli stati seguenti: Senza autenticazione, Autenticato, Backup successivo.

Esempio di output:

```
Disk     Size   Notary status
-------- ------ --------------
1        123123465798 Notarized
2        123123465798 Notarized
```

get content

Scrive il contenuto del disco specificato nel punto di ripristino nell'output standard (stdout).

RIEPILOGO:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

Opzioni

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

Elabora l'hash del disco specificato nel punto di ripristino utilizzando l'algoritmo SHA-2 (256-bit) e lo scrive nell'output stdout.

RIEPILOGO:

© Acronis International GmbH, 2003-2024

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Opzioni

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

Descrizione delle opzioni

Opzione	Descrizione
--arc=BACKUP_NAME	Il nome del file di backup ottenibile dalle proprietà del backup nella console di Cyber Protect. È necessario specificare il file di backup con l'estensione tibx.
--backup=RECOVERY_POINT_ID	L'identificatore del punto di ripristino
--disk=DISK_NUMBER	Numero del disco (lo stesso scritto nell'output del comando "get content")

--loc=URI	URI di una posizione di backup. I possibili formati dell'opzione "--loc" sono i seguenti:
	• Nome del percorso locale (Windows)
	`c:/upload/backups`
	• Nome del percorso locale (Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• Archiviazione nel cloud
	`--loc=<indirizzo_IP>:443 --cert=<percorso_certificato> [--storage_path=/1]`
	`<indirizzo_IP>` – è possibile trovarlo nel registro di sistema in Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri
	`<percorso_certificato>` – percorso del file del certificato per accedere a Cyber Protect Cloud. In Windows, ad esempio, il certificato si trova in `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<nomeutente>.crt` dove <nomeutente> è il nome account dell'utente per accedere a Cyber Protect Cloud.

--log=PATH	Consente la scrittura dei registri tramite il percorso (PATH) specificato; il valore è

© Acronis International GmbH, 2003-2024

	relativo solo al percorso locale, il formato è lo stesso del parametro `--loc=URI`. Il livello di registrazione è DEBUG.
--password=PASSWORD	Una password di crittografia per il backup. Se il backup non è crittografato, lasciare vuoto il valore.

--raw	Nasconde le intestazioni (le prime due righe) dell'output del comando. Viene utilizzando quando è necessario analizzare il l'output del comando.
	Esempio di output senza "`--raw`":
	`GUID Date Date timestamp`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	Output con "`--raw`":
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

--utc	Mostra le date nel formato UTC

--progress	Mostra il progresso dell'operazione.
	Per esempio:
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

Troncamento registro

Questa opzione è disponibile per i backup di database Microsoft SQL Server e per backup a livello di disco in cui è abilitata l'opzione di backup dell'applicazione Microsoft SQL Server.

L'opzione consente di determinare se i registri delle transazioni di SQL Server vengono troncati in seguito al corretto completamento di un backup.

L'impostazione predefinita è: **Abilitata**.

Quando l'opzione è abilitata, è possibile ripristinare un database solo a un determinato momento temporizzato del processo di creazione del backup da parte del software. Disabilitare questa opzione se si esegue il backup di registri di transazioni utilizzando il motore di backup nativo di Microsoft SQL Server. Dopo un ripristino sarà possibile applicare i registri delle transazioni e ripristinare così un database a un qualsiasi momento temporizzato.

© Acronis International GmbH, 2003-2024

Creazione snapshot LVM

Questa opzione è disponibile solo per le macchine fisiche.

Questa opzione è disponibile per i backup a livello di disco di volumi gestiti da Linux Logical Volume Manager (LVM). Questi volumi sono chiamati anche volumi logici.

Questa opzione definisce la modalità di creazione dello snapshot di un volume logico. Il software di backup è in grado di eseguire questa operazione da sé o basandosi su Linux Logical Volume Manager (LVM).

L'impostazione predefinita è: **Tramite il software di backup**.

- **Tramite il software di backup**. I dati dello snapshot sono conservati principalmente nella RAM. Il backup è più veloce e non richiede spazio non allocato nel gruppo di volumi. Per questo, si consiglia di modificare l'impostazione predefinita solo in caso di problemi con il backup di volumi logici.
- **Tramite LVM**. Lo snapshot viene archiviato nello spazio non allocato del gruppo di volumi. In caso di mancanza di spazio non allocato, lo snapshot verrà creato dal software di backup.

Lo snapshot viene utilizzato solo durante l'operazione di backup ed è automaticamente eliminato al termine dell'operazione. Non viene conservato alcun file temporaneo.

Punti di montaggio

Questa opzione è disponibile solo in Windows per un backup a livello di file di un'origine di dati che include volumi montati o volumi condivisi del cluster.

Questa opzione è disponibile solo quando si seleziona per il backup una cartella che nella gerarchia delle cartelle è superiore al punto di montaggio. (un punto di montaggio è una cartella a cui un volume aggiuntivo è collegato logicamente).

- Se tale cartella (una cartella principale) è selezionata per il backup e l'opzione **Punti di montaggio** è abilitata, tutti i file che si trovano sul volume montato verranno inclusi nel backup. Se l'opzione **Punti di montaggio** è disabilitata, il punto di montaggio nel backup sarà vuoto. Durante il ripristino di una cartella principale, il contenuto del punto di montaggio verrà ripristinato o meno, a seconda che l'opzione di ripristino **Punti di montaggio** sia abilitata o disabilitata.
- Se viene selezionato il punto di montaggio direttamente o si seleziona una cartella all'interno del volume montato, le cartelle selezionate verranno considerate cartelle comuni. Il loro backup verrà eseguito a prescindere dallo stato dell'opzione **Punti di montaggio** e verranno ripristinate a prescindere dallo stato dell'**opzione di ripristino Punti di montaggio**.

L'impostazione predefinita è: **Disabilitata**.

© Acronis International GmbH, 2003-2024

Nota
È possibile eseguire il backup di macchine virtuali Hyper-V che si trovano in un volume condiviso del cluster eseguendo il backup dei file richiesti o del volume completo con il backup a livello di file. È sufficiente spegnere le macchine virtuali per assicurarsi che il loro backup sia eseguito in stato coerente.

Esempio

Si ipotizzi che la cartella **C:\Dati1** rappresenti un punto di montaggio per il volume montato. Il volume contiene le cartelle **Cartella1** e **Cartella2**. Si crea un piano di protezione per il backup a livello di file dei dati.

Selezionando la casella di controllo del volume C e abilitando l'opzione **Punti di montaggio**, la cartella **C:\Dati1** nel backup conterrà **Cartella1** e **Cartella2**. Quando si esegue il ripristino dei dati di cui è stato eseguito il backup, assicurarsi di utilizzare in modo corretto l'**opzione di ripristino** Punti di montaggio.

Selezionando la casella di controllo del volume C e disabilitando l'opzione **Punti di montaggio**, la cartella **C:\Dati1** nel backup sarà vuota.

Selezionando la casella di controllo della cartella **Dati1**, **Cartella1** o **Cartella2**, le cartelle spuntate verranno incluse nel backup come cartelle ordinarie, a prescindere dallo stato dell'opzione **Punti di montaggio**.

Snapshot multivolume

Questa opzione è disponibile per i backup di macchine virtuali che eseguono Windows o Linux.

Questa opzione si applica al backup a livello di disco. Questa opzione si applica anche al backup a livello di file quando questo file viene eseguito creando uno snapshot. (L'opzione "Snapshot di backup a livello di file" consente di specificare se viene creato uno snapshot durante il backup a livello di file).

L'opzione consente di stabilire se creare gli snapshot di volumi multipli contemporaneamente oppure uno per uno.

L'impostazione predefinita è:

- Se almeno una macchina che esegue Windows è selezionata per il backup: **Abilitata**.
- Altrimenti: **Disabilitata**.

Quando questa opzione è abilitata, gli snapshot di tutti i volumi inclusi nel backup vengono creati simultaneamente. Utilizzare questa opzione per creare un backup coerente di dati estesi su volumi multipli, ad esempio per un database Oracle.

Quando questa opzione è disabilitata, gli snapshot dei volumi vengono creati uno dopo l'altro. Di conseguenza, se i dati si estendono sui vari volumi, il backup risultante potrebbe non essere coerente.

© Acronis International GmbH, 2003-2024

One-click Recovery

Nota
Questa funzionalità è disponibile con il pacchetto Advanced Backup.

Con One-click Recovery è possibile ripristinare automaticamente il backup del disco del sistema. Può trattarsi del backup dell'intero sistema o di un backup di dischi o volumi specifici del sistema.

One-click Recovery supporta le seguenti operazioni:

- Ripristino automatico dall'ultimo backup
- Ripristino da un backup specifico (anche noto come punto di ripristino) interno all'archivio di backup

One-click Recovery supporta i seguenti storage di backup:

- Secure Zone
- Cartella locale
- Cartella di rete
- Archiviazione nel cloud

Importante
È necessario sospendere la crittografia BitLocker fino al successivo riavvio del sistema quando si esegue una delle operazioni seguenti:

- Creazione, modifica o eliminazione della Secure Zone.
- Abilitazione o disabilitazione di Startup Recovery Manager.
- [Solo se Startup Recovery Manager non è stato già abilitato] Esecuzione del primo backup dopo aver abilitato One-click Restore nel piano di protezione. Questa operazione abilita automaticamente Startup Recovery Manager.
- Aggiornamento di Startup Recovery Manager, ad esempio aggiornando la protezione.

Se la crittografia BitLocker non è stata sospesa durante queste operazioni, dopo aver riavviato il sistema è necessario specificare il PIN BitLocker.

Abilitazione di One-click Recovery

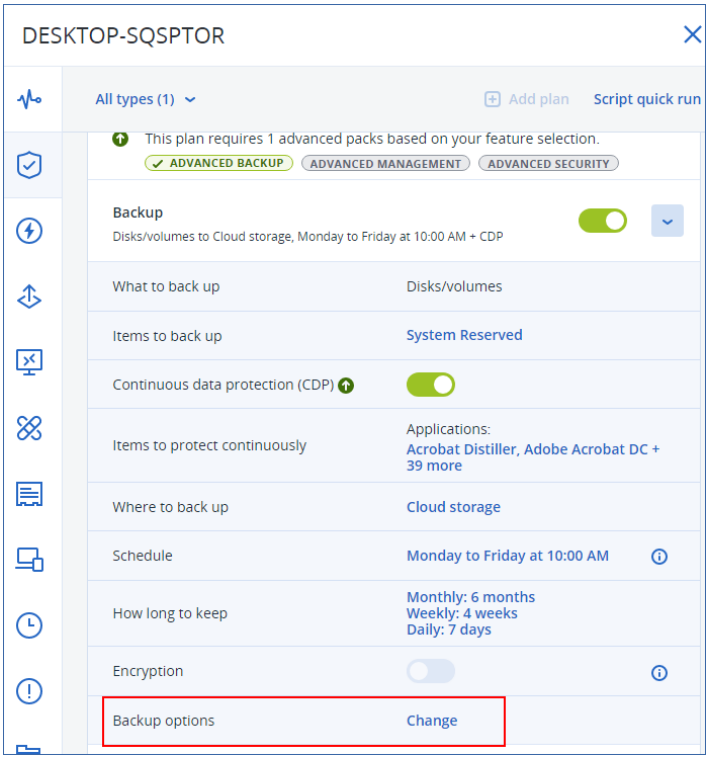
One-click Recovery è un'opzione di backup nel piano di protezione. Per ulteriori informazioni su come creare un piano, consultare "Creazione di un piano di protezione" (pag. 218).

© Acronis International GmbH, 2003-2024

Nota
L'abilitazione di One-click Recovery abilita anche Startup Recovery Manager nell sistema di destinazione. Se non è possibile abilitare Startup Recovery Manager, l'operazione di backup che crea i backup One-click Recovery non avrà esito positivo. Per ulteriori informazioni su Startup Recovery Manager, consultare "Startup Recovery Manager" (pag. 746).

Per abilitare One-click Recovery

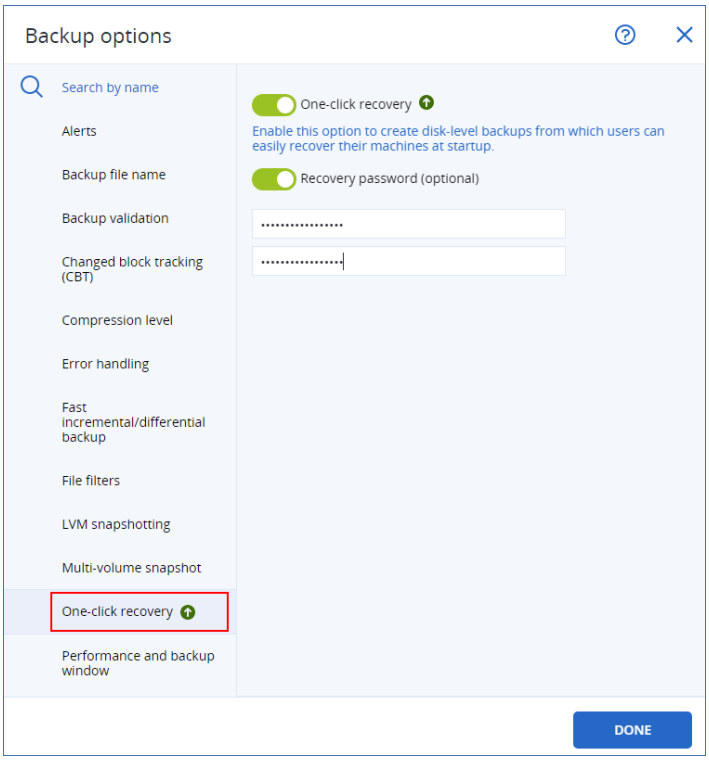
1. In un piano di protezione, espandere il modulo **Backup**.
2. In **Cosa includere nel backup**, selezionare **Intera macchina** o **Disco/Volumi**.
3. [Se è selezionato **Disco/volumi**]. In **Elementi di cui eseguire il backup**, specificare il disco o i volumi di cui eseguire il backup.
4. In **Opzioni di backup**, fare clic su **Modifica**, quindi selezionare **One-click Recovery**.



5. Abilitare l'opzione **One-click Recovery**.
6. [Facoltativo] Abilitare l'opzione **Password di ripristino** e specificare una password.

Importante
Specificare una password di ripristino è fortemente consigliato. Verificare che l'utente che esegue la funzionalità One-click Recovery nel sistema di destinazione conosca tale password.

© Acronis International GmbH, 2003-2024



7. Fare clic su **Fine**.
8. Configurare gli altri elementi del piano di protezione in base alle necessità, quindi salvare il piano.

Dopo l'esecuzione del piano di protezione e la creazione del backup, One-click Recovery diventa accessibile agli utenti del sistema protetto.

Importante
Quando si aggiorna l'agente di protezione, One-click Recovery non sarà temporaneamente disponibile. Per riabilitare la funzionalità, eseguire un backup, al termine del quale One-click Recovery sarà di nuovo disponibile.

Disabilitazione di One-click Recovery

È possibile disabilitare One-click Recovery per un workload specifico come segue:

- Disabilitare l'opzione **One-click Recovery** nel piano di protezione applicato al workload.
- Revocare il piano di protezione in cui l'opzione **One-click Recovery** è abilitata.
- Eliminare il piano di protezione in cui l'opzione **One-click Recovery** è abilitata.

Ripristino di una macchina con One-click Recovery

Prerequisiti

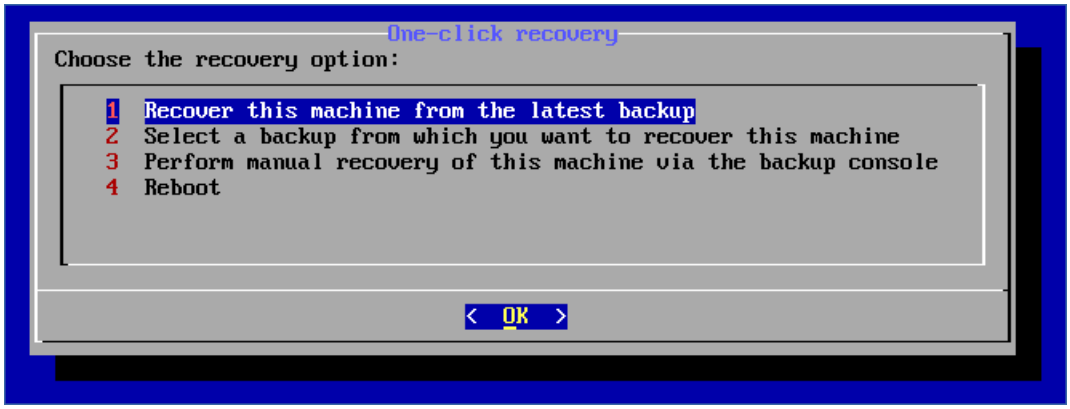
- Al sistema è applicato un piano di protezione con l'opzione di backup **One-click Recovery**.
- È presente almeno un backup di disco del sistema.

© Acronis International GmbH, 2003-2024

Per ripristinare un sistema

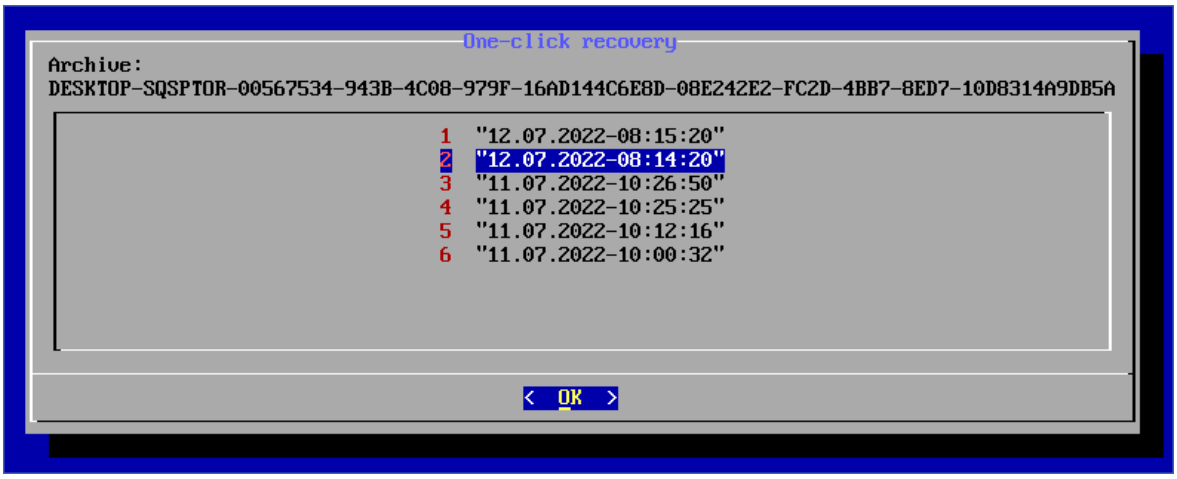
1. Riavviare il sistema che si desidera ripristinare.
2. Durante il riavvio, premere F11 per aprire Startup Recovery Manager.

   Viene aperta la finestra del supporto di ripristino.
3. Selezionare **Acronis Cyber Protect**.
4. [Se nel piano di protezione è stata specificata una password] Inserire la password di ripristino, quindi fare clic su **OK**.
5. Selezionare un'opzione One-click Recovery.
   - Per ripristinare in modo automatico il backup più recente, selezionare la prima opzione, quindi fare clic su **OK**.
   - Per ripristinare un altro backup dall'archivio di backup, selezionare la seconda opzione, quindi fare clic su **OK**.



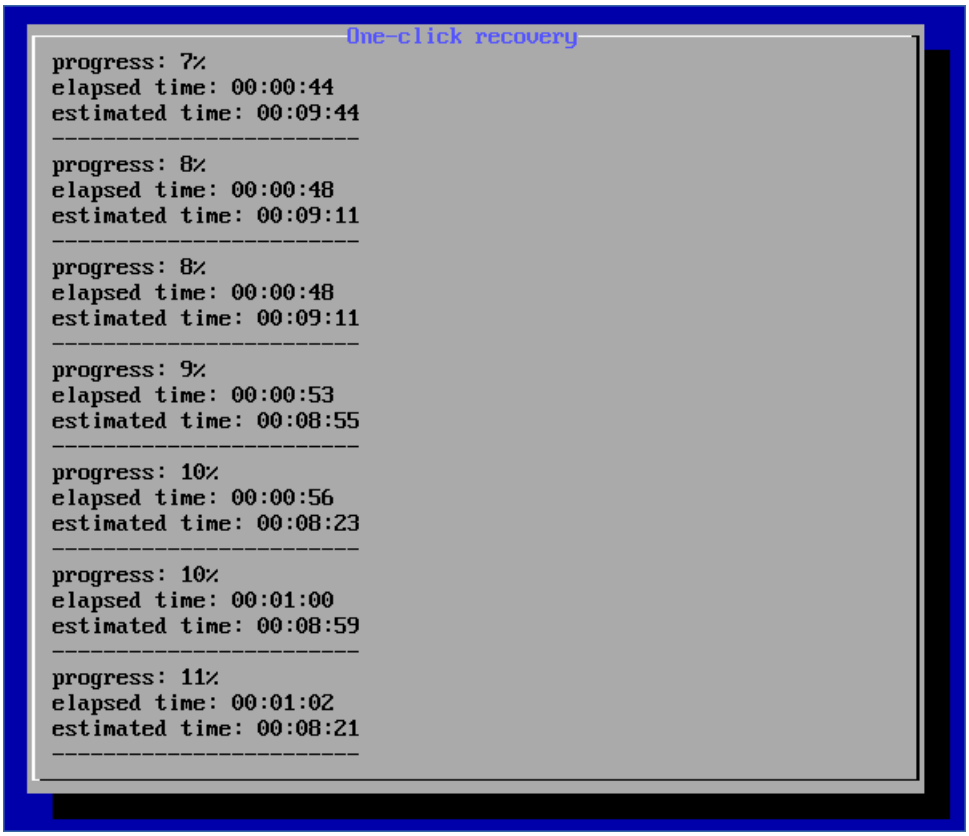
6. Confermare la selezione facendo clic su **Sì**.

   Viene aperta la finestra del supporto di ripristino, quindi si chiude. La procedura di ripristino continua senza interfaccia.
7. [Se si sceglie di ripristinare un backup specifico] Selezionare il backup da ripristinare, quindi fare clic su **OK**.



Dopo qualche momento, il ripristino si avvia e ne viene visualizzato l'avanzamento. Una volta completato il ripristino, il sistema si riavvia.

© Acronis International GmbH, 2003-2024



Prestazioni e finestra di backup

Questa opzione consente di impostare tre livelli di prestazioni del backup (alto, basso, non consentito) per ogni ora in una settimana. In questo modo è possibile definire una finestra di backup durante la quale è consentito l'avvio e l'arresto dei backup. I livelli di prestazione alto e basso sono configurabili in termini di priorità dei processi e velocità di output.

L'opzione non è disponibile per i backup eseguiti dagli agenti cloud, come i backup di siti Web o di server posizionati sul sito di ripristino cloud.

L'opzione ha effetto solo per i processi di backup e replica del backup. I comandi post-backup e le altre operazioni incluse in un piano di protezione (ad esempio, convalida) verranno eseguite indipendentemente da questa opzione.

L'impostazione predefinita è: **Disabilitata**.

Se l'opzione è disabilitata, i backup possono essere eseguiti in qualsiasi orario, con i parametri seguenti, a prescindere che i parametri siano stati modificati rispetto al valore predefinito:

- Priorità CPU: **Bassa** (corrisponde a **Inferiore al normale** in Windows)
- Velocità output: **Illimitata**

Quando questa opzione è abilitata, i backup pianificati sono consentiti o bloccati in base ai parametri prestazionali specificati per l'ora corrente. All'inizio dell'ora in cui i backup sono bloccati, il processo di backup viene arrestato automaticamente e viene generato un avviso. Anche se i backup

© Acronis International GmbH, 2003-2024

pianificati sono bloccati, è possibile avviare un backup manualmente. Tale backup utilizzerà i parametri prestazionali dell'ora più recente in cui i backup erano consentiti.

Nota
È possibile configurare le prestazioni e la finestra di backup per ogni singola posizione di replica. Per accedere alle impostazioni della posizione di replica, nel piano di protezione fare clic sull'icona ingranaggio accanto al nome della posizione, quindi fare clic su **Prestazioni e finestra di backup**.

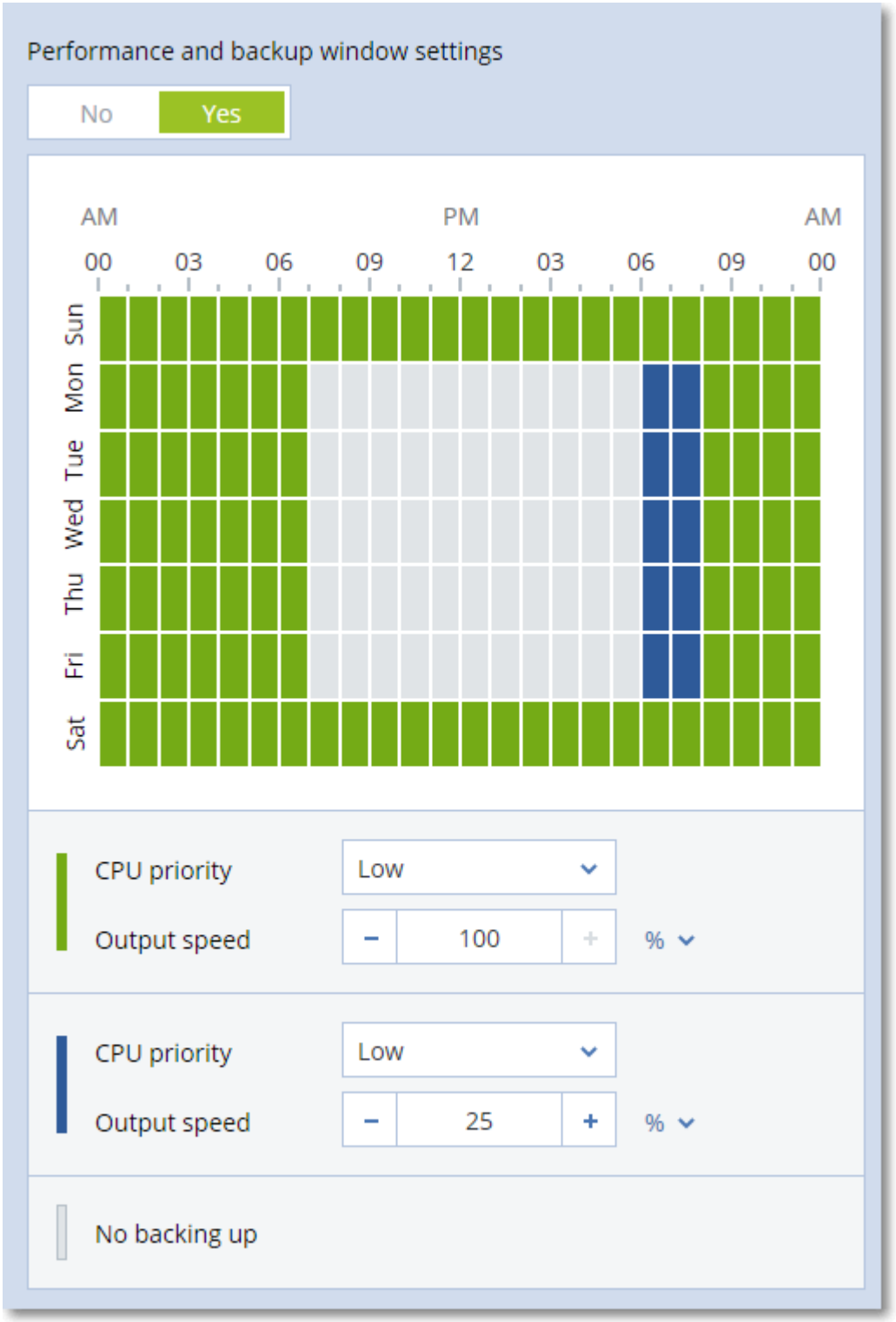
Finestra di backup

Ogni rettangolo rappresenta un'ora di un giorno della settimana. Fare clic su un rettangolo per alternare tra i seguenti stati:

- **Verde:** il backup è consentito con i parametri specificati nella sezione verde sottostante.
- **Blu:** il backup è consentito con i parametri specificati nella sezione blu sottostante.
  Questo stato non è disponibile se il formato del backup è impostato su **Versione 11**.
- **Grigio:** il backup è bloccato.

È possibile selezionare e trascinare per modificare lo stato di più rettangoli simultaneamente.

© Acronis International GmbH, 2003-2024



Priorità CPU

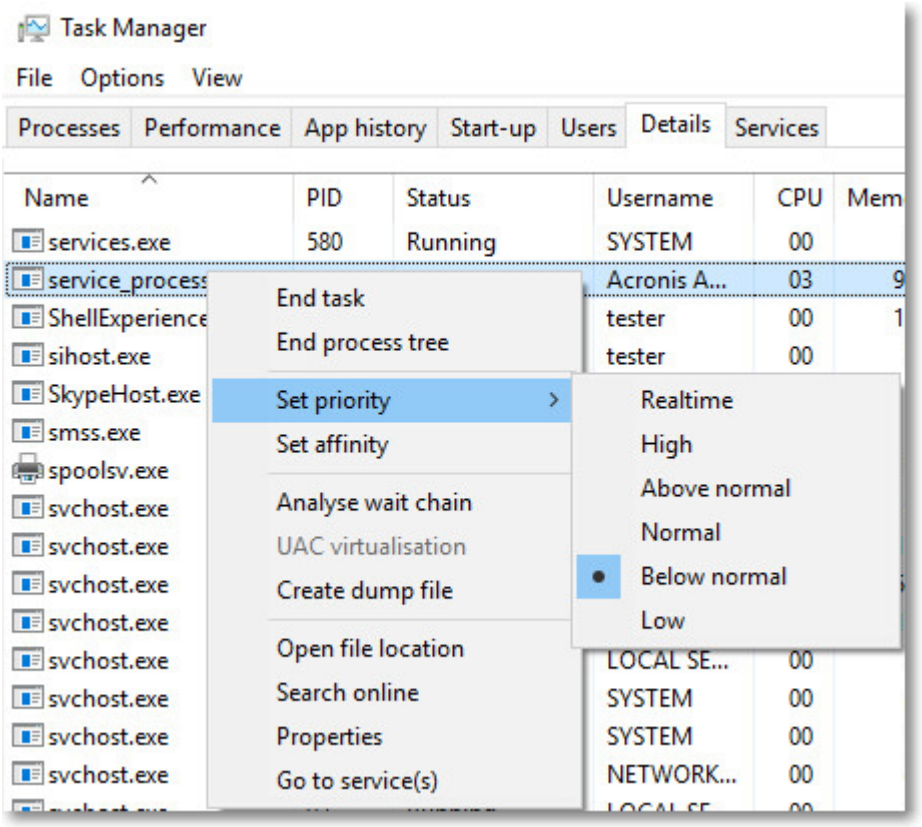
Questa opzione definisce la priorità del processo di backup nel sistema operativo.

Le impostazioni disponibili sono: **Bassa**, **Normale**, **Alto**.

© Acronis International GmbH, 2003-2024

La priorità di un processo eseguito in un sistema determina la quantità di risorse del sistema e della CPU allocate a quel processo. Riducendo la priorità del backup si rendono disponibili più risorse per altre applicazioni. L'innalzamento della priorità del backup può accelerare la procedura di backup, poiché richiede al sistema operativo di allocare maggiori risorse, come la CPU, all'applicazione di backup. Tuttavia, l'effetto finale dipenderà dall'utilizzo complessivo della CPU e da altri fattori, come la velocità in/out del disco o il traffico di rete.

Questa opzione imposta la priorità del processo di backup (**service_process.exe)** in Windows e la qualità del processo di backup (**service_process)** in Linux e macOS.



La tabella seguente riepiloga il mapping di questa impostazione in Windows, Linux e macOS.

Priorità Cyber Protection	Priorità Windows	Qualità per Linux e macOS
Basso	Inferiore al normale	10
Normale	Normale	0
Alto	Alto	-10

Velocità di output durante il backup

Questo parametro consente di limitare la velocità di scrittura del disco rigido (durante il backup in una cartella locale) o la velocità di trasferimento dei dati di backup attraverso la rete (durante il

© Acronis International GmbH, 2003-2024

backup in una condivisione di rete o archivio nel cloud).

Quando l'opzione è abilitata, è possibile specificare la massima velocità di output consentita:

- Come percentuale della velocità di scrittura stimata del disco rigido di destinazione (durante il backup in una cartella locale) o della velocità massima stimata della connessione di rete (durante il backup in una condivisione di rete o archivio nel cloud).

  Questa impostazione è applicabile solo se l'agente è in esecuzione su Windows.
- In KB/secondo (per tutte le destinazioni).

Consegna fisica dei dati

Questa opzione è disponibile se la destinazione del backup o della replica è il cloud storage e se il formato di backup è impostato su **Versione 12**.

Questa opzione è inoltre valida per i backup del disco e per i backup di file creati dall'Agente per Windows, dall'Agente per Linux, dall'Agente per Mac, dall'Agente per VMware, dall'Agente per Hyper-V e dall'Agente per Virtuozzo.

Utilizzare questa opzione per inviare il primo backup completo creato da un piano di protezione al cloud storage su un'unità disco rigido mediante il servizio di Consegna fisica dei dati. I successivi backup incrementali vengono eseguiti sulla rete.

Per i backup locali con replica nel cloud, i backup incrementali proseguono e vengono salvati in locale fino a quando il backup iniziale viene caricato nel cloud storage. A questo punto tutte le modifiche incrementali sono replicate nel cloud e la replica prosegue in base alla pianificazione del backup.

L'impostazione predefinita è: **Disabilitata**.

Informazioni sul servizio di Consegna fisica dei dati

L'interfaccia Web del servizio di Consegna fisica dei dati è disponibile solo agli amministratori.

Per informazioni dettagliate sull'utilizzo del servizio e sullo strumento di creazione dell'ordine, consultare la Guida dell'amministratore del servizio di Consegna fisica dei dati. Per accedere al documento, fare clic sull'icona del punto interrogativo nell'interfaccia Web del servizio.

Panoramica del servizio di Consegna fisica dei dati

1. [Per inviare backup per i quali è stato impostato il cloud storage come posizione di backup primaria]
   a. Creare un nuovo piano di protezione con backup nel cloud.
   b. Nella riga **Opzioni di backup**, fare clic su **Modifica**.
   c. Nell'elenco delle opzioni disponibili, fare clic su **Consegna fisica dei dati**.

   È possibile eseguire il backup direttamente su un'unità rimovibile o in una cartella locale o di rete e quindi copiare o spostare il backup sull'unità.

© Acronis International GmbH, 2003-2024

2. [Per inviare backup locali con replica nel cloud]

   Nota
   Questa opzione è supportata con la versione dell'agente di protezione dalla release C21.06 o successive.

   a. Creare un nuovo piano di protezione con backup in un storage locale o di rete.
   b. Fare clic su **Aggiungi posizione** e selezionare **Archiviazione nel cloud**.
   c. Nella riga della posizione **Archiviazione nel cloud**, fare clic sull'icona ingranaggio e selezionare **Consegna fisica dei dati**.
3. In **Usa la Consegna fisica dei dati**, fare clic su **Sì** e quindi su **Fine**.
   L'opzione Crittografia è abilitata automaticamente nel piano di protezione perché tutti i backup inviati devono essere crittografati.
4. Nella riga **Crittografia**, fare clic su **Specificare una password** e immettere una password di crittografia.
5. Nella riga **Consegna fisica dei dati**, selezionare l'unità rimovibile nella quale verrà salvato il backup iniziale.
6. Fare clic su **Crea** per salvare il piano di protezione.
7. Dopo aver completato il primo backup, utilizzare l'interfaccia Web del servizio di Consegna fisica dei dati per scaricare lo strumento per la creazione dell'ordine e creare l'ordine.
   Per accedere all'interfaccia Web, inserire le credenziali nel portale di gestione, fare clic su **Panoramica** > **Utilizzo**, quindi su **Consegna fisica dei dati** in **Gestisci servizio**.

   Importante
   Dopo aver eseguito il backup completo iniziale, i backup successivi devono essere eseguiti con lo stesso piano di protezione. Un altro piano di protezione, anche se con gli stessi parametri e per lo stesso sistema, richiede un altro ciclo di Consegna fisica dei dati.

8. Imballare le unità e quindi spedirle al data center.

   Importante
   Attenersi scrupolosamente alle informazioni di imballaggio contenute nella Guida dell'amministratore del servizio di Consegna fisica dei dati.

9. Tenere traccia dello stato dell'ordine tramite l'interfaccia Web del servizio. Tenere presente che i backup successivi non avranno esito positivo fino a quando il backup iniziale non viene caricato nell'archivio cloud.

Comandi pre/post

L'opzione permette di definire i comandi da avviare automaticamente prima e dopo la procedura di backup.

Il seguente schema illustra quando vengono avviati i comandi pre/post.

© Acronis International GmbH, 2003-2024

Comandi pre-backup	Backup	Comandi post-backup

Esempio di come utilizzare i comandi pre/post:

- Eliminare alcuni file temporanei dal disco prima di avviare il backup.
- Configurare un prodotto antivirus di terze parti da avviare ogni volta prima dell'inizio del backup.
- Copiare selettivamente i backup in un'altra posizione. Questa opzione può risultare utile poiché la replica configurata in un piano di protezione copia *ogni* backup nelle posizioni successive.

L'agente esegue la replica *dopo* aver eseguito il comando post-backup.

Il programma non supporta comandi interattivi, ad es. comandi che richiedono un input dell'utente (ad esempio, “pause”).

Comandi pre-backup

Per specificare un comando/file batch da eseguire prima dell'avvio della procedura di backup.

1. Abilitare l'opzione **Esegui un comando prima del backup**.
2. Nel campo **Comando...**, immettere un comando o individuare un file batch. Il programma non supporta comandi interattivi, ovvero comandi che richiedono l'immissione dell'utente (ad esempio "pause").
3. Nel campo **Directory di lavoro**, specificare il percorso della directory in cui sarà eseguito il comando/file batch.
4. Nel campo **Argomenti**, specificare gli argomenti di esecuzione del comando, se necessario.
5. A seconda del risultato che si desidera ottenere, selezionare le opzioni appropriate descritte nella tabella seguente.
6. Fare clic su **Fine**.

Casella di controllo	**Selezione**			
Interrompi il backup se l'esecuzione del comando fallisce*	Selezionato	Cancellato	Selezionato	Cancellato
Non eseguire il backup fino al termine dell'esecuzione del comando	Selezionato	Selezionato	Cancellato	Cancellato
Risultato				
	Impostazione	Esegui il backup	N/D	Esegui il backup

© Acronis International GmbH, 2003-2024

	predefinita Esegui il backup solo dopo che il comando è stato eseguito con successo. Interrompi il backup se l'esecuzione del comando fallisce.	solo dopo che il comando è stato eseguito nonostante l'esito negativo o positivo.		simultaneamente con l'esecuzione del comando senza tener conto del risultato dell'esecuzione del comando.

* Un comando viene considerato non riuscito se il codice di uscita non è uguale a zero.

Nota
Se uno script non riesce a causa di un conflitto correlato a una versione della libreria richiesta da Linux, escludere le variabili di ambiente `LD_LIBRARY_PATH` e `LD_PRELOAD` aggiungendo allo script le righe seguenti:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Comandi post-backup

Per specificare un comando/file eseguibile da avviare una volta completato il backup.

1. Abilitare l'interruttore **Esegui un comando dopo il backup**.
2. Nel campo **Comando...**, immettere un comando o individuare un file batch.
3. Nel campo **Directory di lavoro**, specificare il percorso della directory in cui sarà eseguito il comando/file batch.
4. Nel campo **Argomenti**, specificare gli argomenti dell'esecuzione del comando, se richiesto.
5. Selezionare la casella di controllo **Interrompi il backup se l'esecuzione del comando fallisce** se l'esecuzione corretta del comando è fondamentale. Il comando viene considerato non riuscito se il codice di uscita non è uguale a zero. Se l'esecuzione del comando fallisce, lo stato di backup sarà impostato su **Errore**.
   Quando la casella non è selezionata, il risultato dell'esecuzione del comando non influisce sull'esito negativo o positivo del backup. È possibile tracciare il risultato dell'esecuzione dei comandi nella scheda **Attività**.
6. Fare clic su **Fine**.

Comandi prima/dopo la cattura dei dati

Questa opzione consente di definire i comandi da avviare automaticamente prima e dopo l'acquisizione dei dati (ovvero, creando lo snapshot dei dati). L'acquisizione dei dati viene eseguita all'inizio della procedura di backup.

Lo schema seguente illustra quando vengono eseguiti i comandi pre/post acquisizione dati.

© Acronis International GmbH, 2003-2024

	<---------- Backup ---------->				
Comandi pre-backup	Comandi pre-acquisizione dei dati	Acquisizione dati	Comandi post-acquisizione dei dati	Scrittura dei dati nel set di backup	Comandi post-backup

Interazione con altre opzioni di backup

L'esecuzione dei comandi pre/post acquisizione dati può essere modificata da altre opzioni di backup.

Se l'opzione **Snapshot multivolume** è abilitata, i comandi pre/post acquisizione dati verranno eseguiti una sola volta, perché gli snapshot per tutti i volumi vengono creati simultaneamente. Se l'opzione **Snapshot multivolume** è disabilitata, i comandi pre/post acquisizione dati verranno eseguiti per ogni volume di cui viene eseguito il backup, perché gli snapshot vengono creati in sequenza, un volume dopo l'altro.

Se l'opzione **Servizio Copia Shadow del volume** è abilitata, la sequenza dei comandi pre/post acquisizione dati e delle azioni di Microsoft VSS sarà la seguente:

Comandi pre-acquisizione dati -> Sospensione VSS -> Acquisizione dati -> Ripristino VSS -> Comandi post-acquisizione dei dati

Utilizzando i comandi pre/post acquisizione dati, è possibile sospendere e richiamare un database o un'applicazione non compatibile con VSS. Poiché l'acquisizione dei dati richiede pochi secondi, i tempi di inattività del database o dell'applicazione saranno minimi.

Comandi pre-acquisizione dei dati

Per specificare un file di comando/batch da eseguire prima dell'acquisizione dati

1. Abilitare l'opzione **Esegui un comando prima dell'acquisizione dei dati**.
2. Nel campo **Comando...**, immettere un comando o individuare un file batch. Il programma non supporta comandi interattivi, ovvero comandi che richiedono l'immissione dell'utente (ad esempio "pause").
3. Nel campo **Directory di lavoro**, specificare il percorso della directory in cui sarà eseguito il comando/file batch.
4. Nel campo **Argomenti**, specificare gli argomenti di esecuzione del comando, se necessario.
5. A seconda del risultato che si desidera ottenere, selezionare le opzioni appropriate descritte nella tabella seguente.
6. Fare clic su **Fine**.

Casella di controllo	Selezione

© Acronis International GmbH, 2003-2024

Interrompi il backup se l'esecuzione del comando fallisce*	Selezionato	Cancellato	Selezionato	Cancellato
Non eseguire l'acquisizione dei dati fino al termine dell'esecuzione del comando	Selezionato	Selezionato	Cancellato	Cancellato
Risultato				
	Impostazione predefinita Esegui l'acquisizione dei dati solo dopo che il comando è stato eseguito con successo. Interrompi il backup se l'esecuzione del comando fallisce.	Esegui l'acquisizione dei dati solo dopo che il comando è stato eseguito nonostante l'esito negativo o positivo.	N/D	Esegui l'acquisizione dei dati simultaneamente al comando e senza tener conto del risultato dell'esecuzione del comando.

* Un comando viene considerato non riuscito se il codice di uscita non è uguale a zero.

Nota
Se uno script non riesce a causa di un conflitto correlato a una versione della libreria richiesta da Linux, escludere le variabili di ambiente `LD_LIBRARY_PATH` e `LD_PRELOAD` aggiungendo allo script le righe seguenti:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Comandi post-acquisizione dei dati

Per specificare un file di comando/batch da eseguire prima dell'acquisizione dati

1. Abilitare l'opzione **Esegui un comando dopo l'acquisizione dei dati**.
2. Nel campo **Comando...**, immettere un comando o individuare un file batch. Il programma non supporta comandi interattivi, ovvero comandi che richiedono l'immissione dell'utente (ad esempio "pause").
3. Nel campo **Directory di lavoro**, specificare il percorso della directory in cui sarà eseguito il comando/file batch.

© Acronis International GmbH, 2003-2024

4. Nel campo **Argomenti**, specificare gli argomenti di esecuzione del comando, se necessario.
5. A seconda del risultato che si desidera ottenere, selezionare le opzioni appropriate descritte nella tabella seguente.
6. Fare clic su **Fine**.

Casella di controllo	**Selezione**			
Interrompi il backup se l'esecuzione del comando fallisce*	Selezionato	Cancellato	Selezionato	Cancellato
Non eseguire il backup fino al termine dell'esecuzione del comando	Selezionato	Selezionato	Cancellato	Cancellato
Risultato				
	Impostazione predefinita Continua il backup solo dopo che il comando è stato eseguito con successo.	Esegui il backup solo dopo che il comando è stato eseguito nonostante l'esito negativo o positivo.	N/D	Continua il backup simultaneamente con il comando e senza tener conto del risultato dell'esecuzione del comando.

* Un comando viene considerato non riuscito se il codice di uscita non è uguale a zero.

Programmazione

Questa opzione consente di determinare se i backup vengono avviati esattamente secondo la pianificazione o in ritardo e quante virtual machine vengono sottoposte a backup contemporaneamente.

Per ulteriori informazioni su come configurare la pianificazione del backup, consultare "Esecuzione di un backup da una pianificazione" (pag. 428).

L'impostazione predefinita è: **Ripartisci orari di avvio backup in una finestra dell'orario**. **Ritardo massimo**: **30 minuti**.

È possibile selezionare una delle seguenti opzioni:

- **Avvia tutti i backup esattamente come pianificato**
  I backup di macchine fisiche inizieranno quando previsto dalla pianificazione. I backup delle macchine virtuali verranno eseguiti in successione per una macchina alla volta.

© Acronis International GmbH, 2003-2024

- **Ripartisci orari di avvio all'interno di una finestra dell'orario**

  I backup di macchine fisiche verranno avviati in ritardo rispetto alla data/ora prevista nella pianificazione. Il valore di ritardo per ciascun sistema viene selezionato in maniera casuale e rientra in un intervallo compreso tra zero e il massimo valore specificato dall'utente. Per evitare un sovraccarico di rete, potrebbe essere opportuno utilizzare questa impostazione durante la creazione di un backup durante il backup di sistemi multipli in una posizione di rete. Il valore di ritardo per ciascun sistema è determinato quando il piano di protezione viene applicato al sistema e rimane invariato fino a quando non si modifica il piano di protezione cambiando il valore di ritardo massimo.

  I backup delle macchine virtuali verranno eseguiti in successione per una macchina alla volta.
- **Limita il numero di backup eseguiti simultaneamente tramite**

  Utilizzare questa opzione per gestire il backup parallelo di virtual machine il cui backup è eseguito al livello di hypervisor (backup agentless).

  I piani di protezione per i quali è selezionata questa opzione possono essere eseguiti insieme ad altri piani di protezione eseguiti dallo stesso agente nello stesso momento. Quando si seleziona questa opzione, è necessario specificare il numero di backup paralleli per ogni piano. Il numero totale di sistemi il cui backup viene eseguito simultaneamente da tutti i piani è limitato a 10 per agente. Per informazioni su come cambiare il limite predefinito, consultare "Limitare il numero totale di macchine virtuali di cui viene eseguito il backup simultaneo" (pag. 718).

  I piani di protezione nei quali questa opzione non è selezionata eseguono le operazioni di backup in sequenza, una virtual machine dopo l'altra.

Backup settore per settore

L'opzione è disponibile solo per backup a livello di disco.

Questa opzione consente di stabilire se creare una copia esatta di un disco o volume su un livello fisico.

L'impostazione predefinita è: **Disabilitata**.

Se questa opzione è abilitata, tutti i settori del disco o del volume saranno sottoposti a backup, inclusi gli spazi non allocati e i settori liberi da dati. Il backup derivante avrà le stesse dimensioni del disco sottoposto a backup (se l'opzione "Livello di compressione" è impostata su **Nessuno**). Il software passa automaticamente alla modalità settore per settore quando esegue il backup di unità con file system non riconosciuti o non supportati.

Nota
Non sarà possibile eseguire il ripristino dei dati dell'applicazione dai backup creati con la modalità Settore per settore.

Suddivisione

L'opzione consente di selezionare il metodo di suddivisione dei backup di grandi dimensioni in file più piccoli.

© Acronis International GmbH, 2003-2024

Nota
La suddivisione non è disponibile nei piani di protezione che utilizzano il cloud storage come destinazione di backup.

L'impostazione predefinita è:

- Se la posizione di backup è una cartella locale o di rete (SMB) e il formato del backup è Versione 12: **Dimensione fissa - 200 GB**
  Questa impostazione consente al software di backup di operare con volumi di dati di grandi dimensioni nel file system NTFS, senza gli effetti negativi causati dalla frammentazione del file.
- Altrimenti: **Automatico**

Sono disponibili le seguenti impostazioni.

- **Automatico**
  Il backup viene suddiviso se supera le dimensioni file supportate dal file system.
- **Dimensione fissa**
  Inserire la dimensione desiderata del file o selezionarla dall'elenco a discesa.

Gestione fallimento dell'attività

Questa opzione determina il comportamento del programma quando l'esecuzione pianificata di un piano di protezione non riesce o il sistema viene riavviato mentre è in corso un backup. Questa opzione non è valida quando un piano di protezione viene avviato manualmente.

Se l'opzione è abilitata, il programma tenterà di eseguire di nuovo il piano di protezione. È possibile specificare il numero di tentativi e l'intervallo di tempo tra questi. Il programma interrompe l'esecuzione dei tentativi non appena un tentativo viene completato correttamente oppure viene eseguito il numero specificato di tentativi, a seconda dell'evento che si verifica per primo.

Se questa opzione è abilitata e il sistema si riavvia durante l'esecuzione di un backup, l'operazione di backup viene completata. Pochi minuti dopo il riavvio, l'operazione di backup riprenderà automaticamente e il file di backup verrà completato con i dati mancanti. In questo caso d'uso, l'opzione **Intervallo tra i tentativi** non è importante.

L'impostazione predefinita è: **Abilitata**.

Nota
Questa opzione non è disponibile nei backup forensi.

Condizioni di avvio dell'attività

Questa opzione è disponibile per i sistemi operativi Windows e Linux.

Questa opzione determina il comportamento del programma nel caso in cui un'attività stia per essere avviata (arrivi l'orario pianificato o si verifichi l'evento specificato nella pianificazione), ma la

© Acronis International GmbH, 2003-2024

condizione (o una di più condizioni) non sia soddisfatta. Per ulteriori informazioni sulle condizioni, fare riferimento a "Condizioni di avvio" (pag. 434).

L'impostazione predefinita è: **Attendi che le condizioni della pianificazione siano soddisfatte**.

Attendi che le condizioni della pianificazione siano soddisfatte

Con queste impostazioni, l'unità di pianificazione inizia a monitorare le condizioni e avvia l'attività una volta che le condizioni sono soddisfatte. Se non sono presenti le condizioni, l'attività non è avviata.

Per gestire una situazione in cui le condizioni non sono soddisfatte per troppo tempo e ulteriori ritardi del backup diventano rischiosi, è possibile impostare l'intervallo di tempo dopo cui l'attività verrà eseguita senza tener conto delle condizioni. Selezionare la casella di controllo **Esegui comunque l'attività dopo** e specificare l'intervallo di tempo. L'attività inizierà appena le condizioni sono soddisfatte OPPURE il ritardo di tempo massimo scade, a seconda di quale si verifica prima.

Ignora l'esecuzione dell'attività

Il ritardo di un'attività potrebbe non essere accettabile, per esempio, quando è necessario eseguirla esattamente all'ora specificata. In questi casi è opportuno ignorare l'attività piuttosto che attendere le condizioni, soprattutto se le attività si verificano relativamente spesso.

Servizio Copia Shadow del volume (VSS)

Questa opzione è applicabile solo nei sistemi operativi Windows.

Stabilisce se un backup può riuscire nel caso in cui uno o più writer del Servizio Copia Shadow del volume non funzionano e quale provider deve notificare alle applicazioni VSS-aware che il backup sta per essere avviato.

L'utilizzo del Servizio Copia Shadow del volume garantisce lo stato omogeneo di tutti i dati utilizzati dalle applicazioni; in particolare, il completamento di tutte le transazioni del database al momento della creazione dello snapshot dei dati da parte del software di backup. La coerenza dei dati a sua volta garantisce che l'applicazione venga ripristinata nello stato corretto e che sia operativa subito dopo il ripristino.

Lo snapshot viene utilizzato solo durante l'operazione di backup ed è automaticamente eliminato al termine dell'operazione. Non viene conservato alcun file temporaneo.

È anche possibile utilizzare i Comandi pre/post acquisizione di dati per assicurarsi che il backup dei dati venga eseguito in uno stato omogeneo. Ad esempio, specificare i comandi pre-acquisizione di dati che sospenderanno il database e scaricheranno tutte le cache per garantire che tutte le transazioni siano completate; quindi, specificare i comandi post-acquisizione dei dati che consentiranno di riprendere le operazioni del database dopo l'acquisizione dello snapshot.

© Acronis International GmbH, 2003-2024

Nota
Non viene eseguito il backup dei file e delle cartelle specificate nella chiave del Registro di sistema **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**. In particolare, non viene eseguito il backup dei file di dati di Outlook offline (.ost) perché sono specificati nel valore **OutlookOST** di questa chiave.

Ignora writer VSS non riusciti

È possibile selezionare una delle seguenti opzioni:

- **Ignora writer VSS non riusciti**
  Con questa opzione è possibile ottenere backup corretti e completi anche se uno o più writer VSS non funzionano.

  Importante
  I backup application-aware non avranno mai esito positivo se il writer specifico dell'applicazione non funziona. Ad esempio, se si sta eseguendo il backup application-aware dei dati di un SQL Server, e se il writer **SqlServerWriter** non funziona, l'intera operazione di backup non avrà esito positivo.

  Quando questa opzione è attivata, verranno eseguiti fino a tre tentativi consecutivi per creare uno snapshot VSS.
  Nel primo tentativo, vengono richiesti tutti i writer VSS. Se il tentativo non riesce, viene ripetuto. Se anche il secondo tentativo non riesce, il writer VSS non funzionante verrà escluso dall'ambito dell'operazione di backup e verrà eseguito un terzo tentativo. Se questo ultimo tentativo riesce, il backup viene completato con un avviso che segnala i writer VSS non funzionanti. Se il terzo tentativo non si conclude correttamente, il backup non riuscirà.
- **Richiedi la riuscita dell'elaborazione per tutti i writer VSS**
  Se uno qualsiasi dei writer VSS non funziona, l'intera operazione di backup avrà esito negativo.

Selezionare il provider di snapshot

È possibile selezionare una delle seguenti opzioni:

- **Seleziona automaticamente provider di snapshot**.
  Consente la selezione automatica tra provider di snapshot hardware, provider di snapshot software e Microsoft Software Shadow Copy Provider.
- **Utilizza Microsoft Software Shadow Copy Provider**
  Si consiglia di scegliere questa opzione quando si esegue il backup dei server delle applicazioni (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint o Active Directory).

© Acronis International GmbH, 2003-2024

Abilita backup completo VSS

Se l'opzione è abilitata, i registri di Microsoft Exchange Server e di altre applicazioni VSS-aware (eccetto Microsoft SQL Server) verranno troncati dopo ciascun backup completo, incrementale o differenziale del disco.

L'impostazione predefinita è: **Disabilitata**.

Lasciare l'opzione disabilitata nei seguenti casi:

- Se si utilizza Agente per Exchange o software di terze parti per il backup dei dati di Exchange Server. Questa procedura è necessaria, poiché il troncamento del registro interferirà con i backup di registro transazione consecutivi.
- Se si utilizza software di terze parti per il backup dei dati di SQL Server. Questo è necessario, poiché il software di terze parti utilizzerà il backup a livello del disco risultante per il "proprio" backup completo. Di conseguenza, il backup differenziale successivo dei dati di SQL Server fallirà. I backup continueranno a fallire fino a quando il software di terze parti creerà il "proprio" backup completo successivo.
- Se sulla macchina sono in esecuzione altre applicazioni compatibili con VSS ed è necessario conservare i loro registri per qualunque motivo.

Importante
L'abilitazione di questa opzione non produce il troncamento dei registri di Microsoft SQL Server. Per troncare il registro di SQL Server dopo un backup, abilitare l'opzione di backup Troncamento log.

Servizio Copia Shadow del volume per macchine virtuali

Questa opzione consente di stabilire se devono essere creati snapshot inattivi di virtual machine.

L'impostazione predefinita è: **Abilitata**.

Quando l'opzione è disabilitata, verrà creato uno snapshot non inattivo. Il backup della virtual machine verrà eseguito in uno stato crash-consistent.

Quando questa opzione è attivata, le transazioni di tutte le applicazioni compatibili con VSS in esecuzione su una macchina virtuale verranno completate, quindi verrà creato uno snapshot inattivo.

Se non è possibile creare uno snapshot inattivo dopo il numero di tentativi specificati nell'opzione "Gestione degli errori" e il backup delle applicazioni è attivato, il backup verrà interrotto.

Se non è possibile creare uno snapshot inattivo dopo il numero di tentativi specificati nell'opzione "Gestione degli errori" e il backup delle applicazioni è disattivato, verrà creato un backup crash-consistent. Per interrompere il backup invece di creare un backup crash-consistent, selezionare la casella di controllo **Interrompi il backup se non è possibile creare uno snapshot inattivo**.

La tabella seguente riepiloga le impostazioni disponibili e i relativi risultati.

© Acronis International GmbH, 2003-2024

Impostazioni	Lo snapshot inattivo è stato creato correttamente		Lo snapshot inattivo non è stato creato	
	Backup applicazioni abilitato	**Backup applicazioni disabilitato**	**Backup applicazioni abilitato**	**Backup applicazioni disabilitato**
Servizio Copia Shadow del volume per macchine virtuali abilitato **Interrompi il backup se non è possibile creare uno snapshot inattivo** non selezionato	Viene creato uno snapshot inattivo. Viene creato un backup application-consistent.	Viene creato uno snapshot inattivo. Viene creato un backup application-consistent.	Backup non riuscito.	Viene creato uno snapshot non inattivo. Viene creato un backup crash-consistent.
Servizio Copia Shadow del volume per macchine virtuali abilitato **Interrompi il backup se non è possibile creare uno snapshot inattivo** selezionato	Viene creato uno snapshot inattivo. Viene creato un backup application-consistent.	Viene creato uno snapshot inattivo. Viene creato un backup application-consistent.	Backup non riuscito.	Backup non riuscito.
Servizio Copia Shadow del volume per macchine virtuali disabilitato	Viene creato uno snapshot non inattivo. Viene creato un backup crash-consistent.	Viene creato uno snapshot non inattivo. Viene creato un backup crash-consistent.	Viene creato uno snapshot non inattivo. Viene creato un backup crash-consistent.	Viene creato uno snapshot non inattivo. Viene creato un backup crash-consistent.

Abilitando il **Servizio Copia Shadow del volume per macchine virtuali** si attivano anche gli script di pre-blocco e post-sblocco che possono essere presenti nella virtual machine di cui è stato eseguito il backup. Per ulteriori informazioni su questi script, fare riferimento a "Esecuzione automatica degli script di pre blocco e post sblocco" (pag. 710).

Per creare una snapshot inattiva, il software di backup applica VSS in una virtual machine utilizzando Strumenti VMware, Hyper-V Integration Services, Virtuozzo Guest Tools, Red Hat Virtualization Guest Tools o QEMU Guest Tools, rispettivamente.

© Acronis International GmbH, 2003-2024

Nota
Per le virtual machine Red Hat Virtualization (oVirt), è consigliabile installare QEMU Guest Tools invece di Red Hat Virtualization Guest Tools. Alcune versioni di Red Hat Virtualization Guest Tools non supportano le snapshot compatibili con l'applicazione.

Questa opzione non ha effetto sulle virtual machine Scale Computing HC3. Per queste, la disattivazione dipende dalla presenza di strumenti di Scale installati o meno nella virtual machine.

Backup settimanale

Questa opzione determina quali backup sono considerati "settimanali" nelle regole di conservazione e negli schemi di backup. Un backup settimanale è il primo backup creato dopo l'inizio di una settimana.

L'impostazione predefinita è: **Lunedì**.

Registro eventi di Windows

Questa opzione è disponibile quando solo per il sistema operativo Windows

Questa opzione consente di stabilire se gli agenti che operano sulla macchina devono salvare gli eventi delle operazioni di backup nel registro eventi applicazioni di Windows (per visualizzare questo registro, avviare eventvwr.exe o selezionare **Pannello di controllo** > **Strumenti di amministrazione** > **Visualizzatore eventi**). È possibile filtrare gli eventi da registrare.

L'impostazione predefinita è: **Disabilitata**.

Ripristino

Panoramica del ripristino

La seguente tabella riassume le opzioni di ripristino disponibili. Utilizzare la tabella per scegliere un piano di ripristino adatto per le proprie esigenze.

Nota
Non è possibile ripristinare i backup nella console di Cyber Protect per i tenant in modalità Conformità. Per ulteriori informazioni su come ripristinare questi backup, consultare "Ripristino dei backup per i tenant in modalità Conformità" (pag. 1112).

Cosa convalidare	Metodo di ripristino
Sistema fisico (Windows o Linux)	Uso della console di Cyber Protect Uso di supporti di avvio
Sistema fisico	Uso di supporti di avvio

© Acronis International GmbH, 2003-2024

(Mac)	
Virtual machine (VMware, Hyper-V, Red Hat Virtualization (oVirt) o Scale Computing HC3)	Uso della console di Cyber Protect Uso di supporti di avvio
Virtual machine o contenitore (Virtuozzo, Virtuozzo Hybrid Server, o Virtuozzo Hybrid Infrastructure)	Uso della console di Cyber Protect
Configurazione ESXi	Uso di supporti di avvio
File/cartelle	Uso della console di Cyber Protect Download di file dall'archivio nel cloud Uso di supporti di avvio Estrazione di file dai backup locali
Stato del sistema	Uso della console di Cyber Protect
Database SQL	Uso della console di Cyber Protect
Database Exchange	Uso della console di Cyber Protect
Caselle di posta di Exchange	Uso della console di Cyber Protect
Siti Web	Uso della console di Cyber Protect
Microsoft 365	
Caselle postali (Agente locale per Microsoft 365)	Uso della console di Cyber Protect
Caselle postali (Agente cloud per Microsoft 365)	Uso della console di Cyber Protect
Cartelle pubbliche	Uso della console di Cyber Protect
File di OneDrive	Uso della console di Cyber Protect
Dati di SharePoint Online	Uso della console di Cyber Protect
Google Workspace	
Caselle postali	Uso della console di Cyber Protect
File di Google Drive	Uso della console di Cyber Protect
File di unità condivise	Uso della console di Cyber Protect

© Acronis International GmbH, 2003-2024

Ripristino tra piattaforme

Il ripristino tra piattaforme è disponibile per i backup di interi sistemi e i backup di dischi che contengono un sistema operativo.

Questo tipo di ripristino viene eseguito nei seguenti casi:

- Un backup viene creato da un tipo di agente, ma viene ripristinato da un altro tipo di agente.
- Un backup con agente viene ripristinato a livello di hypervisor (ripristino agentless), oppure un backup agentless viene ripristinato da un agente (ripristino con agente).
- Un backup viene ripristinato su un hardware diverso (incluso su hardware virtuale).

Nota
Alcuni dispositivi periferici, come le stampanti, potrebbero non essere ripristinati correttamente quando si esegue un ripristino tra piattaforme.

La tabella seguente mostra alcuni esempi di ripristino tra piattaforme.

Ripristino tra piattaforme	
Backup agentless	Ripristino con agente
Backup con agente	Ripristino agentless
Backup eseguito da Agente per Windows	Ripristino eseguito da Agente per VMware
Backup eseguito da Agente per VMware	Ripristino eseguito da Agente per Hyper-V
Backup eseguito da Agente per Windows installato su una virtual machine VMware ESXi (con agente)	Ripristino eseguito da Agente per VMware (agentless) sullo stesso host VMware ESXi
Backup eseguito da Agente per Windows	Ripristino eseguito da Agente per Windows installato su un sistema con hardware diverso
Backup di un sistema fisico	Ripristino come virtual machine

Note per gli utenti di Mac

- A partire dal sistema operativo El Capitan 10.11, alcuni file di sistema, cartelle e processi sono contrassegnati per la protezione con l'attributo di file esteso com.apple.rootless. Questa funzione è denominata System Integrity Protection (SIP). Il file protetti includono le applicazioni preinstallate e la maggior parte delle cartelle in /system, /bin, /sbin, /usr.
  Il file e le cartelle protetti non possono essere sovrascritti durante un ripristino dal sistema operativo. Per sovrascrivere i file protetti, eseguire il ripristino da un supporto di avvio.
- A partire da macOS Sierra 10.12, i file utilizzati raramente possono essere spostati in iCloud mediante la funzionalità Store in Cloud. Alcuni piccoli footprint di questi file rimangono nel file system. Viene eseguito il backup di tali footprint anziché dei file originali.

© Acronis International GmbH, 2003-2024

Se si ripristina un footprint nella posizione originale, questo viene sincronizzato con iCloud e il file originale diventa disponibile. Se si ripristina un footprint in una posizione diversa, questo non potrà essere sincronizzato con iCloud e il file originale non sarà disponibile.

Ripristino sicuro

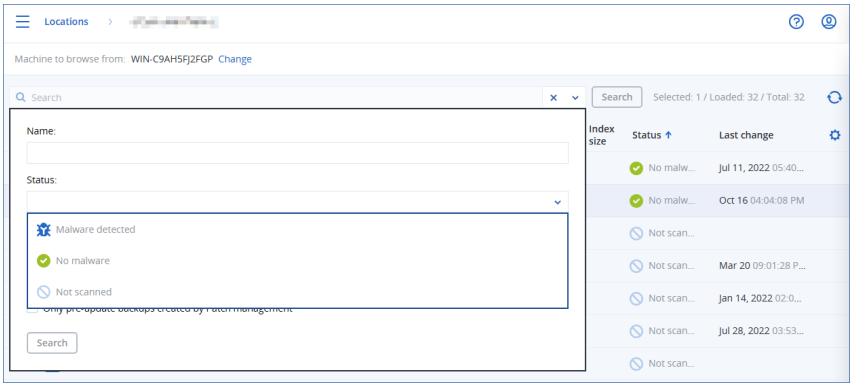
Utilizzare il ripristino sicuro con i backup dell'**Intera macchina** o i backup di **dischi/volumi** di workload Windows per garantire che vengano ripristinati solo dati privi di malware, anche se il backup contiene file infetti.

Durante un'operazione di ripristino sicuro, il backup viene scansionato automaticamente alla ricerca di malware. Quindi, l'agente di protezione ripristina il backup nel workload di destinazione ed elimina ogni eventuale file infetto. Di conseguenza, il backup ripristinato è privo di malware.

Inoltre, al backup viene assegnato uno degli stati seguenti:

- Malware rilevato
- Nessun malware
- Non scansionato

È possibile utilizzare lo stato per filtrare gli archivi di backup.



Limitazioni

- Il ripristino sicuro è supportato sui sistemi Windows fisici e virtuali nei quali è installato un agente di protezione.
- È inoltre supportato per i backup dell'**Intera macchina** o di **dischi/volumi**.
- La scansione anti-malware è supportata solo per i volumi NTFS. I volumi non NTFS vengono ripristinati senza scansione anti-malware.
- Il ripristino sicuro non è supportato per i backup con Protezione continua dei dati (CDP) nell'archivio. Per i recuperare i dati da un backup CDP, eseguire un'operazione di ripristino di **File/cartelle** aggiuntiva. Per ulteriori informazioni sui backup CDP, consultare "Protezione continua dei dati (CDP)" (pag. 416).

© Acronis International GmbH, 2003-2024

Ripristino di una macchina

Ripristino di sistemi fisici

In questa sezione viene descritto il ripristino delle macchine fisiche mediante l'utilizzo dell'interfaccia Web.

Utilizzare supporti di avvio anziché l'interfaccia Web se occorre ripristinare:

- Un sistema che esegue macOS
- Un sistema di un tenant in modalità Conformità
- Da qualsiasi sistema operativo a bare metal o a un sistema offline
- La struttura dei volumi logici (volumi creati da Logical Volume Manager su Linux). Il supporto consente di ricreare la struttura del volume logico in modo automatico.

Nota
Non è possibile ripristinare i backup del disco di sistemi Mac con processori Intel su Mac con processori Apple Silicon, e viceversa. È possibile ripristinare file e cartelle.

Ripristino con riavvio

Il ripristino di un sistema operativo e di volumi crittografati con BitLocker richiede un riavvio. È possibile scegliere se riavviare il sistema automaticamente o assegnare lo stato **Richiesta interazione**. Il sistema operativo ripristinato va online automaticamente.

Importante
I backup dei volumi crittografati vengono ripristinati come non crittografati.

Per il ripristino di volumi crittografati con BitLocker non deve essere presente un volume non crittografato nello stesso sistema; tale volume deve disporre di almeno un 1 GB di spazio disponibile. Se una delle condizioni non viene soddisfatta, il ripristino avrà esito negativo.

Per il ripristino di un volume di sistema crittografato non è richiesta alcuna azione aggiuntiva. Per ripristinare un volume crittografato non di sistema, è necessario per prima cosa bloccarlo, ad esempio aprendo un file che risiede su tale volume. In caso contrario, il ripristino continuerà senza riavvio e il volume ripristinato potrebbe non essere riconosciuto da Windows.

Nota
Se il ripristino non riesce e il riavvio del sistema genera l'errore `Impossibile acquisire il file dalla partizione`, provare a disabilitare l'avvio protetto. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a Disabilitare l'avvio protetto nella documentazione Microsoft.

Per ripristinare una macchina fisica

© Acronis International GmbH, 2003-2024

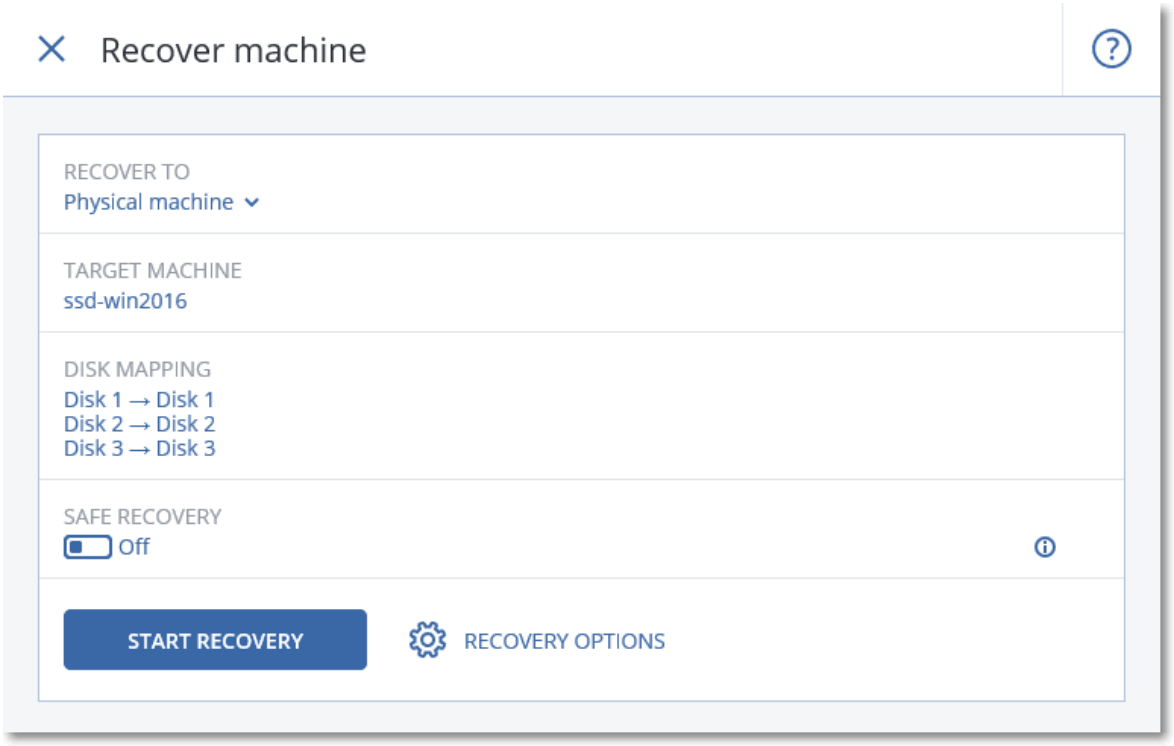
1. Selezionare il sistema di cui è stato eseguito il backup.
2. Fare clic su **Ripristino**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.

   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Eseguire una delle seguenti operazioni:

   - Se la posizione di backup è il cloud o un archivio condiviso (a cui possono accedere altri agenti), fare clic su **Seleziona macchina** e selezionare una macchina di destinazione che sia online, quindi selezionare un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda Archivio di backup.
   - Ripristinare il sistema come descritto in "Ripristino di dischi mediante i supporti di avvio".
4. Fare clic su **Ripristina** > **Intera macchina**.

   Il software esegue automaticamente la mappatura dei dischi dal backup ai dischi della macchina di destinazione.

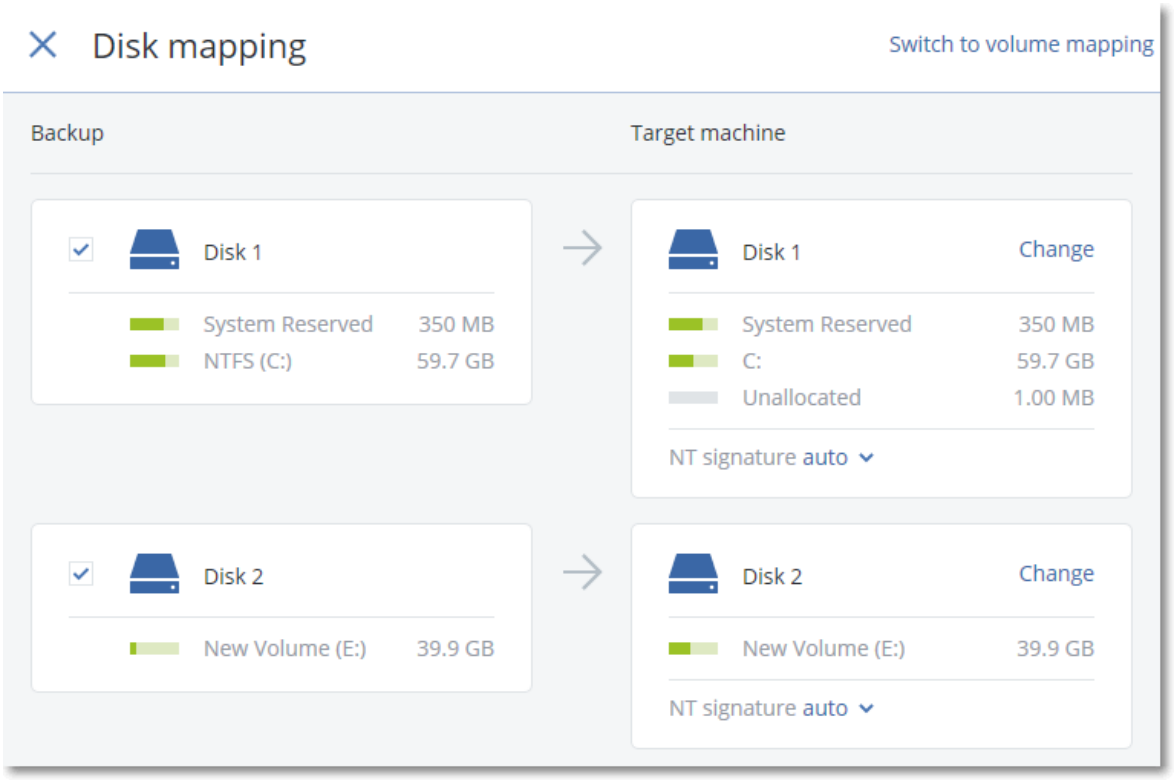
   Per eseguire il ripristino in un'altra macchina fisica, fare clic su **Macchina di destinazione**, quindi selezionare un sistema di destinazione che sia online.



5. Se non si è soddisfatti del risultato della mappatura o se tale operazione non ha avuto esito positivo, fare clic su **Mappatura volume** per ripetere la mappatura dei dischi in modalità manuale.

   La sezione dedicata alla mappatura consente anche di scegliere singoli dischi o volumi per il ripristino. È possibile passare in rassegna i vari dischi e volumi in ripristino tramite il collegamento **Passa a...** nell'angolo in alto a destra.

© Acronis International GmbH, 2003-2024



6. [Disponibile soltanto per i sistemi Windows nei quali è installato un agente di protezione] Abilitare l'opzione **Ripristino sicuro** per verificare che i dati ripristinati siano privi di malware. Per ulteriori informazioni sul funzionamento del ripristino sicuro, consultare "Ripristino sicuro" (pag. 506).
7. Fare clic su **Avvia ripristino**.
8. Confermare che si desidera sovrascrivere i dischi con le versioni di cui si è eseguito il backup. Scegliere se riavviare il sistema automaticamente.

L'avanzamento del ripristino viene mostrato nella scheda **Attività**.

Da macchina fisica a macchina virtuale

È possibile ripristinare un sistema fisico in una virtual machine in uno degli hypervisor supportati. Si tratta inoltre di un meccanismo per migrare un sistema fisico in una virtual machine. Per ulteriori informazioni sui percorsi di migrazione P2V supportati, fare riferimento a "Migrazione del sistema".

In questa sezione viene descritto il ripristino di un sistema fisico come virtual machine utilizzando l'interfaccia web. L'operazione può essere eseguita se almeno uno degli agenti dell'hypervisor di riferimento è installato e registrato in Acronis Management Server. Per esempio, il ripristino su VMware ESXi richiede almeno un Agente per VMware, il ripristino su Hyper-V richiede almeno un Agente per Hyper-V installato e registrato nell'ambiente.

Il ripristino tramite l'interfaccia web non è disponibile ai tenant in modalità Conformità.

© Acronis International GmbH, 2003-2024

Nota
Non è possibile ripristinare le macchine virtuali MacOS su host Hyper-V, perché Hyper-V non supporta MacOS. È invece possibile ripristinare le macchine virtuali MacOS su un host VMware installato su hardware Mac.

Inoltre, non è possibile ripristinare i backup di sistemi fisici macOS come virtual machine.

Per ripristinare una macchina fisica come macchina virtuale

1. Selezionare il sistema di cui è stato eseguito il backup.
2. Fare clic su **Ripristino**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.
   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Eseguire una delle seguenti operazioni:
   - Se la posizione di backup è il cloud o un archivio condiviso (a cui possono accedere altri agenti), fare clic su **Seleziona macchina** e selezionare un sistema che sia online, quindi selezionare un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda Archivio di backup.
   - Ripristinare il sistema come descritto in "Ripristino di dischi mediante i supporti di avvio".
4. Fare clic su **Ripristina** > **Intera macchina**.
5. In **Ripristina in**, selezionare **Macchina virtuale**.
6. Fare clic su **Macchina di destinazione**.
   a. Selezionare l'hypervisor.

      Nota
      Almeno uno degli agenti per l'hypervisor di riferimento deve essere installato e registrato in Acronis Management Server.

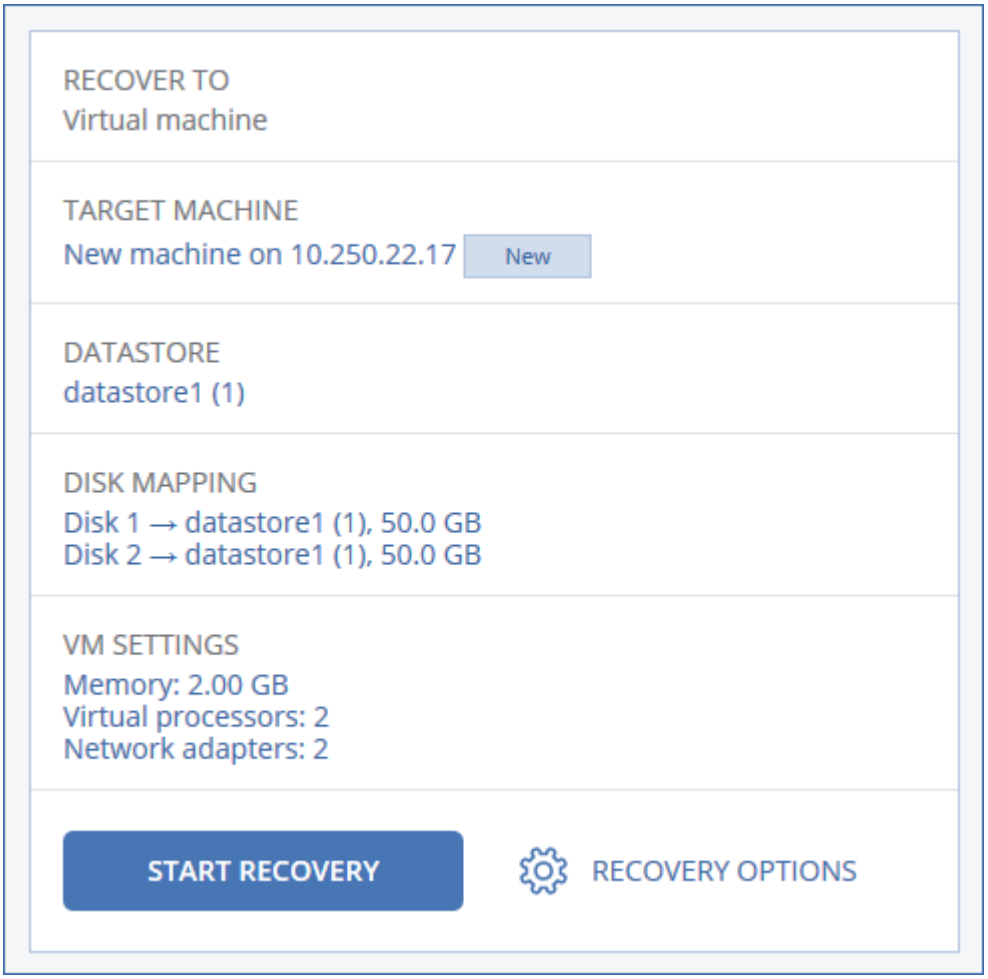
   b. Selezionare se eseguire il ripristino di un sistema nuovo o uno già esistente. L'opzione sistema nuovo è preferibile in quanto non richiede che la configurazione del disco della macchina di destinazione corrisponda perfettamente alla configurazione del disco nel backup.
   c. Selezionare l'host e specificare il nome del nuovo sistema oppure selezionare una macchina di destinazione esistente.
   d. Fare clic su **OK**.
7. [Per Virtuozzo Hybrid Infrastructure] Fare clic su **Impostazioni VM** per selezionare **Versione**. Facoltativamente, è possibile cambiare la dimensione della memoria, il numero di processori e le connessioni di rete della virtual machine.

© Acronis International GmbH, 2003-2024

Nota
La selezione della versione è un passaggio obbligatorio per Virtuozzo Hybrid Infrastructure.

8. [Facoltativo] Configurare le opzioni di ripristino aggiuntive:
   - [Non disponibile per Virtuozzo Hybrid Infrastructure] Fare clic su **Datastore** per ESXi o su **Percorso** per Hyper-V, quindi selezionare il datastore (archivio) per la virtual machine.
   - Fare clic su **Mappatura disco** per selezionare il datastore (spazio di archiviazione), l'interfaccia e la modalità di provisioning per ogni disco virtuale. La sezione dedicata alla mappatura consente anche di scegliere singoli dischi per il ripristino.

     In Virtuozzo Hybrid Infrastructure è possibile selezionare soltanto la policy di archiviazione dei dischi di destinazione. A tal fine, selezionare il disco di destinazione desiderato e fare clic su Modifica. Nel pannello visualizzato, fare clic sull'icona ingranaggio, selezionare la policy di archiviazione, quindi fare clic su Fine.
   - [Per VMware ESXi, Hyper-V e Red Hat Virtualization/oVirt] Fare clic su **Impostazioni VM** per cambiare la dimensione della memoria, il numero di processori e le connessioni di rete della virtual machine.



9. [Disponibile soltanto per i sistemi Windows nei quali è installato un agente di protezione] Abilitare l'opzione **Ripristino sicuro** per verificare che i dati ripristinati siano privi di malware.

© Acronis International GmbH, 2003-2024

Per ulteriori informazioni sul funzionamento del ripristino sicuro, consultare "Ripristino sicuro" (pag. 506).

10. Fare clic su **Avvia ripristino**.
11. Quando si esegue il ripristino in una macchina virtuale esistente, confermare che si desidera sovrascrivere i dischi.

L'avanzamento del ripristino viene mostrato nella scheda **Attività**.

Ripristino di una macchina virtuale

È possibile ripristinare le macchine virtuali dai rispettivi backup.

Nota
Non è possibile ripristinare i backup nella console di Cyber Protect per i tenant in modalità Conformità. Per ulteriori informazioni su come ripristinare questi backup, consultare "Ripristino dei backup per i tenant in modalità Conformità" (pag. 1112).

Prerequisiti

- Durante il ripristino in una macchina virtuale, questa deve essere arrestata. Per impostazione predefinita, il software interrompe la macchina senza preavviso. Una volta completato il ripristino, l'utente dovrà avviare la macchina manualmente. Questo comportamento può essere modificato utilizzando l'opzione di ripristino della Gestione dell'alimentazione delle VM (fare clic su **Opzioni di ripristino** > **Gestione energetica MV**).

Procedura

1. Eseguire una delle seguenti operazioni:
   - Selezionare un sistema di cui è stato eseguito il backup e fare clic su **Ripristino**, quindi selezionare un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda Archivio di backup.
2. Fare clic su **Ripristina** > **Intera macchina**.
3. Se si desidera eseguire il ripristino in una macchina fisica, selezionare **Macchina fisica** in **Ripristina in**. Altrimenti, ignorare questo passaggio.
   Il ripristino in una macchina fisica è possibile solo se la configurazione del disco della macchina di destinazione corrisponde esattamente alla configurazione del disco nel backup.
   In questo caso, procedere al passaggio 4 in "Macchina fisica". In caso contrario, è preferibile eseguire la migrazione V2P con l'uso di supporti di avvio.
4. [Facoltativo] Per impostazione predefinita, il software seleziona automaticamente il sistema originale come macchina di destinazione. Per eseguire il ripristino in un'altra macchina virtuale, fare clic su **Macchina di destinazione** ed eseguire le seguenti operazioni:
   a. Selezionare l'hypervisor (**VMware ESXi**, **Hyper-V**, **Virtuozzo**, **Virtuozzo Hybrid Infrastructure**, **Scale Computing HC3** o **oVirt**).
      Solo le macchine virtuali Virtuozzo possono essere ripristinate in Virtuozzo. Per ulteriori informazioni sulla migrazione V2V, fare riferimento a "Migrazione del sistema".

© Acronis International GmbH, 2003-2024

b. Selezionare se eseguire il ripristino di un sistema nuovo o uno già esistente.

c. Selezionare l'host e specificare il nome del nuovo sistema oppure selezionare una macchina di destinazione esistente.

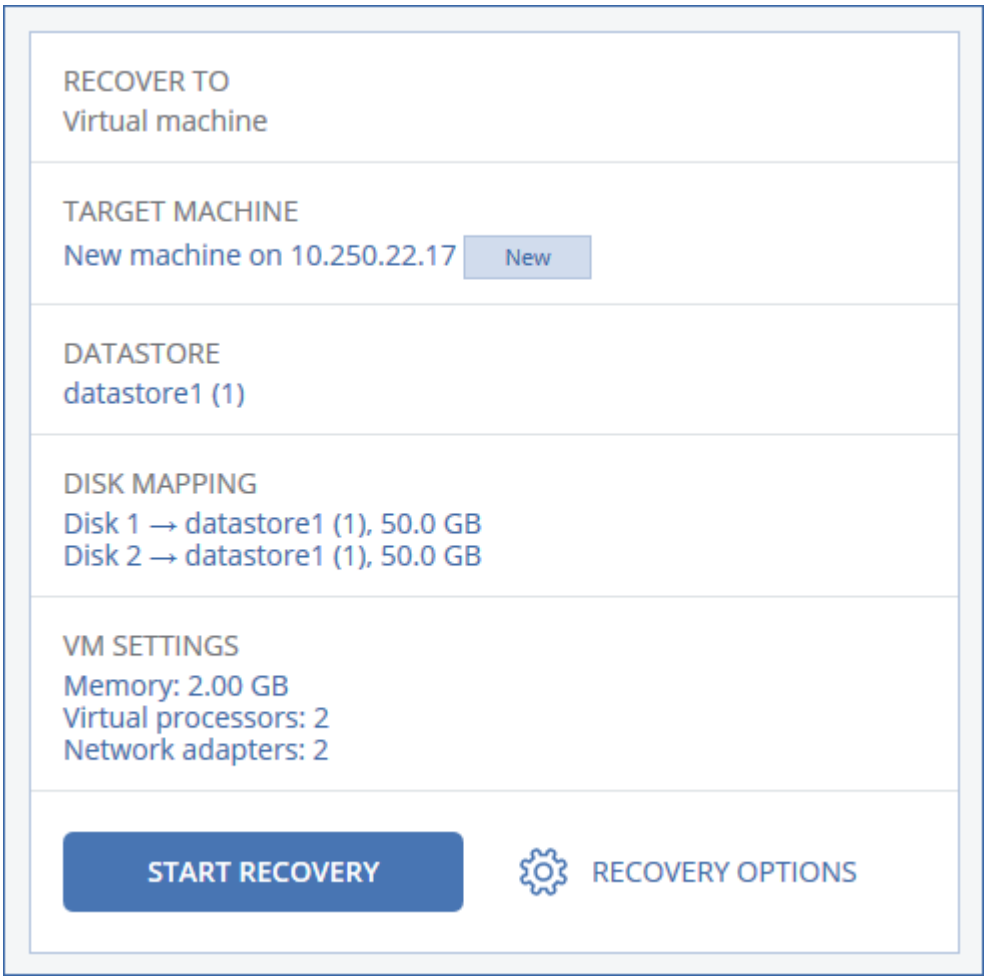
d. Fare clic su **OK**.

5. Configurare le opzioni di ripristino aggiuntive necessarie.
   - [Facoltativo] [Non disponibile per Virtuozzo Hybrid Infrastructure e Scale Computing HC3] Per selezionare il datastore per la virtual machine, fare clic su **Datastore** per ESXi o su **Percorso** per Hyper-V e Virtuozzo, oppure su **Dominio di archiviazione** per Red Hat Virtualization (oVirt), quindi selezionare il datastore (archivio) per la virtual machine.
   - [Facoltativo] Fare clic su **Mappatura disco** per visualizzare il datastore (archivio), l'interfaccia e la modalità di provisioning per ogni disco virtuale. È possibile modificare queste impostazioni, a meno che non sia in corso il ripristino di un contenitore Virtuozzo o una macchina virtuale Virtuozzo Hybrid Infrastructure.

     In Virtuozzo Hybrid Infrastructure è possibile selezionare soltanto la policy di archiviazione dei dischi di destinazione. A tal fine, selezionare il disco di destinazione desiderato e fare clic su **Modifica**. Nel pannello visualizzato, fare clic sull'icona ingranaggio, selezionare la policy di archiviazione, quindi fare clic su **Fine**.

     La sezione dedicata alla mappatura consente anche di scegliere singoli dischi per il ripristino.
   - [Facoltativo] [Disponibile per VMware ESXi, Hyper-V e Virtuozzo] Per cambiare la dimensione della memoria, il numero di processori e le connessioni di rete della virtual machine fare clic su **Impostazioni VM**.
   - [Per Virtuozzo Hybrid Infrastructure] Per cambiare la dimensione della memoria, il numero di processori della virtual machine, selezionare **Versione**.

© Acronis International GmbH, 2003-2024



6. [Disponibile soltanto per i sistemi Windows nei quali è installato un agente di protezione] Abilitare l'opzione **Ripristino sicuro** per verificare che i dati ripristinati siano privi di malware. Per ulteriori informazioni sul funzionamento del ripristino sicuro, consultare "Ripristino sicuro" (pag. 506).
7. Fare clic su **Avvia ripristino**.
8. Quando si esegue il ripristino in una macchina virtuale esistente, confermare che si desidera sovrascrivere i dischi.

L'avanzamento del ripristino viene mostrato nella scheda **Attività**.

Ripristino di dischi mediante i supporti di avvio

Per informazioni su come creare supporti di avvio, fare riferimento a "Creazione di un supporto di avvio fisico" (pag. 725).

Nota
Non è possibile ripristinare i backup del disco di sistemi Mac con processori Intel su Mac con processori Apple Silicon, e viceversa. È possibile ripristinare file e cartelle.

Per ripristinare dischi mediante i supporti di avvio

© Acronis International GmbH, 2003-2024

1. Avvio della macchina di destinazione mediante supporti di avvio.
2. [Solo quando si effettua il ripristino di un Mac] Se si effettua il ripristino di dischi o volumi con formattazione APFS in un sistema non originale o su bare metal, ricreare manualmente la configurazione originale del disco:
   a. Fare clic su **Utilità disco**.
   b. Cancellare e formattare il disco di destinazione in APFS. Per istruzioni, fare riferimento a https://support.apple.com/en-us/HT208496#erasedisk.
   c. Per ricreare la configurazione originale del disco. Per istruzioni, fare riferimento a https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15.
   d. Fare clic su **Utility disco** > **Esci da Utility disco**.
3. Fare clic su **Gestisci questa macchina localmente** o su **Supporto di ripristino avviabile** due volte, a seconda del tipo di supporto in uso.
4. Se nella rete è abilitato un server proxy, fare clic su **Strumenti** > **Server proxy** e specificare il nome host/indirizzo IP, la porta e le credenziali del server proxy. Altrimenti, ignorare questo passaggio.
5. [Facoltativo] Durante il ripristino di Windows o Linux, fare clic su **Strumenti** > **Registrare il supporto al servizio Cyber Protection**, quindi specificare il token di registrazione ottenuto durante il download del supporto. In questo modo non è necessario inserire le credenziali o un codice di registrazione per accedere all'archivio cloud, come descritto nel passaggio 8.
6. Nella schermata iniziale, fare clic su **Ripristina**.
7. Fare clic su **Seleziona dati**, quindi selezionare **Sfoglia**.
8. Specificare la posizione di backup:
   - Per il ripristino dall'archivio nel cloud, selezionare **Archiviazione nel cloud**. Immettere le credenziali dell'account a cui è assegnata la macchina con il backup.

     Quando si ripristina Windows o Linux, è possibile richiedere un codice di registrazione da utilizzare al posto delle credenziali. Fare clic su **Usare il codice di registrazione** > **Richiedi il codice**. Il software mostra il link di registrazione e il codice di registrazione. È possibile copiare queste informazioni ed eseguire la procedura di registrazione su un altro sistema. Il codice di registrazione resta valido per un'ora.
   - Per il ripristino da una cartella locale o di rete, passare alla cartella in **Cartelle locali** o **Cartelle di rete**.
   - Per il ripristino da posizioni di backup su cloud storage pubblico come Microsoft Azure, Amazon S3, Wasabi o compatibili con S3, fare clic su **Registrare il supporto al servizio Cyber Protection**, quindi configurare il ripristino tramite l'interfaccia web. Per ulteriori informazioni sulla gestione dei supporti a distanza tramite l'interfaccia web, consultare "Operazioni remoto con un supporto di avvio" (pag. 743).

   Fare clic su **OK** per confermare la selezione.
9. Selezionare il backup da cui ripristinare i dati. Se richiesto, immettere la password per il backup.

© Acronis International GmbH, 2003-2024

10. In **Contenuto del backup**, selezionare i dischi che si desidera ripristinare. Fare clic su **OK** per confermare la selezione.
11. In **Dove ripristinare**, il software esegue automaticamente la mappatura dei dischi selezionati verso i dischi di destinazione.

    Se la mappatura non ha esito positivo o i risultati non sono considerati soddisfacenti, è possibile mappare di nuovo i dischi manualmente.

    Nota
    La modifica del layout dei dischi può compromettere l'avviabilità del sistema operativo. Se non si è completamente sicuri, utilizzare il layout del disco originale del sistema.

12. [Durante il ripristino di Linux] Se il sistema di cui è stato eseguito il backup disponeva di volumi logici (LVM) e si desidera ripristinare la struttura LVM originale:
    a. Accertarsi che il numero di dischi della macchina di destinazione e la capacità di ciascun disco siano uguali o superiori a quelli del sistema originale, quindi fare clic su **Applica RAID/LVM**.
    b. Esaminare la struttura del volume, quindi fare clic su **Applica RAID/LVM** per crearla.
13. [Facoltativo] Fare clic su **Opzioni di ripristino** per specificare eventuali impostazioni aggiuntive.
14. Fare clic su **OK** per iniziare il ripristino.

Utilizzo di Universal Restore

I sistemi operativi più recenti possono comunque essere avviati anche quando vengono ripristinati su hardware diverso, incluse le piattaforme VMware o Hyper-V. Se un sistema operativo ripristinato non riesce ad avviarsi, utilizzare lo strumento Universal Restore per aggiornare i driver e i moduli necessari per l'avvio del sistema operativo.

Universal Restore è applicabile a Windows e Linux.

Per applicare Universal Restore

1. Avviare la macchina dal supporto di avvio.
2. Fare clic su **Applica Universal Restore**.
3. Se sulla macchina sono presenti più sistemi operativi, sceglierne uno a cui applicare Universal Restore.
4. [Solo per Windows] Configurare le impostazioni aggiuntive.
5. Fare clic su **OK**.

© Acronis International GmbH, 2003-2024

Preparazione delle unità

Prima di applicare Universal Restore a un sistema operativo Windows, assicurarsi di disporre dei driver del nuovo controller del disco rigido e del chipset. Questi driver sono fondamentali per l'avvio del sistema operativo. Utilizzare il CD o il DVD distribuito dal fornitore dell'hardware oppure scaricare i driver dal sito Web del fornitore. I file dei driver devono avere l'estensione *.inf. Se si scaricano i driver in formato *.exe, *.cab o *.zip, estrarli utilizzando un'applicazione di terze parti.

La procedura migliore comporta la conservazione dei driver di tutto l'hardware utilizzato nell'organizzazione in un unico repository, ordinato per tipo di dispositivo o mediante le configurazioni hardware. È possibile conservare una copia del repository in un DVD o un'unità flash; scegliere alcuni driver e aggiungerli al supporto di avvio; creare il supporto di avvio personalizzato con i driver necessari (e la configurazione di rete necessaria) per ciascuno dei server in uso. In alternativa, è possibile specificare semplicemente il percorso del repository ogni volta che viene utilizzato Universal Restore.

Verificare l'accesso ai driver nell'ambiente di avvio

Assicurarsi di avere accesso alla periferica con i driver quando si lavora dal supporto di avvio. Usare il supporto basato su WinPE se la periferica è disponibile in Windows, ma il supporto basato su Linux non la rileva.

Ricerca automatica dei driver

Specificare la posizione in cui il programma ricercherà il driver HAL (Hardware Abstraction Layer), il driver del controller disco rigido e i driver dell'adattatore di rete:

- Se i driver si trovano su un disco del fornitore o su altri supporti rimovibili, attivare **Cerca nel supporto rimovibile**.
- Se i driver sono posizionati in una cartella di rete o nel supporto di avvio, specificare il percorso della cartella nel campo **Aggiungi cartella**.

Inoltre, Universal Restore cerca la cartella predefinita di archiviazione dei driver di Windows. Il percorso della cartella è indicato nel valore di registro **DevicePath**, che si trova nella chiave di registro **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. La cartella di archiviazione è solitamente WINDOWS/inf.

Universal Restore eseguirà la ricerca ricorsiva in tutte le sottocartelle della cartella specificata e individuerà i driver del controller HAL e disco rigido più adatti fra tutti quelli disponibili installandoli nel sistema. Universal Restore ricerca anche il driver dell'adattatore di rete; il percorso del driver

© Acronis International GmbH, 2003-2024

individuato viene quindi trasmesso mediante Universal Restore al sistema operativo. Se l'hardware dispone di più schede di interfacce di rete, Universal Restore tenterà di configurare tutti i driver delle schede.

Driver di archiviazione di massa da installare in ogni caso

Questa impostazione è necessaria se:

- L'hardware dispone di un controller di archiviazione di massa specifico, ad esempio RAID (in particolare NVIDIA RAID) o un adattatore Fibre Channel.
- È stata effettuata la migrazione di un sistema a una macchina virtuale che utilizza un controller di disco rigido SCSI. Utilizzare i driver SCSI forniti con il software di virtualizzazione o scaricare le versioni più recenti dei driver dal sito Web del produttore del software.
- Se la ricerca automatica dei driver non consente di avviare il sistema.

Specificare i driver appropriati facendo clic su **Aggiungi driver**. I driver qui definiti verranno installati, con avvisi appropriati, anche se il programma trova un driver migliore.

Procedura di Universal Restore

Una volta specificate le impostazioni necessarie, fare clic su **OK**.

Se Universal Restore non è in grado di trovare un driver compatibile nelle posizioni specificate, visualizzerà una richiesta relativa alla periferica che presenta il problema. Eseguire una delle seguenti operazioni:

- Aggiungere il driver a una delle posizioni specificate precedentemente e fare clic su **Riprova**.
- Se non si ricorda la posizione, fare clic su **Ignora** per continuare la procedura. Se il risultato non è quello desiderato, riapplicare Universal Restore. Quando si configura l'operazione, specificare il driver necessario.

Dopo l'avvio, Windows avvierà la procedura standard per l'installazione del nuovo hardware. Il driver dell'adattatore di rete verrà installato in modalità non interattiva se il driver dispone della firma di Microsoft Windows. In caso contrario, Windows richiederà la conferma per installare il driver non firmato.

Successivamente, sarà possibile configurare la connessione di rete e specificare i driver per l'adattatore video, l'USB e altri dispositivi.

Universal Restore in Linux

È possibile applicare Universal Restore ai sistemi operativi Linux con versione del kernel 2.6.8 o successiva.

Quando Universal Restore è applicato a un sistema operativo Linux, aggiorna un file system temporaneo noto come disco RAM iniziale (initrd). Ciò garantisce che il sistema operativo possa eseguire l'avvio sul nuovo hardware.

© Acronis International GmbH, 2003-2024

Universal Restore aggiunge moduli per il nuovo hardware (inclusi i driver delle periferiche) al disco RAM iniziale. Normalmente trova i moduli necessari nella directory **/lib/modules**. Se Universal Restore non è in grado di trovare un modulo necessario, registra il nome del file del modulo nel registro.

Universal Restore può modificare la configurazione del caricatore di avvio GRUB. Ciò potrebbe essere necessario, per esempio, per garantire l'avviabilità del sistema quando la nuova macchina ha un layout del volume diverso dalla macchina originale.

Universal Restore non modifica mai il kernel Linux.

Ripristino del disco RAM originale iniziale

È possibile ripristinare il disco RAM iniziale originale, se necessario.

Il disco RAM iniziale è archiviato sulla macchina in un file. Prima di aggiornare il disco RAM iniziale per la prima volta, Universal Restore ne salva una copia nella stessa directory. Il nome della copia è il nome del file, seguito dal suffisso **_acronis_backup.img**. Questa copia non verrà sovrascritta se si esegue Universal Restore più di una volta (per esempio, dopo aver aggiunto i driver mancanti).

Per ripristinare il disco RAM iniziale originale, eseguire una delle seguenti operazioni:

- Rinominare la copia di conseguenza. Per esempio, eseguire un comando simile al seguente:

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- Specificare la copia nella riga **initrd** della configurazione del caricatore di avvio GRUB.

Ripristino di file

Ripristino di file nella console di Cyber Protect

Nota
Non è possibile ripristinare i backup nella console di Cyber Protect per i tenant in modalità Conformità. Per ulteriori informazioni su come ripristinare questi backup, consultare "Ripristino dei backup per i tenant in modalità Conformità" (pag. 1112).

1. Selezionare la macchina che conteneva in origine i dati che si desidera ripristinare.
2. Fare clic su **Ripristino**.
3. Selezionare il punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.
   Se il sistema selezionato è fisico e si trova offline, i punti di ripristino non vengono mostrati. Eseguire una delle seguenti operazioni:
   - [Consigliata] Se la posizione di backup è il cloud o un archivio condiviso (a cui possono accedere altri agenti), fare clic su **Seleziona macchina** e selezionare una macchina di destinazione che sia online, quindi selezionare un punto di ripristino.

© Acronis International GmbH, 2003-2024

- Selezionare un punto di ripristino nella scheda Archivio di backup.
- Scaricare i file dall'archivio nel cloud.
- Utilizzare i supporti di avvio.

4. Fare clic su **Ripristina** > **File/cartelle**.
5. Esplorare la cartella richiesta o utilizzare la barra di ricerca per ottenere l'elenco dei file e delle cartelle necessari.

   La ricerca è indipendente dalla lingua.

   È possibile utilizzare uno o più caratteri jolly (* e ?). Per ulteriori dettagli sull'utilizzo dei caratteri jolly, fare riferimento a "Maschera" (pag. 469).

   Nota
   Non è possibile eseguire ricerche nei backup del disco che si trovano nell'archivio nel cloud.
6. Selezionare i dati che si desidera ripristinare.
7. Se si desidera salvare i file come file .zip, fare clic su **Download** e selezionare la posizione in cui salvare i dati, quindi fare clic su **Salva**. Altrimenti, ignorare questo passaggio.

   Il download non è disponibile se la selezione contiene cartelle o se la dimensione totale dei file selezionati supera 100 MB. Per recuperare rapidamente maggiori quantità di dati dal cloud, attenersi alla procedura "Download di file dall'archivio nel cloud" (pag. 521).
8. Fare clic su **Ripristina**.

   In **Ripristina in**, fare clic per selezionare la destinazione dell'operazione di ripristino, o lasciare la destinazione predefinita. La destinazione predefinita varia in base all'origine del backup.

   Sono disponibili le destinazioni seguenti:
   - Il sistema di origine (se vi è stato installato un agente di protezione).

     Si tratta del sistema che conteneva in origine i file che si desidera ripristinare.
   - Altri sistemi su cui è installato un agente di protezione: sistemi fisici, virtual machine e host di virtualizzazione sui quali è installato un agente di protezione, oppure appliance virtuali.

     È possibile ripristinare i file su sistemi fisici, virtual machine e host di virtualizzazione sui quali è installato un agente di protezione. Non è possibile ripristinare i file su virtual machine nelle quali non è installato un agente di protezione (ad eccezione delle virtual machine Virtuozzo).
   - Container o virtual machine Virtuozzo.

     È possibile ripristinare i file su container Virtuozzo e virtual machine con alcune limitazioni. Per ulteriori informazioni, fare riferimento a "Limiti al ripristino di file nella console di Cyber Protect" (pag. 525).
9. In **Percorso**, selezionare la destinazione del ripristino. È possibile selezionare una delle seguenti opzioni:
   - [Quando si esegue il ripristino nel sistema originale] La posizione originale.
   - Una cartella locale o uno storage connesso in locale nel sistema di destinazione.

© Acronis International GmbH, 2003-2024

Nota
I collegamenti simbolici non sono supportati.

- Una cartella di rete che sia accessibile dalla macchina di destinazione.

10. Fare clic su **Avvia ripristino**.
11. Selezionare una delle opzioni di sovrascrittura dei file:
    - **Sovrascrivi i file esistenti**
    - **Sovrascrivi il file esistente se meno recente**
    - **Non sovrascrivere i file esistenti**

L'avanzamento del ripristino viene mostrato nella scheda **Attività**.

Download di file dall'archivio nel cloud

Nella console web di ripristino è possibile esplorare il cloud storage, visualizzare il contenuto dei backup e scaricare file e cartelle di cui è stato eseguito il backup.

Nota
Possono accedere alla console Web Restore solo gli amministratori Cyber Protection del cliente o gli utenti del tenant cliente. Ai ruoli utente a livello del partner non è consentito l'accesso.

Limitazioni

- Non è possibile scaricare i backup di dischi, volumi o interi punti di ripristino.
- Quando si esplorano i backup a livello di disco, i volumi logici (come LVM e LDM) non vengono visualizzati.
- Non è possibile esplorare i backup dello stato del sistema, dei database SQL e dei database di Exchange.

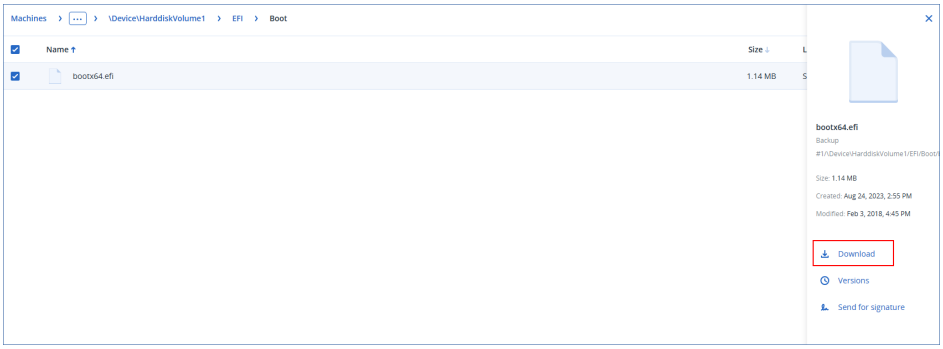
Per scaricare file e cartelle dal cloud storage

1. Nella console di Cyber Protection selezionare il workload richiesto, quindi fare clic su **Ripristina**.
2. [Se sono disponibili più posizioni di backup] Selezionare la posizione del backup, quindi fare clic su **Altri metodi di ripristino**.
3. Fare clic su **Scarica file**.
4. In **Sistemi**, fare clic sul nome del workload, quindi sull'archivio di backup.
   Un archivio di backup contiene uno o più backup (punti di ripristino).
5. Fare clic sul numero di backup (punto di ripristino) da cui scaricare file o cartelle, quindi navigare fino agli elementi richiesti.
6. Selezionare le caselle di controllo accanto agli elementi da scaricare.

Nota
Se si selezionano più elementi, questi vengono scaricati in un file ZIP.

© Acronis International GmbH, 2003-2024

7. Fare clic su **Download**.



Verifica dell'autenticità dei file con Notary Service

Se l'autenticazione è stata abilitata durante il backup, è possibile verificare l'autenticità di un file sottoposto a backup.

Per verificare l'autenticità dei file

1. Selezionare il file, come descritto nei passaggi da 1 a 6 della sezione "Ripristino di file mediante l'interfaccia Web" o nei passaggi da 1 a 5 della sezione "Scaricare i file dall'archivio nel cloud".
2. Verificare che il file selezionato sia contrassegnato dall'icona seguente: . Ciò significa che il file è autenticato.
3. Eseguire una delle seguenti operazioni:
   - Fare clic su **Verifica**.
     Il software controlla l'autenticità del file e mostra il risultato.
   - Fare clic su **Ottieni certificato**.
     In una finestra del browser Web viene visualizzato un certificato che conferma l'autenticazione del file. La finestra contiene inoltre le istruzioni per verificare manualmente l'autenticità dei file.

Firma di file con ASign

Nota
Questa funzionalità è disponibile con il pacchetto Advanced Backup.

ASign è un servizio che consente a più utenti di firmare un file di cui è stato eseguito il backup in modo elettronico. Questa funzionalità è disponibile solo per i backup a livello di file archiviati nel cloud.

È possibile firmare solo una versione del file alla volta. Se il file viene sottoposto a backup più volte, è necessario scegliere la versione da firmare e solo questa verrà firmata.

Ad esempio, è possibile utilizzare ASign per la firma dei file seguenti:

© Acronis International GmbH, 2003-2024

- Contratti di affitto o locazione
- Contratti di vendita
- Contratti di acquisto di beni
- Contratti di erogazione di prestito
- Fogli di autorizzazione
- Documenti finanziari
- Documenti assicurativi
- Esclusioni di responsabilità
- Documenti sanitari
- Documenti di ricerca
- Certificati di autenticità dei prodotti
- Contratti di non divulgazione
- Lettere di proposta
- Contratti di riservatezza
- Contratti con terzisti indipendenti

Per firmare una versione del file

1. Selezionare il file, come descritto nei passaggi da 1 a 6 della sezione "Ripristino di file mediante l'interfaccia Web" o nei passaggi da 1 a 5 della sezione "Scaricare i file dall'archivio nel cloud".
2. Assicurarsi che nel riquadro di sinistra siano selezionate data e ora corrette.
3. Fare clic su **Firma questa versione del file**.
4. Specificare la password per l'account di archiviazione nel cloud con il quale il backup è archiviato. Il login dell'account viene visualizzato nella finestra del prompt.
   L'interfaccia del servizio ASign si apre in una finestra del browser Web.
5. Aggiungere altri firmatari specificandone gli indirizzi e-mail. Non è possibile aggiungere o rimuovere i firmatari dopo aver inviato gli inviti. Assicurarsi quindi che l'elenco includa tutti coloro la cui firma è richiesta.
6. Fare clic su **Invita a firmare** per inviare gli inviti ai firmatari.
   Ciascun firmatario riceve un'e-mail con la richiesta di firma. Quando tutti i firmatari richiesti hanno firmato il file, questo viene vidimato e firmato tramite il servizio di vidimazione Notary Service.
   Si riceve una notifica per ogni firma apposta dai vari firmatari e al completamento dell'intero processo. È possibile accedere alla pagina Web di ASign facendo clic su **Visualizza dettagli** in qualsiasi messaggio e-mail ricevuto.
7. Una volta completato il processo, passare alla pagina Web di ASign e fare clic su **Ottieni documento** per scaricare un documento in formato .pdf contenente:

© Acronis International GmbH, 2003-2024

- La pagina del certificato di firma che raccoglie tutte le firme.
- La pagina di audit trail con la cronologia delle attività: data e ora in cui l'invito è stato spedito ai firmatari, data e ora in cui ciascun firmatario ha firmato il file ecc.

Ripristino di file mediante i supporti di avvio

Per informazioni su come creare supporti di avvio, fare riferimento a "Creazione di supporti di avvio".

Per ripristinare file mediante i supporti di avvio

1. Avviare la macchina di destinazione mediante il supporto di avvio.
2. Fare clic su **Gestisci questa macchina localmente** o su **Supporto di ripristino avviabile** due volte, a seconda del tipo di supporto in uso.
3. Se nella rete è abilitato un server proxy, fare clic su **Strumenti** > **Server proxy** e specificare il nome host/indirizzo IP, la porta e le credenziali del server proxy. Altrimenti, ignorare questo passaggio.
4. [Facoltativo] Durante il ripristino di Windows o Linux, fare clic su **Strumenti** > **Registrare il supporto al servizio Cyber Protection**, quindi specificare il token di registrazione ottenuto durante il download del supporto. In questo modo non è necessario inserire le credenziali o un codice di registrazione per accedere all'archivio cloud, come descritto nel passaggio 7.
5. Nella schermata iniziale, fare clic su **Ripristina**.
6. Fare clic su **Seleziona dati**, quindi selezionare **Sfoglia**.
7. Specificare la posizione di backup:
   - Per il ripristino dall'archivio nel cloud, selezionare **Archiviazione nel cloud**. Immettere le credenziali dell'account a cui è assegnata la macchina con il backup.

     Quando si ripristina Windows o Linux, è possibile richiedere un codice di registrazione da utilizzare al posto delle credenziali. Fare clic su **Usare il codice di registrazione** > **Richiedi il codice**. Il software mostra il link di registrazione e il codice di registrazione. È possibile copiare queste informazioni ed eseguire la procedura di registrazione su un altro sistema. Il codice di registrazione resta valido per un'ora.
   - Per il ripristino da una cartella locale o di rete, passare alla cartella in **Cartelle locali** o **Cartelle di rete**.
   - Per il ripristino da posizioni di backup su cloud storage pubblico come Microsoft Azure, Amazon S3, Wasabi o compatibili con S3, fare clic su **Registrare il supporto al servizio Cyber Protection**, quindi configurare il ripristino tramite l'interfaccia web. Per ulteriori informazioni sulla gestione dei supporti a distanza tramite l'interfaccia web, consultare "Operazioni remoto con un supporto di avvio" (pag. 743).

   Fare clic su **OK** per confermare la selezione.
8. Selezionare il backup da cui ripristinare i dati. Se richiesto, immettere la password per il backup.

© Acronis International GmbH, 2003-2024

9. In **Contenuto del backup**, selezionare **Cartelle/file**.
10. Selezionare i dati che si desidera ripristinare. Fare clic su **OK** per confermare la selezione.
11. Specificare una cartella in **Dove ripristinare**. Facoltativamente, è possibile impedire la sovrascrittura delle versioni più nuove dei file o escludere alcuni file dal ripristino.
12. [Facoltativo] Fare clic su **Opzioni di ripristino** per specificare eventuali impostazioni aggiuntive.
13. Fare clic su **OK** per iniziare il ripristino.

Estrazione di file dai backup locali

È possibile sfogliare i contenuti dei backup ed estrarre i file necessari.

Requisiti

- Questa funzionalità è disponibile solo in Windows utilizzando Esplora file.
- Il file system di cui si esegue il backup deve essere uno dei seguenti: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS o HFS+.

Prerequisiti

- È necessario installare un agente di protezione sulla macchina in cui si sfoglia il backup.
- Il backup deve essere archiviato in una cartella locale o su una condivisione di rete (SMB/CIFS).

Per estrarre i file da un backup

1. Passare alla posizione del backup utilizzando Esplora file.
2. Fare doppio clic sul file di backup. I nomi dei file si basano sul seguente modello:
   `<nome sistema> - <GUID piano di protezione>`
3. Se il backup è crittografato, inserire la password per la crittografia. Altrimenti, ignorare questo passaggio.
   Esplora file visualizza i punti di ripristino.
4. Fare doppio clic sul punto di ripristino.
   Esplora file visualizza i dati inclusi nel backup.
5. Passare alla cartella richiesta.
6. Copiare i file richiesti in una cartella o nel file system.

Limiti al ripristino di file nella console di Cyber Protect

Tenant in modalità Conformità

Non è possibile ripristinare i backup nella console di Cyber Protect per i tenant in modalità Conformità. Per ulteriori informazioni su come ripristinare questi backup, consultare "Ripristino dei backup per i tenant in modalità Conformità" (pag. 1112).

© Acronis International GmbH, 2003-2024

Ripristino in container o virtual machine Virtuozzo

- L'agente guest QEMU deve essere installato nella virtual machine di destinazione.
- [Applicabile solo per il ripristino su container] I punti di montaggio all'interno dei container non possono essere utilizzati come destinazione del ripristino. Ad esempio, non è possibile ripristinare i file in un secondo disco rigido o in una condivisione NFS montata in un container.
- Quando si ripristinano file in una virtual machine Windows, e se l'opzione di ripristino "Sicurezza a livello di file" (pag. 532) è abilitata, nei file ripristinati viene impostato l'attributo bit archivio.
- I file che contengono caratteri non ANSI nel nome vengono ripristinati con nomi non corretti nei sistemi che eseguono Windows Server 2012 o versioni precedenti e nei sistemi che eseguono Windows 7 o versioni precedenti.
- Per ripristinare file su virtual machine CentOS o Red Hat Enterprise Linux eseguite su Virtuozzo Hybrid Server, è necessario modificare il file `qemu-ga` come indicato di seguito:
  - Nella virtual machine di destinazione, passare a `/etc/sysconfig/`, quindi aprire il file `qemu-ga` per la modifica.
  - Passare alla riga seguente, e quindi eliminare tutto dopo il segno di uguale (=):

    ```
    BLACKLIST_RPC=
    ```

  - Riavviare l'Agente guest QEMU eseguendo il seguente comando:

    ```
    systemctl restart qemu-guest-agent
    ```

Ripristino dello stato del sistema

Nota
Non è possibile ripristinare i backup nella console di Cyber Protect per i tenant in modalità Conformità. Per ulteriori informazioni su come ripristinare questi backup, consultare "Ripristino dei backup per i tenant in modalità Conformità" (pag. 1112).

1. Selezionare la macchina di cui ripristinare lo stato del sistema.
2. Fare clic su **Ripristino**.
3. Selezionare un punto di ripristino di stato di sistema. Notare che i punti di ripristino vengono filtrati in base alla posizione.
4. Fare clic su **Ripristina stato del sistema**.
5. Confermare che si desidera sovrascrivere lo stato di sistema con le versioni di cui si è eseguito il backup.

L'avanzamento del ripristino viene mostrato nella scheda **Attività**.

© Acronis International GmbH, 2003-2024

Ripristino della configurazione ESXi

Per ripristinare una configurazione ESXi, è necessario disporre di un supporto di avvio basato su Linux. Per informazioni su come creare supporti di avvio, fare riferimento a "Creazione di un supporto di avvio fisico" (pag. 725).

Se si esegue il ripristino di una configurazione ESXi a un host non originale e se l'host originale è ancora connesso al vCenter Server, disconnettere l'host e rimuoverlo dal vCenter Server per evitare che si verifichino problemi non previsti durante il ripristino. Per mantenere l'host originale assieme all'host ripristinato, aggiungerlo di nuovo al termine del ripristino.

Le macchine virtuali in esecuzione sull'host non sono incluse nel backup della configurazione di ESXi. Tali macchine possono essere sottoposte a backup e ripristinate separatamente.

Per ripristinare una configurazione di ESXi

1. Avviare la macchina di destinazione mediante il supporto di avvio.
2. Fare clic su **Gestisci questa macchina localmente**.
3. Nella schermata iniziale, fare clic su **Ripristina**.
4. Fare clic su **Seleziona dati**, quindi selezionare **Sfoglia**.
5. Specificare la posizione di backup:
   - Passare alla cartella in **Cartelle locali** o **Cartelle di rete**.

   Fare clic su **OK** per confermare la selezione.
6. Nel campo **Mostra**, selezionare **Configurazioni ESXi**.
7. Selezionare il backup da cui ripristinare i dati. Se richiesto, immettere la password per il backup.
8. Fare clic su **OK**.
9. In **Dischi da utilizzare per i nuovi datastore**, eseguire le seguenti operazioni:
   - In **Ripristina ESXi in**, selezionare il disco in cui verrà ripristinata la configurazione dell'host. Se si esegue il ripristino della configurazione all'host originale, viene selezionato il disco originale per impostazione predefinita.
   - [Facoltativo] In **Utilizzo dei nuovi datastore**, selezionare i dischi in cui verranno creati nuovi datastore. Prestare attenzione poiché tutti i dati presenti nei dischi selezionati andranno perduti. Per preservare le macchine virtuali nei datastore esistenti, non selezionare alcun disco.
10. Se vengono selezionati dischi per i nuovi datastore, indicare il metodo di creazione del datastore in **Creazione di nuovi datastore**: **Creare un datastore per disco** o **Creare un datastore su tutti i dischi rigidi selezionati**.
11. [Facoltativo] In **Mappatura di rete**, cambiare il risultato della mappatura automatica degli switch virtuali presenti nel backup verso gli adattatori di rete fisici.
12. [Facoltativo] Fare clic su **Opzioni di ripristino** per specificare eventuali impostazioni aggiuntive.
13. Fare clic su **OK** per iniziare il ripristino.

© Acronis International GmbH, 2003-2024

Opzioni di ripristino

Per modificare le opzioni di ripristino, fare clic su **Opzioni di ripristino** durante la configurazione del ripristino.

Disponibilità delle opzioni di ripristino

La serie di opzioni di ripristino disponibili dipende dai seguenti fattori:

- L'ambiente in cui opera l'agente che esegue il ripristino (Windows, Linux, macOS o supporto di avvio).
- Il tipo di dati di cui si esegue il ripristino (dischi, file, macchine virtuali, dati di applicazioni).

La tabella seguente riepiloga la disponibilità delle opzioni di ripristino.

	Dischi			**File**				**Macchine virtuali**	**SQL e Exchange**
	Windows	**Linux**	**Supporto di avvio**	**Windows**	**Linux**	**macOS**	**Supporto di avvio**	**ESXi, Hyper-V e Virtuozzo**	**Windows**
Convalida del backup	+	+	+	+	+	+	+	+	+
Modalità di avvio	+	-	-	-	-	-	-	+	-
Data e ora dei file	-	-	-	+	+	+	+	-	-
Gestione degli errori	+	+	+	+	+	+	+	+	+
Esclusioni file	-	-	-	+	+	+	+	-	-
Sicurezza a livello di file	-	-	-	+	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-
Ripristino	-	-	-	+	+	+	+	-	-

© Acronis International GmbH, 2003-2024

percorso completo									
Punti di montaggio	-	-	-	+	-	-	-	-	-
Prestazioni	+	+	-	+	+	+	-	+	+
Comandi pre/post	+	+	-	+	+	+	-	+	+
Modifica SID	+	-	-	-	-	-	-	-	-
Gestione energetica MV	-	-	-	-	-	-	-	+	-
Registro eventi di Windows	+	-	-	+	-	-	-	Solo Hyper-V	+

Convalida del backup

Questa opzione determina se convalidare un backup per garantire che non sia danneggiato, prima che i dati siano ripristinati da questo. Questa operazione viene eseguita dall'agente di protezione.

L'impostazione predefinita è: **Disabilitata**.

Per ulteriori informazioni sulla convalida tramite verifica checksum, fare riferimento a "Verifica checksum" (pag. 209).

Nota
A seconda delle impostazioni selezionate dal service provider, la convalida potrebbe non essere disponibile quando si esegue il backup nell'archivio nel cloud.

Modalità di avvio

Questa opzione è disponibile durante il ripristino di una macchina fisica o virtuale da un backup a livello di disco che contiene un sistema operativo Windows.

L'opzione consente di selezionare la modalità di avvio (BIOS o UEFI) utilizzata da Windows dopo il ripristino. Se la modalità di avvio della macchina originale è diversa dalla modalità di avvio selezionata, il software:

- Inizializza il disco sul quale è in corso il ripristino del volume di sistema, in base alla modalità di avvio selezionata (MBR per BIOS, GPT per UEFI).
- Imposta il sistema operativo Windows affinché si avvii usando la modalità di avvio selezionata.

© Acronis International GmbH, 2003-2024

L'impostazione predefinita è: **Come nella macchina di destinazione.**

È possibile selezionare uno dei casi seguenti:

- **Come nella macchina di destinazione**
  L'agente in esecuzione nella macchina di destinazione rileva la modalità di avvio attualmente in uso da parte di Windows ed esegue le impostazioni in base alla modalità di avvio individuata.
  È il valore più sicuro che risulta automaticamente in un sistema avviabile, a meno che non siano applicate le limitazioni indicate di seguito. Poiché l'opzione **Modalità di avvio** non è presente nel supporto di avvio, l'agente sul supporto presuppone sempre che questo sia il valore scelto.
- **Come nella macchina di cui è stato eseguito il backup**
  L'agente in esecuzione nella macchina di destinazione legge la modalità di avvio dal backup ed esegue le impostazioni in base ad essa. È così più agevole ripristinare un sistema su una macchina diversa, anche se questa adotta un'altra modalità di avvio, e quindi sostituire il disco nella macchina di cui è stato eseguito il backup.
- **BIOS**
  L'agente in esecuzione nella macchina di destinazione esegue le impostazioni per usare il BIOS.
- **UEFI**
  L'agente in esecuzione nella macchina di destinazione esegue le impostazioni per usare UEFI.

Una volta modificata un'impostazione, la procedura di mapping del disco verrà ripetuta. L'operazione richiede alcuni minuti.

Raccomandazioni

Se è necessario trasferire Windows tra UEFI e BIOS:

- Ripristinare l'intero disco nella stessa posizione in cui si trova il volume di sistema. Se si ripristina soltanto il volume di sistema su un volume esistente, l'agente non sarà in grado di inizializzare il disco di destinazione in modo adeguato.
- Ricordare che il BIOS non consente l'utilizzo di oltre 2 TB di spazio su disco.

Limitazioni

- Il trasferimento tra UEFI e BIOS è supportato per:
  - Sistemi operativi Windows a 64 bit a partire da Windows 7
  - Sistemi operativi Windows Server a 64 bit a partire da Windows Server 2008 SP1
- Il trasferimento tra UEFI e BIOS non è supportato se il backup è archiviato su una periferica a nastro.

Se il trasferimento di un sistema tra UEFI e BIOS non è supportato, l'agente agisce come se l'impostazione **Come nella macchina di cui è stato eseguito il backup** è selezionata. Se la macchina di destinazione supporta sia UEFI che BIOS, è necessario abilitare manualmente la modalità di avvio corrispondente alla macchina originale. Altrimenti, il sistema non verrà avviato.

© Acronis International GmbH, 2003-2024

Data e ora dei file

Questa opzione è disponibile solo per il ripristino di file.

Questa opzione definisce se ripristinare la data e l'ora dei file dal backup o assegnare ai file la data e l'ora correnti.

Se questa opzione è disabilitata, i file verranno assegnati alla data e all'ora correnti.

L'impostazione predefinita è: **Abilitata**.

Gestione degli errori

Queste opzioni permettono di specificare come trattare gli errori che si potrebbero verificare durante il ripristino.

Riprova se si verifica un errore

L'impostazione predefinita è: **Abilitata. Numero di tentativi: 30. Intervallo tra i tentativi: 30 secondi.**

Quando si verifica un errore recuperabile, il programma riprova ad eseguire l'operazione non riuscita. È possibile impostare l'intervallo di tempo e il numero dei tentativi. I tentativi avranno termine appena l'operazione è stata completata correttamente OPPURE quando viene eseguito il numero specificato dei tentativi, a seconda dell'evento che si verifica prima.

Non visualizzare i messaggi e le finestre di dialogo durante l'elaborazione (modalità nascosta)

L'impostazione predefinita è: **Disabilitata**.

Con la modalità nascosta abilitata, il programma gestirà automaticamente le situazioni che richiedono l'intervento dell'utente. Se un'operazione non può continuare in assenza di un'interazione dell'utente, non sarà portata a termine. I dettagli dell'operazione, inclusi eventuali errori, potranno essere visualizzati nel registro dell'operazione.

Salva le informazioni di sistema se il ripristino con riavvio non riesce

Questa opzione è disponibile per il ripristino di un disco o volume su una macchina fisica che esegue Windows o Linux.

L'impostazione predefinita è: **Disabilitata**.

Se questa opzione è abilitata è possibile specificare una cartella sul disco locale (incluse unità flash o HDD collegate alla macchina di destinazione) o su una condivisione di rete in cui verranno salvati il log, le informazioni di sistema e i file del dump di arresto anomalo. Questo file consente al personale del supporto tecnico di identificare il problema.

© Acronis International GmbH, 2003-2024

Esclusioni file

Questa opzione è disponibile solo per il ripristino di file.

L'opzione definisce i file e le cartelle da ignorare durante il processo di ripristino, escludendoli in tal modo dall'elenco di elementi ripristinati.

Nota
Le esclusioni consentono di ignorare la selezione degli elementi dei dati da ripristinare. Per esempio, se si seleziona di ripristinare il file FilePersonale.tmp e di escludere tutti i file in formato .tmp, il file FilePersonale.tmp non verrà ripristinato.

Sicurezza a livello di file

Questa opzione è disponibile solo per il ripristino di file da backup eseguiti a livello di disco o di file o da volumi formattati NTFS.

Questa opzione definisce se ripristinare dei permessi per i file NTFS insieme ai file.

L'impostazione predefinita è: **Abilitata**.

È possibile scegliere se ripristinare le autorizzazioni o lasciare che i file ereditino le autorizzazioni NFTS dalla cartella in cui vengono ripristinati.

Flashback

Questa opzione è applicabile quando si ripristinano dischi e volumi su macchine fisiche e virtuali, eccetto macchine Mac.

Questa opzione funzione solo se il layout del volume del disco da ripristinare corrisponde esattamente a quello del disco di destinazione.

Se l'opzione è abilitata, vengono ripristinate solo le differenze tra i dati contenuti nel backup e quelli del disco di destinazione. In questo modo si accelera il ripristino delle macchine fisiche e virtuali. I dati vengono confrontati a livello di blocco.

Quando si ripristina una macchina fisica, l'impostazione predefinita è: **Disabilitata**.

Quando si ripristina una macchina virtuale, l'impostazione predefinita è: **Abilitata**.

Ripristino percorso completo

Questa opzione è disponibile solo per il ripristino dei dati da un backup a livello di file.

Se l'opzione è abilitata, il percorso completo del file viene ricreato nella posizione di destinazione.

L'impostazione predefinita è: **Disabilitata**.

Punti di montaggio

Questa opzione è disponibile solo in Windows per il ripristino dei dati da un backup a livello di file.

© Acronis International GmbH, 2003-2024

Abilitare questa opzione per ripristinare file e cartelle archiviati nei volumi montati e di cui è stato eseguito il backup con l'opzione Punti di montaggio abilitata.

L'impostazione predefinita è: **Disabilitata**.

Questa opzione è disponibile solo quando si seleziona per il ripristino una cartella che nella gerarchia delle cartelle è superiore al punto di montaggio. Se vengono selezionate per il ripristino cartelle all'interno del punto di montaggio o il punto di montaggio stesso, gli elementi selezionati verranno ripristinati a prescindere dal valore dell'opzione **Punti di montaggio**.

Nota
Considerare che se il volume non è montato al momento del ripristino, i dati verranno ripristinati direttamente nella cartella che costituiva il punto di montaggio al momento del backup.

Prestazioni

Questa opzione consente di stabilire la priorità del processo di backup nel sistema operativo.

Le impostazioni disponibili sono: **Bassa**, **Normale**, **Alto**.

L'impostazione predefinita è: **Normale**.

La priorità di un processo eseguito in un sistema determina la quantità di risorse del sistema e della CPU allocate a quel processo. Abbassando la priorità del ripristino si rendono disponibili altre risorse per altre operazioni. Aumentando la priorità del ripristino è possibile accelerare la procedura di ripristino richiedendo al sistema operativo di allocare maggiori risorse all'applicazione che eseguiranno il ripristino. Tuttavia, l'effetto finale dipenderà dal generale utilizzo della CPU e da altri fattori come la velocità di I/O del disco o il traffico di rete.

Comandi pre/post

L'opzione permette di definire i comandi da avviare automaticamente prima e dopo la procedura di ripristino.

Esempio di come utilizzare i comandi pre/post:

- Lanciare il comando **Checkdisk** per trovare e correggere errori di file system, errori fisici o settori danneggiati prima dell'avvio del ripristino o dopo la fine del ripristino.

Il programma non supporta comandi interattivi, ovvero comandi che richiedono l'immissione dell'utente (ad esempio "pause").

Un comando post-ripristino non verrà eseguito se il ripristino procede con il riavvio.

Comandi pre-ripristino

Per specificare un comando/file batch da eseguire prima dell'avvio della procedura di ripristino.

© Acronis International GmbH, 2003-2024

1. Abilitare l'opzione **Esegui un comando prima del ripristino**.
2. Nel campo **Comando...**, immettere un comando o individuare un file batch. Il programma non supporta comandi interattivi, ovvero comandi che richiedono l'immissione dell'utente (ad esempio "pause").
3. Nel campo **Directory di lavoro**, specificare il percorso della directory in cui sarà eseguito il comando/file batch.
4. Nel campo **Argomenti**, specificare gli argomenti di esecuzione del comando, se necessario.
5. A seconda del risultato che si desidera ottenere, selezionare le opzioni appropriate descritte nella tabella seguente.
6. Fare clic su **Fine**.

Casella di controllo	**Selezione**			
Interrompi l'attività di ripristino se l'esecuzione del comando fallisce*	Selezionato	Cancellato	Selezionato	Cancellato
Non eseguire il ripristino fino al termine dell'esecuzione del comando	Selezionato	Selezionato	Cancellato	Cancellato
Risultato				
	Impostazione predefinita Esegui il ripristino solo dopo che il comando è stato eseguito con successo. Interrompi l'attività di ripristino se l'esecuzione del comando fallisce.	Esegui il ripristino solo dopo che il comando è stato eseguito nonostante l'esito negativo o positivo.	N/D	Esegui il ripristino simultaneamente al comando e senza tener conto del risultato dell'esecuzione del comando.

* Un comando viene considerato non riuscito se il codice di uscita non è uguale a zero.

Comandi post ripristino

Per specificare un comando/file eseguibile da avviare una volta completato il ripristino.

1. Abilitare l'interruttore **Esegui un comando dopo il ripristino**.
2. Nel campo **Comando...**, immettere un comando o individuare un file batch.

© Acronis International GmbH, 2003-2024

3. Nel campo **Directory di lavoro**, specificare il percorso della directory in cui sarà eseguito il comando/file batch.
4. Nel campo **Argomenti**, specificare gli argomenti dell'esecuzione del comando, se richiesto.
5. Selezionare la casella di controllo **Interrompi l'attività di ripristino se l'esecuzione del comando fallisce** se l'esecuzione corretta del comando è fondamentale. Il comando viene considerato non riuscito se il codice di uscita non è uguale a zero. Se l'esecuzione del comando fallisce, lo stato di ripristino sarà impostato su **Errore**.

   Quando la casella di controllo non è selezionata, il risultato dell'esecuzione del comando non influisce sull'esito negativo o positivo del ripristino. È possibile tracciare il risultato dell'esecuzione dei comandi nella scheda **Attività**.
6. Fare clic su **Fine**.

Nota
Un comando post-ripristino non verrà eseguito se il ripristino procede con il riavvio.

Modifica SID

Questa opzione viene applicata quando viene eseguito il ripristino di Windows 8.1/Windows Server 2012 R2 o versioni precedenti.

Questa opzione non è applicabile quando il ripristino in una virtual machine viene eseguito da Agente per VMware, Agente per Hyper-V, Agente per Scale Computing HC3 o Agente per oVirt.

L'impostazione predefinita è: **Disabilitata**.

Il software può generare un identificatore di sicurezza univoco (SID computer) per il sistema operativo ripristinato. Questa opzione è necessaria soltanto per assicurare l'utilizzabilità del software di terze parti che dipende dal SID del computer.

Microsoft non supporta ufficialmente il cambio del SID su un sistema distribuito o ripristinato. L'utente utilizza questa opzione a proprio rischio.

Gestione energetica MV

Queste opzioni sono disponibili quando il ripristino in una virtual machine viene eseguito dall'Agente per VMware, dall'Agente per Hyper-V, dall'Agente per Virtuozzo, dall'Agente per Scale Computing HC3 o dall'Agente per oVirt.

Spegni le macchine virtuali di destinazione quando viene avviato il ripristino

L'impostazione predefinita è: **Abilitata**.

Il ripristino su un macchina virtuale esistente non è possibile se la macchina è in linea, pertanto la macchina viene spenta automaticamente appena viene avviato il ripristino. Gli utenti saranno disconnessi dalla macchina e i dati non memorizzati andranno perduti.

Deselezionare la casella per questa opzione se si preferisce spegnere le macchine virtuali manualmente prima del ripristino.

© Acronis International GmbH, 2003-2024

Avvia la macchina virtuale di destinazione quando il ripristino è completo

L'impostazione predefinita è: **Disabilitata**.

Dopo che una macchina è stata ripristinata da un backup di un'altra macchina, esiste la possibilità che la copia della macchina esistente appaia sulla rete. Per maggiore certezza, avviare la macchina virtuale ripristinata manualmente dopo aver preso le necessarie precauzioni.

Registro eventi di Windows

Questa opzione è disponibile quando solo per il sistema operativo Windows

Questa opzione consente di stabilire se gli agenti che operano sulla macchina devono salvare gli eventi delle operazioni di ripristino nel registro eventi applicazioni di Windows (per visualizzare questo registro, avviare eventvwr.exe o selezionare **Pannello di controllo** > **Strumenti di amministrazione** > **Visualizzatore eventi**). È possibile filtrare gli eventi da registrare.

L'impostazione predefinita è: **Disabilitata**.

Operazioni con backup

La scheda Archivio di backup

La scheda **Archivio di backup** consente di accedere a tutti i backup, inclusi quelli dei sistemi offline, dei sistemi che non sono più registrati nel servizio Cyber Protection, dei backup ai cloud pubblici come Microsoft Azure e dei backup orfani[1].

I backup creati tramite `acrocmd` sono contrassegnati come orfani. Anche i backup creati nella versione 12.5 del prodotto vengono identificati come orfani.

Nota
Si noti che anche i backup orfani vengono addebitati.

I backup archiviati in una posizione condivisa (ad esempio in una condivisione SMB o NFS) sono visibili a tutti gli utenti che dispongono dell'autorizzazione di lettura per tale posizione.

In Windows, i file di backup ereditano le autorizzazioni di accesso dalla cartella principale. Si consiglia pertanto di limitare le autorizzazioni di lettura per questa cartella.

Nell'archivio nel cloud, gli utenti possono accedere solo ai propri backup.

Un amministratore può visualizzare i backup in cloud per conto di qualsiasi account appartenente a una determinata unità o società e ai relativi gruppi figlio, selezionando il cloud storage dell'account. Per selezionare il dispositivo da utilizzare per ottenere i dati dal cloud, fare clic su **Modifica** nella

[1] Si definisce orfano un backup che non è più associato a un piano di protezione.

© Acronis International GmbH, 2003-2024

riga **Macchina da esplorare da**. La scheda **Archivio di backup** mostra i backup di tutti i sistemi che sono stati registrati nell'account selezionato.

I backup creati dall'Agente *cloud* per Microsoft 365 e i backup dei dati di Google Workspace non vengono visualizzati nella posizione **Archiviazione nel cloud**, ma in una sezione distinta denominata **Backup di applicazioni cloud**.

Le posizioni di backup utilizzate nei piani di protezione vengono automaticamente aggiunte alla scheda **Archivio di backup**. Per aggiungere una cartella personalizzata (ad esempio, un dispositivo USB rimovibile) all'elenco delle posizioni di backup, fare clic su **Sfoglia** e specificare il percorso della cartella.

Se sono stati aggiunti o eliminati alcuni backup usando un gestore di file, fare clic sull'icona dell'ingranaggio accanto al nome della posizione, quindi fare clic su **Aggiorna**.

Attenzione!
Non tentare di modificare i file di backup manualmente, perché ciò potrebbe causare il danneggiamento dei file e rendere i backup inutilizzabili. È consigliabile inoltre utilizzare la replica di backup invece di spostare i file di backup manualmente.

Una posizione di backup (ad eccezione dell'archivio nel cloud) non viene più visualizzata nella scheda **Archivio di backup** se tutti i sistemi il cui backup sia mai stato eseguito sulla posizione vengono eliminati dal servizio Cyber Protection. In questo modo si evita che vengano addebitati dei costi per i backup archiviati nella posizione. Non appena viene eseguito il backup nella posizione, questa viene nuovamente aggiunta insieme ai backup che contiene.

Nella scheda **Archivio di backup** è possibile filtrare i backup dell'elenco in base ai seguenti criteri:

- **Solo con dati forensi** – verranno mostrati solo i backup contenenti dati forensi.
- **Solo backup precedenti all'aggiornamento creati con lo strumento per la gestione delle patch**– verranno mostrati solo i backup creati con lo strumento per la gestione delle patch eseguito prima dell'installazione delle patch.

Per selezionare un punto di ripristino utilizzando la scheda Archivio di backup

1. Nella scheda **Archivio di backup**, selezionare la posizione in cui vengono archiviati i backup.
   Il software mostra tutti i backup che l'account è autorizzato a visualizzare nella posizione selezionata. I backup vengono accorpati in gruppi. I nomi dei gruppi si basano sul seguente modello:
   `<nome sistema> - <nome piano di protezione>`
2. Selezionare un gruppo da cui ripristinare i dati.
3. [Facoltativo] fare clic su **Modifica** accanto a **Macchina da esplorare da**, quindi selezionare un'altra macchina. Alcuni backup possono essere esplorati solo da agenti specifici. Ad esempio, è necessario selezionare un sistema che esegue l'Agente per SQL per sfogliare i backup dei database di Microsoft SQL Server.

© Acronis International GmbH, 2003-2024

Importante
Tenere presente che **Macchina da esplorare da** indica una destinazione predefinita per il ripristino da un backup di macchina fisica. Dopo aver selezionato un punto di ripristino e aver fatto clic su **Ripristina**, controllare di nuovo l'impostazione **Macchina di destinazione** per accertarsi che si desidera eseguire il ripristino su tale macchina specifica. Per cambiare la destinazione di ripristino, specificare un altro sistema in **Macchina da esplorare da**.

4. Fare clic su **Mostra backup**.
5. Selezionare il punto di ripristino.

Per aggiungere una posizione di backup

Nota
Questa operazione è disponibile solo in presenza di un agente online.

Nella scheda **Archivio di backup**, fare clic su **Aggiungi posizione**.

Selezionare una posizione tra i seguenti tipi, quindi fare clic su **Fine**:

- Cartella locale
- Cartella di rete
- Secure Zone
- Cartella NFS
- Cloud pubblico

Montaggio di volumi da un backup

Il montaggio di volumi da un backup a livello del disco consente di accedere ai volumi come se fossero dischi fisici.

Il montaggio di volumi nella modalità lettura/scrittura consente di modificare il contenuto di backup, vale a dire salvare, spostare, creare, eliminare file o cartelle ed eseguire gli elementi eseguibili composti da un unico file. In questa modalità, il software crea un backup incrementale che contiene le modifiche apportate al contenuto del backup. Tenere presente che nessuno dei backup successivi conterrà tali modifiche.

Requisiti

- Questa funzionalità è disponibile solo in Windows utilizzando Esplora file.
- Sul sistema che esegue l'operazione di montaggio deve essere installato l'Agente per Windows.
- Il file system di cui si esegue il backup deve essere supportato dalla versione Windows in esecuzione nel sistema.
- Il backup deve essere archiviato in una cartella locale, su una condivisione di rete (SMB/CIFS) o nella Secure Zone.

© Acronis International GmbH, 2003-2024

Scenari di utilizzo

- Condivisione dei dati

  I volumi montati possono essere facilmente condivisi in rete.
- Soluzione di ripristino di database "Band-aid"

  Monta un volume che contiene un database SQL di una macchina che ha subito un guasto di recente. Ciò fornirà l'accesso al database fino al ripristino della macchina guasta. È possibile adottare questo approccio anche per il ripristino granulare dei dati di Microsoft SharePoint tramite SharePoint Explorer.
- Rimozione dei virus offline

  Se una macchina è stata infettata, montare il backup, pulirla con un programma antivirus (oppure trovare l'ultimo backup non infetto), quindi eseguire il ripristino della macchina da quel backup.
- Controllo degli errori

  Se un ripristino con ridimensionamento del volume non è riuscito, ciò potrebbe essere dovuto a un errore del file system di cui è stato eseguito il backup. Montare il backup in modalità lettura/scrittura. A questo punto, verificare la presenza di errori sul volume montato tramite il comando `chkdsk /r`. Dopo aver risolto gli errori e aver creato un nuovo backup incrementale, ripristinare il sistema da questo backup.

Per montare un volume da un backup

1. Passare alla posizione del backup utilizzando Esplora file.
2. Fare doppio clic sul file di backup. I nomi dei file si basano sul seguente modello:

   `<nome sistema> - <GUID piano di protezione>`
3. Se il backup è crittografato, inserire la password per la crittografia. Altrimenti, ignorare questo passaggio.

   Esplora file visualizza i punti di ripristino.
4. Fare doppio clic sul punto di ripristino.

   Esplora file visualizza i volumi di cui è stato eseguito il backup.

   Nota
   Fare doppio clic su un volume per sfogliarne il contenuto. È possibile copiare file e cartelle dal backup in qualsiasi cartella del file system.

5. Fare clic con il pulsante destro su un volume da montare, quindi selezionare una delle seguenti opzioni:
   a. **Monta**

      Nota
      È possibile montare in modalità lettura/scrittura soltanto l'ultimo backup nell'archivio (catena di backup).

   b. **Monta in modalità di sola lettura**.

© Acronis International GmbH, 2003-2024

6. Se il backup è archiviato in una condivisione di rete, fornire le credenziali di accesso. Altrimenti, ignorare questo passaggio.
   Il software monta il volume selezionato. La prima lettera inutilizzata viene assegnata al volume.

Per smontare un volume.

1. Accedere a **Computer** (**Questo PC** a partire da Windows 8.1) tramite Esplora file.
2. Fare clic con il pulsante destro del mouse sul volume montato.
3. Fare clic su **Smonta**.
4. [Facoltativo] Se il volume è stato montato in modalità lettura/scrittura e il relativo contenuto è stato modificato, selezionare se creare un backup incrementale contenente le modifiche. Altrimenti, ignorare questo passaggio.

Il software smonta il volume selezionato.

Convalida di backup

La convalida di un backup consente di verificare che sia possibile recuperare i dati che questo contiene. Per ulteriori informazioni su questa operazione, fare riferimento a "Convalida" (pag. 205).

Nota
Questa funzionalità è disponibile nei tenant cliente per i quali la quota di **Advanced Backup - Server** o la quota di **Advanced Backup - NAS** è abilitata come parte del pacchetto Advanced Backup.

Per convalidare un backup

1. Selezionare il workload di cui è stato eseguito il backup.
2. Fare clic su **Ripristino**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.
   Se il workload è offline, i punti di ripristino non vengono visualizzati. Eseguire una delle seguenti operazioni:
   - Se la posizione di backup è il cloud o un archivio condiviso (a cui possono accedere altri agenti), fare clic su **Seleziona macchina**, scegliere un workload di destinazione che sia online, quindi selezionare un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda Archivio di backup. Per ulteriori informazioni sui backup, fare riferimento a "La scheda Archivio di backup" (pag. 536).
4. Fare clic sull'icona ingranaggio e quindi su **Convalida**.
5. Selezionare l'agente che eseguirà la convalida.
6. Selezionare il metodo di convalida.
7. Se il backup è crittografato, inserire la password per la crittografia.
8. Fare clic su **Avvia**.

 © Acronis International GmbH, 2003-2024

Esportazione di backup

L'operazione di esportazione determina la creazione di una copia autosufficiente del backup nella posizione specificata. Il backup originale resta intatto. L'esportazione dei backup consente di separare un backup specifico da una catena di backup incrementali e differenziali per velocizzare un eventuale ripristino, scrivendo su supporti rimovibili o scollegabili o per altri scopi.

Nota
Questa funzionalità è disponibile nei tenant cliente per i quali la quota di **Advanced Backup - Server** o la quota di **Advanced Backup - NAS** è abilitata come parte del pacchetto Advanced Backup.

Il risultato di un'operazione di esportazione è sempre un backup completo. Se si desidera copiare l'intera catena di backup in una posizione diversa e mantenere più punti di ripristino, utilizzare un piano di copia del backup. Per ulteriori informazioni sul piano, fare riferimento a "Replica di backup" (pag. 202).

Il nome del file di backup del backup esportato è lo stesso del backup originale, ad eccezione della sequenza di numeri. Se più backup della stessa catena di backup vengono esportati nella stessa posizione, ai nomi dei file di tutti i backup - ad eccezione del primo - viene aggiunta una sequenza numerica di quattro cifre.

I backup esportati ereditano le impostazioni e la password di crittografia dal backup originale. Quando si esporta un backup crittografato è necessario specificare la password.

Per esportare un backup

1. Selezionare il workload di cui è stato eseguito il backup.
2. Fare clic su **Ripristino**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.
   Se il workload è offline, i punti di ripristino non vengono visualizzati. Eseguire una delle seguenti operazioni:
   - Se la posizione di backup è il cloud o un archivio condiviso (a cui possono accedere altri agenti), fare clic su **Seleziona macchina**, scegliere un workload di destinazione che sia online, quindi selezionare un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda Archivio di backup. Per ulteriori informazioni sui backup, fare riferimento a "La scheda Archivio di backup" (pag. 536).
4. Fare clic sull'icona ingranaggio quindi su **Esporta**.
5. Selezionare l'agente che eseguirà l'esportazione.
6. Se il backup è crittografato, inserire la password per la crittografia. Altrimenti, ignorare questo passaggio.

© Acronis International GmbH, 2003-2024

7. Specificare la destinazione per l'esportazione.
8. Fare clic su **Avvia**.

Eliminazione di backup

Un archivio di backup contiene uno o più backup. È possibile eliminare backup specifici (punti di ripristino) in un archivio o l'intero archivio.

Se si elimina l'archivio di backup, si eliminano tutti i backup che contiene. Se si eliminano tutti i backup di un workload si eliminano gli archivi di backup che contengono tali backup.

È possibile eliminare i backup utilizzando la console di Cyber Protect, dalla scheda **Dispositivi** e dalla scheda **Archivio di backup**. Inoltre, è possibile eliminare i backup dal cloud storage utilizzando la console Web Restore.

Attenzione!
Se l'archivio immutabile è disabilitato, i dati dei backup vengono eliminati in modo permanente e non sarà possibile ripristinarli.

Per eliminare backup o archivi di backup

Nella scheda Dispositivi

Questa procedura si applica solo ai workload online.

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare i backup del workload da eliminare.
3. Fare clic su **Ripristino**.
4. [Se sono disponibili più posizioni di backup] Selezionare la posizione del backup.
5. [Per eliminare tutti i backup del workload] Fare clic su **Elimina tutti**.
   L'eliminazione di tutti i backup comporta anche l'eliminazione degli archivi di backup che contengono tali backup.
6. [Per eliminare un backup specifico] Selezionare il backup (punto di ripristino) da eliminare, quindi fare clic su **Azioni** > **Elimina**.
7. [Se si eliminano tutti i backup] Selezionare la casella di controllo, quindi fare clic su **Elimina** per confermare la decisione.
8. [Quando si elimina un backup specifico] Fare clic su **Elimina** per confermare la decisione.

Nella scheda Archivio di backup

Questa procedura si applica ai workload online e offline.

1. Nella console di Cyber Protect, passare a **Archivio di backup**.
2. Selezionare la posizione da cui eliminare i backup.
3. Selezionare l'archivio di backup da cui eliminare i backup.

© Acronis International GmbH, 2003-2024

Il nome dell'archivio utilizza il seguente modello:

- Archivi di backup non cloud-to-cloud: <nome workload> - <nome piano di protezione>
- Archivi di backup cloud-to-cloud: <nome utente> o <nome unità> o <nome team> - <servizio cloud> - <nome piano di protezione>

4. [Per eliminare l'intero archivio di backup] Fare clic su **Elimina**.
   L'eliminazione di un archivio di backup elimina tutti i backup contenuti in quell'archivio.
5. [Per eliminare un backup specifico nell'archivio di backup] Fare clic su **Mostra backup**.
   a. Selezionare il backup (punto di ripristino) da eliminare.
   b. Fare clic su **Azioni** > **Elimina**.
6. [Quando si elimina un archivio di backup] Selezionare la casella di controllo, quindi fare clic su **Elimina** per confermare la decisione.
7. [Quando si elimina un backup specifico] Fare clic su **Elimina** per confermare la decisione.

Nella console Web Restore

Questa procedura si applica solo agli archivi di backup nel cloud storage.

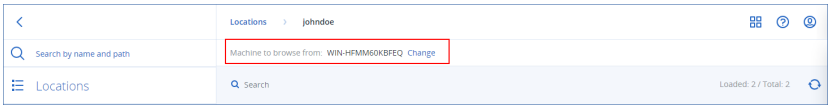
1. Nella console di Cyber Protection, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare i backup del workload da eliminare, quindi fare clic su **Ripristina**.
3. [Se sono disponibili più posizioni di backup] Selezionare la posizione del backup, quindi fare clic su **Altri metodi di ripristino**.
4. Fare clic su **Scarica file**.
   L'utente viene reindirizzato alla console Web Restore.
5. Nella console Web Restore, in **Macchine**, fare clic sul nome del workload.
6. In **Ultima versione**, fare clic sulla data, quindi su **Elimina**.
   Questa azione è disponibile solo al livello dell'archivio di backup. Non è possibile esaminare in dettaglio l'archivio ed eliminare da questo backup specifici.
7. Fare clic su **Elimina** per confermare la decisione.

Eliminazione dei backup fuori dalla console di Cyber Protect

Si consiglia di eliminare i backup tramite la console di Cyber Protect. Se si eliminano i backup dal cloud storage tramite la console Web Restore o si eliminano i backup locali tramite un file manager, sarà necessario aggiornare la posizione del backup per poter sincronizzare le modifiche con la console di Cyber Protect.

Prerequisito

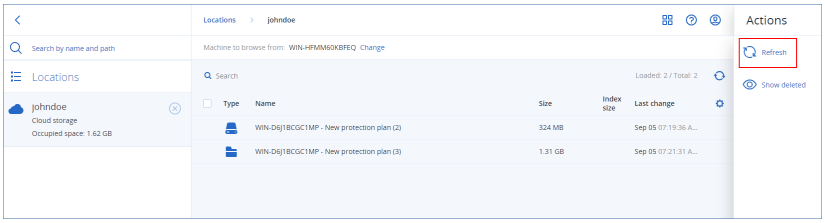
- Un agente online che può accedere alla posizione di backup deve essere selezionato come **Macchina da esplorare da** nella console di Cyber Protect.



Per aggiornare una posizione di backup

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Archivio di backup**.
2. Selezionare la posizione di backup in cui sono stati archiviati i backup eliminati.
3. Nel pannello **Azioni**, fare clic su **Aggiorna**.



Analisi del rilevamento dei colli di bottiglia

La funzionalità di rilevamento dei colli di bottiglia aiuta a comprendere dove intervenire per migliorare le prestazioni, perché evidenzia i componenti più lenti del sistema durante un processo di backup o ripristino.

Poiché i colli di bottiglia si verificano *sempre* durante un evento di trasmissione, il loro rilevamento non implica che debbano essere risolti. I backup possono essere già sufficientemente rapidi e rientrare nelle finestre di backup in modo perfetto, oltre a rispettare gli SLA pertinenti; in genere non ci sono problemi da risolvere.

È possibile visualizzare e tracciare con facilità i colli di bottiglia nella scheda **Dettagli attività**. A tal fine, nella console di Cyber Protect, passare a **Monitoraggio > Attività** e fare clic sull'attività pertinente. Per ulteriori informazioni sulla visualizzazione dei colli di bottiglia, consultare "Visualizzazione dei dettagli sui colli di bottiglia" (pag. 546) e "Per quali workload, agenti e posizioni di backup vengono visualizzati i colli di bottiglia?" (pag. 547).

Cos'è un collo di bottiglia?

I colli di bottiglia sono in genere causati da un componente lento nella catena di elaborazione, ovvero un componente che crea una coda di attesa per gli altri componenti.

La funzionalità di rilevamento del collo di bottiglia consente di tenere traccia di questi elementi durante il processo di backup e ripristino, consentendo di capire quale tra i tipi di componente seguenti è il più lento:

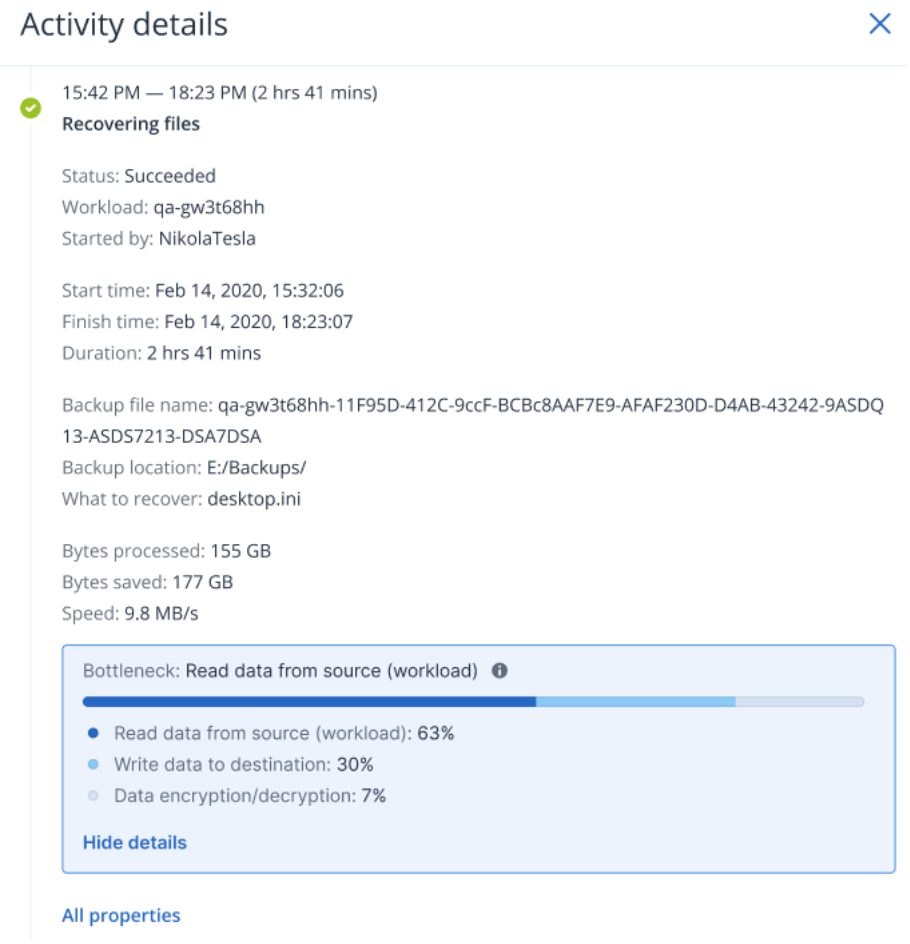
- **Origine**: una sola panoramica consente di determinare se la velocità di lettura dall'origine del backup/del ripristino sta causando un collo di bottiglia.
- **Destinazione**: per comprendere se la velocità di scrittura verso la destinazione di backup incide sulle prestazioni.
- **Agente**: per comprendere se l'agente sta elaborando i dati con la giusta velocità.

Il tipo di collo di bottiglia, che sia causato dall'origine, dalla destinazione o dall'agente può variare nelle diverse fasi dell'attività di backup/ripristino. Le percentuali mostrate nella sezione **Collo di bottiglia** della scheda **Dettagli attività** seguente (ad esempio, **Lettura dati da origine (workload): 63%**), rappresentano la percentuale di tempo in cui questo tipo di collo di bottiglia

© Acronis International GmbH, 2003-2024

viene riscontrato. In questo caso, per il 63% del tempo in cui si è svolta l'attività di ripristino, il tipo di collo di bottiglia stava leggendo i dati; in altre parole, la metrica indica la bassa velocità di lettura dei dati dall'archivio di backup da parte dell'agente.

Analogamente, per il 30% del tempo il collo di bottiglia è stato causato dalla bassa velocità di scrittura dei dati nella destinazione del ripristino (**Scrittura dati su destinazione: 30%**).



Nota
Si consiglia di visualizzare le statistiche relative ai colli di bottiglia nella scheda **Dettagli attività**. Queste statistiche sono disponibili solo per le attività che durano più di un minuto.

Come ridurre i colli di bottiglia

Come indicato sopra, la funzionalità di rilevamento dei colli di bottiglia evidenza il flusso di dati in *lettura* e *scrittura* tra i componenti del backup. Le statistiche di *lettura* si riferiscono al flusso di dati dall'origine dei dati all'agente che esegue l'operazione di backup/ripristino, mentre le statistiche di *scrittura* si riferiscono al flusso di dati tra l'agente e l'archivio di backup (la destinazione).

Per ridurre i colli di bottiglia e migliorare le prestazioni dei flussi di dati di lettura/scrittura, è necessario analizzare il canale tra l'agente e l'archivio di origine/backup dei dati. È possibile, ad

© Acronis International GmbH, 2003-2024

esempio, confrontare le prestazioni dei dischi rigidi se l'agente sta eseguendo il backup di alcuni file locali.

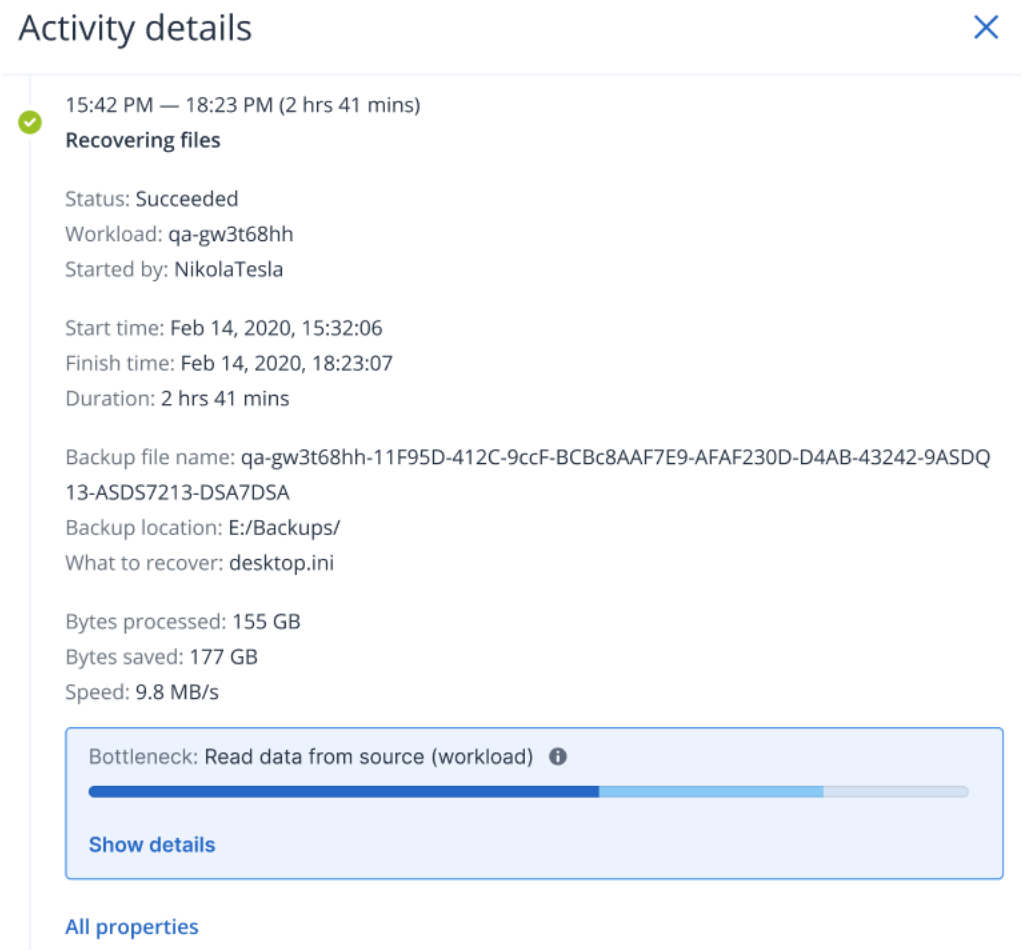
Visualizzazione dei dettagli sui colli di bottiglia

È possibile visualizzare i colli di bottiglia rilevati per qualsiasi tipo di backup, replica di backup o processo di ripristino (verso qualsiasi tipo di cartella o posizione di destinazione), inclusi i backup di virtual machine, i backup di sistemi e i backup di file/cartelle. È inoltre possibile visualizzare i colli di bottiglia relativi alle repliche delle virtual machine e alle attività di failback.

Per ulteriori informazioni sulla definizione e sui concetti chiave relativi ai colli di bottiglia, consultare "Analisi del rilevamento dei colli di bottiglia" (pag. 544).

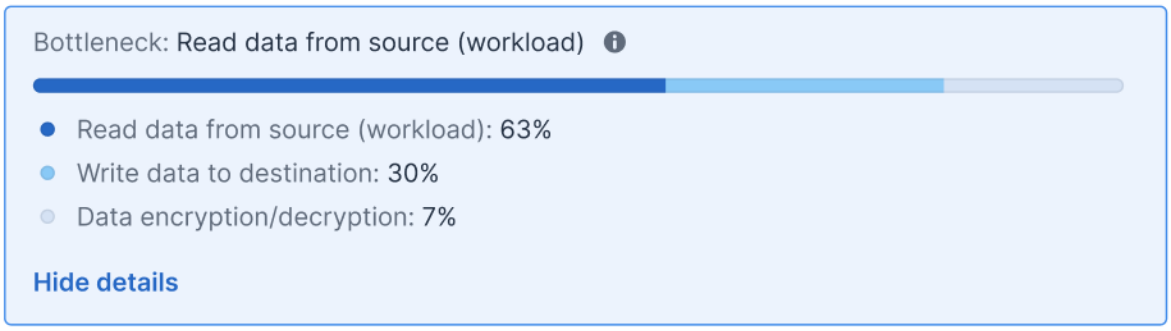
Per visualizzare i dettagli sui colli di bottiglia

1. Nella console di Cyber Protect, passare a **Monitoraggio > Attività**.
2. Fare clic sull'attività pertinente.
   Nella scheda **Dettagli attività**, la sezione **Collo di bottiglia** è mostrata in blu.



3. Fare clic su **Mostra dettagli** per visualizzare i colli di bottiglia incontrati con la maggiore frequenza durante le operazioni di backup/ripristino.
   È possibile espandere la sezione **Collo di bottiglia** per mostrare un riepilogo dei tipi di collo di bottiglia pertinenti.

© Acronis International GmbH, 2003-2024



Nell'esempio precedente, il collo di bottiglia responsabile del 63% del tempo impiegato dall'intera operazione è causato dall'operazione di *lettura* (eseguita dall'agente).

Nota
I valori del collo di bottiglia si aggiornano in modo dinamico per ogni minuto di esecuzione dell'attività corrispondente.

Per quali workload, agenti e posizioni di backup vengono visualizzati i colli di bottiglia?

Il rilevamento dei colli di bottiglia è disponibile per i seguenti tipi di workload, agenti e posizioni di backup:

- Backup di disco/immagine eseguiti da:
  - Agente per Azure
  - Agente per Windows
  - Agente per Linux
  - Agente per Mac
  - Agente per VMware (sia Virtual Appliance che Windows, inclusa le attività di replica di VM e il failback dalla replica (ripristino da replica))
  - Agente per Hyper-V
  - Agente per Scale Computing
  - Agente per oVirt (KVM)
  - Agente per Virtuozzo Infrastructure Platform
  - Agente per Virtuozzo
  - Agente per VMware Cloud Director (vCD-BA)
- Backup a livello di file
  - Agente per Windows
  - Agente per Linux
  - Agente per Mac

© Acronis International GmbH, 2003-2024

- Backup delle applicazioni
  - Agente per SQL
  - Agente per Exchange
  - Agente per MySQL/MariaDB
  - Agente per Oracle
  - Agente per SAP HANA
- Posizioni di backup
  - Acronis Cloud Storage (incluso lo storage in hosting del Partner)
  - Cloud storage pubblico
  - Condivisioni di rete (SMB + NFS)
  - Cartelle locali
  - Posizioni definite da script
  - Acronis Secure Zone

Backup di workload su cloud pubblici

Nota
Questa funzionalità fa parte del pacchetto Advanced Backup, che a sua volta è parte del servizio Cyber Protection. Tenere presente che l'aggiunta di questa funzionalità a un piano di protezione può essere soggetta a costi aggiuntivi.

È possibile selezionare servizi di cloud pubblico, come Microsoft Azure e Amazon S3 (Simple Storage Service), come destinazioni di backup nella console di Cyber Protect.

Per configurare le posizioni di backup nei cloud pubblici, è necessario essere un Amministratore dell'azienda o un Amministratore di unità, o avere uno dei seguenti ruoli definiti nel servizio di Cyber Protection: Amministratore Cyber, Amministratore o Utente.

Definizione di una posizione di backup in Microsoft Azure

Nota
Per configurare le posizioni di backup in Microsoft Azure, è necessario disporre di uno tra i seguenti ruoli definiti nel servizio Cyber Protection: Amministratore dell'azienda, Utente, Amministratore Cyber.

Per eseguire il backup di workload su Microsoft Azure, è necessario definire la posizione di backup di Microsoft Azure nella console di Cyber Protect, e connettersi all'abbonamento Microsoft Azure pertinente. Questa operazione può essere eseguita nei modi seguenti:

- Quando si crea o modifica un piano di protezione.
- Quando si definiscono e gestiscono posizioni di storage di backup.

© Acronis International GmbH, 2003-2024

Importante
Sia gli utenti amministratori che quelli non amministratori possono eseguire il backup dei workload su Microsoft Azure.

Gli utenti non amministratori possono aggiungere l'accesso a un abbonamento Microsoft Azure (consultare "Gestione dell'accesso agli abbonamenti Microsoft Azure" (pag. 559)), ma possono applicare i piani di protezione solo se la posizione di backup è collegata all'abbonamento Microsoft Azure da loro aggiunto, e per i workload registrati nella console di Cyber Protect a loro nome.

Gli utenti amministratori possono applicare i piani di protezione se la posizione di backup è collegata agli abbonamenti di Microsoft Azure da loro aggiunti o agli abbonamenti aggiunti da altri amministratori, e per i workload registrati nella console di Cyber Protect a nome di qualsiasi utente.

Per definire una posizione di backup in Microsoft Azure

1. Nella console di Cyber Protect, procedere come segue:
   - Se si sta creando o modificando un piano di protezione, passare a **Dispositivi** e selezionare il workload di cui si intende eseguire il backup su Microsoft Azure. Nella sezione **Backup** del piano di protezione del workload selezionato, fare clic sul collegamento nella riga **Dove eseguire il backup**.

     Per ulteriori informazioni su come lavorare con i piani di protezione, consultare "Piani e moduli di protezione" (pag. 217).
   - Se si stanno gestendo le posizioni degli storage di backup e si desidera aggiungere Microsoft Azure come nuova posizione, passare a **Archivio di backup**.

     Per ulteriori informazioni sulla gestione delle posizioni dello storage di backup, consultare "La scheda Archivio di backup" (pag. 536).
2. Fare clic su **Aggiungi posizione**.
3. Nell'elenco a discesa **Cloud pubblici**, selezionare **Microsoft Azure**.
4. Se l'abbonamento Microsoft Azure pertinente è già registrato nella console di Cyber Protect, selezionarlo dall'elenco degli abbonamenti.

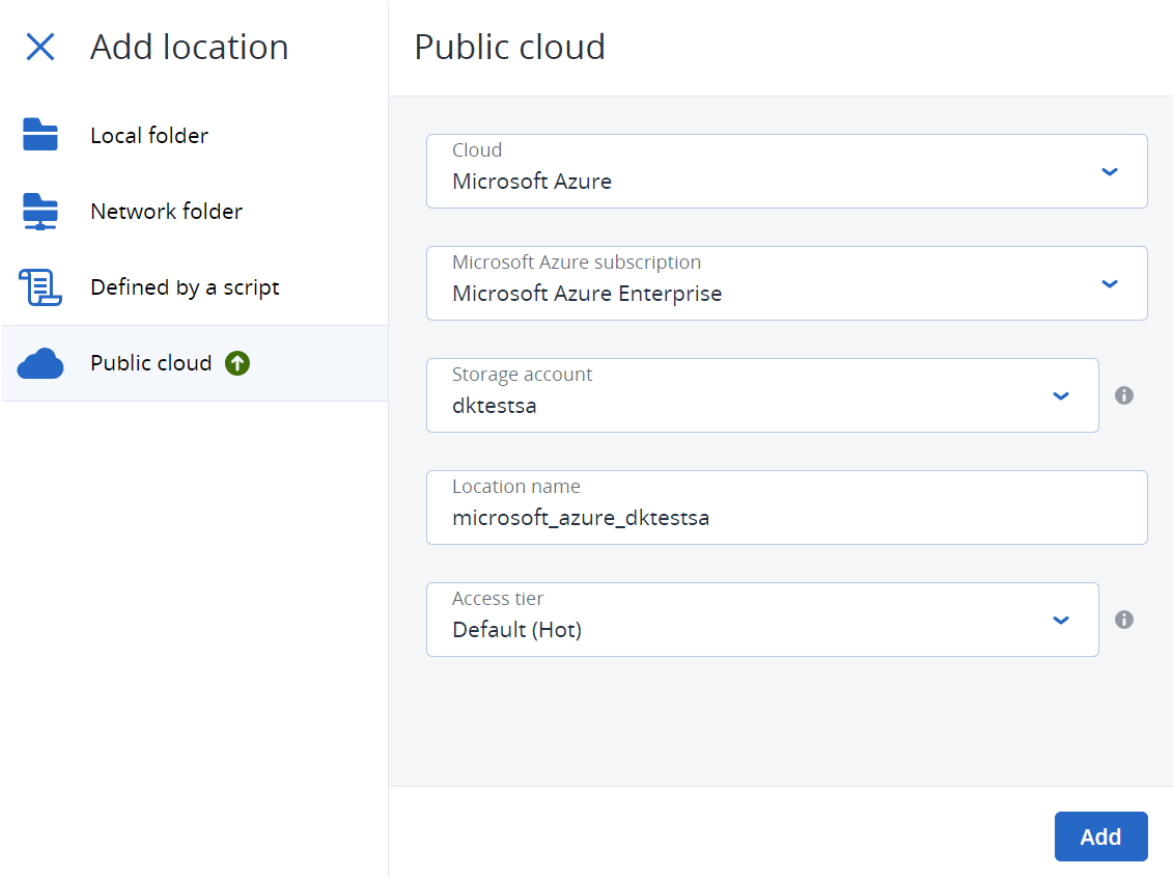
   Se l'abbonamento pertinente non è registrato nella console di Cyber Protect, fare clic su **Aggiungi** e quindi, nella finestra visualizzata, su **Accedi**. Il sistema reindirizza l'utente alla pagina di login di Microsoft. Per ulteriori informazioni su come aggiungere e definire l'accesso a un abbonamento Microsoft Azure, consultare "Aggiunta dell'accesso a un abbonamento Microsoft Azure" (pag. 560).
5. Nel campo **Account di storage**, selezionare l'account pertinente.

   Nota
   Al momento sono supportati soltanto gli account di storage Microsoft Azure con suffissi di endpoint regolari, che contengono `core.windows.net`. In aggiunta, l'account di storage selezionato deve essere un tipo di account StorageV2.

© Acronis International GmbH, 2003-2024

Per impostazione predefinita, i campi **Nome posizione** e **Livello di accesso** vengono compilati automaticamente in base all'account di storage selezionato. Il nome della posizione visualizzato è `microsoft_azure_[storage account]` e il livello di accesso selezionato è **Predefinito (Ad accesso frequente)**. Entrambi i campi possono essere modificati come necessario.

Nota
Se si modifica il nome di una posizione, inserire un nome univoco (il nome deve essere esclusivo del tenant cliente). Se il nome aggiunto esiste già nell'account di storage, Acronis aggiunge un numero di suffisso al nome. Ad esempio, se **Microsoft Azure Storage** esiste già, il nome viene automaticamente aggiornato in **Microsoft Azure Storage_01**.



6. Fare clic su **Aggiungi**.
   Se si sta creando o modificando un piano di protezione, la posizione di backup Microsoft Azure viene impostata come posizione nella riga **Dove eseguire il backup**. Una volta eseguito il backup (sia manualmente che in base alla pianificazione), questo viene salvato nella posizione predefinita.
   Se si stanno gestendo le posizioni dello storage di backup, è possibile visualizzare e aggiornare i dettagli della posizione come necessario. La posizione Microsoft Azure è disponibile anche durante la definizione di una posizione di backup per i workload. Per ulteriori informazioni, consultare "Visualizzazione e aggiornamento delle posizioni di backup nel cloud pubblico" (pag. 555).

© Acronis International GmbH, 2003-2024

Definizione di una posizione di backup in Amazon S3

Nota
Per configurare le posizioni di backup in Amazon S3, è necessario disporre di uno tra i seguenti ruoli definiti nel servizio Cyber Protection: Amministratore dell'azienda, Utente, Amministratore Cyber.

Per eseguire il backup di un workload su Amazon S3, è necessario definire la posizione di backup di Amazon S3 nella console di Cyber Protect, quindi connettersi alla relativa connessione Amazon S3. È possibile agire nei modi seguenti:

- Quando si crea o modifica un piano di protezione.
- Quando si definiscono e gestiscono posizioni di storage di backup.

Importante
Sia gli utenti amministratori che quelli non amministratori possono eseguire il backup dei workload su Amazon S3.

Gli utenti non amministratori possono aggiungere l'accesso a una connessione Amazon S3 (consultare "Gestione dell'accesso ad altri servizi di cloud storage pubblico" (pag. 563)), ma possono applicare i piani di protezione solo se la posizione di backup è collegata alla connessione Amazon S3 da loro aggiunta, e per i workload registrati nella console di Cyber Protect a loro nome.

Gli utenti amministratori possono applicare i piani di protezione se la posizione di backup è collegata alle connessioni Amazon S3 da loro aggiunte o agli abbonamenti aggiunti da altri amministratori, e per i workload registrati nella console di Cyber Protect a nome di qualsiasi utente.

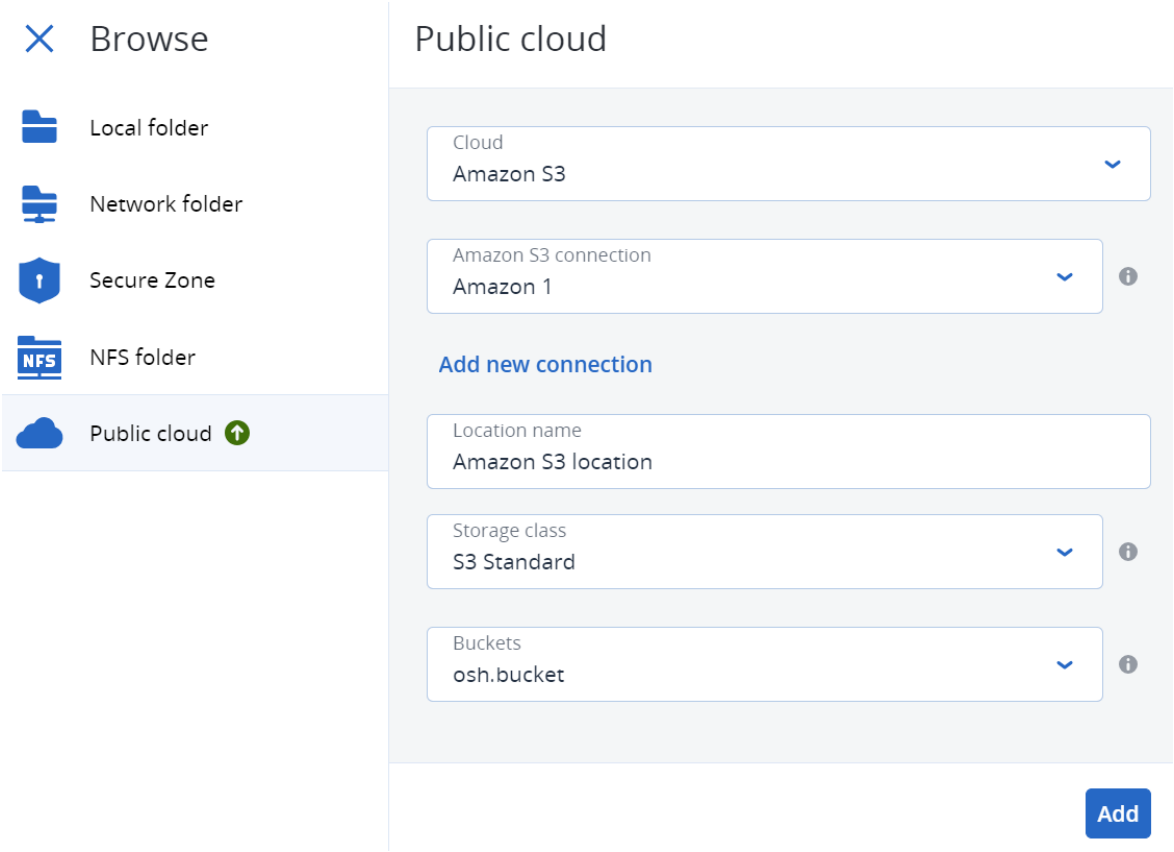
Per definire una posizione di backup in Amazon S3

1. Nella console di Cyber Protect, procedere come segue:
   - Se si sta creando o modificando un piano di protezione, passare a **Dispositivi** e selezionare il workload di cui si intende eseguire il backup su Amazon S3. Nella sezione **Backup** del piano di protezione del workload selezionato, fare clic sul collegamento nella riga **Dove eseguire il backup**.
     Per ulteriori informazioni su come lavorare con i piani di protezione, consultare "Piani e moduli di protezione" (pag. 217).
   - Se si stanno gestendo le posizioni degli storage di backup e si desidera aggiungere Amazon S3 come nuova posizione, passare a **Archivio di backup**.
     Per ulteriori informazioni sulla gestione delle posizioni dello storage di backup, consultare "La scheda Archivio di backup" (pag. 536).
2. Fare clic su **Aggiungi posizione**.
3. Nell'elenco a discesa **Cloud pubblici**, selezionare **Amazon S3**.

© Acronis International GmbH, 2003-2024

4. Se la connessione ad Amazon S3 pertinente è già registrata nella console di Cyber Protect, selezionarla dall'elenco.

   Se la connessione pertinente non è registrata nella console di Cyber Protect, fare clic su **Aggiungi nuova connessione**. Per ulteriori informazioni sull'aggiunta e la definizione dell'accesso a una connessione Amazon S3, consultare "Aggiunta dell'accesso a una connessione al cloud pubblico" (pag. 564). Una volta aggiunta la connessione, continuare con il passaggio successivo.



5. Definire quanto segue:
   - Nel campo **Nome posizione**, inserire il nome della posizione di backup.

     Nota
     Il nome della posizione deve essere univoco per il tenant cliente. Se il nome aggiunto esiste già nella connessione, Acronis aggiunge al nome un numero di suffisso. Ad esempio, se **Storage Amazon S3** esiste già, il nome verrà automaticamente modificato in **Storage Amazon S3 1**.

   - Nel campo **Classe di storage**, selezionare una delle seguenti classi di storage supportate:
     - S3 Standard
     - Standard - Accesso non frequente (S3 Standard-IA)
     - Una zona - Accesso non frequente (S3 One Zone-IA)

© Acronis International GmbH, 2003-2024

- S3 Intelligent Tiering

- Nel campo **Bucket**, selezionare il bucket di Amazon S3 pertinente.

6. Fare clic su **Aggiungi**.

   Se si sta creando o modificando un piano di protezione, la posizione di backup Amazon S3 viene impostata come posizione nella riga **Dove eseguire il backup**. Una volta eseguito il backup (sia manualmente che in base alla pianificazione), questo viene salvato nella posizione definita.

   Se si stanno gestendo le posizioni dello storage di backup, è possibile visualizzare e aggiornare i dettagli della posizione come necessario. La posizione Amazon S3 è disponibile anche durante la definizione di una posizione di backup per i workload. Per ulteriori informazioni, consultare "Visualizzazione e aggiornamento delle posizioni di backup nel cloud pubblico" (pag. 555).

Definizione di una posizione di backup in Wasabi

Nota
Per configurare le posizioni di backup in Wasabi, è necessario disporre di uno tra i seguenti ruoli definiti nel servizio Cyber Protection: Amministratore dell'azienda, Utente, Amministratore Cyber.

Per eseguire il backup di un workload su Wasabi, è necessario definire la posizione di backup di Wasabi nella console di Cyber Protect, quindi connettersi alla relativa connessione Wasabi. È possibile agire nei modi seguenti:

- Quando si crea o modifica un piano di protezione.
- Quando si definiscono e gestiscono posizioni di storage di backup.

Importante
Sia gli utenti amministratori che quelli non amministratori possono eseguire il backup dei workload su Wasabi.

Gli utenti non amministratori possono aggiungere l'accesso a una connessione Wasabi (consultare "Gestione dell'accesso ad altri servizi di cloud storage pubblico" (pag. 563)), ma possono applicare i piani di protezione solo se la posizione di backup è collegata alla connessione Wasabi da loro aggiunta, e per i workload registrati nella console di Cyber Protect a loro nome.

Gli utenti amministratori possono applicare i piani di protezione se la posizione di backup è collegata alle connessioni Wasabi da loro aggiunte o agli abbonamenti aggiunti da altri amministratori, e per i workload registrati nella console di Cyber Protect a nome di qualsiasi utente.

Per definire una posizione di backup in Wasabi

1. Nella console di Cyber Protect, procedere come segue:
   - Se si sta creando o modificando un piano di protezione, passare a **Dispositivi** e selezionare il workload di cui si intende eseguire il backup su Wasabi. Nella sezione **Backup** del piano di protezione del workload selezionato, fare clic sul collegamento nella riga **Dove eseguire il**

© Acronis International GmbH, 2003-2024

backup.

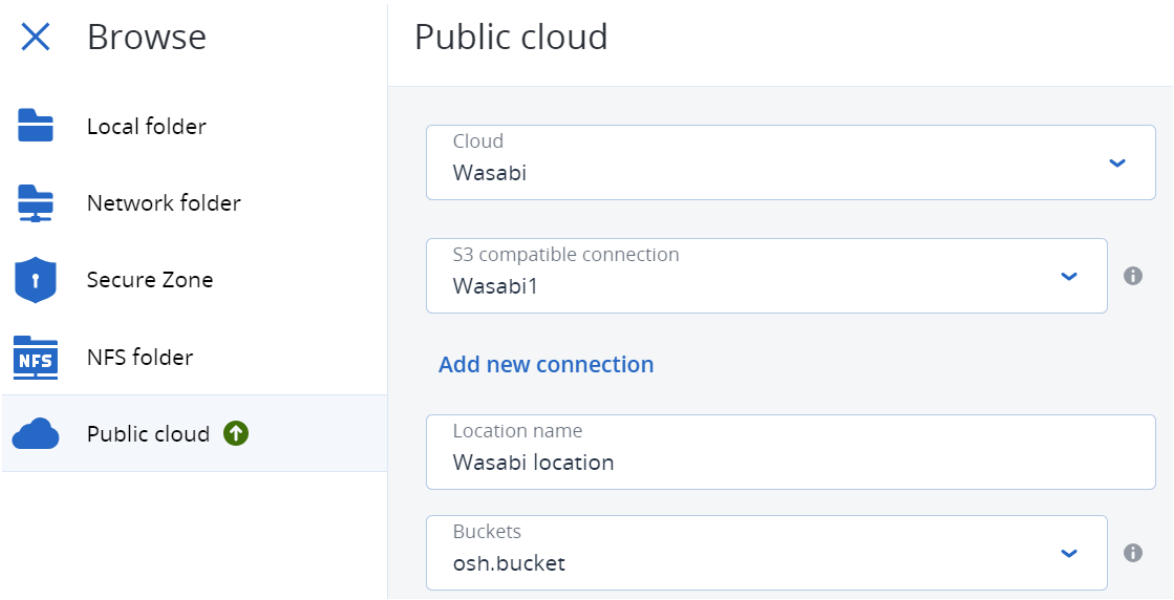
Per ulteriori informazioni su come lavorare con i piani di protezione, consultare "Piani e moduli di protezione" (pag. 217).

- Se si stanno gestendo le posizioni degli storage di backup e si desidera aggiungere Wasabi come nuova posizione, passare a **Archivio di backup**.

  Per ulteriori informazioni sulla gestione delle posizioni dello storage di backup, consultare "La scheda Archivio di backup" (pag. 536).

2. Fare clic su **Aggiungi posizione**.
3. Nell'elenco a discesa **Cloud pubblici**, selezionare **Wasabi**.
4. Se la connessione a Wasabi pertinente è già registrata nella console di Cyber Protect, selezionarla dall'elenco delle connessioni.

   Se la connessione pertinente non è registrata nella console di Cyber Protect, fare clic su **Aggiungi nuova connessione**. Per ulteriori informazioni sull'aggiunta e la definizione dell'accesso a una connessione Wasabi, consultare "Aggiunta dell'accesso a una connessione al cloud pubblico" (pag. 564). Una volta aggiunta la connessione, continuare con il passaggio successivo.



5. Definire quanto segue:
   - Nel campo **Nome posizione**, inserire il nome della posizione di backup.

     Nota
     Il nome della posizione deve essere univoco per il tenant cliente. Se il nome aggiunto esiste già nella connessione, Acronis aggiunge al nome un numero di suffisso. Ad esempio, se **Storage Wasabi** esiste già, il nome verrà automaticamente modificato in **Storage Wasabi 1**.

   - Nel campo **Bucket**, selezionare il bucket di Wasabi pertinente.
6. Fare clic su **Aggiungi**.

© Acronis International GmbH, 2003-2024

Se si sta creando o modificando un piano di protezione, la posizione di backup Wasabi viene impostata come posizione nella riga **Dove eseguire il backup**. Una volta eseguito il backup (sia manualmente che in base alla pianificazione), questo viene salvato nella posizione definita.

Se si stanno gestendo le posizioni dello storage di backup, è possibile visualizzare e aggiornare i dettagli della posizione come necessario. La posizione Wasabi è disponibile anche durante la definizione di una posizione di backup per i workload. Per ulteriori informazioni, consultare "Visualizzazione e aggiornamento delle posizioni di backup nel cloud pubblico" (pag. 555).

Visualizzazione e aggiornamento delle posizioni di backup nel cloud pubblico

È possibile visualizzare e aggiornare le posizioni di backup di Microsoft Azure, Amazon S3 e Wasabi definite nel modulo **Archivio di backup** oppure durante la creazione o la modifica di un piano di protezione.

Per informazioni sulla rimozione dell'accesso a un abbonamento Microsoft Azure dalla console di Cyber Protect, consultare "Rimozione dell'accesso a un abbonamento Microsoft Azure" (pag. 562). Per informazioni su come rimuovere l'accesso ad altre connessioni al cloud pubblico, consultare "Gestione dell'accesso ad altri servizi di cloud storage pubblico" (pag. 563).

Nota
Non è possibile aggiornare o eliminare manualmente una posizione di backup nel cloud pubblico dal modulo **Archivio di backup**. I contenuti della posizione di backup vengono aggiornati automaticamente dopo ogni operazione di backup o ripristino.

Per visualizzare le posizioni di backup nel cloud pubblico

1. Nella console di Cyber Protect, passare a **Archivio di backup**.
   Viene visualizzato un elenco di posizioni di backup, con informazioni sulla capacità di storage e sul numero di backup assegnati a ogni posizione.
   Per ulteriori informazioni su come lavorare con le posizioni di backup elencate, consultare "La scheda Archivio di backup" (pag. 536).
2. Selezionare la posizione pertinente.
   Viene elencato ogni backup corrente relativo alla posizione selezionata.
3. (Facoltativo) Fare clic su un backup per visualizzarne ulteriori dettagli.

Per aggiornare una posizione di backup nel cloud pubblico in un piano di protezione

1. Passare al piano di protezione pertinente e selezionare **Modifica**.
2. Fare clic sul collegamento nella riga **Dove eseguire il backup**.
3. Selezionare una posizione esistente dall'elenco delle posizioni di backup, oppure fare clic su **Aggiungi posizione** per aggiungere una nuova posizione.
   Se l'abbonamento Microsoft Azure o la connessione al cloud pubblico in questione sono già registrati nel console di Cyber Protect, selezionarlo dall'elenco visualizzato.

© Acronis International GmbH, 2003-2024

Se si sta aggiungendo un nuovo abbonamento Microsoft Azure, verrà richiesto di autenticare le informazioni dell'account Microsoft (consultare "Aggiunta dell'accesso a un abbonamento Microsoft Azure" (pag. 560)). Per ulteriori informazioni sulle autorizzazioni necessarie per la connessione a Microsoft Azure, consultare l'articolo 72684 della Knowledge Base sulla sicurezza e la verifica della connessione a Microsoft Azure.

Gestione dell'accesso agli account di cloud pubblico

Per abilitare i servizi Acronis Cyber Protection nelle piattaforme di cloud pubblico, è necessario configurare l'accesso agli account di cloud pubblico pertinenti.

Ad esempio, se si lavora con Microsoft Azure è necessario accedere all'abbonamento Microsoft Azure. Dopo aver aggiunto l'abbonamento nella console di Cyber Protect, è possibile selezionarlo durante la configurazione di un backup diretto su Microsoft Azure. Allo stesso modo, quando si lavora con Amazon S3 e Wasabi, sono necessarie le chiavi di accesso pertinenti associate alle policy specifiche relative al backup.

L'accesso ai cloud pubblici è gestito tramite il menu **Infrastruttura** nella console di Cyber Protect.

Importante
La convalida del backup è disabilitata per i backup su cloud storage pubblico, per evitare costi eccessivi per il traffico in uscita. Inoltre, al momento non è possibile creare una nuova associazione della posizione di backup su un cloud pubblico allo stesso tenant del cliente o a uno diverso se la posizione è stata precedentemente rimossa. Per ulteriori informazioni, contattare il supporto tecnico.

Requisiti di accesso necessari per il backup su cloud storage pubblico

Quando si effettua il backup diretto su servizi di cloud storage pubblico, è necessario considerare i requisiti di accesso specifici per ogni piattaforma:

- Microsoft Azure
- Amazon S3
- Wasabi

Esecuzione del backup su Microsoft Azure

Per connettersi a un abbonamento Microsoft Azure sono necessarie diverse autorizzazioni. Per ulteriori informazioni, consulta l'articolo 72684 della Knowledge Base sulla sicurezza e gli audit della connessione Microsoft Azure.

Backup su Amazon S3

Per eseguire il backup su Amazon S3 è necessario considerare diversi requisiti durante la definizione delle posizioni di backup di Amazon S3:

© Acronis International GmbH, 2003-2024

- Classi di storage supportate
- Autorizzazioni delle policy
- Chiavi di accesso
- Impostazioni del bucket

Classi di storage supportate

Attualmente, sono supportate le classi di storage Amazon S3 seguenti:

- S3 Standard
- Standard - Accesso non frequente (S3 Standard-IA)
- Una zona - Accesso non frequente (S3 One Zone-IA)
- S3 Intelligent Tiering

Autorizzazioni delle policy

Quando si esegue il backup su Amazon S3, all'account Amazon dell'utente devono essere applicate le autorizzazioni minime per garantire che Acronis possa eseguire il backup dei workload pertinenti su Amazon S3. Ciò significa che gli utenti interessati devono poter accedere alla console di gestione AWS e che la policy pertinente deve essere applicata ai gruppi di cui sono membri.

Esempi

La seguente policy di esempio mostra il set minimo di autorizzazioni per un'ampia gamma di risorse. L'asterisco * indica tutte le risorse.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource": "*" },
{ "Effect": "Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, {
"Effect": "Allow", "Action": [ "s3:GetBucketLocation", "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:ListBucket" ], "Resource": "*" } ] }
```

La seguente policy di esempio mostra le autorizzazioni minime limitate a uno specifico bucket. `[BUCKETNAME]` deve essere sostituito con il nome del bucket.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource":
"arn:aws:s3:::[BUCKETNAME]" }, { "Effect": "Allow", "Action":
"sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:PutObject", "s3:GetObject", "s3:DeleteObject" ],
```


© Acronis International GmbH, 2003-2024

```
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect": "Allow", "Action": [
"s3:ListBucket" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Chiavi di accesso

Acronis richiede le chiavi di accesso per ogni connessione ad Amazon S3; tali chiavi vengono utilizzate durante la definizione della connessione ad Amazon S3. Per ulteriori informazioni sulla generazione delle chiavi di accesso e degli ID della chiave di accesso, consultare la documentazione di Amazon S3.

Impostazioni del bucket

Quando si utilizzano i bucket di Amazon S3 come posizione di backup, assicurarsi che il bucket sia configurato con le impostazioni predefinite, incluso il blocco di tutto l'accesso pubblico (l'impostazione predefinita è **On**). Per ulteriori informazioni sul funzionamento dei bucket, consultare la documentazione di Amazon S3.

Nota
Al momento, Acronis non supporta il controllo delle versioni del bucket e il blocco degli oggetti in Amazon S3, anche se queste funzioni sono abilitate per il bucket.

Backup su Wasabi

Per eseguire il backup su Wasabi è necessario considerare diversi requisiti durante la definizione delle posizioni di backup:

- Autorizzazioni delle policy
- Chiavi di accesso
- Impostazioni del bucket

Autorizzazioni delle policy

Quando si definisce una posizione di backup in Wasabi, assicurarsi che ai gruppi e agli utenti pertinenti siano applicate le policy corrette in Wasabi.

Esempi

La seguente policy di esempio mostra il set minimo di autorizzazioni con un vasto ambito di risorse. L'asterisco * indica qualsiasi risorsa.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
```


© Acronis International GmbH, 2003-2024

```
"s3:GetBucketLocation", "Resource": "*" }, { "Effect": "Allow", "Action": [
"iam:CreateRole", "iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole"
], "Resource": "*" }, { "Effect": "Allow", "Action": [ "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": "s3:ListBucket", "Resource": "*" } ] }
```

La seguente policy di esempio mostra autorizzazioni limitate con un ambito limitato di risorse. `[BUCKETNAME]` deve essere sostituito con il nome del bucket, `[ACCOUNTID]` con l'ID dell'account Wasabi.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "iam:CreateRole", "iam:AttachRolePolicy",
"sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "arn:aws:iam::
[ACCOUNTID]:*" }, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject" ], "Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect":
"Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Chiavi di accesso

Acronis richiede le chiavi di accesso per ogni connessione a Wasabi; tali chiavi vengono utilizzate durante la definizione della connessione a Wasabi. Per ulteriori informazioni sulla generazione delle chiavi di accesso e degli ID della chiave di accesso, consultare la documentazione di Wasabi.

Impostazioni del bucket

Quando si utilizzano i bucket Wasabi come posizione di backup, assicurarsi che il bucket sia configurato con le impostazioni predefinite. Per ulteriori informazioni sul funzionamento dei bucket, consultare la documentazione di Wasabi.

Nota
Al momento, Acronis non supporta il controllo delle versioni del bucket e il blocco degli oggetti in Wasabi, anche se queste funzioni sono abilitate per il bucket.

Gestione dell'accesso agli abbonamenti Microsoft Azure

Connettendosi agli abbonamenti Microsoft Azure pertinenti nella console di Cyber Protect, è possibile eseguire direttamente il backup dei workload di interesse su Microsoft Azure.

La connessione a un abbonamento può essere configurata quando si crea una posizione di backup tramite i menu **Dispositivi** o **Archivio di backup**, come descritto in "Definizione di una posizione di backup in Microsoft Azure" (pag. 548).

In alternativa, gli abbonamenti Microsoft Azure possono essere configurati nella schermata **Cloud pubblici** (passare a **Infrastruttura > Cloud pubblici**). Da qui è anche possibile gestire gli

© Acronis International GmbH, 2003-2024

abbonamenti e le relative operazioni, incluso il rinnovo dell'accesso all'abbonamento, la visualizzazione delle proprietà e delle attività dell'abbonamento o la rimozione dell'abbonamento.

A seconda del ruolo utente assegnato, sarà possibile gestire gli abbonamenti Microsoft Azure aggiunti da altri utenti dell'organizzazione. Ad esempio, un Amministratore dell'azienda, un Amministratore di unità, un utente con il ruolo di Amministratore Cyber o di Amministratore nel servizio Cyber Protection possono visualizzare e gestire gli abbonamenti Microsoft Azure aggiunti da altri amministratori o da utenti senza ruolo di amministratore. Gli utenti senza ruolo di amministratore possono solo visualizzare e accedere agli abbonamenti Microsoft Azure che hanno aggiunto alla console di Cyber Protect.

Nota
I Partner possono gestire gli abbonamenti Microsoft Azure di clienti al di sotto del proprio livello gerarchico. Tuttavia, quando un Partner seleziona **Tutti i clienti**, il menu **Infrastruttura** nella console di Cyber Protect non è disponibile.

Importante
Per eseguire la connessione a un abbonamento Microsoft Azure, Acronis richiede le autorizzazioni minime per eseguire tale connessione. Per ulteriori informazioni sulle autorizzazioni necessarie, fare riferimento all'articolo 72684 della Knowledge Base sulla sicurezza e la verifica della connessione a Microsoft Azure.

Aggiunta dell'accesso a un abbonamento Microsoft Azure

Aggiungendo un abbonamento Microsoft Azure nella console di Cyber Protect, Acronis può accedere in sicurezza all'abbonamento ed eseguire direttamente il backup dei workload di interesse su Microsoft Azure.

Per aggiungere l'accesso a un abbonamento Microsoft Azure

1. Nella console di Cyber Protect, passare a **Infrastruttura > Cloud pubblici**.
2. Fare clic su **Aggiungi**, quindi nell'elenco di opzioni visualizzate, selezionare **Microsoft Azure**.
3. Nella finestra visualizzata, fare clic su **Accedi**. Il sistema reindirizza l'utente alla pagina di login di Microsoft.

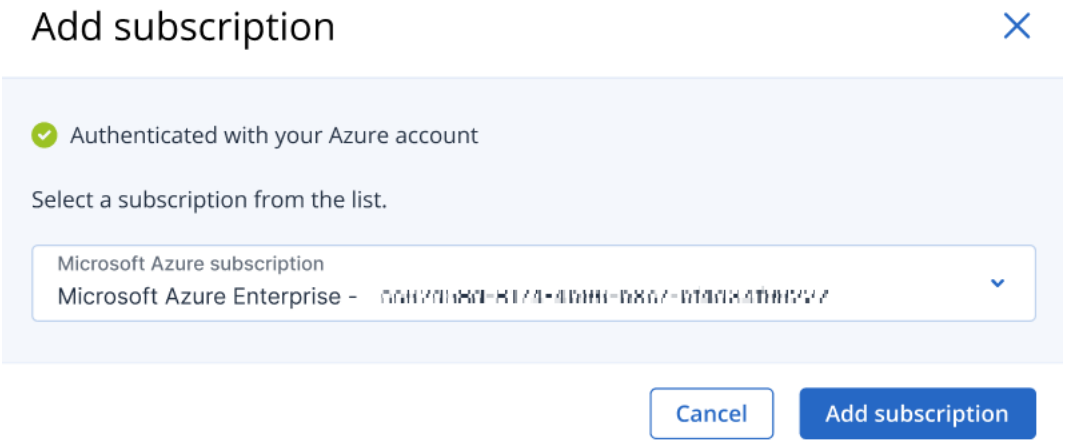
   Nota
   Per completare la connessione all'abbonamento, è necessario che l'utente disponga di uno dei ruoli seguenti in Microsoft Azure AD: Amministratore applicazione cloud, amministratore applicazione o amministratore globale. Inoltre, all'utente deve essere stato assegnato anche il ruolo di Proprietario di ogni abbonamento selezionato.

4. Nella schermata di accesso di Microsoft, immettere le credenziali di accesso e accettare le autorizzazioni richieste. Il processo di connessione si avvia e potrebbe richiedere alcuni minuti.

© Acronis International GmbH, 2003-2024

Per ulteriori informazioni su come accedere in sicurezza a Microsoft Azure e all'abbonamento, fare riferimento all'articolo 72684 della Knowledge Base sulla sicurezza e la verifica della connessione a Microsoft Azure.

5. Una volta completata la connessione, selezionare l'abbonamento pertinente dall'elenco a discesa nella finestra di dialogo visualizzata, quindi fare clic su **Aggiungi abbonamento**.



L'abbonamento viene aggiunto all'elenco dei cloud pubblici.

Per rinnovare il certificato di accesso annuale dell'abbonamento, consultare "Rinnovo dell'accesso a un abbonamento Microsoft Azure" (pag. 561).

Per rimuovere l'accesso all'abbonamento, consultare "Rimozione dell'accesso a un abbonamento Microsoft Azure" (pag. 562).

Nota
Se l'account Microsoft Azure al quale si è connessi include l'accesso a più Microsoft Azure AD, comprese quelle a cui l'utente è invitato come guest, viene selezionata solo la directory utente predefinita. Per utilizzare la directory nella quale si è utenti guest, è necessario creare un nuovo utente in quella specifica Microsoft Azure AD. A questo punto l'utente potrà accedere a questo account e connettersi all'abbonamento pertinente.

Rinnovo dell'accesso a un abbonamento Microsoft Azure

Una volta registrato nella console di Cyber Protect, l'accesso all'abbonamento Microsoft Azure è configurato automaticamente per un anno da Acronis con un certificato gratuito e di accesso esclusivo. Quando il certificato è prossimo alla data di scadenza, il suo rinnovo è semplice e rapido.

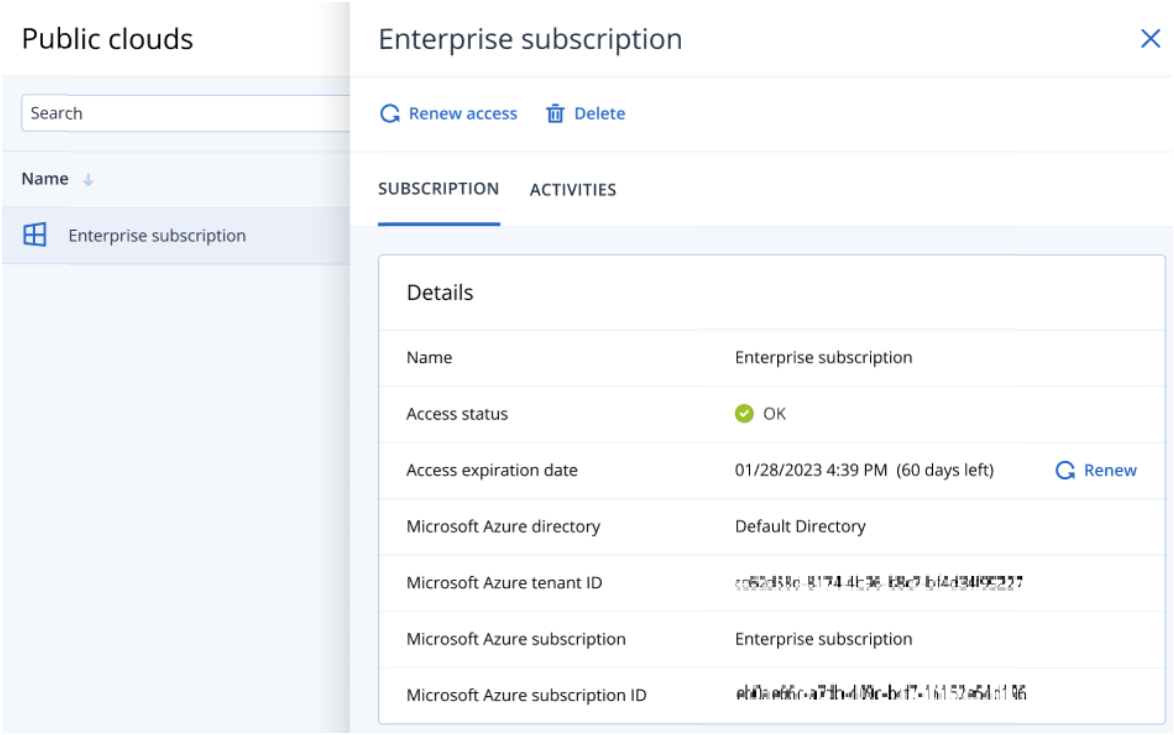
Per rinnovare il certificato di accesso a un abbonamento Microsoft Azure

1. Nella console di Cyber Protect, passare a **Infrastruttura > Cloud pubblici**.
2. Selezionare l'abbonamento pertinente dall'elenco visualizzato.

Nota
La colonna **Stato dell'accesso** indica lo stato corrente del certificato di accesso per ogni abbonamento e mostra uno dei due stati seguenti: **OK** o **Scaduto**.

© Acronis International GmbH, 2003-2024

3. Nel pannello a destra fare clic su **Rinnova accesso**.
   In alternativa, fare clic sulla scheda **Abbonamento**, quindi su **Rinnova** nel campo **Data di scadenza dell'accesso**.



4. Nella schermata di accesso di Microsoft, immettere le credenziali di accesso e accettare le autorizzazioni richieste. Il processo di connessione si avvia e potrebbe richiedere alcuni minuti.
   Una volta completata correttamente l'autenticazione, l'accesso viene rinnovato in automatico per un anno.
   Per ulteriori informazioni sulle autorizzazioni necessarie, fare riferimento all'articolo 72684 della Knowledge Base sulla sicurezza e la verifica della connessione a Microsoft Azure.

Rimozione dell'accesso a un abbonamento Microsoft Azure

Si consiglia di rimuovere l'accesso all'abbonamento Microsoft Azure se non si esegue più il backup di workload su Microsoft Azure.

Per rimuovere l'accesso a un abbonamento Microsoft Azure

Importante
Non è possibile rimuovere un abbonamento se viene utilizzato per eseguire il backup su Microsoft Azure.

1. Nella console di Cyber Protect, passare a **Infrastruttura > Cloud pubblici**.
2. Selezionare l'abbonamento pertinente dall'elenco visualizzato.
3. Nel pannello a destra fare clic su **Elimina**.

© Acronis International GmbH, 2003-2024

Nota
Possono essere rimossi soltanto gli abbonamenti aggiunti dall'utente. È possibile rimuovere un abbonamento anche se si è un Amministratore dell'azienda o un Amministratore di unità, o se all'utente è stato assegnato il ruolo di Amministratore Cyber o di Amministratore nel servizio Cyber Protection.

4. Nel messaggio di conferma visualizzato, fare clic su **Rimuovi**.

Gestione dell'accesso ad altri servizi di cloud storage pubblico

Nota
Questa sezione si riferisce alla gestione dell'accesso per tutti i servizi di cloud storage pubblico diversi da Microsoft Azure, descritto in "Gestione dell'accesso agli abbonamenti Microsoft Azure" (pag. 559).

Il collegamento al relativo account di cloud pubblico nella console di Cyber Protect, consente di eseguire direttamente il backup dei workload sul cloud storage pubblico pertinente.

È possibile configurare connessioni ad account di cloud storage pubblico durante la creazione di una posizione di backup tramite il menu **Dispositivi** o **Archivio di backup**. In alternativa, è possibile configurare le connessioni al cloud pubblico nella schermata **Cloud pubblici** (passare a **Infrastruttura > Cloud pubblici**). Da qui è anche possibile gestire le operazioni sulla connessione, inclusi il rinnovo dell'accesso alla connessione, la visualizzazione delle proprietà e delle attività della connessione o la rimozione della connessione.

A seconda del ruolo utente assegnato, sarà possibile gestire le connessioni al cloud pubblico aggiunte da altri utenti dell'organizzazione. Ad esempio, un Amministratore dell'azienda, un Amministratore di unità, un utente con il ruolo di Amministratore Cyber o di Amministratore nel servizio Cyber Protection possono visualizzare e gestire le connessioni al cloud pubblico aggiunte da altri amministratori o da utenti senza ruolo di amministratore. Gli utenti senza ruolo di amministratore possono solo visualizzare e accedere alle connessioni di cloud pubblico che hanno aggiunto alla console di Cyber Protect.

Nota
I Partner possono gestire le connessioni al cloud pubblico dei clienti al di sotto del loro livello nella gerarchia. Tuttavia, quando un Partner seleziona **Tutti i clienti**, il menu **Infrastruttura** nella console di Cyber Protect non è disponibile.

Importante
Quando ci si connette a una connessione di cloud pubblico, Acronis richiede un certo numero di permessi. Per ulteriori informazioni, consultare "Requisiti di accesso necessari per il backup su cloud storage pubblico" (pag. 556).

© Acronis International GmbH, 2003-2024

Aggiunta dell'accesso a una connessione al cloud pubblico

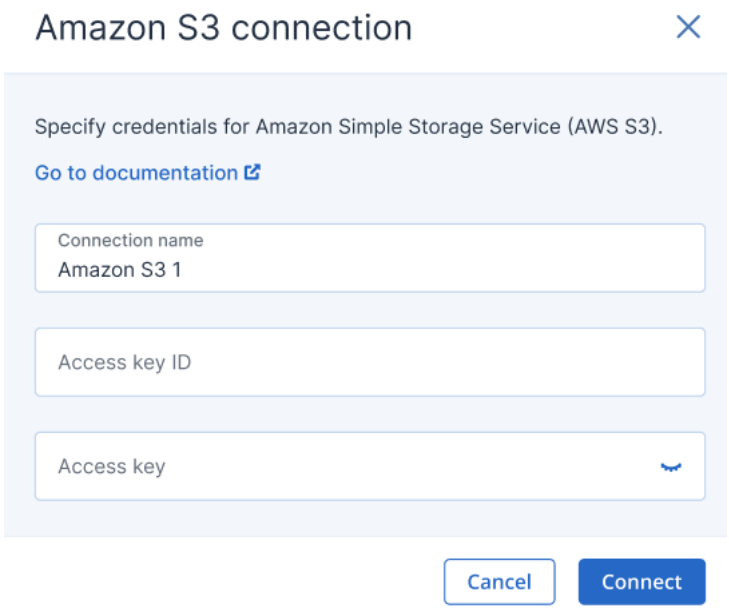
Dopo aver aggiunto una connessione al cloud pubblico (come Amazon S3 o Wasabi) nella console Cyber Protect, Acronis può accedere in modo sicuro alle risorse cloud ed eseguire direttamente il backup dei workload sullo storage cloud pubblico pertinente.

Per aggiungere l'accesso a una connessione al cloud pubblico

1. Nella console di Cyber Protect, passare a **Infrastruttura > Cloud pubblici**.
2. Fare clic su **Aggiungi**, quindi selezionare una delle seguenti opzioni:
   - **Amazon S3**

     Nella finestra di dialogo visualizzata, procedere come segue.
     - **Nome connessione**: il nome della connessione Amazon S3.
     - **ID chiave di accesso**: l'ID chiave di accesso dell'utente per il servizio Amazon S3.
     - **Chiave di accesso**: la chiave di accesso dell'utente per il servizio Amazon S3.

       La chiave di accesso e l'ID chiave di accesso consentono ad Acronis di accedere alle classi di storage e ai bucket della connessione pertinente. Per ulteriori informazioni sulle chiavi di accesso e sulle autorizzazioni richieste da Acronis, consultare "Requisiti di accesso necessari per il backup su cloud storage pubblico" (pag. 556).



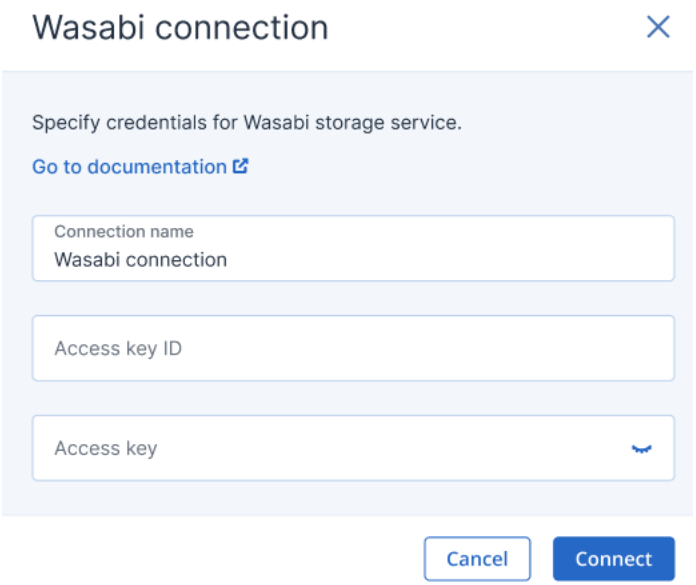
   - **Wasabi**

     Nella finestra di dialogo visualizzata, procedere come segue.
     - **Nome connessione**: il nome della connessione Wasabi.
     - **ID chiave di accesso**: l'ID chiave di accesso dell'utente per il servizio Wasabi.
     - **Chiave di accesso**: la chiave di accesso dell'utente per il servizio Wasabi.

       La chiave di accesso e l'ID chiave di accesso consentono ad Acronis di accedere alle classi di storage e ai bucket della connessione pertinente. Per ulteriori informazioni sulle chiavi di

© Acronis International GmbH, 2003-2024

accesso e sulle autorizzazioni richieste da Acronis, consultare "Requisiti di accesso necessari per il backup su cloud storage pubblico" (pag. 556).



3. Fare clic su **Connettere**.
   La procedura di connessione inizia; potrebbe richiedere diversi minuti. Una volta terminata, la connessione viene aggiunta all'elenco dei cloud pubblici.
   Per rinnovare il certificato di accesso annuale per la connessione, consultare "Rinnovo dell'accesso a una connessione al cloud pubblico" (pag. 565).
   Per rimuovere l'accesso alla connessione, consultare "Rimozione dell'accesso a una connessione al cloud pubblico" (pag. 566).

Rinnovo dell'accesso a una connessione al cloud pubblico

Una volta registrata una connessione al cloud pubblico nella console di Cyber Protect, Acronis assegna automaticamente un certificato di accesso gratuito e univoco che consente l'accesso alla connessione al cloud pubblico. Il certificato è valido per un anno. Quando il certificato è prossimo alla data di scadenza, sarà possibile rinnovarlo.

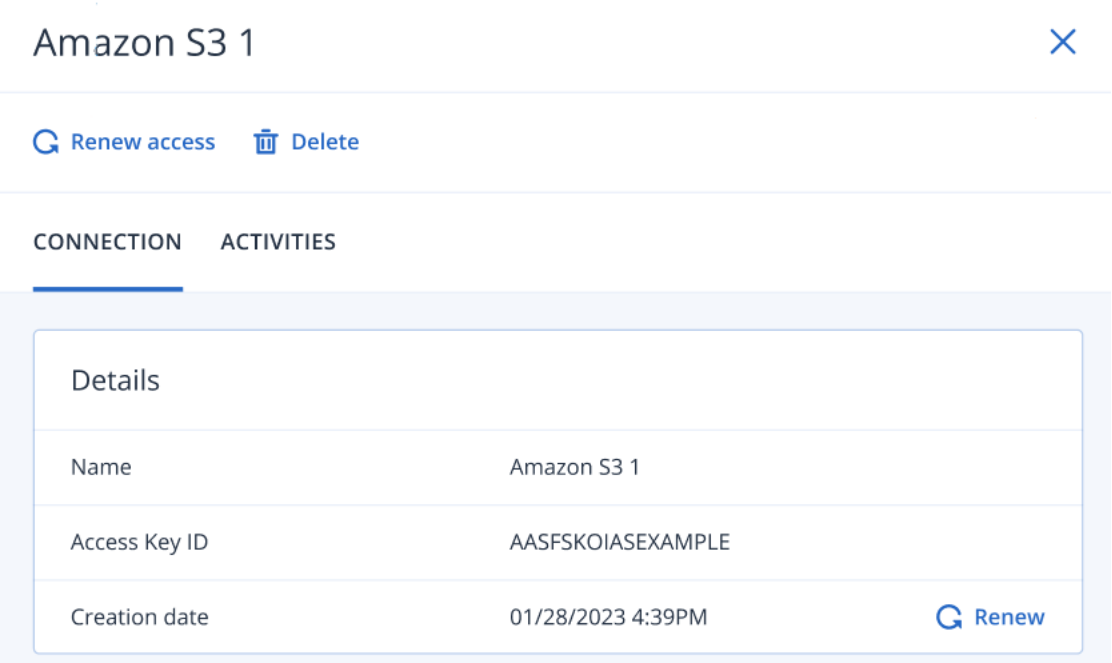
Per rinnovare il certificato di accesso per la connessione al cloud pubblico

1. Nella console di Cyber Protect, passare a **Infrastruttura > Cloud pubblici**.
2. Selezionare la connessione pertinente dall'elenco.

   Nota
   La colonna **Stato dell'accesso** indica lo stato corrente del certificato di accesso per ogni connessione e mostra uno dei due stati seguenti: **OK** o **Scaduto**.

3. Nel pannello a destra fare clic su **Rinnova accesso**.
   In alternativa, fare clic sulla scheda **Connessione**, quindi su **Rinnova** nella riga **Data di creazione**.

© Acronis International GmbH, 2003-2024



Una volta completata correttamente l'autenticazione, l'accesso viene rinnovato in automatico per un anno.

Rimozione dell'accesso a una connessione al cloud pubblico

È necessario rimuovere l'accesso alle connessioni al cloud pubblico se non si esegue il backup dei workload sui cloud pubblici.

Per rimuovere l'accesso a una connessione al cloud pubblico

Importante
Non è possibile rimuovere una connessione se è utilizzata per i backup in un cloud pubblico.

1. Nella console di Cyber Protect, passare a **Infrastruttura > Cloud pubblici**.
2. Selezionare la connessione dall'elenco.
3. Nel pannello a destra fare clic su **Elimina**.

   Nota
   Possono essere rimosse soltanto le connessioni aggiunte dall'utente. È possibile rimuovere una connessione anche se si è un Amministratore dell'azienda o un Amministratore di unità, o se è stato assegnato il ruolo di Amministratore Cyber o di Amministratore nel servizio Cyber Protection.

4. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

© Acronis International GmbH, 2003-2024

Protezione delle applicazioni Microsoft

Protezione di Microsoft SQL Server e Microsoft Exchange Server

Nota
Il backup di Microsoft SQL è supportato solo per i database eseguiti su file system NTFS, REFS e FAT32. ExFat non è supportato.

Esistono due metodi che consentono di proteggere le applicazioni Microsoft:

- **Backup di database**
  Si tratta del backup a livello di file dei database e dei metadati ad essi associati. I database possono essere ripristinati in un'applicazione in uso o come file.
- **Backup compatibile con l'applicazione**
  Si tratta di un backup a livello di disco che raccoglie anche i metadati delle applicazioni. Questi metadati consentono l'esplorazione e il ripristino dei dati delle applicazioni senza eseguire il ripristino dell'intero disco o volume. È possibile ripristinare il disco o il volume anche interamente. Ciò significa che è possibile utilizzare un'unica soluzione e un unico piano di protezione sia a scopo di disaster recovery che di protezione dati.

Per Microsoft Exchange Server, è possibile selezionare **Backup caselle di posta**. Si tratta di un backup di singole caselle di posta tramite il protocollo Servizi Web Exchange. È possibile ripristinare le caselle di posta o gli elementi di una casella di posta in un'istanza di Exchange Server attiva o in Microsoft 365. Il backup delle caselle di posta è supportato per Microsoft Exchange Server 2010 Service Pack 1 (SP1) e versioni successive.

Protezione di Microsoft SharePoint

Una farm di Microsoft SharePoint è formata da server front-end che eseguono i servizi SharePoint, server di database che eseguono Microsoft SQL Server e, in via facoltativa, server di applicazioni che scaricano alcuni servizi di SharePoint dai server front-end. Alcuni server front-end e server delle applicazioni possono essere identici tra loro.

Per proteggere un'intera farm di SharePoint:

- Eseguire il backup di tutti i server di database con backup compatibili con le applicazioni.
- Eseguire il backup di tutti i server front-end univoci e i server delle applicazioni con il backup consueto a livello di disco.

I backup di tutti i server dovrebbero essere eseguiti nell'ambito della stessa pianificazione.

Per proteggere solo il contenuto, è possibile eseguire separatamente il backup dei database dei contenuti.

© Acronis International GmbH, 2003-2024

Protezione di un controller di dominio

Un sistema che esegue i Servizi di dominio di Active Directory può essere protetto tramite un backup application-aware. Se un dominio comprende più di un controller di dominio, e uno di questi viene ripristinato, viene eseguito un ripristino non autorevole e, in seguito al ripristino, non si verifica un rollback USN.

Ripristino delle applicazioni

La seguente tabella riassume le opzioni disponibili per il ripristino delle applicazioni.

	Da un backup di database	**Da un backup compatibile con l'applicazione**	**Da un backup di disco**
Microsoft SQL Server	Database in un'istanza di SQL Server attiva Database come file	Intera macchina Database in un'istanza di SQL Server attiva Database come file	Intera macchina
Microsoft Exchange Server	Database in un'istanza di Exchange attiva Database come file Ripristino granulare a un'istanza di Exchange attiva o Microsoft 365*	Intera macchina Database in un'istanza di Exchange attiva Database come file Ripristino granulare a un'istanza di Exchange attiva o Microsoft 365*	Intera macchina
Server di database di Microsoft SharePoint	Database in un'istanza di SQL Server attiva Database come file Ripristino granulare tramite SharePoint Explorer	Intera macchina Database in un'istanza di SQL Server attiva Database come file Ripristino granulare tramite SharePoint Explorer	Intera macchina
Server Web front-end di Microsoft SharePoint	-	-	Intera macchina
Servizi di dominio Active Directory	-	Intera macchina	-

© Acronis International GmbH, 2003-2024

* Il ripristino granulare è disponibile anche dal backup di una casella di posta. Il ripristino di elementi dati di Exchange in Microsoft 365 e viceversa è supportato a condizione che l'Agente per Microsoft 365 sia installato in locale.

Prerequisiti

Prima di configurare il backup dell'applicazione, accertarsi che siano soddisfatti i requisiti indicati qui di seguito.

Per controllare lo stato di VSS writer, utilizzare il comando `vssadmin list writers`.

Requisiti comuni

Per Microsoft SQL Server, accertarsi che si verifichino le seguenti condizioni:

- È stata avviata almeno un'istanza di Microsoft SQL Server.
- Il writer di SQL per VSS è attivato.

Per Microsoft Exchange Server, accertarsi che si verifichino le seguenti condizioni:

- Il servizio Archivio informazioni di Microsoft Exchange è avviato.
- Windows PowerShell è installato. Per Exchange 2010 o versioni successive, la versione di Windows PowerShell è almeno 2.0.
- Microsoft .NET Framework è installato.
  Per Exchange 2007, la versione di Microsoft .NET Framework è almeno 2.0.
  Per Exchange 2010 o versioni successive, la versione di Microsoft .NET Framework è almeno 3.5.
- Che il writer di Exchange per VSS sia attivato.

Nota
Il funzionamento dell'Agente per Exchange richiede un ampio archivio temporaneo. Per impostazione predefinita, i file temporanei si trovano in `%ProgramData%\Acronis\Temp`. Predisporre nel volume in cui si trova la cartella `%ProgramData%` una quantità di spazio disponibile pari almeno al 15% di quella di un database di Exchange. In alternativa, è possibile modificare la posizione dei file temporanei prima di creare i backup di Exchange, come descritto in Changing Temp Files and Folder Location (40040) (in inglese).

Su un controller di dominio, accertarsi che si verifichino le seguenti condizioni:

- Il writer di Active Directory per VSS è attivato.

Quando si crea un piano di protezione, accertarsi che si verifichino le seguenti condizioni:

- Per le macchine fisiche e i sistemi in cui è installato l'agente, l'opzione di backup Servizio Copia Shadow del volume è abilitata.
- Per le macchine virtuali, l'opzione di backup Servizio Copia Shadow del volume per macchine virtuali è abilitata.

© Acronis International GmbH, 2003-2024

Requisiti aggiuntivi per i backup compatibili con l'applicazione

Quando si crea un piano di protezione, accertarsi che per il backup sia selezionata l'opzione **Intera macchina**. L'opzione di backup **Settore per settore** deve essere disattivata nel piano di protezione; in caso contrario non sarà possibile eseguire il ripristino dei dati dell'applicazione da tali backup. Se il piano viene eseguito con la modalità **Settore per settore** a causa del passaggio automatico a tale modalità, il ripristino dei dati dell'applicazione non sarà comunque possibile.

Requisiti per le macchine virtuali ESXi

Se l'applicazione viene eseguita su macchine virtuali il cui backup è eseguito dall'Agente per VMware, accertarsi che si verifichino le seguenti condizioni:

- La macchina virtuale di cui viene eseguito il backup risponde ai requisiti relativi al backup e al ripristino compatibili con l'applicazione riportati nell'articolo sulle implementazioni di Windows Backup nella documentazione di VMware: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html.
- Gli strumenti VMware sono installati e aggiornati nel sistema.
- La funzionalità Controllo dell'account utente (UAC) è disattivata nel sistema. Affinché UAC non risulti disattivato, è necessario fornire le credenziali dell'amministratore di dominio incorporato (DOMAIN\Administrator) durante l'attivazione del backup dell'applicazione.
  Affinché UAC non risulti disattivato, è necessario fornire le credenziali dell'amministratore di dominio incorporato (DOMAIN\Administrator) durante l'attivazione del backup dell'applicazione.

  Nota
  Utilizzare l'account di amministratore di dominio incorporato che è stato configurato durante la creazione del dominio. Gli account creati successivamente non sono supportati.

Requisiti per le macchine virtuali Hyper-V

Se l'applicazione viene eseguita su macchine virtuali il cui backup è eseguito dall'Agente per Hyper-V, accertarsi che si verifichino le seguenti condizioni:

- Il sistema operativo guest è Windows Server 2008 o versioni successive.
- Per Hyper-V 2008 R2: il sistema operativo guest è Windows Server 2008/2008 R2/2012.
- La macchina virtuale non dispone di dischi dinamici.
- Esiste una connessione di rete tra l'host Hyper-V e il sistema operativo guest. Tale connessione è necessaria per eseguire le query WMI remote all'interno della macchina virtuale.
- La funzionalità Controllo dell'account utente (UAC) è disattivata nel sistema. Affinché UAC non risulti disattivato, è necessario fornire le credenziali dell'amministratore di dominio incorporato (DOMAIN\Administrator) durante l'attivazione del backup dell'applicazione.
  Affinché UAC non risulti disattivato, è necessario fornire le credenziali dell'amministratore di dominio incorporato (DOMAIN\Administrator) durante l'attivazione del backup dell'applicazione.

© Acronis International GmbH, 2003-2024

Nota
Utilizzare l'account di amministratore di dominio incorporato che è stato configurato durante la creazione del dominio. Gli account creati successivamente non sono supportati.

- La configurazione della macchina virtuale soddisfa i seguenti criteri:
  - I servizi di integrazione Hyper-V sono installati e aggiornati. L'aggiornamento critico è https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - Nelle impostazioni della macchina virtuale è abilitata l'opzione **Gestione** > **Servizi di integrazione** > **Backup (checkpoint del volume)**.
  - Per Hyper-V 2012 e versioni successive: nella macchina virtuale non sono presenti checkpoint.
  - Per Hyper-V 2012 R2 e versioni successive: la macchina virtuale è dotata di un controller SCSI (controllare in **Impostazioni** > **Hardware**).

Backup di database

Prima di eseguire il backup dei database, accertarsi che siano soddisfatti i requisiti elencati in "Prerequisiti".

Selezionare i database come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Selezione di database SQL

Un backup di un database SQL contiene i file di database (.mdf, .ndf), file di registro (.ldf) e altri file associati. Il backup dei file viene eseguito con l'aiuto del servizio SQL Writer. È necessario che il sevizio sia in esecuzione nel momento in cui VSS (Volume Shadow Copy Service) richiede un backup o un ripristino.

I registri transazioni di SQL vengono troncati dopo ciascun backup eseguito correttamente. Il troncamento del log SQL può essere disabilitato nelle opzioni del piano di protezione.

Per selezionare i database di SQL

1. Fare clic su **Dispositivi** > **Microsoft SQL**.
   Il software mostra la struttura ad albero dei gruppi di disponibilità Always On (AAG) di SQL Server, i sistemi in cui è in esecuzione Microsoft SQL Server, le istanze di SQL Server e i database.
2. Passare ai dati di cui si vuole eseguire il backup.
   Espandere i nodi della struttura ad albero o fare doppio clic sulle voci dell'elenco a destra dell'albero stesso.
3. Selezionare i dati di cui eseguire il backup. È possibile selezionare AAG, sistemi in cui è in esecuzione SQL Server, istanze di SQL Server o database singoli.
   - Se si seleziona un AAG, vengono sottoposti a backup anche tutti i database compresi nell'AAG selezionato. Per ulteriori informazioni sull'esecuzione del backup degli AAG o dei singoli database AAG, fare riferimento a "Protezione dei gruppi di disponibilità Always On (AAG)".

© Acronis International GmbH, 2003-2024

- Se si seleziona un sistema in cui è in esecuzione SQL Server, vengono sottoposti a backup anche tutti i database associati a tutte le istanze di SQL Server in esecuzione sul sistema selezionato.
- Se si seleziona un'istanza di SQL Server, vengono sottoposti a backup anche tutti i database collegati all'istanza selezionata.
- Se si selezionano i database correttamente, verrà eseguito solo il backup dei database selezionati.

4. Fare clic su **Proteggi**. Se richiesto, fornire le credenziali di accesso per i dati di SQL Server.

   Se si utilizza l'autenticazione Windows, l'account deve essere membro del gruppo **Operatori di Backup** o **Administrators** sul sistema e membro del ruolo **sysadmin** su ciascuna delle istanze di cui verrà eseguito il backup.

   Se si utilizza l'autenticazione SQL Server, l'account deve essere membro del ruolo **sysadmin** su ciascuna delle istanze di cui verrà eseguito il backup.

Selezione di dati di Exchange Server

La seguente tabella presenta un riepilogo dei dati di Microsoft Exchange Server che è possibile selezionare per il backup e i diritti utente minimi necessari per il backup dei dati.

Versione di Exchange	Elementi di dati	Diritti utente
2007	Gruppi di archiviazione	Appartenenza al gruppo di ruoli **Amministratori organizzazione di Exchange**
2010/2013/2016/2019	Database, Gruppi di Disponibilità Database (DAG)	Appartenenza al gruppo di ruoli **Gestione server**.

Un backup completo contiene tutti i dati Exchange Server selezionati.

Un backup incrementale contiene i blocchi di file di database modificati, i file del punto di arresto e un piccolo numero di file di log che sono più recenti rispetto ai punti di arresto di database corrispondenti. Poiché i cambiamenti ai file di database sono inclusi nel backup, non è necessario eseguire il backup di tutti i record del registro delle transazioni in seguito al backup precedente. Solo il registro più recente del punto di arresto dovrà essere eseguito di nuovo dopo un ripristino. Ciò garantisce un recupero rapido e assicura l'esito positivo del backup del database, anche se la registrazione circolare è attivata.

I file di registro transazioni vengono troncati dopo ciascun backup eseguito correttamente.

Per selezionare dati di Exchange Server

1. Fare clic su **Dispositivi** > **Microsoft Exchange**.

   Il software mostra la struttura ad albero dei gruppi di disponibilità database (DAG) di Exchange Server, dei sistemi in cui è in esecuzione Microsoft Exchange Server e dei database di Exchange Server. Se l'Agente per Exchange è stato configurato come descritto in "Backup caselle di posta" (pag. 579), la struttura visualizza anche le caselle di posta.
2. Passare ai dati di cui si vuole eseguire il backup.

 © Acronis International GmbH, 2003-2024

Espandere i nodi della struttura ad albero o fare doppio clic sulle voci dell'elenco a destra dell'albero stesso.

3. Selezionare i dati di cui eseguire il backup.
   - Se si seleziona un DAG, viene eseguito il backup di una copia di ogni database incluso nel cluster. Per ulteriori informazioni sul backup dei DAG, fare riferimento a "Protezione dei gruppi di disponibilità del database (DAG)" (pag. 575).
   - Se si seleziona un sistema in cui è in esecuzione Microsoft Exchange Server, vengono sottoposti a backup anche tutti i database montati nell'istanza di Exchange Server in esecuzione sul sistema selezionato.
   - Se si selezionano i database correttamente, verrà eseguito solo il backup dei database selezionati.
   - Se l'Agente per Exchange è stato configurato come descritto in "Backup caselle di posta" (pag. 579), è possibile selezionare le caselle di posta di cui eseguire il backup.

   Se la selezione include più database, questi vengono elaborati due alla volta. Quando si conclude il backup del primo gruppo, ha inizio il backup del gruppo successivo.
4. Se richiesto, fornire le credenziali di accesso per i dati.
5. Fare clic su **Proteggi**.

Protezione dei gruppi di disponibilità Always On (AAG)

Nota
Questa funzionalità è disponibile con il pacchetto Advanced Backup.

Panoramica delle soluzioni a disponibilità elevata di SQL Server

La funzionalità Windows Server Failover Clustering (WSFC) consente di configurare un SQL Server a disponibilità elevata attraverso la ridondanza a livello di istanza (istanza del cluster di failover, FCI) o a livello di database (gruppo di disponibilità Always On, AAG). È inoltre possibile combinare entrambi i metodi.

In un'istanza del cluster di failover, i database SQL sono posizionati in un archivio condiviso. Questa archiviazione è accessibile solo dal nodo del cluster attivo. Se il nodo attivo si guasta, si verifica un failover e un nodo diverso diventa attivo.

In un gruppo di disponibilità, ogni replica di database si trova su un nodo diverso. Se la replica principale diventa non disponibile, una replica secondaria che si trova su un nodo diverso viene assegnata al ruolo principale.

Quindi, i cluster stessi operano già come soluzione di ripristino d'emergenza. Tuttavia, in alcuni casi i cluster potrebbero non offrire la protezione dati: ad esempio se il database logico è danneggiato o quando l'intero cluster cessa di funzionare. Anche le soluzioni cluster non proteggono da modifiche dannose del contenuto, poiché esse vengono replicate immediatamente su tutti i nodi del cluster.

© Acronis International GmbH, 2003-2024

Configurazioni cluster supportate

Questo software di backup supporta *solo* il gruppo di disponibilità Always On (AAG) per SQL Server 2012 o versioni successive. Le altre configurazioni cluster, ad esempio le istanze del cluster di failover, il mirroring del database o il log shipping *non* sono supportate.

Quanti agenti sono necessari per il backup e ripristino dei dati del cluster?

Per il corretto backup e ripristino dei dati di un cluster, l'Agente per SQL deve essere installato in ogni nodo del cluster WSFC.

Backup dei database compresi in un AAG

1. Installare l'Agente per SQL su ogni nodo del cluster WSFC.
2. Selezionare l'AAG da sottoporre a backup come descritto in "Selezione di database SQL".

   È necessario selezionare l'AAG per eseguire il backup di tutti i database dell'AAG. Per eseguire il backup di un insieme di database, definire questo insieme di database in tutti i nodi dell'AAG.

   Attenzione!
   L'insieme di database deve essere esattamente lo stesso, in tutti i nodi. Se anche un solo insieme è diverso, o non è definito su tutti i nodi, il backup del cluster non funzionerà correttamente.
3. Configurare l'opzione di backup Modalità backup cluster.

Ripristino dei database compresi in un AAG

1. Selezionare i database da ripristinare, quindi il punto di ripristino da cui ripristinare i database.

   Quando si seleziona un database in cluster in **Dispositivi** > **Microsoft SQL** > **Database** e si fa clic su **Ripristina**, il software mostra solo i punti di ripristino corrispondenti agli orari in cui è avvenuto il backup della copia selezionata del database.

   Il modo più semplice per visualizzare tutti i punti di ripristino di un database in cluster è selezionare il backup dell'intero AAG nella scheda Archivio di backup. I nomi dei backup dell'AAG si basano sul modello seguente: `<nome AAG> - <nome piano di protezione>` e presentano un'icona speciale.
2. Per configurare il ripristino, attenersi alla procedura descritta in "Ripristino dei database SQL", a partire dal passaggio 5.

   Il software definisce automaticamente un nodo del cluster in cui ripristinare i dati. Il nome del nodo viene visualizzato nel campo **Ripristina in**. È possibile cambiare manualmente il nodo di destinazione.

© Acronis International GmbH, 2003-2024

Importante
Non è possibile sovrascrivere un database compreso in un gruppo di disponibilità Always On durante un ripristino. Microsoft SQL Server impedisce questa operazione. È necessario escludere il database di destinazione dall'AAG prima del ripristino. In alternativa, ripristinare il database come un nuovo database non AAG. Al termine del ripristino, è possibile recuperare la configurazione originale dell'AAG.

Protezione dei gruppi di disponibilità del database (DAG)

Nota
Questa funzionalità è disponibile con il pacchetto Advanced Backup.

Panoramica dei cluster di Exchange Server

L'idea principale dei cluster di Exchange è fornire elevata disponibilità dei database con failover rapido e nessuna perdita dei dati. Di solito, viene raggiunto con una o più copie dei database o gruppi di archiviazione sui membri del cluster (nodi del cluster). Se il nodo del cluster che ospita la copia attiva del database o la copia attiva del database stessa subisce un guasto, l'altro nodo che ospita la copia passiva effettua automaticamente le operazioni del nodo guasto e fornisce accesso ai servizi di Exchange con un tempo di inattività minimo. Quindi, i cluster stessi operano già come soluzione di ripristino d'emergenza.

Tuttavia, in alcuni casi le soluzioni con cluster di failover potrebbero non offrire la protezione dati: ad esempio se il database logico è danneggiato o se un determinato database in un cluster non dispone di una copia (replica) o, ancora, quando l'intero cluster cessa di funzionare. Anche le soluzioni cluster non proteggono da modifiche dannose del contenuto, poiché esse vengono replicate immediatamente su tutti i nodi del cluster.

Backup compatibile con i cluster

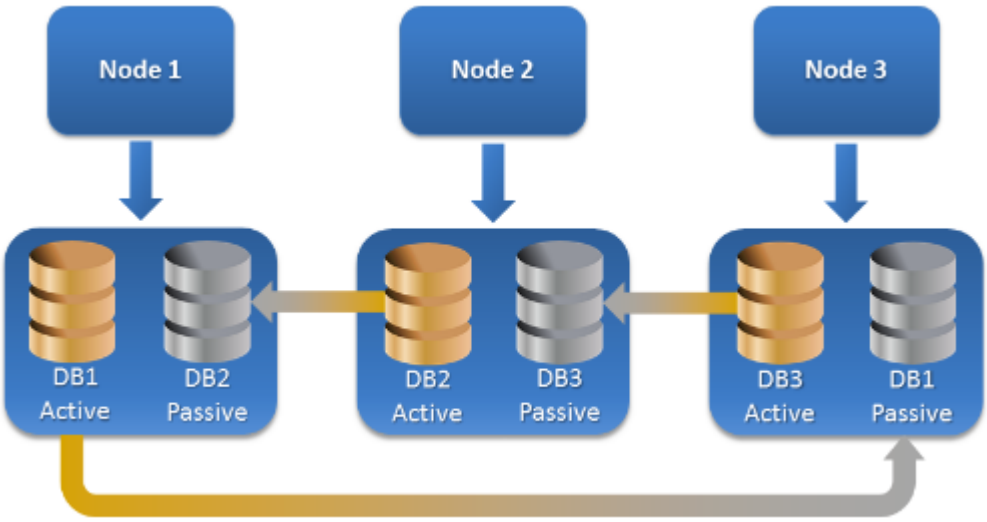
Il backup compatibile con i cluster consente di eseguire il backup di una sola copia dei dati nel cluster. Se i dati cambiano posizione nel cluster (a causa di uno switchover o di un failover), il software terrà traccia di tutti i riposizionamenti di questi dati e ne eseguirà il backup in modo sicuro.

Configurazioni cluster supportate

Il backup compatibile con i cluster è supportato *solo* per il Gruppo di Disponibilità Database (DAG) in Exchange Server 2010 o versioni successivi. Le altre configurazioni cluster, ad esempio il cluster a copia singola (SCC) e la replica continua cluster (CCR) per Exchange 2007 *non* sono supportate.

DAG è un gruppo che comprende fino a 16 server di cassette postali di Exchange. Ogni nodo è in grado di ospitare una copia del database delle caselle postali di un altro nodo. Ogni nodo può ospitare copie attive e passive dei database. È possibile creare fino a 16 copie di ciascun database.

© Acronis International GmbH, 2003-2024



Quanti agenti sono necessari per il backup e ripristino dei dati compatibile con i cluster?

Per un backup e ripristino corretto dei database di un cluster, è necessario che l'Agente per Exchange sia installato su ciascun nodo del cluster di Exchange.

Nota
Dopo aver installato l'agente su uno dei nodi, la console di Cyber Protect visualizza il DAG e i relativi nodi in **Dispositivi** > **Microsoft Exchange** > **Database**. Per installare l'Agente per Exchange nel resto dei nodi, selezionare il DAG, fare clic su **Dettagli**, quindi selezionare **Installa agente** accanto a ogni nodo.

Backup dei dati dei cluster di Exchange

1. Durante la creazione di un piano di protezione, selezionare il DAG come descritto in "Selezione di dati di Exchange Server" (pag. 572).
2. Configurare le opzioni di backup "Modalità backup cluster" (pag. 464).
3. Specificare le altre impostazioni del piano di protezione come necessario.

Importante
Per il backup compatibile con il cluster, verificare di selezionare il DAG stesso. Se si selezionano singoli nodi o database all'interno del DAG, viene eseguito esclusivamente il backup degli elementi selezionati e l'opzione **Modalità backup cluster** viene ignorata.

Ripristino dei dati del cluster di Exchange

1. Selezionare il punto di ripristino dei database da ripristinare. Non è possibile selezionare un intero cluster per il ripristino.

© Acronis International GmbH, 2003-2024

Quando si seleziona un database in cluster in **Dispositivi** > **Microsoft Exchange** > **Database** > `<nome cluster>` > `<nome nodo>` e si fa clic su **Ripristina**, il software mostra solo i punti di ripristino corrispondenti agli orari in cui è avvenuto il backup della copia selezionata del database.

Il modo più semplice per visualizzare tutti i punti di ripristino di un database in cluster è selezionarne il backup nella scheda Archivio di backup.

2. Attenersi alla procedura descritta in "Ripristino dei database di Exchange" (pag. 590), a partire dal passaggio 5.

   Il software definisce automaticamente un nodo del cluster in cui ripristinare i dati. Il nome del nodo viene visualizzato nel campo **Ripristina in**. È possibile cambiare manualmente il nodo di destinazione.

Backup compatibile con l'applicazione

Il backup del disco compatibile con l'applicazione è disponibile per le macchine fisiche, le macchine virtuali ESXi e le macchine virtuali Hyper-V.

Quando si esegue il backup di una macchina virtuale che esegue Microsoft SQL Server, Microsoft Exchange Server o i Servizi di dominio di Active Directory, abilitare **Backup applicazione** come ulteriore protezione dei dati di tali applicazioni.

Perché utilizzare il backup compatibile con l'applicazione?

Utilizzando il backup compatibile con l'applicazione, si ha la certezza che:

- Il backup delle applicazioni viene eseguito in uno stato in uno stato di coerenza e sarà pertanto disponibile immediatamente dopo il ripristino del sistema.
- È possibile ripristinare i database SQL ed Exchange, le caselle di posta e i relativi elementi senza dover ripristinare l'intero sistema.
- I registri transazioni di SQL vengono troncati dopo ciascun backup eseguito correttamente. Il troncamento del log SQL può essere disabilitato nelle opzioni del piano di protezione. I file di registro transazioni di Exchange vengono troncati soltanto sulle macchine virtuali. È possibile abilitare l'opzione backup completo VSS se si desidera troncare il file di registro transazioni di Exchange su una macchina fisica.
- Se un dominio comprende più di un controller di dominio, e uno di questi viene ripristinato, viene eseguito un ripristino non autorevole e, in seguito al ripristino, non si verifica un rollback USN.

Requisiti per l'utilizzo di backup compatibili con le applicazioni

Su una macchina fisica, devono essere installati l'Agente per SQL e/o l'Agente per Exchange, oltre all'Agente per Windows.

© Acronis International GmbH, 2003-2024

Su una macchina virtuale non è richiesta l'installazione di alcun agente; si presuppone che il backup della macchina sia eseguito mediante l'Agente per VMware (Windows) o l'Agente per Hyper-V.

Nota
Nelle virtual machine Hyper-V e VMware ESXi che eseguono Windows Server 2022, il backup application-aware non è supportato in modalità agentless, ovvero quando il backup viene eseguito dall'Agente per Hyper-V o dall'Agente per VMware, rispettivamente. Per proteggere le applicazioni Microsoft su questi sistemi, installare l'Agente per Windows nel sistema operativo guest.

L'Agente per VMware (appliance virtuale) può creare backup compatibili con l'applicazione ma non è in grado di ripristinare i dati dell'applicazione da questi. Per ripristinare i dati dell'applicazione dai backup creati da questo agente, è necessario installare l'Agente per VMware (Windows), l'Agente per SQL o l'Agente per Exchange in un sistema che abbia accesso alla posizione in cui i backup vengono archiviati. Durante la configurazione del ripristino dei dati applicazione, selezionare il punto di ripristino nella scheda **Archivio di backup**, quindi selezionare questo sistema in **Macchina da esplorare**.

Gli altri requisiti sono indicati nelle sezioni Prerequisiti e Diritti utente necessari.

Nota
I backup application-aware delle virtual machine Hyper-V possono non riuscire generando errori simili a "WMI 'ExecQuery' non ha eseguito la query" oppure "Non è possibile creare un nuovo processo tramite WMI" se i backup vengono eseguiti su un host con carico elevato, a causa dell'assenza o di un ritardo nella risposta da parte di Windows Management Instrumentation. Provare a rieseguire i backup in un intervallo di tempo in cui il carico sull'host è inferiore.

Diritti utente necessari per i backup application-aware

Un backup compatibile con l'applicazione contiene metadati di applicazioni compatibili con VSS che sono presenti sul disco. Per accedere a tali metadati, l'agente ha bisogno di un account che disponga di diritti appropriati, elencati di seguito. All'utente verrà richiesto di specificare tale account durante l'attivazione del backup dell'applicazione.

- Per SQL Server:
  L'account deve essere membro del gruppo **Operatori di Backup** o **Administrators** sul sistema e membro del ruolo **amministratore di sistema** su ognuna delle istanze di cui si intende eseguire il backup.

  Nota
  È supportata solo l'autenticazione Windows.

- Per Exchange Server:
  Exchange 2007: L'account deve essere un membro del gruppo **Amministratori** del sistema e membro del gruppo di ruoli **Amministratori dell'organizzazione di Exchange**.

© Acronis International GmbH, 2003-2024

Exchange 2010 e versioni successive: L'account deve essere un membro del gruppo **Amministratori** del sistema e membro del gruppo di ruoli **Gestione organizzazione**.

- Per Active Directory:

  L'account deve essere un amministratore di dominio.

Requisiti aggiuntivi per le macchine virtuali

Se l'applicazione viene eseguita su macchine virtuali il cui backup è eseguito dall'Agente per VMware o dall'Agente per Hyper-V, accertarsi che la funzionalità Controllo account utente (UAC) sia disattivata sulla macchina.

Affinché UAC non risulti disattivato, è necessario fornire le credenziali dell'amministratore di dominio incorporato (DOMAIN\Administrator) durante l'attivazione del backup dell'applicazione.

Nota
Utilizzare l'account di amministratore di dominio incorporato che è stato configurato durante la creazione del dominio. Gli account creati successivamente non sono supportati.

Requisiti aggiuntivi per i sistemi che eseguono Windows

Per tutte le versioni di Windows è necessario disabilitare i criteri di controllo dell'account utente per consentire i backup application-aware.

Affinché UAC non risulti disattivato, è necessario fornire le credenziali dell'amministratore di dominio incorporato (DOMAIN\Administrator) durante l'attivazione del backup dell'applicazione.

Nota
Utilizzare l'account di amministratore di dominio incorporato che è stato configurato durante la creazione del dominio. Gli account creati successivamente non sono supportati.

Per disabilitare i criteri di controllo dell'account utente in Windows

1. Nell'editor del Registro di sistema, individuare la seguente chiave del registro:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. Modificare il valore **EnableLUA** in **0**.
3. Riavviare la macchina.

Backup caselle di posta

Il backup delle caselle di posta è supportato per Microsoft Exchange Server 2010 Service Pack 1 (SP1) e versioni successive.

Il backup della casella di posta è disponibile se almeno una Agente per Exchange è registrato nel server di gestione. L'agente deve essere installato su una macchina che appartiene alla stessa foresta di Active Directory di Microsoft Exchange.

Prima di eseguire il backup delle caselle di posta, è necessario connettere l'Agente per Exchange alla macchina che esegue il ruolo server **Accesso Client** (CAS) di Microsoft Exchange Server. In Exchange

© Acronis International GmbH, 2003-2024

2016 e versioni successive, il ruolo CAS non è disponibile come opzione di installazione distinta. Viene installato automaticamente come parte del ruolo di server delle caselle di posta. Pertanto, è possibile collegare l'agente a qualsiasi server eseguendo il **ruolo Casella di posta**.

Nota
È possibile ripristinare caselle di posta ed elementi di caselle di posta da backup di database e da backup application-aware. Per ulteriori informazioni, consultare "Ripristino di caselle di posta di Exchange e relativi elementi" (pag. 592). Con i backup di database e i backup application-aware non è possibile creare piani di protezione per singole caselle di posta.

Per connettere l'Agente per Exchange

1. Fare clic su **Dispositivi** > **Aggiungi**.
2. Fare clic su **Microsoft Exchange Server**.
3. Fare clic su **Caselle di posta di Exchange**.
   Se non sono presenti Agenti per Exchange registrati nel server di gestione, il software suggerisce di installarne uno. Dopo l'installazione, ripetere questa procedura a partire dal passaggio 1.
4. [Facoltativo] Se nel server di gestione sono registrati più Agenti per Exchange, fare clic su **Agente**, quindi modificare l'agente che eseguirà il backup.
5. In **Server di Accesso Client**, specificare il nome di dominio completo (FQDN) della macchina in cui è abilitato il ruolo **Accesso Client** di Microsoft Exchange Server.
   In Exchange 2016 e versioni successive, i servizi di Accesso Client vengono installati automaticamente come parte del ruolo di server delle caselle di posta. Pertanto, è possibile specificare qualsiasi server eseguendo il **ruolo Casella di posta**. In questa sezione, ci si riferirà a questo server come CAS.
6. In **Tipo di autenticazione**, selezionare il tipo di autenticazione utilizzato dal CAS. È possibile selezionare **Kerberos** (impostazione predefinita) oppure **Di base**.
7. [Solo per l'autenticazione di base] Selezionare il protocollo da utilizzare. È possibile selezionare **HTTPS** (impostazione predefinita) oppure **HTTP**.
8. [Solo per l'autenticazione di base con protocollo HTTPS] Se il CAS utilizza un certificato SSL ottenuto da un'autorità di certificazione e si desidera che il software controlli il certificato alla connessione al CAS, selezionare la casella di controllo **Controlla certificato SSL**. Altrimenti, ignorare questo passaggio.
9. Specificare le credenziali di un account che verrà utilizzato per accedere al CAS. I requisiti dell'account sono elencati in "Diritti utente necessari".
10. Fare clic su **Aggiungi**.

Di conseguenza, le caselle di posta vengono visualizzate in **Dispositivi** > **Microsoft Exchange** > **Caselle di posta**.

Selezione delle caselle di posta di Exchange Server

Selezionare le caselle di posta come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

© Acronis International GmbH, 2003-2024

Per selezionare le caselle di posta di Exchange

1. Fare clic su **Dispositivi** > **Microsoft Exchange**.
   Il software mostra la struttura ad albero dei database e delle caselle di posta di Exchange.
2. Fare clic su **Caselle di posta**, quindi selezionare le caselle di posta di cui effettuare il backup.
3. Fare clic su **Proteggi**.

Diritti utente necessari

Per accedere alle caselle di posta, l'Agente per Exchange richiede un account con i diritti appropriati. All'utente viene richiesto di specificare tale account durante la configurazione delle varie attività con le caselle di posta.

L'appartenenza dell'account al gruppo di ruoli **Gestione organizzazione** consente l'accesso a qualsiasi casella di posta, anche quelle che verranno create successivamente.

I diritti utente minimi richiesti sono indicati di seguito:

- L'account deve essere membro del gruppo di ruoli **Gestione server** e **Gestione destinatari**.
- Per l'utente deve essere abilitato il ruolo di gestione **ApplicationImpersonation** per tutti gli utenti o gruppi di utenti alle cui caselle di posta accederà l'agente.
  Per ulteriori informazioni sulla configurazione del ruolo di gestione **ApplicationImpersonation**, fare riferimento all'articolo della Microsoft Knowledge Base indicato di seguito: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

Ripristino di database SQL

È possibile ripristinare i database SQL da backup di database e da backup application-aware. Per ulteriori informazioni sulla differenza tra i due tipi di backup, fare riferimento a "Protezione di Microsoft SQL Server e Microsoft Exchange Server" (pag. 567).

È possibile ripristinare i database SQL nell'istanza originale, in un'istanza diversa nel sistema originale o su un'istanza in un sistema diverso dall'originale. Quando si esegue un ripristino su un sistema diverso dall'originale, l'Agente per SQL deve essere installato sul sistema di destinazione.

È inoltre possibile ripristinare i database come file.

Se si utilizza l'autenticazione Windows per l'istanza SQL, sarà necessario fornire le credenziali per un account membro del gruppo **Operatori di Backup** o **Administrators** nel sistema e membro del ruolo **amministratore di sistema** sull'istanza di destinazione. Se si utilizza l'autenticazione SQL Server, sarà necessario fornire le credenziali per un account membro del ruolo **amministratore di sistema** sull'istanza di destinazione.

I database di sistema sono ripristinati come database dell'utente, con alcune distinzioni. Per ulteriori informazioni su queste distinzioni, fare riferimento a "Ripristino di database di sistema" (pag. 588).

Durante un ripristino, l'avanzamento dell'operazione è visibile nella console di Cyber Protect, nella scheda **Monitoraggio** > **Attività**.

© Acronis International GmbH, 2003-2024

Ripristino di database SQL nel sistema originale

È possibile ripristinare i database SQL nell'istanza originale, in un'istanza diversa nel sistema originale o in un'istanza in un sistema diverso dall'originale.

Per ripristinare i database SQL nel sistema originale

Da un backup di database

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Microsoft SQL**.
2. Selezionare l'istanza di SQL Server o fare clic sul nome dell'istanza per selezionare gli specifici database da ripristinare, quindi fare clic su **Ripristino**.
   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Per ripristinare i dati in un sistema diverso dall'originale, fare riferimento a "Ripristino di database SQL in un sistema diverso dall'originale" (pag. 584).
3. Selezionare un punto di ripristino.
   I punti di ripristino vengono filtrati in base alla posizione.
4. Fare clic su **Ripristina** > **Database su un'istanza**.
   Per impostazione predefinita, l'istanza e i database vengono ripristinati su quelli originali. È anche possibile ripristinare un database originale come nuovo database.
5. [Quando si esegue il ripristino su un'istanza non originale nello stesso sistema] Fare clic su **Istanza SQL Server di destinazione**, selezionare l'istanza di destinazione, quindi fare clic su **Fine**.
6. [Quando si ripristina un database come nuovo database] Fare clic sul nome del database e quindi, in **Ripristina in** fare clic su **Nuovo database**.
   - Specificare il nome del nuovo database.
   - Specificare il percorso del nuovo database.
   - Specificare il percorso del registro.
7. [Facoltativo] [Non disponibile quando si ripristina un database come nuovo database] Per cambiare lo stato del database dopo il ripristino, fare clic sul nome del database e scegliere uno dei seguenti stati, quindi fare clic su **Fine**.
   - **Pronto per l'utilizzo (RECUPERO CON RIPRISTINO)** (impostazione predefinita)
     Al termine del ripristino, il database sarà pronto per l'uso. Gli utenti avranno accesso completo al database. Il software eseguirà il ripristino di tutte le transazioni non eseguite del database ripristinato archiviate nel registro transazione. Non sarà possibile ripristinare registri transazione aggiuntivi dai backup Microsoft SQL nativi.
   - **Non operativo (RECUPERO SENZA RIPRISTINO)**
     Al termine del ripristino, il database non sarà pronto per l'uso. Gli utenti non avranno accesso ad esso. Il software conserverà tutte le transazioni non eseguite del database ripristinato. Sarà possibile ripristinare registri transazione aggiuntivi dai backup Microsoft SQL nativi e quindi raggiungere il punto di ripristino necessario.
   - **Sola lettura (RECUPERO CON STANDBY)**

© Acronis International GmbH, 2003-2024

Al termine del ripristino, gli utenti avranno accesso in sola lettura al database. Il software annullerà tutte le transazioni non eseguite. Tuttavia, salverà le azioni di annullamento in un file di standby temporaneo, in modo che gli effetti del ripristino possano essere riportati allo stato precedente.

Questo valore viene utilizzato principalmente per rilevare il punto temporale in cui si è verificato un errore di SQL Server.

8. Fare clic su **Avvia ripristino**.

Da un backup compatibile con l'applicazione

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare il sistema che conteneva in origine i dati che si desidera ripristinare, quindi fare clic su **Ripristino**.

   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Per ripristinare i dati in un sistema diverso dall'originale, fare riferimento a "Ripristino di database SQL in un sistema diverso dall'originale" (pag. 584).
3. Selezionare un punto di ripristino.

   I punti di ripristino vengono filtrati in base alla posizione.
4. Fare clic su **Ripristina** > **Database SQL**.
5. Selezionare l'istanza di SQL Server o fare clic sul nome dell'istanza per selezionare gli specifici database da ripristinare, quindi fare clic su **Ripristina**.

   Per impostazione predefinita, l'istanza e i database vengono ripristinati su quelli originali. È anche possibile ripristinare un database originale come nuovo database.
6. [Quando si esegue il ripristino su un'istanza non originale nello stesso sistema] Fare clic su **Istanza SQL Server di destinazione**, selezionare l'istanza di destinazione, quindi fare clic su **Fine**.
7. [Quando si ripristina un database come nuovo database] Fare clic sul nome del database e quindi, in **Ripristina in** fare clic su **Nuovo database**.
   - Specificare il nome del nuovo database.
   - Specificare il percorso del nuovo database.
   - Specificare il percorso del registro.
8. [Facoltativo] [Non disponibile quando si ripristina un database come nuovo database] Per cambiare lo stato del database dopo il ripristino, fare clic sul nome del database e scegliere uno dei seguenti stati, quindi fare clic su **Fine**.
   - **Pronto per l'utilizzo (RECUPERO CON RIPRISTINO)** (impostazione predefinita)

     Al termine del ripristino, il database sarà pronto per l'uso. Gli utenti avranno accesso completo al database. Il software eseguirà il ripristino di tutte le transazioni non eseguite del database ripristinato archiviate nel registro transazione. Non sarà possibile ripristinare registri transazione aggiuntivi dai backup Microsoft SQL nativi.
   - **Non operativo (RECUPERO SENZA RIPRISTINO)**

© Acronis International GmbH, 2003-2024

Al termine del ripristino, il database non sarà pronto per l'uso. Gli utenti non avranno accesso ad esso. Il software conserverà tutte le transazioni non eseguite del database ripristinato. Sarà possibile ripristinare registri transazione aggiuntivi dai backup Microsoft SQL nativi e quindi raggiungere il punto di ripristino necessario.

- **Sola lettura (RECUPERO CON STANDBY)**

  Al termine del ripristino, gli utenti avranno accesso in sola lettura al database. Il software annullerà tutte le transazioni non eseguite. Tuttavia, salverà le azioni di annullamento in un file di standby temporaneo, in modo che gli effetti del ripristino possano essere riportati allo stato precedente.

  Questo valore viene utilizzato principalmente per rilevare il punto temporale in cui si è verificato un errore di SQL Server.

9. Fare clic su **Avvia ripristino**.

Ripristino di database SQL in un sistema diverso dall'originale

È possibile ripristinare sia i backup application-aware che i backup di database su istanze di SQL Server su sistemi di destinazione diversi dall'originale, nei quali è installato l'Agente per SQL. I backup devono trovarsi nel cloud storage o in uno storage condiviso al quale possa accedere il sistema di destinazione.

La versione di SQL Server nel sistema di destinazione deve essere la stessa del sistema di origine o più recente.

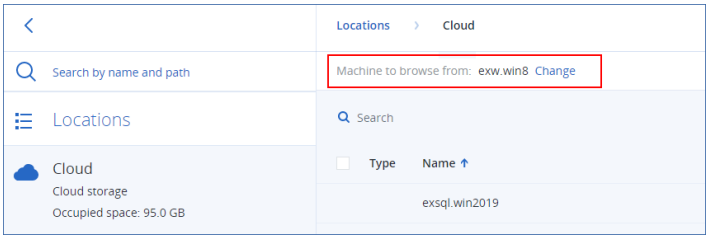
Per ripristinare i database SQL in un sistema diverso dall'originale

Dallo storage di backup

Questa procedura si applica ai backup application-aware e ai backup di database.

1. Nella console di Cyber Protect, passare a **Archivio di backup**.
2. Selezionare la posizione del set di backup dal quale ripristinare i dati.
3. In **Macchina da esplorare da** selezionare il sistema di destinazione.

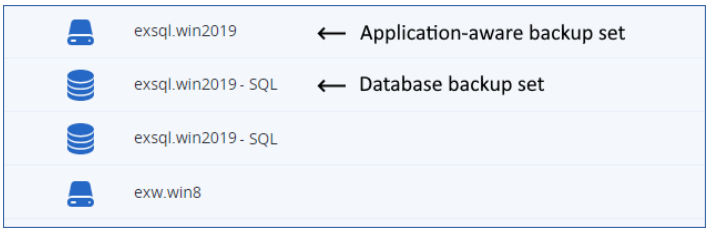
   Si tratta del sistema nel quale verranno ripristinati i dati. Tale sistema di destinazione deve essere online.



4. Selezionare il set di backup, quindi nel pannello **Azioni** fare clic su **Mostra backup**.

   I set di backup application-aware e i set di backup di database presentano icone differenti.

© Acronis International GmbH, 2003-2024



5. Selezionare il punto di ripristino dal quale ripristinare i dati.
6. [Per i backup di database] Fare clic su **Ripristina database SQL**.
7. [Per i backup application-aware] Fare clic su **Ripristina** > **Database SQL**.
8. Selezionare l'istanza di SQL Server o fare clic sul nome dell'istanza per selezionare gli specifici database da ripristinare, quindi fare clic su **Ripristina**.
9. [Se è presente più di un'istanza SQL nel sistema di destinazione] Fare clic su **Istanza SQL Server di destinazione**, selezionare l'istanza di destinazione, quindi fare clic su **Fine**.
10. Fare clic sul nome del database, specificare il nuovo percorso del database e del registro e quindi fare clic su **Fine**.

    È possibile specificare lo stesso percorso in entrambi i campi, come ad esempio:

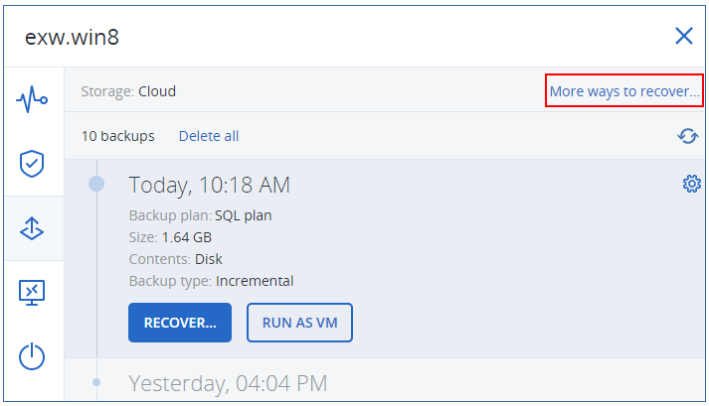
    ```
    C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
    ```

11. Fare clic su **Avvia ripristino**.

Dai dispositivi

Questa procedura si applica solo ai backup application-aware.

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare il sistema che conteneva in origine i dati che si desidera ripristinare, quindi fare clic su **Ripristino**.
3. [Se il sistema di origine è online] Fare clic su **Altri metodi di ripristino**.



4. Fare clic su **Seleziona macchina** per selezionare il sistema di destinazione, quindi fare clic su **OK**.

   Si tratta del sistema nel quale verranno ripristinati i dati. Tale sistema di destinazione deve essere online.
5. Selezionare un punto di ripristino.

© Acronis International GmbH, 2003-2024

I punti di ripristino vengono filtrati in base alla posizione.

6. Fare clic su **Ripristina** > **Database SQL**.
7. Selezionare l'istanza di SQL Server o fare clic sul nome dell'istanza per selezionare gli specifici database da ripristinare, quindi fare clic su **Ripristina**.
8. [Se è presente più di un'istanza SQL nel sistema di destinazione] Fare clic su **Istanza SQL Server di destinazione**, selezionare l'istanza di destinazione, quindi fare clic su **Fine**.
9. Fare clic sul nome del database, specificare il nuovo percorso del database e del registro e quindi fare clic su **Fine**.

   È possibile specificare lo stesso percorso in entrambi i campi, come ad esempio:

   ```
   C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
   ```

10. Fare clic su **Avvia ripristino**.

Ripristino di database SQL come file

È possibile ripristinare i database come file. Questa opzione può essere utile se è necessario estrarre i dati per il data mining, l'audit o per un'ulteriore elaborazione con strumenti di terze parti. Per sapere come collegare i file dei database SQL a un'istanza di SQL Server, fare riferimento a "Collegamento di database di SQL Server" (pag. 589).

È possibile ripristinare i database come file nel sistema originale o su sistemi di destinazione diversi dall'originale, nei quali è installato l'Agente per SQL. Quando si ripristinano i dati su sistemi diversi dall'originale, i backup devono trovarsi nel cloud storage o in uno storage condiviso al quale possa accedere il sistema di destinazione.

Nota
Il ripristino di database come file è l'unico metodo di ripristino se si utilizza l'Agente per VMware (Windows). Non è possibile ripristinare i database usando l'Agente per VMware (appliance virtuale).

Per ripristinare i database SQL come file

Da un backup di database

Questa procedura si applica ai sistemi di origine online.

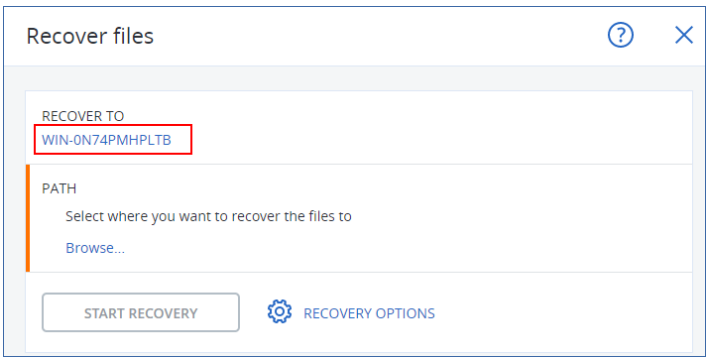
1. Nella console di Cyber Protect, passare a **Dispositivi** > **Microsoft SQL**.
2. Selezionare i database da ripristinare, quindi fare clic su **Ripristino**.
3. Selezionare un punto di ripristino.

   I punti di ripristino vengono filtrati in base alla posizione.
4. Fare clic su **Ripristina** > **Database come file**.
5. [Se il ripristino viene eseguito su un sistema diverso dall'originale] In **Ripristina in**, selezionare il sistema di destinazione.

   Si tratta del sistema nel quale verranno ripristinati i dati. Tale sistema di destinazione deve essere online.

© Acronis International GmbH, 2003-2024

Per modificare la selezione, fare clic sul nome del sistema, selezionare un altro sistema, quindi fare clic su **OK**.



6. In **Percorso**, fare clic su **Sfoglia** e selezionare una cartella locale o di rete in cui salvare i file, quindi fare clic su **Fine**.
7. Fare clic su **Avvia ripristino**.

Da un backup compatibile con l'applicazione

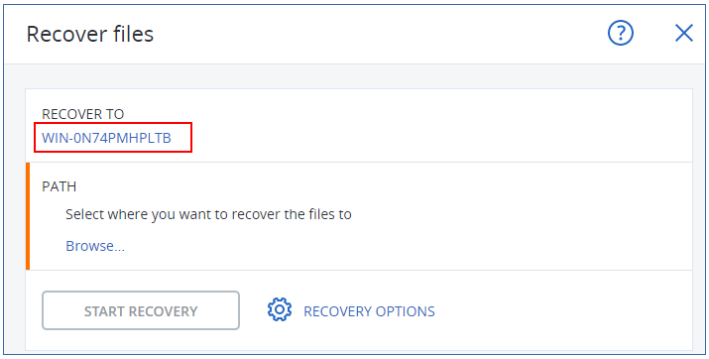
Questa procedura si applica ai sistemi di origine online.

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare il sistema che conteneva in origine i dati che si desidera ripristinare, quindi fare clic su **Ripristino**.
3. Selezionare un punto di ripristino.

   I punti di ripristino vengono filtrati in base alla posizione.
4. Fare clic su **Ripristina** > **Database SQL**, selezionare i database da ripristinare, quindi fare clic su **Ripristina come file**.
5. [Se il ripristino viene eseguito su un sistema diverso dall'originale] In **Ripristina in**, selezionare il sistema di destinazione.

   Si tratta del sistema nel quale verranno ripristinati i dati. Tale sistema di destinazione deve essere online.

   Per modificare la selezione, fare clic sul nome del sistema, selezionare un altro sistema, quindi fare clic su **OK**.



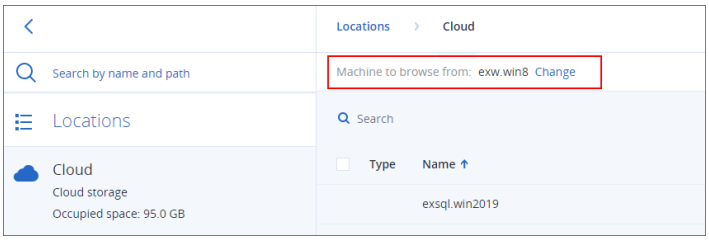
6. In **Percorso**, fare clic su **Sfoglia** e selezionare una cartella locale o di rete in cui salvare i file, quindi fare clic su **Fine**.
7. Fare clic su **Avvia ripristino**.

© Acronis International GmbH, 2003-2024

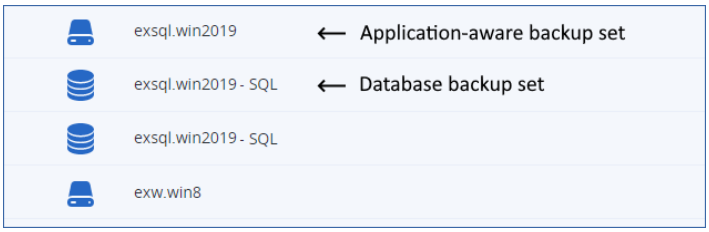
Da un backup su un sistema offline

Questa procedura si applica ai backup application-aware e ai backup di database su sistemi di origine offline.

1. Nella console di Cyber Protect, passare a **Archivio di backup**.
2. Selezionare la posizione del set di backup dal quale ripristinare i dati.
3. In **Macchina da esplorare da** selezionare il sistema di destinazione.
   Si tratta del sistema nel quale verranno ripristinati i dati. Tale sistema di destinazione deve essere online.



4. Selezionare il set di backup, quindi nel pannello **Azioni** fare clic su **Mostra backup**.
   I set di backup application-aware e i set di backup di database presentano icone differenti.



5. Selezionare il punto di ripristino dal quale ripristinare i dati.
6. [Per i backup di database] Fare clic su **Ripristina database SQL**.
7. [Per i backup application-aware] Fare clic su **Ripristina** > **Database SQL**.
8. Selezionare l'istanza di SQL Server o fare clic sul nome dell'istanza per selezionare gli specifici database da ripristinare, quindi fare clic su **Ripristina come file**.
9. In **Percorso**, fare clic su **Sfoglia** e selezionare una cartella locale o di rete in cui salvare i file, quindi fare clic su **Fine**.
10. Fare clic su **Avvia ripristino**.

Ripristino di database di sistema

Tutti i database di sistema di un'istanza vengono ripristinati simultaneamente. Quando si esegue il ripristino dei database di sistema, il software riavvia automaticamente l'istanza di destinazione in modalità utente singolo. Al termine del ripristino, il software riavvia l'istanza e ripristina altri database (se presenti).

Altri elementi da prendere in considerazione quando si ripristina un database di sistema:

- È possibile ripristinare i database di sistema solo in un'istanza della stessa versione dell'istanza originale.

© Acronis International GmbH, 2003-2024

- I database di sistema vengono sempre ripristinati nello stato "pronto per l'uso".

Ripristino del database master

I database di sistema includono il database **master**. Il database **master** registra informazioni su tutti i database dell'istanza. Quindi, il database **master** in un backup contiene informazioni sui database esistenti nell'istanza al momento del backup. Dopo il ripristino del database **master**, è possibile eseguire le seguenti azioni:

- I database visualizzati nell'istanza dopo il backup non sono visibili dall'istanza. Per riportare questi database alla produzione, collegarli manualmente all'istanza utilizzando SQL Server Management Studio.
- I database eliminati dopo il backup sono visualizzati nell'istanza come non in linea. Eliminare questi database utilizzando SQL Server Management Studio.

Collegamento di database di SQL Server

Questa sezione descrive come collegare un database a SQL Server utilizzando SQL Server Management Studio. È possibile collegare solo un database alla volta.

Il collegamento di un database richiede una delle seguenti autorizzazioni: **CREA DATABASE**, **CREA QUALSIASI DATABASE** o **MODIFICA QUALSIASI CONTROLLO DATABASE**. Normalmente, queste autorizzazioni sono concesse al ruolo **amministratore di sistema** dell'istanza.

Per collegare un database

1. Eseguire Microsoft SQL Server Management Studio.
2. Connettere l'istanza di SQL Server richiesta, quindi espanderla.
3. Fare clic con il pulsante destro su **Database** e selezionare **Collega**.
4. Fare clic su **Aggiungi**.
5. Nella finestra di dialogo **Individua file del database**, trovare e selezionare il file .mdf del database.
6. Nella sezione **Dettagli del database**, assicurarsi che il resto dei file del database (file .ndf e .ldf) siano stati trovati.

   Dettagli. I file dei database di SQL Server potrebbero non essere trovati automaticamente, se:
   - non si trovano nella posizione predefinita o non si trovano nella stessa cartella del file del database principale (.mdf). Soluzione: Specificare manualmente il percorso dei file richiesti nella colonna **Percorso file corrente**.
   - È stato ripristinato un set incompleto di file che compongono il database. Soluzione: Ripristinare i file del database SQL Server mancanti dal backup.
7. Quando sono stati trovati tutti i file, selezionare **OK**.

© Acronis International GmbH, 2003-2024

Ripristino dei database di Exchange

In questa sezione viene descritto il ripristino sia dai backup di database che dai backup compatibili con l'applicazione.

È possibile ripristinare i dati di Exchange Server in un Exchange Server live. Può trattarsi dell'Exchange Server originale o di un Exchange Server con la stessa versione che viene eseguita sul sistema con lo stesso nome di dominio completo (FQDN). L'Agente per Exchange deve essere installato sulla macchina di destinazione.

La seguente tabella presenta un riepilogo dei dati di Exchange Server che è possibile selezionare per il ripristino e i diritti utente minimi necessari richiesti per il recupero dei dati.

Versione di Exchange	Elementi di dati	Diritti utente
2007	Gruppi di archiviazione	Appartenenza al gruppo di ruoli **Amministratori organizzazione di Exchange**.
2010/2013/2016/2019	Database	Appartenenza al gruppo di ruoli **Gestione server**.

In alternativa, è possibile ripristinare i database (gruppi di archiviazione) come file. I file di database, insieme ai file dei log delle transazioni, verranno estratti dal backup a una cartella specificata dall'utente. Ciò può essere utile se è necessario estrarre dati per il controllo o per un'ulteriore elaborazione con strumenti di terze parti; oppure quando il ripristino fallisce per qualche motivo e si sta cercando una soluzione per montare i database manualmente.

Se si utilizza soltanto l'Agente per VMware (Windows), il ripristino di database come file è l'unico metodo di ripristino disponibile. Non è possibile ripristinare i database usando l'Agente per VMware (appliance virtuale).

Faremo riferimento sia ai database che ai gruppi di archiviazione come "database" in tutte le /procedure seguenti.

Per ripristinare i database di Exchange in un'istanza di Exchange Server attiva

1. Eseguire una delle seguenti operazioni:
   - Quando si effettua il ripristino da un backup application-aware, in **Dispositivi**, selezionare il sistema che in origine conteneva i dati da ripristinare.
   - Quando si effettua il ripristino dal backup di un database, fare clic su **Dispositivi** > **Microsoft Exchange** > **Database**, quindi selezionare i database da ripristinare.
2. Fare clic su **Ripristino**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.

   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Eseguire una delle seguenti operazioni:
   - [Solo quando si effettua il ripristino da un backup application-aware] Se la posizione di backup è il cloud o un'archiviazione condivisa (a cui possono accedere altri agenti), fare clic su

© Acronis International GmbH, 2003-2024

Seleziona macchina e selezionare un sistema online con l'Agente per Exchange, quindi selezionare un punto di ripristino.

- Selezionare un punto di ripristino nella scheda Archivio di backup.

Il sistema scelto per sfogliare una delle azioni di cui sopra diventa una macchina di destinazione per il recupero dei dati di Exchange.

4. Eseguire una delle seguenti operazioni:
   - Quando si effettua il ripristino da un backup compatibile con l'applicazione, fare clic su **Ripristina** > **Database di Exchange**, selezionare i database da ripristinare, quindi fare clic su **Ripristina**.
   - Durante il ripristino dal backup di un database, fare clic su **Ripristina** > **Database in un server Exchange**.
5. Per impostazione predefinita, i database vengono ripristinati su quelli originali. Se il database di origine non esiste, verrà ricreato.

   Per ripristinare il database come nuovo database:

   a. Fare clic sul nome del database.

   b. In **Ripristina in**, selezionare **Nuovo database**.

   c. Specificare il nome del nuovo database.

   d. Specificare il percorso del nuovo database e del registro. La cartella specificata non deve contenere i file di database e di log originali.
6. Fare clic su **Avvia ripristino**.

L'avanzamento del ripristino viene mostrato nella scheda Attività.

Per ripristinare i database di Exchange come file

1. Eseguire una delle seguenti operazioni:
   - Quando si effettua il ripristino da un backup application-aware, in **Dispositivi**, selezionare il sistema che in origine conteneva i dati da ripristinare.
   - Quando si effettua il ripristino dal backup di un database, fare clic su **Dispositivi** > **Microsoft Exchange** > **Database**, quindi selezionare i database da ripristinare.
2. Fare clic su **Ripristino**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.

   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Eseguire una delle seguenti operazioni:
   - [Solo quando si effettua il ripristino da un backup application-aware] Se la posizione di backup è il cloud o un'archiviazione condivisa (a cui possono accedere altri agenti), fare clic su **Seleziona macchina** e selezionare un sistema online con l'Agente per Exchange o l'Agente per VMware, quindi selezionare un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda Archivio di backup.

© Acronis International GmbH, 2003-2024

Il sistema scelto per sfogliare una delle azioni di cui sopra diventa una macchina di destinazione per il recupero dei dati di Exchange.

4. Eseguire una delle seguenti operazioni:
   - Quando si effettua il ripristino da un backup compatibile con l'applicazione, fare clic su **Ripristina** > **Database di Exchange**, selezionare i database da ripristinare, quindi fare clic su **Ripristina come file**.
   - Durante il ripristino dal backup di un database, fare clic su **Ripristina** > **Database come file**.
5. Fare clic su **Sfoglia** e selezionare una cartella locale o di rete in cui salvare i file.
6. Fare clic su **Avvia ripristino**.

L'avanzamento del ripristino viene mostrato nella scheda Attività.

Montaggio di database di Exchange Server

Dopo il ripristino dei file del database, è possibile portare i database in linea montandoli. Il montaggio viene effettuato utilizzando Exchange Management Console, Exchange System Manager o Exchange Management Shell.

I database ripristinati saranno in stato Arresto anomalo. Un database in stato Arresto anomalo può essere montato dal sistema se viene ripristinato nella sua posizione originale (ovvero, le informazioni del database originale sono presenti in Active Directory). Quando si ripristina un database in una posizione alternativa (come un nuovo database o come database di recupero), non è possibile montare il database fino a quando viene portato in stato Spegnimento corretto utilizzando il comando `Eseutil /r <Enn>`. `<Enn>` consente di specificare il prefisso del file di registro del database (o del gruppo di archiviazione che contiene il database) a cui è necessario applicare i file del registro transazioni.

All'account utilizzato per collegare un database deve essere delegato un ruolo amministratore di Exchange Server e il gruppo Administrators locale per il server di destinazione.

Per dettagli su come montare database, consultare i seguenti articoli:

- Per Exchange 2010 o versione successiva: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Per Exchange 2007: https://technet.microsoft.com/it-it/library/aa998871(v=EXCHG.80).aspx

Ripristino di caselle di posta di Exchange e relativi elementi

È possibile ripristinare le caselle di posta di Exchange e i relativi elementi dai backup seguenti:

- Backup di database
- Backup application-aware
- Backup di caselle di posta

È possibile ripristinare gli elementi seguenti:

© Acronis International GmbH, 2003-2024

- Caselle di posta (tranne le caselle di posta archiviate)
- Cartelle pubbliche

  Nota
  Disponibile solo da backup di database. Vedere "Selezione di dati di Exchange Server" (pag. 572).

- Elementi della cartella pubblica
- Cartelle e-mail
- Messaggi e-mail
- Eventi di calendario
- Attività
- Contatti
- Voci del diario
- Note

È possibile utilizzare la ricerca per individuare gli elementi.

È possibile ripristinare le caselle di posta o gli elementi di una casella di posta in un'istanza di Exchange Server attiva o in Microsoft 365.

Ripristino in un server Exchange

Il ripristino granulare può essere eseguito su Microsoft Exchange Server 2010 Service Pack 1 (SP1) e versioni successive. Il backup di origine può contenere database o caselle di posta di qualsiasi versione di Exchange supportata.

Il ripristino granulare può essere attuato dall'Agente per Exchange o dall'Agente per VMware (Windows). L'Exchange Server di destinazione e la macchina in cui è eseguito l'agente devono appartenere alla stessa foresta di Active Directory.

Quando una casella di posta viene ripristinata in una casella di posta esistente, vengono sovrascritti gli elementi già esistenti con ID corrispondenti.

Il ripristino di elementi di caselle di posta non sovrascrive alcun elemento. Il percorso completo di un elemento della casella di posta viene invece ricreato nella cartella di destinazione.

Requisiti sugli account utente

A una casella di posta che viene ripristinata da un backup deve essere associato un account utente di Active Directory.

È possibile ripristinare le caselle di posta degli utenti e il rispettivo contenuto solo se gli account utente associati sono *abilitati*. È possibile ripristinare caselle postali condivise, caselle postali sala e caselle postali attrezzatura solo se gli account utente sono *disabilitati*.

Le caselle di posta che non soddisfano le condizioni precedenti verranno ignorate durante il ripristino.

© Acronis International GmbH, 2003-2024

Se alcune caselle di posta vengono ignorate, il ripristino sarà "Completato con avvisi". Se tutte le caselle di posta vengono ignorate, il ripristino non andrà a buon fine.

Ripristino in Microsoft 365

Il ripristino di elementi dati di Exchange in Microsoft 365 e viceversa è supportato a condizione che l'Agente per Microsoft 365 sia installato in locale.

Il ripristino può essere eseguito dagli backup di Microsoft Exchange Server 2010 e versioni successive.

Quando una casella di posta viene ripristinata in una casella di posta di Microsoft 365 esistente, gli elementi esistenti restano integri e gli elementi ripristinati vengono posizionati accanto a quelli esistenti.

Quando si esegue il ripristino di una singola casella di posta, è necessario selezionare la casella di posta Microsoft 365 di destinazione. Quando si esegue il ripristino di più caselle di posta con un'unica operazione di ripristino, il software tenta di ripristinare ogni casella di posta nella casella di posta dell'utente con lo stesso nome. Se l'utente non viene individuato, la casella di posta viene ignorata. Se alcune caselle di posta vengono ignorate, il ripristino sarà "Completato con avvisi". Se tutte le caselle di posta vengono ignorate, il ripristino non andrà a buon fine.

Per altre informazioni sul ripristino in Microsoft 365, fare riferimento a "Protezione dei dati di Microsoft 365" (pag. 608).

Ripristino delle caselle postali

Per ripristinare le caselle di posta dal backup di un database o da un backup compatibile con l'applicazione

1. [Solo quando si effettua il ripristino da un backup di database a Microsoft 365] Se l'Agente per Microsoft 365 non è installato nel sistema che esegue Exchange Server di cui è stato eseguito il backup, attenersi alla seguente procedura:
   - Se nell'organizzazione non è disponibile un Agente per Microsoft 365, installare l'Agente per Microsoft 365 nel sistema di cui è stato eseguito il backup (o in un altro sistema con la stessa versione di Microsoft Exchange Server).
   - Se nell'organizzazione è già disponibile un Agente per Microsoft 365, copiare le librerie dal nel sistema di cui è stato eseguito il backup (o da un altro sistema con la stessa versione di Microsoft Exchange Server) al sistema in cui è installato l'Agente per Microsoft 365, come descritto in Copiare le librerie di Microsoft Exchange.
2. Eseguire una delle seguenti operazioni:
   - Quando si effettua il ripristino da un backup application-aware: in **Dispositivi**, selezionare il sistema che in origine conteneva i dati da ripristinare.
   - Quando si effettua il ripristino dal backup di un database, fare clic su **Dispositivi** > **Microsoft Exchange** > **Database**, quindi selezionare il database che in origine conteneva i dati da ripristinare.
3. Fare clic su **Ripristino**.

© Acronis International GmbH, 2003-2024

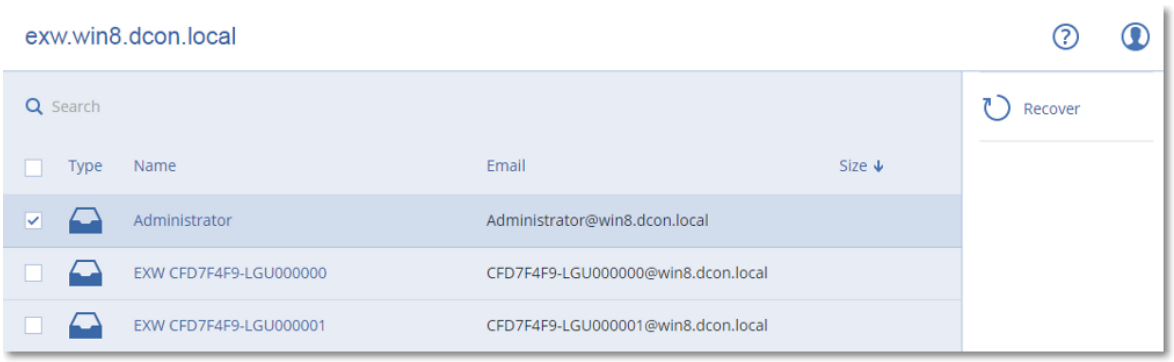
4. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.

   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Utilizzare altri metodi di ripristino:

   - [Solo quando si effettua il ripristino da un backup application-aware] Se la posizione di backup è il cloud o un'archiviazione condivisa (a cui possono accedere altri agenti), fare clic su **Seleziona macchina** e selezionare un sistema online con l'Agente per Exchange o l'Agente per VMware, quindi selezionare un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda Archivio di backup.

   Sarà il sistema scelto per eseguire la ricerca per una delle azioni descritte sopra ad eseguire il ripristino e non il sistema originale, che è offline.
5. Fare clic su **Ripristina** > **Caselle di posta di Exchange**.
6. Selezionare le caselle di posta che si desidera ripristinare.

   È possibile cercare le caselle di posta per nome. I caratteri jolly non sono supportati.



7. Fare clic su **Ripristina**.
8. [Solo quando si effettua il ripristino in Microsoft 365]:
   a. In **Ripristina in**, selezionare **Microsoft 365**.
   b. [Se nel passaggio 6 è stata selezionata solo una casella di posta] In **Cassetta postale di destinazione**, specificare la casella di posta di destinazione.
   c. Fare clic su **Avvia ripristino**.

   Non sono necessari ulteriori passaggi per questa procedura.

   Fare clic su **Macchina di destinazione con Microsoft Exchange Server** per selezionare o cambiare il sistema di destinazione. Questo passaggio consente di eseguire il ripristino in un sistema che non esegue l'Agente per Exchange.

   Specificare il nome di dominio completo (FQDN) di un sistema in cui è abilitato il ruolo **Accesso Client** (in Microsoft Exchange Server 2010/2013) o il **ruolo Casella di posta** (in Microsoft Exchange Server 2016 o versioni successive). Il sistema deve appartenere alla stessa foresta di Active Directory del sistema che esegue il ripristino.
9. Se richiesto, specificare le credenziali di un account che verrà utilizzato per accedere al computer. I requisiti dell'account sono elencati in "Diritti utente necessari".
10. [Facoltativo] Fare clic su **Database per creare nuovamente caselle di posta mancanti** per cambiare il database selezionato automaticamente.

© Acronis International GmbH, 2003-2024

11. Fare clic su **Avvia ripristino**.

L'avanzamento del ripristino viene mostrato nella scheda **Attività**.

Per ripristinare una casella di sposta da un backup di caselle di posta

1. Fare clic su **Dispositivi** > **Microsoft Exchange** > **Caselle di posta**.
2. Selezionare la casella di posta da ripristinare e fare clic su **Ripristino**.

   È possibile cercare le caselle di posta per nome. I caratteri jolly non sono supportati.

   Se la casella di posta è stata eliminata, selezionarla nella scheda Archivio di backup, quindi fare clic su **Mostra backup**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.
4. Fare clic su **Ripristina** > **Casella di posta**.
5. Eseguire i passaggi da 8 a 11 della procedura descritta precedentemente.

Ripristino di elementi di casella di posta

Per ripristinare elementi delle caselle di posta dal backup di un database o da un backup compatibile con l'applicazione

1. [Solo quando si effettua il ripristino da un backup di database a Microsoft 365] Se l'Agente per Microsoft 365 non è installato nel sistema che esegue Exchange Server di cui è stato eseguito il backup, attenersi alla seguente procedura:
   - Se nell'organizzazione non è disponibile un Agente per Microsoft 365, installare l'Agente per Microsoft 365 nel sistema di cui è stato eseguito il backup (o in un altro sistema con la stessa versione di Microsoft Exchange Server).
   - Se nell'organizzazione è già disponibile un Agente per Microsoft 365, copiare le librerie dal nel sistema di cui è stato eseguito il backup (o da un altro sistema con la stessa versione di Microsoft Exchange Server) al sistema in cui è installato l'Agente per Microsoft 365, come descritto in Copiare le librerie di Microsoft Exchange.
2. Eseguire una delle seguenti operazioni:
   - Quando si effettua il ripristino da un backup application-aware: in **Dispositivi**, selezionare il sistema che in origine conteneva i dati da ripristinare.
   - Quando si effettua il ripristino dal backup di un database, fare clic su **Dispositivi** > **Microsoft Exchange** > **Database**, quindi selezionare il database che in origine conteneva i dati da ripristinare.
3. Fare clic su **Ripristino**.
4. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.

   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Utilizzare altri metodi di ripristino:
   - [Solo quando si effettua il ripristino da un backup application-aware] Se la posizione di backup è il cloud o un'archiviazione condivisa (a cui possono accedere altri agenti), fare clic su

© Acronis International GmbH, 2003-2024

Seleziona macchina e selezionare un sistema online con l'Agente per Exchange o l'Agente per VMware, quindi selezionare un punto di ripristino.

- Selezionare un punto di ripristino nella scheda Archivio di backup.

Sarà il sistema scelto per eseguire la ricerca per una delle azioni descritte sopra ad eseguire il ripristino e non il sistema originale, che è offline.

5. Fare clic su **Ripristina** > **Caselle di posta di Exchange**.
6. Fare clic sulla casella di posta che conteneva in origine gli elementi che si desidera ripristinare.
7. Selezionare gli elementi che si desidera ripristinare.

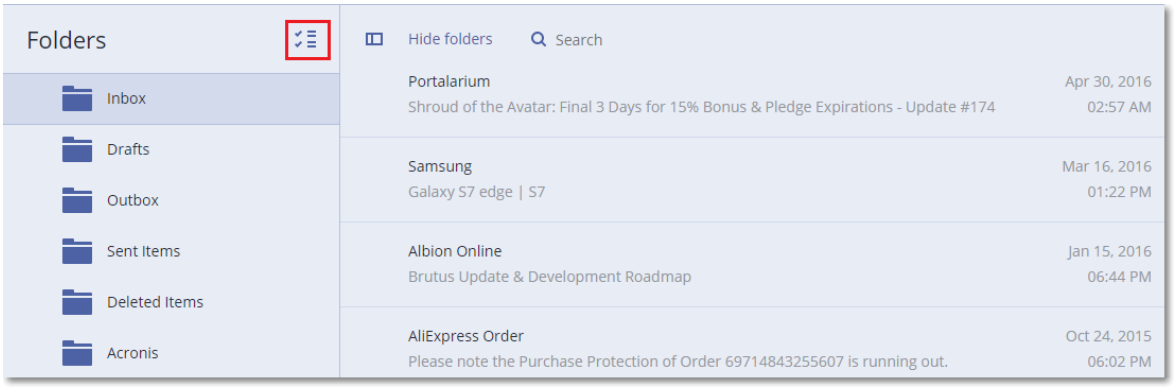
   Sono disponibili le opzioni di ricerca seguenti. I caratteri jolly non sono supportati.

   - Per i messaggi e-mail: ricerca per oggetto, mittente, destinatario e data.
   - Per gli eventi: ricerca per titolo e data.
   - Per le attività: ricerca per titolo e data.
   - Per i contatti: ricerca per nome, indirizzo e-mail e numero di telefono.

   Quando è selezionato un messaggio e-mail, è possibile fare clic su **Mostra il contenuto** per visualizzarne il contenuto, inclusi gli allegati.

   Nota
   Fare clic sul nome di un file allegato per scaricarlo.

   Per poter selezionare le cartelle, fare clic sull'icona di ripristino delle cartelle.



8. Fare clic su **Ripristina**.
9. Per eseguire il ripristino in Microsoft 365, selezionare **Microsoft 365** in **Ripristina in**.

   Per effettuare il ripristino in un server Exchange, mantenere il valore predefinito **Microsoft Exchange** in **Ripristina in**.
10. [Solo quando si effettua il ripristino su un server Exchange] Fare clic su **Macchina di destinazione con Microsoft Exchange Server** per selezionare o cambiare il sistema di destinazione. Questo passaggio consente di eseguire il ripristino in un sistema che non esegue l'Agente per Exchange.

    Specificare il nome di dominio completo (FQDN) di un sistema in cui è abilitato il ruolo **Accesso Client** (in Microsoft Exchange Server 2010/2013) o il **ruolo Casella di posta** (in Microsoft

© Acronis International GmbH, 2003-2024

Exchange Server 2016 o versioni successive). Il sistema deve appartenere alla stessa foresta di Active Directory del sistema che esegue il ripristino.
Se richiesto, specificare le credenziali di un account che verrà utilizzato per accedere al computer. I requisiti dell'account sono elencati in "Diritti utente necessari".

11. In **Cassetta postale di destinazione**, visualizzare, cambiare o specificare la casella di posta di destinazione.
    Per impostazione predefinita, viene selezionata la casella di posta originale. Se tale casella di posta non esiste o se è stato selezionato una macchina di destinazione non originale, è necessario specificare la casella di posta di destinazione.
12. [Solo quando si ripristinano i messaggi e-mail] In **Cartella di destinazione** visualizzare o modificare la cartella di destinazione nella casella di posta di destinazione. Per impostazione predefinita, la cartella **Elementi ripristinati** è selezionata. A causa delle limitazioni di Microsoft Exchange, eventi, attività, note e contatti vengono ripristinati nella posizione originale anche se viene specificata una qualsiasi altra **Cartella di destinazione**.
13. Fare clic su **Avvia ripristino**.

L'avanzamento del ripristino viene mostrato nella scheda **Attività**.

Per ripristinare un elemento di una casella di posta dal backup di una casella di posta

1. Fare clic su **Dispositivi** > **Microsoft Exchange** > **Caselle di posta**.
2. Selezionare la casella di posta che conteneva in origine gli elementi da ripristinare, quindi fare clic su **Ripristino**.
   È possibile cercare le caselle di posta per nome. I caratteri jolly non sono supportati.
   Se la casella di posta è stata eliminata, selezionarla nella scheda Archivio di backup, quindi fare clic su **Mostra backup**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.
4. Fare clic su **Ripristina** > **Messaggi e-mail**.
5. Selezionare gli elementi che si desidera ripristinare.
   Sono disponibili le opzioni di ricerca seguenti. I caratteri jolly non sono supportati.
   - Per i messaggi e-mail: ricerca per oggetto, mittente, destinatario e data.
   - Per gli eventi: ricerca per titolo e data.
   - Per le attività: ricerca per titolo e data.
   - Per i contatti: ricerca per nome, indirizzo e-mail e numero di telefono.

   Quando è selezionato un messaggio e-mail, è possibile fare clic su **Mostra il contenuto** per visualizzarne il contenuto, inclusi gli allegati.

   Nota
   Fare clic sul nome di un file allegato per scaricarlo.

© Acronis International GmbH, 2003-2024

Quando è selezionato un messaggio e-mail, è possibile fare clic su **Invia come e-mail** per inviare il messaggio a un indirizzo e-mail. Il messaggio verrà inviato dall'indirizzo e-mail dell'account di amministratore.

Per poter selezionare le cartelle, fare clic sull'icona di ripristino delle cartelle:

6. Fare clic su **Ripristina**.
7. Eseguire i passaggi da 9 a 13 della procedura descritta precedentemente.

Copiare le librerie di Microsoft Exchange

Durante il ripristino di caselle di posta di Exchange o di elementi di caselle di posta in Microsoft 365, può essere necessario copiare le seguenti librerie dal sistema di cui è stato eseguito il backup (o da un altro sistema con la stessa versione di Microsoft Exchange Server) al sistema in cui è installato l'Agente per Microsoft 365.

Copiare i seguenti file in base alla versione di Microsoft Exchange Server di cui è stato eseguito il backup.

Versione Microsoft Exchange Server	Librerie	Posizione predefinita

Microsoft Exchange Server 2010	`ese.dll`
	`esebcli2.dll`
	`store.exe`
		`%ProgramFiles%\Microsoft\Exchange Server\V14\bin`

Microsoft Exchange Server 2013	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll`	`%WINDIR%\system32`
Microsoft Exchange Server 2016, 2019	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll` `msvcp110.dll`	`%WINDIR%\system32`

Le librerie devono essere collocate nella cartella `%ProgramData%\Acronis\ese`. Se tale cartella non esiste, è necessario crearla manualmente.

Modificare le credenziali di accesso a SQL Server o al server di Exchange

È possibile modificare le credenziali di accesso a SQL Server o al server di Exchange senza reinstallare l'agente.

Per modificare le credenziali di accesso a SQL Server o al server di Exchange

© Acronis International GmbH, 2003-2024

1. Fare clic su **Dispositivi**, e quindi su **Microsoft SQL** or **Microsoft Exchange**.
2. Selezionare il Gruppo di disponibilità Always On, il Gruppo di Disponibilità Database, l'istanza di SQL Server, oppure il server di Microsoft Exchange per i quali modificare le credenziali di accesso.
3. Fare clic su **Specifica credenziali**.
4. Specificare le nuove credenziali di accesso e fare clic su **OK**.

Per modificare le credenziali di accesso al server di Exchange per il backup della casella di posta

1. Fare clic su **Dispositivi** > **Microsoft Exchange** e quindi espandere **Caselle di posta**.
2. Selezionare il server di Exchange per il quale si desidera modificare le credenziali di accesso.
3. Fare clic su **Impostazioni**.
4. Alla voce **Account amministratore di Exchange**, specificare le nuove credenziali di accesso e fare clic su **Salva**.

Protezione dei dispositivi mobili

L'app Cyber Protect consente di eseguire il backup dei dati dei dispositivi mobili nell'archivio cloud e di ripristinarli in caso di perdita o danneggiamento. Tenere presente che per eseguire il backup nell'archivio cloud è necessario disporre di un account e di un abbonamento al servizio cloud.

Dispositivi mobili supportati

È possibile installare l'app Cyber Protect sui dispositivi mobili che eseguono uno dei seguenti sistemi operativi:

- Da iOS 14 a iOS 16 (iPhone, iPod, iPad)
- Da Android 9 a Android 13

Elementi di cui è possibile eseguire il backup

- Contatti (nome, numero di telefono e indirizzo e-mail)
- Foto (vengono conservati dimensione e formato originale delle foto)
- Video
- Calendari
- Promemoria (solo dispositivi iOS)

Informazioni fondamentali

- È possibile eseguire il backup dei dati esclusivamente nello spazio di archiviazione nel cloud.
- Ogni volta che si apre l'app, viene visualizzato il riepilogo delle modifiche ai dati ed è possibile avviare manualmente un backup.

© Acronis International GmbH, 2003-2024

- La funzionalità **Backup continuo** è attivata per impostazione predefinita. Se questa impostazione è attivata, l'app Cyber Protect rileva in automatico e all'istante i nuovi dati, e li carica nel cloud.
- L'impostazione **Utilizza solo Wi-Fi** è abilitata per impostazione predefinita nelle impostazioni dell'app. Se questa impostazione è attivata, l'app Cyber Protect eseguirà il backup dei dati solo quando è disponibile una connessione Wi-Fi. Se la connessione Wi-Fi si interrompe, il processo di backup non si avvia. Per fare in modo che l'app utilizzi la connessione mobile, disattivare questa opzione.
- La funzione di ottimizzazione della batteria del dispositivo potrebbe impedire il corretto funzionamento dell'app Cyber Protect. Per eseguire il backup puntualmente, potrebbe essere necessario arrestare l'ottimizzazione della batteria per l'app.
- Due modalità consentono di risparmiare energia:
  - La funzionalità **Esegui il backup solo se in carica**, che è disabilitata per impostazione predefinita. Se questa impostazione è attivata, l'app Cyber Protect eseguirà il backup dei dati solo quando il dispositivo è collegato all'alimentazione elettrica. Se il dispositivo viene scollegato dall'alimentazione elettrica durante un processo di backup continuo, il backup viene sospeso.
  - La modalità **Modalità a basso consumo energetico**, che è abilitata per impostazione predefinita. Se questa impostazione è attivata, l'app Cyber Protect eseguirà il backup dei dati solo se il livello di carica della batteria non è troppo basso. Se il livello di carica della batteria si riduce troppo, il backup continuo viene sospeso.
- È possibile accedere ai dati di cui è stato eseguito il backup da qualsiasi dispositivo mobile registrato con il proprio account. Questa funzionalità è utile per trasferire i dati da un vecchio dispositivo mobile a uno nuovo. I contatti e le foto di un dispositivo Android possono essere trasferiti a un dispositivo iOS e viceversa. È inoltre possibile scaricare foto, video o contatti su qualsiasi dispositivo utilizzando la console di Cyber Protect.
- I dati di cui è stato eseguito il backup da dispositivi mobili registrati nell'account sono disponibili soltanto in tale account. Nessun altro potrà visualizzare o ripristinare i dati dell'utente.
- Nell'app Cyber Protect è possibile ripristinare solo le versioni più recenti dei dati. Se è necessario ripristinare dati da una versione di backup specifica, utilizzare la console di Cyber Protect su un tablet o su un computer.
- Le regole di conservazione non sono applicate al backup dei dispositivi mobili.
- [Solo per dispositivi Android] Se durante il backup è presente una scheda SD, anche i dati in essa contenuti verranno inseriti nel backup. I dati verranno ripristinati in una scheda SD, nella cartella **Ripristinato da backup** se tale scheda è presente durante il ripristino. In caso contrario, l'app chiederà di specificare una posizione differente in cui ripristinare i dati.

Per scaricare l'app Cyber Protect

A seconda del dispositivo mobile, installare l'app da App Store o Google Play.

© Acronis International GmbH, 2003-2024

Per avviare il backup dei dati

1. Aprire l'app di backup.
2. Accedere con il proprio account.
3. Toccare **Imposta** per creare il backup. Questo pulsante è visibile solo quando non sono presenti backup del dispositivo mobile.
4. Selezionare le categorie di dati di cui eseguire il backup. Per impostazione predefinita, sono selezionate tutte le categorie.
5. [Passaggio facoltativo] Abilitare **Crittografa backup** per proteggere il backup con la crittografia. In questo caso, è necessario anche:
   a. Inserire due volte una password per la crittografia.

      Nota
      Accertarsi di annotare la password, perché non sarà possibile ripristinare o modificare una password dimenticata.

   b. Toccare **Crittografa**.
6. Toccare **Esegui backup**.
7. Consentire all'app di accedere ai dati personali. Non verrà eseguito il backup delle categorie di dati per cui viene negato l'accesso.

Il backup viene avviato.

Per ripristinare i dati in un dispositivo mobile

Attenzione!
Per recuperare i dati di un dispositivo mobile, è necessario utilizzare l'account dell'utente finale.

1. Aprire l'app Cyber Protect.
2. Toccare **Sfoglia**.
3. Toccare il nome del dispositivo.
4. Eseguire una delle seguenti operazioni:
   - Per ripristinare tutti i dati di cui è stato eseguito il backup, toccare **Ripristina tutto**. Non è necessaria alcuna azione aggiuntiva.
   - Per ripristinare una o più categorie di dati, toccare **Seleziona**, quindi toccare le caselle di controllo corrispondenti alle categorie di dati necessarie. Toccare **Ripristina**. Non è necessaria alcuna azione aggiuntiva.
   - Per ripristinare uno o più elementi di dati appartenenti alla stessa categoria, toccare la categoria di dati. Procedere ai passaggi successivi.
5. Eseguire una delle seguenti operazioni:

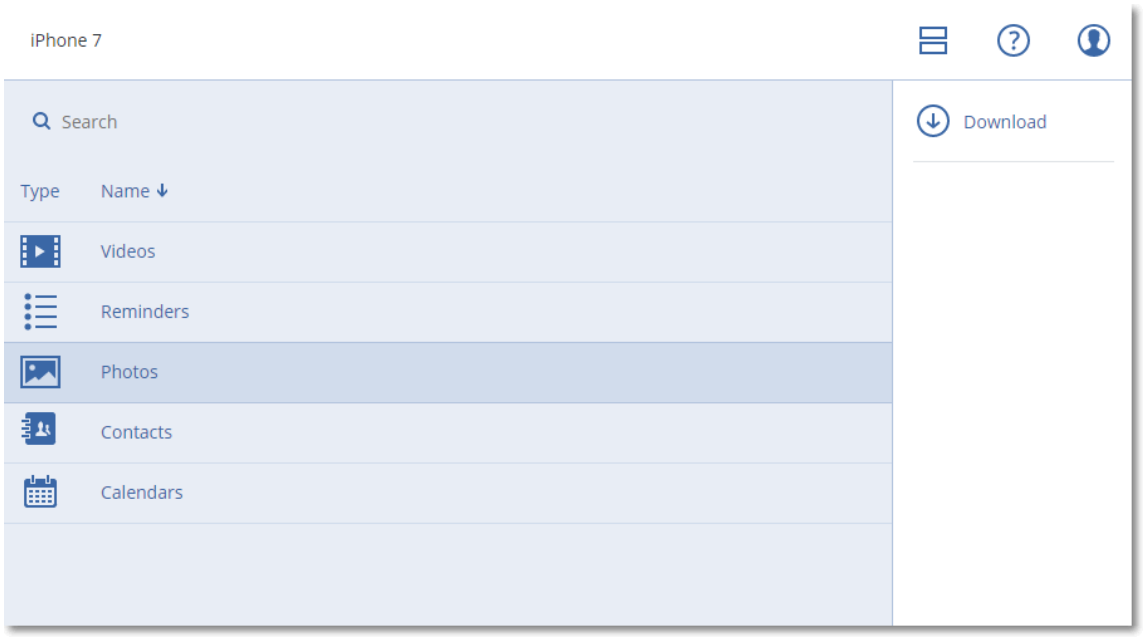
© Acronis International GmbH, 2003-2024

- Per ripristinare un singolo elemento di dati, toccare l'elemento.
- Per ripristinare uno o più elementi di dati, toccare **Seleziona**, quindi toccare le caselle di controllo corrispondenti agli elementi di dati richiesti.

6. Toccare **Ripristina**.

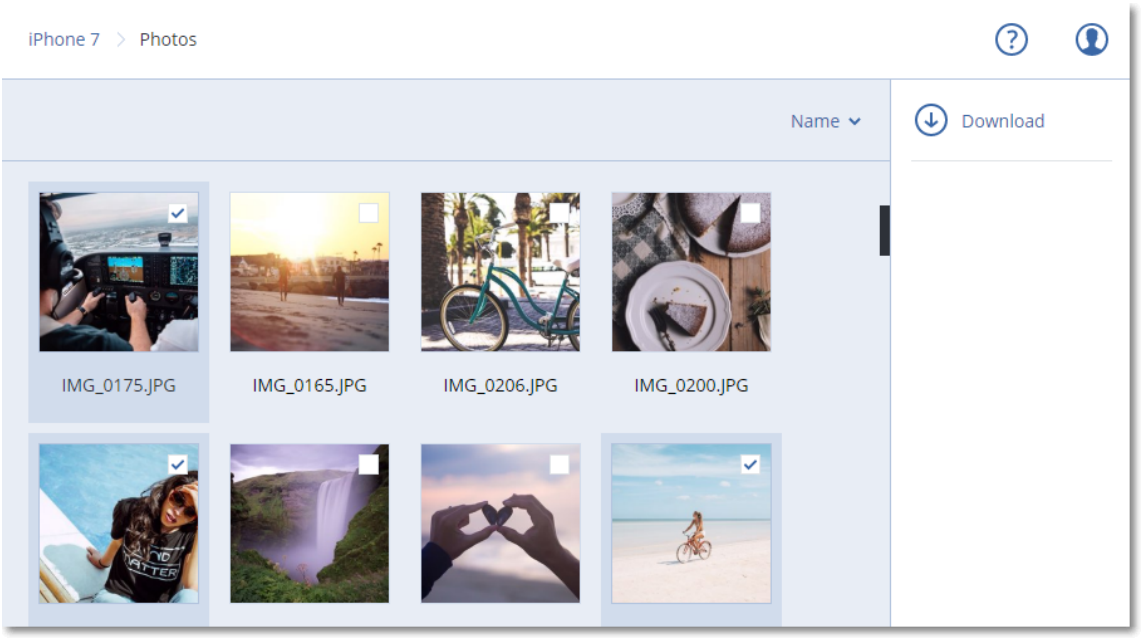
Come rivedere i dati tramite la console di Cyber Protect

1. Su un computer, aprire il browser e digitare l'URL della console di Cyber Protect.
2. Accedere con il proprio account.
3. In **Tutti i dispositivi**, fare clic su **Ripristina** sotto il nome del dispositivo mobile.
4. Eseguire una delle seguenti operazioni:
   - Per scaricare tutte le foto, i video, i contatti, i calendari o i promemoria, selezionare la categoria di dati corrispondente. Fare clic su **Download**.



   - Per scaricare singole foto, video, contatti, calendari o promemoria, fare clic sul nome della relativa categoria di dati, quindi selezionare le caselle di controllo corrispondenti agli elementi di dati richiesti. Fare clic su **Download**.

© Acronis International GmbH, 2003-2024



- Per visualizzare l'anteprima di una foto o un contatto, fare clic sul nome della relativa categoria di dati, quindi fare clic sull'elemento di dati richiesto.

Protezione dei dati per Exchange ospitato

Di quali elementi è possibile eseguire il backup?

È possibile eseguire il backup delle caselle di posta utente, di gruppo e condivise. Facoltativamente, è possibile scegliere di eseguire il backup delle caselle di posta di archiviazione (**In-Place Archive**) delle caselle di posta selezionate.

Quali elementi è possibile ripristinare?

Dal backup di una casella postale è possibile ripristinare i seguenti elementi:

- Caselle postali
- Cartelle e-mail
- Messaggi e-mail
- Eventi di calendario
- Attività
- Contatti
- Voci del diario
- Note

È possibile utilizzare la ricerca per individuare gli elementi.

© Acronis International GmbH, 2003-2024

Durante il ripristino di caselle di posta, elementi delle caselle di posta, cartelle pubbliche e elementi delle cartelle pubbliche, è possibile selezionare se sovrascrivere o meno gli elementi nella posizione di destinazione.

Quando una casella di posta viene ripristinata in una casella di posta esistente, vengono sovrascritti gli elementi già esistenti con ID corrispondenti.

Il ripristino di elementi di caselle di posta non sovrascrive alcun elemento. Il percorso completo di un elemento della casella di posta viene invece ricreato nella cartella di destinazione.

Selezione delle caselle di posta di Exchange Online

Selezionare le caselle di posta come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Per selezionare le caselle di posta di Exchange Online

1. Fare clic su **Dispositivi > Exchange ospitato**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Exchange ospitato, selezionare l'organizzazione i cui dati utente devono essere sottoposti a backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per eseguire il backup delle caselle di posta di tutti gli utenti e di tutte le caselle condivise (incluse quelli che verranno create in futuro), espandere il nodo **Utenti**, selezionare **Tutti gli utenti** e quindi fare clic su **Raggruppa backup**.
   - Per eseguire il backup di singole caselle di posta utente o di caselle condivise, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare gli utenti la cui casella di posta si desidera sottoporre a backup e quindi fare clic su **Backup**.
   - Per eseguire il backup delle caselle di posta di tutti i gruppi (incluse quelli dei gruppi che verranno creati in futuro), espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, quindi fare clic su **Raggruppa backup**.
   - Per eseguire il backup di singole caselle di posta di gruppo, espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, selezionare i gruppi le cui caselle di posta si desidera sottoporre a backup e quindi fare clic su **Backup**.

Ripristino di caselle postali e di elementi delle caselle postali

Ripristino delle caselle postali

1. Fare clic su **Dispositivi > Exchange ospitato**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Exchange ospitato, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:

© Acronis International GmbH, 2003-2024

- Per ripristinare una casella di posta utente, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente la cui casella di posta si desidera ripristinare e quindi fare clic su **Ripristino**.
- Per ripristinare una casella di posta condivisa, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare la casella condivisa che si desidera ripristinare e quindi fare clic su **Ripristino**.
- Per ripristinare una casella di posta di gruppo, espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, selezionare il gruppo la cui casella di posta si desidera ripristinare e quindi fare clic su **Ripristino**.
- Se la casella di posta utente, di gruppo o condivisa è stata eliminata, selezionarla nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.

È possibile cercare gli utenti e i gruppi per nome. I caratteri jolly non sono supportati.

4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina** > **Intera casella di posta**.
6. Se al servizio Cyber Protection vengono aggiunte più organizzazioni di Exchange ospitato, fare clic su **Organizzazione di Exchange ospitato** per visualizzare, modificare o specificare l'organizzazione di destinazione.

   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.
7. In **Ripristina nelle caselle di posta**, visualizzare, modificare o specificare la casella di posta di destinazione.

   Per impostazione predefinita, viene selezionata la casella di posta originale. Se questa casella di posta non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare la casella di posta di destinazione.
8. Fare clic su **Avvia ripristino**.
9. Selezionare una delle opzioni di sovrascrittura:
   - **Sovrascrivi gli elementi esistenti**
   - **Non sovrascrivere gli elementi esistenti**
10. Fare clic su **Procedi** per confermare la decisione.

Ripristino di elementi di casella di posta

1. Fare clic su **Dispositivi > Exchange ospitato**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Exchange ospitato, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:

© Acronis International GmbH, 2003-2024

- Per ripristinare gli elementi da una casella di posta utente, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente la cui casella di posta conteneva in origine gli elementi da ripristinare e quindi fare clic su **Ripristino**.
- Per ripristinare elementi da una casella di posta condivisa, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare la casella condivisa che originariamente conteneva gli elementi che si desidera ripristinare e quindi fare clic su **Ripristino**.
- Per ripristinare gli elementi da una casella di posta di gruppo, espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, selezionare il gruppo la cui casella di posta conteneva in origine gli elementi da ripristinare e quindi fare clic su **Ripristino**.
- Se la casella di posta utente, di gruppo o condivisa è stata eliminata, selezionarla nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.

È possibile cercare gli utenti e i gruppi per nome. I caratteri jolly non sono supportati.

4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina** > **Messaggi e-mail**.
6. Esplorare la cartella richiesta o utilizzare la ricerca per ottenere l'elenco degli elementi richiesti. Sono disponibili le opzioni di ricerca seguenti. I caratteri jolly non sono supportati.
   - Per i messaggi e-mail: ricerca per oggetto, mittente, destinatario, nome dell'allegato e data.
   - Per gli eventi: ricerca per titolo e data.
   - Per le attività: ricerca per titolo e data.
   - Per i contatti: ricerca per nome, indirizzo e-mail e numero di telefono.
7. Selezionare gli elementi che si desidera ripristinare. Per poter selezionare le cartelle, fare clic sull'icona di ripristino delle cartelle:

   Inoltre, è possibile eseguire una delle seguenti operazioni:
   - Dopo aver selezionato un elemento, fare clic su **Mostra contenuto** per visualizzarne il contenuto, inclusi gli allegati. Fare clic sul nome di un file allegato per scaricarlo.
   - Quando è selezionato un messaggio e-mail o un elemento di calendario, fare clic su **Invia come e-mail** per inviare l'elemento all'indirizzo e-mail specificato. È possibile selezionare il mittente e scrivere un testo da aggiungere all'elemento inoltrato.
   - Solo se il backup non è crittografato, è stata usata la ricerca e selezionato un unico elemento nei risultati della ricerca, è possibile fare clic su **Mostra versioni** per selezionare la versione dell'elemento da ripristinare. È possibile selezionare qualsiasi versione di cui sia stato eseguito il backup, precedente o successiva al punto di ripristino selezionato.
8. Fare clic su **Ripristina**.
9. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Exchange ospitato, fare clic su **Organizzazione di Exchange ospitato** per visualizzare, modificare o specificare l'organizzazione di destinazione.

© Acronis International GmbH, 2003-2024

Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.

10. In **Ripristina nelle caselle di posta**, visualizzare, modificare o specificare la casella di posta di destinazione.

    Per impostazione predefinita, viene selezionata la casella di posta originale. Se questa casella di posta non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare la casella di posta di destinazione.
11. [Solo quando si ripristinano gli elementi in una casella di posta utente o condivisa] In **Percorso** visualizzare o modificare la cartella di destinazione nella casella di posta di destinazione. Per impostazione predefinita, la cartella **Elementi ripristinati** è selezionata.

    Gli elementi delle caselle di posta di gruppo vengono sempre ripristinati nella cartella **Posta in arrivo**.
12. Fare clic su **Avvia ripristino**.
13. Selezionare una delle opzioni di sovrascrittura:
    - **Sovrascrivi gli elementi esistenti**
    - **Non sovrascrivere gli elementi esistenti**
14. Fare clic su **Procedi** per confermare la decisione.

Protezione dei dati di Microsoft 365

Perché eseguire il backup dei dati di Microsoft 365?

Sebbene Microsoft 365 sia un set di servizi cloud, i backup regolari forniscono un ulteriore livello di protezione dagli errori degli utenti e da azioni pericolose intenzionali. È possibile ripristinare gli elementi eliminati da un backup anche dopo la scadenza del periodo di conservazione di Microsoft 365. Inoltre, è possibile conservare una copia locale delle caselle di posta di Exchange Online se richiesto a fini di conformità alle normative.

I dati contenuti nel backup sono compressi automaticamente e occupano meno spazio nella posizione di backup rispetto a quello che occupano nella posizione originaria. Il livello di compressione per i backup cloud-to-cloud è fisso e corrisponde al livello **Normale** dei backup non cloud-to-cloud. Per ulteriori informazioni su questi livelli, consultare "Livello di compressione" (pag. 466).

Agente cloud e agente locale

Per i workload Microsoft 365 sono disponibili due agenti:

- Agente cloud

  L'agente cloud offre funzionalità di backup estese, accessibili direttamente dalla console Cyber Protect. Non è richiesta alcuna installazione. Per ulteriori informazioni, consultare "Utilizzo dell'Agente cloud per Microsoft 365" (pag. 618).

 © Acronis International GmbH, 2003-2024

- Agente locale

  L'agente locale fornisce solo il backup delle caselle di posta di Exchange Online. Questo agente deve essere installato su una macchina Windows connessa a Internet. Per ulteriori informazioni, consultare "Utilizzo dell'Agente installato in locale per Office 365" (pag. 613).

Azure Information Protection (AIP) è supportato da entrambi gli agenti.

Nota
Per i tenant in modalità Conformità è disponibile solo l'agente locale. Questi tenant possono eseguire solo il backup delle caselle di posta di Microsoft 365. Non possono utilizzare le funzionalità aggiuntive previste dall'agente cloud.

La tabella seguente riepiloga le funzionalità degli agenti.

	Agente locale	Agente cloud
Elementi dati di cui è possibile eseguire il backup	**Exchange Online:** caselle di posta utente e caselle di posta condivise (incluse caselle di posta di utenti in un piano Chiosco e caselle di posta in blocco per controversia legale)	• **Exchange Online**: ◦ caselle di posta utente e caselle di posta condivise (incluse caselle di posta di utenti in un piano Chiosco e caselle di posta in blocco per controversia legale) ◦ caselle di posta di gruppo ◦ cartelle pubbliche • **OneDrive**: file e cartelle utenti • **SharePoint Online**: ◦ raccolte siti classiche ◦ siti di gruppo (team) ◦ siti di comunicazione ◦ singoli elementi dati • **Microsoft 365 Teams**: ◦ team completi ◦ canali dei team ◦ file del canale ◦ casella di posta dei team ◦ file e messaggi e-mail nella casella di posta dei team ◦ riunioni ◦ siti dei team • **Notebook di OneNote**: come parte dei backup di OneDrive, SharePoint Online e Microsoft 365 Teams
Backup delle caselle di posta	No	Sì

© Acronis International GmbH, 2003-2024

	Agente locale	Agente cloud
di archiviazione (**In-Place Archive**)		
Pianificazione del backup	Definita dall'utente	Fino a sei volte al giorno*
Posizioni di backup	Archiviazione nel cloud, cartella locale o di rete	Solo Archiviazione nel cloud (incluso storage in hosting del Partner)
Protezione automatica di nuovi utenti, gruppi, siti e team di Microsoft 365	No	Sì, con applicazione di un piano di protezione ai gruppi **Tutti gli utenti**, **Tutti i gruppi**, **Tutti i siti**, **Tutti i team**
Protezione di più di una organizzazione di Microsoft 365	No	Sì
Ripristino granulare	Sì	Sì
Ripristino in altro utente di un'organizzazione	Sì	Sì
Ripristino in altra organizzazione	No	Sì
Ripristino di un server Microsoft Exchange locale	No	No
Numero massimo di elementi di cui è possibile eseguire il backup senza impatto sulle prestazioni	Durante il backup nell'archivio nel cloud: 5.000 caselle di posta per azienda Quando si esegue il backup in altre destinazioni: 2.000 caselle di posta per piano di protezione (senza limiti al numero di caselle di posta per azienda)	10.000 elementi protetti (caselle di posta, OneDrive o siti) per azienda**
Numero massimo di esecuzioni di backup manuali	No	10 esecuzioni manuali in un'ora
Numero massimo di operazioni di ripristino simultanee	No	10 operazioni, incluse quelle di ripristino di Google Workspace

***** L'opzione predefinita è **Una volta al giorno**. Con il pacchetto Advanced Backup è possibile pianificare un massimo di sei backup giornalieri. I backup si avviano a intervalli approssimativi che dipendono dal carico corrente dell'agente cloud, che serve più clienti in un data center. Ciò

© Acronis International GmbH, 2003-2024

garantisce un'equa distribuzione del carico durante il giorno e un'equa qualità del servizio per tutti i clienti.

Nota
Sulla pianificazione della protezione potrebbero avere impatto le attività di servizi di terze parti, ad esempio l'accessibilità dei server di Microsoft 365, le impostazioni relative alla limitazione di banda nei server Microsoft, e altro ancora. Vedere anche https://docs.microsoft.com/en-us/graph/throttling.

** Si consiglia di eseguire il backup degli elementi protetti gradualmente e seguendo questo ordine:

1. Caselle di posta.
2. Dopo aver eseguito il backup di tutte le caselle di posta, procedere con OneDrive.
3. Dopo aver completato il backup di OneDrive, procedere con i siti di SharePoint Online.

A seconda del numero di elementi protetti e della loro dimensione, il primo backup completo può richiedere alcuni giorni.

Diritti utente necessari

In Cyber Protection

L'agente locale deve essere registrato in un account di amministratore dell'azienda e utilizzato a livello di tenant del cliente. Gli amministratori dell'azienda che agiscono a livello di unità, gli amministratori di unità e gli utenti non possono eseguire il backup o il recupero di dati di Microsoft 365.

L'agente cloud può essere utilizzato sia a livello di tenant cliente che a livello di unità. Per ulteriori informazioni sui livelli e sui rispettivi amministratori, consultare "Amministrazione di organizzazioni di Microsoft 365 aggiunte su diversi livelli" (pag. 619).

In Microsoft 365

All'account deve essere assegnato il ruolo Amministratore globale in Microsoft 365.

Per individuare ed eseguire il backup e il ripristino di cartelle pubbliche di Microsoft 365, almeno uno degli account amministratore di Microsoft 365 deve disporre di una casella di posta e di diritti di lettura e scrittura sulle cartelle pubbliche di cui eseguire il backup.

- L'agente locale eseguirà l'accesso a Microsoft 365 utilizzando tale account. Per abilitare l'accesso dell'agente ai contenuti di tutte le caselle di posta, all'account verrà assegnato il ruolo di gestione **ApplicationImpersonation** (Rappresentazione dell'applicazione). Se si modifica la password dell'account, aggiornare la password nella console di Cyber Protect come descritto in "Modifica delle credenziali di accesso di Microsoft 365" (pag. 615).
- L'agente cloud non accede a Microsoft 365. È necessario accedere una volta a Microsoft 365 come amministratore globale per concedere all'agente cloud le autorizzazioni necessarie al suo

© Acronis International GmbH, 2003-2024

funzionamento.

In Microsoft 365 sono necessarie le autorizzazioni seguenti:

- Accedere e leggere i profili degli utenti
- Leggere e scrivere file in tutte le raccolte di siti
- Leggere e scrivere i profili completi di tutti gli utenti
- Leggere e scrivere tutti i gruppi
- Leggere i dati della directory
- Leggere tutti i messaggi del canale
- Leggere e scrivere i metadati gestiti
- Leggere e scrivere elementi ed elenchi in tutte le raccolte di siti
- Avere il pieno controllo di tutte le raccolte di siti
- Leggere e scrivere elementi in tutte le raccolte di siti
- Utilizzare Exchange Web Services con accesso completo a tutte le caselle di posta

- L'agente cloud non memorizza le credenziali dell'account e non le utilizza per eseguire attività di backup e ripristino. La modifica delle credenziali, la disabilitazione o l'eliminazione dell'account non hanno conseguenze sul funzionamento dell'agente cloud.

Limitazioni

- Con l'agente locale è possibile proteggere fino a 5.000 workload. L'agente cloud consente invece di proteggere fino a 50.000 workload.
- Nella console di Cyber Protect vengono visualizzati tutti gli utenti che dispongono di una casella di posta o OneDrive, inclusi gli utenti senza una licenza di Microsoft 365 e gli utenti a cui è impedita l'iscrizione ai servizi di Microsoft 365.
- Il backup delle caselle di posta include solo le cartelle visibili agli utenti. La cartella **Elementi ripristinabili** e le relative cartelle secondarie (**Eliminazioni**, **Versioni**, **Ripuliture**, **Controlli**, **Blocco di individuazione**, **Registrazione del calendario**) non vengono incluse nel backup della casella di posta.
- La creazione automatica di utenti, gruppi, siti o cartelle pubbliche durante un ripristino non è consentita. Se, ad esempio, si desidera ripristinare un sito di SharePoint Online che è stato eliminato, creare innanzitutto un nuovo sito manualmente, quindi specificarlo come sito di destinazione durante il ripristino.
- Non è possibile ripristinare simultaneamente elementi da punti di ripristino differenti, anche se è possibile selezionare tali elementi nei risultati della ricerca.
- Durante il backup, verranno conservate tutte le etichette di riservatezza applicate al contenuto. Pertanto, i contenuti riservati potrebbero non essere visualizzati se vengono ripristinati in una posizione non originale, e se il rispettivo utente dispone di autorizzazioni di accesso differenti.
- Non è possibile applicare più di un piano di backup allo stesso workload.

© Acronis International GmbH, 2003-2024

- Se un piano di backup singolo e un piano di backup di gruppo vengono applicati allo stesso workload, le impostazioni del piano singolo avranno priorità.

Report sul licensing delle utenze di Microsoft 365

Gli amministratori dell'azienda possono scaricare un report sulle utenze di Microsoft 365 protette e sulla gestione del rispettivo licensing. Il report è in formato CSV e include informazioni sullo stato delle licenze e sulla loro ragione di utilizzo. Il report include anche il nome dell'utenza protetta, l'e-mail associata, il gruppo, l'organizzazione Microsoft 365, il nome e il tipo di workload protetto.

Tale report è disponibile solo per i tenant in cui è registrata un'organizzazione Microsoft 365.

Per scaricare il report sul licensing delle utenze di Microsoft 365

1. Accedere alla console di Cyber Protect come amministratore aziendale.
2. Fare clic sull'icona dell'account nell'angolo in alto a destra.
3. Fare clic su **Report sul licensing delle utenze di Microsoft 365**.

Registrazione

Le azioni compiute con le risorse cloud-to-cloud, come la visualizzazione del contenuto di e-mail di cui è stato eseguito il backup, il download di allegati o file, il ripristino di e-mail in caselle di posta diverse da quella originaria o il loro invio come e-mail, possono violare la privacy degli utenti. Queste azioni vengono registrate nel portale di gestione, in **Monitoraggio** > **Registro di audit**.

Utilizzo dell'Agente installato in locale per Office 365

Aggiunta di un'organizzazione di Microsoft 365

Per aggiungere un'organizzazione di Microsoft 365

1. Accedere alla console di Cyber Protect come amministratore aziendale.
2. Fare clic sull'icona dell'account nell'angolo in alto a destra, quindi su **Download** > **Agente per Office 365**.
3. Scaricare l'agente e installarlo nel sistema Windows connesso a Internet.
4. Nella console di Cyber Protect, passare a **Dispositivi** > **Microsoft Office 365 (agente locale)**.
5. Nella finestra visualizzata, immettere l'ID e il segreto dell'applicazione, e l'ID del tenant Microsoft 365. Per ulteriori informazioni su come ottenere queste informazioni, fare riferimento a "Come ottenere l'ID e il segreto dell'applicazione" (pag. 614).
6. Fare clic su **OK**.

Gli elementi dati dell'organizzazione vengono visualizzati nella console di Cyber Protect, nella scheda **Microsoft Office 365 (agente locale)**.

© Acronis International GmbH, 2003-2024

Importante
In un'organizzazione (gruppo aziendale) deve essere presente un unico Agente per Office 365 in locale.

Come ottenere l'ID e il segreto dell'applicazione

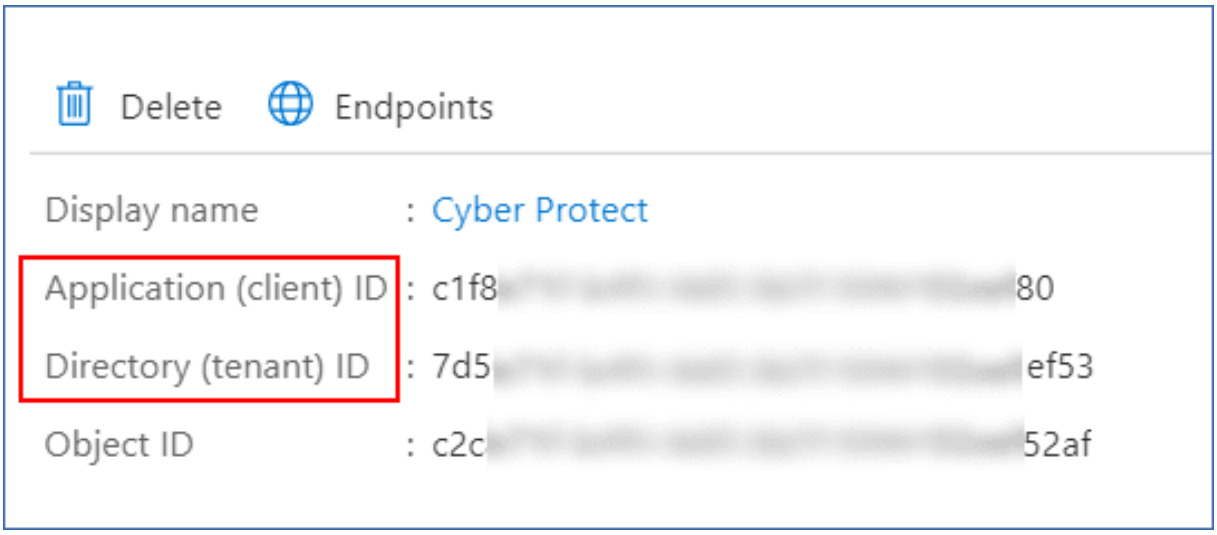
Per utilizzare l'autenticazione più recente per Office 365, è necessario creare un'applicazione personalizzata nell'interfaccia di amministrazione di Entra e garantire a questa autorizzazioni API specifiche. In questo modo è possibile acquisire l'**ID dell'applicazione**, **il segreto dell'applicazione** e l'**ID (tenant) della directory** necessari per accedere alla console di Cyber Protect.

Nota
Sul sistema in cui è installato l'Agente per Office 365, verificare di poter accedere a graph.microsoft.com tramite la porta 443.

Per creare un'applicazione nell'interfaccia di amministrazione di Entra

1. Accedere all'interfaccia di amministrazione di Entra come amministratore.
2. Passare ad **Azure Active Directory** > **Registrazioni app**, quindi fare clic su **Nuova registrazione**.
3. Specificare un nome per l'applicazione personalizzata, ad esempio, Cyber Protection.
4. In **Tipi di account supportati**, selezionare **Account solo in questa directory organizzativa**.
5. Fare clic su **Registra**.

L'applicazione è stata creata. Nell'interfaccia di amministrazione di Entra, passare alla pagina **Panoramica** dell'applicazione e controllare l'ID dell'applicazione (client) e l'ID della directory (tenant).



Per ulteriori informazioni su come creare un'applicazione nell'interfaccia di amministrazione di Entra, consultare la documentazione Microsoft.

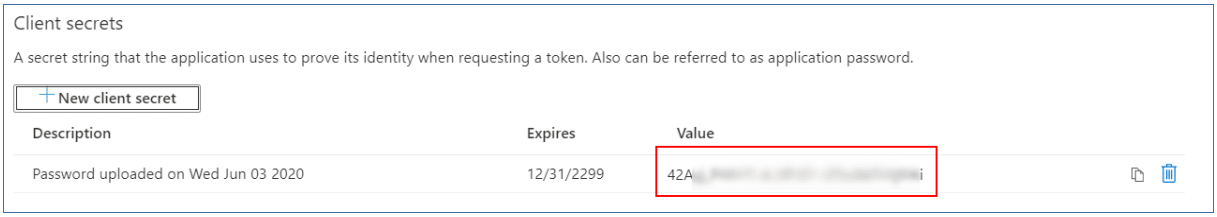
© Acronis International GmbH, 2003-2024

Per concedere all'applicazione le autorizzazioni API necessarie

1. Nell'interfaccia di amministrazione di Entra, passare alle **Autorizzazioni API** dell'applicazione, quindi fare clic su **Aggiungi un'autorizzazione**.
2. Selezionare la scheda delle **API utilizzate nell'organizzazione**, quindi individuare **Office 365 Exchange Online**.
3. Fare clic su **Office 365 Exchange Online** e quindi su **Autorizzazioni applicazione**.
4. Selezionare la casella di controllo **full_access_as_app** e fare clic su **Aggiungi autorizzazioni**.
5. In **Autorizzazioni API**, fare clic su **Aggiungi un'autorizzazione**.
6. Selezionare **Microsoft Graph**.
7. Selezionare **Autorizzazioni applicazione**.
8. Espandere la scheda **Directory** e quindi selezionare la casella di controllo **Directory.Read.All**. Fare clic su **Aggiungi autorizzazioni**.
9. Verificare tutte le autorizzazioni, quindi selezionare **Concedi consenso amministratore per <nome dell'applicazione>**.
10. Confermare la selezione facendo clic su **Sì**.

Per creare segreto dell'applicazione

1. Nell'interfaccia di amministrazione di Entra, passare a **Certificati e segreti** > **Nuovo segreto client**.
2. Nella casella di dialogo visualizzata, selezionare Scadenza: **Mai**, quindi fare clic su **Aggiungi**.
3. Controllare il segreto dell'applicazione nel campo **Valore** e verificare di ricordarlo.



Per ulteriori informazioni sul segreto dell'applicazione, fare riferimento alla documentazione Microsoft.

Modifica delle credenziali di accesso di Microsoft 365

È possibile modificare le credenziali di accesso di Microsoft 365 senza reinstallare l'agente.

Per modificare le credenziali di accesso di Microsoft 365

1. Fare clic su **Dispositivi** > **Microsoft Office 365 (agente locale)**.
2. Selezionare l'organizzazione Microsoft 365.
3. Fare clic su **Specifica credenziali**.
4. Immettere l'ID e il segreto dell'applicazione, e l'ID del tenant Microsoft 365. Per ulteriori informazioni su come ottenere queste informazioni, fare riferimento a "Come ottenere l'ID e il

© Acronis International GmbH, 2003-2024

segreto dell'applicazione" (pag. 614).

5. Fare clic su **OK**.

Protezione delle caselle di posta di Exchange Online

Di quali elementi è possibile eseguire il backup?

È possibile eseguire il backup delle caselle di posta utente e delle caselle condivise. Non è possibile eseguire il backup delle caselle di posta di archiviazione (**In-Place Archive**) e delle caselle di posta di gruppo.

Quali elementi è possibile ripristinare?

Dal backup di una casella postale è possibile ripristinare i seguenti elementi:

- Caselle postali
- Cartelle e-mail
- Messaggi e-mail
- Eventi di calendario
- Attività
- Contatti
- Voci del diario
- Note

È possibile utilizzare la ricerca per individuare gli elementi.

Quando una casella di posta viene ripristinata in una casella di posta esistente, vengono sovrascritti gli elementi già esistenti con ID corrispondenti.

Il ripristino di elementi di caselle di posta non sovrascrive alcun elemento. Il percorso completo di un elemento della casella di posta viene invece ricreato nella cartella di destinazione.

Selezione delle caselle di posta di Microsoft 365

Selezionare le caselle di posta come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Per selezionare le caselle di posta

1. Fare clic su **Microsoft Office 365 (agente locale)**.
2. Selezionare le caselle di posta di cui si desidera eseguire il backup.
3. Fare clic su **Backup**.

© Acronis International GmbH, 2003-2024

Ripristino di caselle postali e di elementi delle caselle postali

Ripristino delle caselle postali

1. Fare clic su **Microsoft Office 365 (agente locale)**.
2. Selezionare la casella di posta da ripristinare e fare clic su **Ripristino**.
   È possibile cercare le caselle di posta per nome. I caratteri jolly non sono supportati.
   Se la casella di posta è stata eliminata, selezionarla nella scheda Archivio di backup, quindi fare clic su **Mostra backup**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.
4. Fare clic su **Ripristina** > **Casella di posta**.
5. In **Cassetta postale di destinazione**, visualizzare, cambiare o specificare la casella di posta di destinazione.
   Per impostazione predefinita, viene selezionata la casella di posta originale. Se tale casella di posta non esiste, è necessario specificare la casella di posta di destinazione.
6. Fare clic su **Avvia ripristino**.

Ripristino di elementi di casella di posta

1. Fare clic su **Microsoft Office 365 (agente locale)**.
2. Selezionare la casella di posta che conteneva in origine gli elementi da ripristinare, quindi fare clic su **Ripristino**.
   È possibile cercare le caselle di posta per nome. I caratteri jolly non sono supportati.
   Se la casella di posta è stata eliminata, selezionarla nella scheda Archivio di backup, quindi fare clic su **Mostra backup**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.
4. Fare clic su **Ripristina** > **Messaggi e-mail**.
5. Selezionare gli elementi che si desidera ripristinare.
   Sono disponibili le opzioni di ricerca seguenti. I caratteri jolly non sono supportati.
   - Per i messaggi e-mail: ricerca per oggetto, mittente, destinatario, nome dell'allegato e data.
   - Per gli eventi: ricerca per titolo e data.
   - Per le attività: ricerca per titolo e data.
   - Per i contatti: ricerca per nome, indirizzo e-mail e numero di telefono.

   Quando è selezionato un messaggio e-mail, è possibile fare clic su **Mostra il contenuto** per visualizzarne il contenuto, inclusi gli allegati.

© Acronis International GmbH, 2003-2024

Nota
Fare clic sul nome di un file allegato per scaricarlo.

Quando è selezionato un messaggio e-mail, è possibile fare clic su **Invia come e-mail** per inviare il messaggio a un indirizzo e-mail. Il messaggio verrà inviato dall'indirizzo e-mail dell'account di amministratore.

Per poter selezionare le cartelle, fare clic sull'icona di ripristino delle cartelle:

6. Fare clic su **Ripristina**.
7. In **Cassetta postale di destinazione**, visualizzare, cambiare o specificare la casella di posta di destinazione.
   Per impostazione predefinita, viene selezionata la casella di posta originale. Se tale casella di posta non esiste, è necessario specificare la casella di posta di destinazione.
8. Fare clic su **Avvia ripristino**.
9. Confermare la propria decisione.

Gli elementi delle caselle di posta vengono sempre ripristinati nella cartella **Elementi ripristinati** della casella di posta di destinazione.

Utilizzo dell'Agente cloud per Microsoft 365

Aggiunta di un'organizzazione di Microsoft 365

Un amministratore può aggiungere una o più organizzazioni di Microsoft 365 a un tenant cliente o a un'unità.

Gli amministratori dell'azienda aggiungono le organizzazioni ai tenant cliente. Gli amministratori di unità e gli amministratori di clienti che agiscono a livello di unità aggiungono le organizzazioni alle unità.

Per aggiungere un'organizzazione di Microsoft 365

1. A seconda della posizione in cui si deve aggiungere l'organizzazione, accedere alla console di Cyber Protect come amministratore dell'azienda o amministratore di unità.
2. [Per gli amministratori dell'azienda che agiscono a livello di unità] Nel portale di gestione, navigare fino all'unità desiderata.
3. Fare clic su **Dispositivi** > **Aggiungi** > **Microsoft 365 Business**.
   Il software reindirizza alla pagina di accesso di Microsoft 365.
4. Accedere a Microsoft 365 con le credenziali di amministratore globale.
   Microsoft 365 visualizza l'elenco di autorizzazioni necessarie per eseguire il backup e il ripristino dei dati dell'organizzazione.
5. Confermare la concessione di tali autorizzazioni al servizio Cyber Protection.

© Acronis International GmbH, 2003-2024

L'organizzazione di Microsoft 365 viene visualizzata nella scheda **Dispositivi** della console di Cyber Protect.

Suggerimenti utili

- L'agente cloud esegue la sincronizzazione con Microsoft 365 ogni 24 ore, a partire dal momento in cui l'organizzazione è aggiunta al servizio Cyber Protection. Se un utente, un gruppo o un sito vengono rimossi, la modifica non viene immediatamente visualizzata nella console di Cyber Protect. Per sincronizzare immediatamente la modifica, selezionare l'organizzazione nella pagina di **Microsoft 365** quindi fare clic su **Aggiorna**.

  Per ulteriori informazioni sulla sincronizzazione delle risorse di un'organizzazione Microsoft 365 e la console di Cyber Protect, fare riferimento a "Individuazione delle risorse di Microsoft 365" (pag. 620).
- Se è stato applicato un piano di protezione al gruppo **Tutti gli utenti**, **Tutti i gruppi** o **Tutti i siti**, gli elementi appena aggiunti vengono inclusi nel backup solo dopo la sincronizzazione.
- In base alla policy di Microsoft, quando un utente, un gruppo o un sito sono rimossi dall'interfaccia utente grafica di Microsoft 365, restano disponibili per qualche giorno tramite l'API. In questo periodo l'elemento rimosso è inattivo (mostrato in grigio) nella console di Cyber Protect e non ne viene eseguito il backup. Quando l'elemento rimosso non è più disponibile neanche tramite l'API, non sarà più visualizzato nella console di Cyber Protect. I relativi backup (se presenti) sono reperibili in **Archivi di backup** > **Backup di applicazioni cloud**.

Amministrazione di organizzazioni di Microsoft 365 aggiunte su diversi livelli

Gli amministratori dell'azienda hanno accesso completo alle organizzazioni di Microsoft 365 che sono aggiunte a livello di tenant cliente.

Gli amministratori dell'azienda hanno accesso limitato alle organizzazioni aggiunte a un'unità. In queste organizzazioni, mostrate con il nome dell'unità tra parentesi, gli amministratori dell'azienda possono eseguire le attività indicate di seguito:

- Ripristinare i dati dai backup.

  Gli amministratori dell'azienda possono ripristinare i dati in tutte le organizzazioni del tenant, indipendente dal livello nel quale tali organizzazioni sono aggiunte.
- Sfogliare i backup e i punti di ripristino nei backup.
- Eliminare i backup e i punti di ripristino nei backup.
- Visualizzare avvisi e attività.

Gli amministratori dell'azienda, quando agiscono a livello di tenant cliente, non possono eseguire le attività indicate di seguito:

- Aggiungere un'organizzazione di Microsoft 365 alle unità.
- Eliminare un'organizzazione di Microsoft 365 dalle unità.
- Sincronizzare le organizzazioni di Microsoft 365 che sono state aggiunte a un'unità.

© Acronis International GmbH, 2003-2024

- Visualizzare, creare, modificare, eliminare, applicare, eseguire o revocare i piani di protezione per gli elementi dati nelle organizzazioni di Microsoft 365 che sono state aggiunte a un'unica.

Gli amministratori dell'azienda e gli amministratori di unità che agiscono a livello di unità hanno accesso completo alle organizzazioni aggiunte a un'unità. Non hanno tuttavia accesso a nessuna delle risorse del tenant cliente padre, inclusi i piani di protezione in esso creati.

Eliminare un'organizzazione di Microsoft 365

L'eliminazione di un'organizzazione di Microsoft 365 non incide sui backup esistenti dei dati dell'organizzazione. Se questi backup non sono più necessari, prima eliminarli e quindi eliminare l'organizzazione di Microsoft 365. In caso contrario, i backup continueranno utilizzare lo spazio di archiviazione nel cloud, che potrebbe essere soggetto fatturazione.

Per ulteriori informazioni su come eliminare i backup, vedere "Per eliminare backup o archivi di backup" (pag. 542).

Per eliminare un'organizzazione di Microsoft 365

1. A seconda della posizione in cui è aggiunta l'organizzazione, accedere alla console di Cyber Protect come amministratore dell'azienda o amministratore di unità.
2. [Per gli amministratori dell'azienda che agiscono a livello di unità] Nel portale di gestione, navigare fino all'unità desiderata.
3. Passare a **Dispositivi** > **Microsoft 365**.
4. Selezionare l'organizzazione e quindi fare clic su **Elimina gruppo**.

I piani di backup applicati al gruppo verranno revocati.

È inoltre necessario revocare manualmente i diritti di accesso dell'applicazione Servizio Backup ai dati dell'organizzazione Microsoft 365.

Per revocare i diritti di accesso

1. Accedere a Microsoft 365 con un ruolo di amministratore globale.
2. Passare a **Interfaccia di amministrazione** > **Azure Active Directory** > **Applicazioni aziendali** > **Tutte le applicazioni**.
3. Selezionare l'applicazione **Servizio Backup** e navigare nei vari livelli.
4. Passare alla scheda **Proprietà** e nel pannello di azione fare clic su **Elimina**.
5. Confermare l'eliminazione.

I diritti di accesso ai dati dell'organizzazione Microsoft 365 verranno revocati dall'applicazione Servizio Backup.

Individuazione delle risorse di Microsoft 365

Quando si aggiunge un'organizzazione Microsoft 365 al servizio Cyber Protection, le risorse di questa organizzazione, come le caselle di posta, gli storage OneDrive, Microsoft Teams e i siti

© Acronis International GmbH, 2003-2024

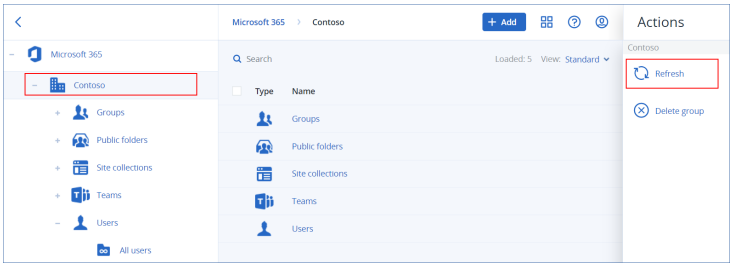
SharePoint, vengono sincronizzate con la console di Cyber Protect. Questa operazione è chiamata individuazione e viene registrata in **Monitoraggio** > **Attività**.

Una volta completata l'operazione di individuazione, le risorse dell'organizzazione Microsoft 365 sono visualizzate nella scheda **Dispositivi** > **Microsoft 365** nella console di Cyber Protect, ed è possibile applicare a queste i piani di backup.

Una volta al giorno, viene eseguita un'operazione di individuazione automatica, per garantire che l'elenco delle risorse nella console di Cyber Protect sia sempre aggiornato. È anche possibile sincronizzare l'elenco su richiesta, avviando manualmente l'operazione di individuazione.

Per eseguire manualmente l'operazione di individuazione

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Microsoft 365**.
2. Selezionare l'organizzazione Microsoft 365 e quindi nel pannello **Azioni**, fare clic su **Aggiorna**.



Nota
È possibile eseguire manualmente un'operazione di individuazione fino a 10 volte in un'ora. Una volta raggiunto questo numero, il numero di esecuzioni consentite viene ripristinato a una per ora, e da questo momento in poi è possibile eseguire un'esecuzione aggiuntiva ogni ora, fino a quando non viene raggiunto di nuovo il totale di 10 esecuzioni per ora.

Impostazione della frequenza dei backup di Microsoft 365

Per impostazione predefinita, i backup di Microsoft 365 vengono eseguiti una volta al giorno e non sono disponibili ulteriori opzioni di pianificazione.

Se nel tenant è abilitato il pacchetto Advanced Backup, è possibile configurare backup più frequenti. È possibile selezionare il numero di backup quotidiani, ma non l'orario di avvio del backup. I backup si avviano automaticamente a intervalli approssimativi che dipendono dal carico corrente dell'agente cloud, che serve più clienti in un data center. Ciò garantisce un'equa distribuzione del carico durante il giorno e un'equa qualità del servizio per tutti i clienti.

Sono disponibili le seguenti opzioni.

Opzioni di pianificazione	Intervallo approssimativo tra ciascun backup
Una volta al giorno	24 ore
Due volte al giorno (predefinito)	12 ore

© Acronis International GmbH, 2003-2024

Opzioni di pianificazione	Intervallo approssimativo tra ciascun backup
3 volte al giorno	8 ore
6 volte al giorno	4 ore

Nota
A seconda del carico sull'agente cloud e della possibile limitazione di banda sul lato Microsoft 365, un backup potrebbe iniziare più tardi del previsto o richiedere più tempo per essere completato. Se il backup dura di più rispetto all'intervallo medio tra due backup, il backup successivo verrà ripianificato, il che potrebbe risultare in un numero di backup al giorno inferiore rispetto a quanto selezionato. Ad esempio, potrebbe essere possibile completare solo due backup al giorno, anche se ne sono stati selezionati sei al giorno.

I backup delle caselle di posta di gruppo possono essere eseguiti una sola volta al giorno.

Protezione dei dati di Exchange Online

Di quali elementi è possibile eseguire il backup?

È possibile eseguire il backup delle caselle di posta utente, di gruppo e condivise. Facoltativamente, è possibile scegliere di eseguire il backup delle caselle di posta di archiviazione online (**Archivio sul posto**) delle caselle di posta selezionate.

A partire dalla versione 8.0 del servizio Cyber Protection, è possibile eseguire il backup di cartelle pubbliche. Se l'organizzazione è stata aggiunta al servizio Cyber Protection prima del rilascio della versione 8.0, è necessario riaggiungere l'organizzazione per disporre di questa funzionalità. Non eliminare l'organizzazione ma ripetere semplicemente i passaggi descritti in "Aggiunta di un'organizzazione di Microsoft 365" (pag. 618). Il servizio Cyber Protection ottiene l'autorizzazione per utilizzare l'API corrispondente.

Quali elementi è possibile ripristinare?

Dal backup di una casella postale è possibile ripristinare i seguenti elementi:

- Caselle postali
- Cartelle e-mail
- Messaggi e-mail
- Eventi di calendario
- Attività
- Contatti
- Voci del diario
- Note

Dal backup di una cartella pubblica è possibile ripristinare i seguenti elementi:

© Acronis International GmbH, 2003-2024

- Cartelle secondarie
- Post
- Messaggi e-mail

È possibile utilizzare la ricerca per individuare gli elementi.

Durante il ripristino di caselle di posta, elementi delle caselle di posta, cartelle pubbliche e elementi delle cartelle pubbliche, è possibile selezionare se sovrascrivere o meno gli elementi nella posizione di destinazione.

Selezione delle caselle di posta

Selezionare le caselle di posta come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Per selezionare le caselle di posta di Exchange Online

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione i cui dati utente devono essere sottoposti a backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per eseguire il backup delle caselle di posta di tutti gli utenti e di tutte le caselle condivise (incluse quelli che verranno create in futuro), espandere il nodo **Utenti**, selezionare **Tutti gli utenti** e quindi fare clic su **Raggruppa backup**.
   - Per eseguire il backup di singole caselle di posta utente o di caselle condivise, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare gli utenti la cui casella di posta si desidera sottoporre a backup e quindi fare clic su **Backup**.
   - Per eseguire il backup delle caselle di posta di tutti i gruppi (incluse quelli dei gruppi che verranno creati in futuro), espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, quindi fare clic su **Raggruppa backup**.
   - Per eseguire il backup di singole caselle di posta di gruppo, espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, selezionare i gruppi le cui caselle di posta si desidera sottoporre a backup e quindi fare clic su **Backup**.

     Nota
     Per accedere alla casella di posta di un gruppo, l'Agente cloud per Microsoft 365 utilizza un account con i diritti appropriati. Pertanto, per eseguire il backup di una casella di posta di gruppo, almeno uno dei proprietari del gruppo deve essere un utente di Microsoft 365 con licenza e disporre di una casella di posta. Se il gruppo è privato o con appartenenza nascosta, il proprietario deve essere anche membro del gruppo.

4. Nel pannello del piano di protezione:
   - Verificare che l'elemento **Caselle di posta di Microsoft 365** sia selezionato in **Cosa includere nel backup**.

© Acronis International GmbH, 2003-2024

Se per alcuni degli utenti selezionati singolarmente il servizio Exchange non è incluso nel relativo piano di Microsoft 365, non sarà possibile selezionare questa opzione.

Se per alcuni degli utenti selezionati per il backup di gruppo il servizio Exchange non è incluso nel relativo piano di Microsoft 365, sarà possibile selezionare questa opzione, ma il piano di protezione non verrà applicato a tali utenti.

- Se non si desidera eseguire il backup delle caselle di posta di archiviazione, disattivare l'opzione **Casella di posta di archiviazione**.

Selezione di cartelle pubbliche

Selezionare le cartelle pubbliche come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Nota
Le cartelle pubbliche utilizzano le licenze della quota di backup delle utenze di Microsoft 365.

Per selezionare cartelle pubbliche di Exchange Online

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, espandere l'organizzazione i cui dati devono essere sottoposti a backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Cartelle pubbliche** quindi selezionare **Tutte le cartelle pubbliche**.
4. Eseguire una delle seguenti operazioni:
   - Per eseguire il backup di tutte le cartelle pubbliche (incluse quelle che verranno create in futuro), fare clic su **Raggruppa backup**.
   - Per eseguire il backup di singole cartelle pubbliche, selezionare le cartelle pubbliche di cui eseguire il backup, quindi fare clic su **Backup**.
5. Nel riquadro del piano di protezione, verificare che l'elemento **Caselle di posta di Microsoft 365** sia selezionato in **Cosa includere nel backup**.

Ripristino di caselle postali e di elementi delle caselle postali

Ripristino delle caselle postali

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per ripristinare una casella di posta utente, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente la cui casella di posta si desidera ripristinare e quindi fare clic su **Ripristino**.

© Acronis International GmbH, 2003-2024

- Per ripristinare una casella di posta condivisa, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare la casella condivisa che si desidera ripristinare e quindi fare clic su **Ripristino**.
- Per ripristinare una casella di posta di gruppo, espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, selezionare il gruppo la cui casella di posta si desidera ripristinare e quindi fare clic su **Ripristino**.
- Se la casella di posta utente, di gruppo o condivisa è stata eliminata, selezionarla nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.

È possibile cercare gli utenti e i gruppi per nome. I caratteri jolly non sono supportati.

4. Selezionare un punto di ripristino.

   Nota
   Per visualizzare solo i punti di ripristino che contengono caselle di posta, selezionare **Caselle di posta** in **Filtra per contenuto**.

5. Fare clic su **Ripristina** > **Intera casella di posta**.
6. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.

   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.
7. In **Ripristina nelle caselle di posta**, visualizzare, modificare o specificare la casella di posta di destinazione.

   Per impostazione predefinita, viene selezionata la casella di posta originale. Se questa casella di posta non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare la casella di posta di destinazione.

   Durante il ripristino non è possibile creare una nuova casella di posta di destinazione. Per ripristinare una casella di posta in una nuova, è necessario innanzitutto creare la casella di posta di destinazione nell'organizzazione Microsoft 365 desiderata, quindi attendere che l'agente cloud sincronizzi la modifica. L'agente cloud esegue automaticamente la sincronizzazione con Microsoft 365 ogni 24 ore. Per sincronizzare immediatamente la modifica, nella console di Cyber Protect selezionare l'organizzazione nella pagina di **Microsoft 365** quindi fare clic su **Aggiorna**.
8. Fare clic su **Avvia ripristino**.
9. Selezionare una delle opzioni di sovrascrittura:
   - **Sovrascrivi gli elementi esistenti**
   - **Non sovrascrivere gli elementi esistenti**
10. Fare clic su **Procedi** per confermare la decisione.

© Acronis International GmbH, 2003-2024

Ripristino di elementi di casella di posta

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per ripristinare gli elementi da una casella di posta utente, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente la cui casella di posta conteneva in origine gli elementi da ripristinare e quindi fare clic su **Ripristino**.
   - Per ripristinare elementi da una casella di posta condivisa, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare la casella condivisa che originariamente conteneva gli elementi che si desidera ripristinare e quindi fare clic su **Ripristino**.
   - Per ripristinare gli elementi da una casella di posta di gruppo, espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, selezionare il gruppo la cui casella di posta conteneva in origine gli elementi da ripristinare e quindi fare clic su **Ripristino**.
   - Se la casella di posta utente, di gruppo o condivisa è stata eliminata, selezionarla nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.

   È possibile cercare gli utenti e i gruppi per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.

   Nota
   Per visualizzare solo i punti di ripristino che contengono caselle di posta, selezionare **Caselle di posta** in **Filtra per contenuto**.

5. Fare clic su **Ripristina** > **Messaggi e-mail**.
6. Esplorare la cartella richiesta o utilizzare la ricerca per ottenere l'elenco degli elementi richiesti.

   Sono disponibili le opzioni di ricerca seguenti. I caratteri jolly non sono supportati.
   - Per i messaggi e-mail: ricerca per oggetto, mittente, destinatario, nome dell'allegato e data. È possibile selezionare una data di inizio o una data di fine (entrambe comprese) oppure entrambe le date per effettuare una ricerca in un intervallo di tempo.
   - Per gli eventi: ricerca per titolo e data.
   - Per le attività: ricerca per titolo e data.
   - Per i contatti: ricerca per nome, indirizzo e-mail e numero di telefono.
7. Selezionare gli elementi che si desidera ripristinare. Per poter selezionare le cartelle, fare clic sull'icona di ripristino delle cartelle:

   Durante il ripristino non è possibile creare una nuova casella di posta di destinazione. Per ripristinare un nuovo elemento di una casella di posta in una nuova, è necessario innanzitutto creare l'elemento della casella di posta di destinazione nell'organizzazione Microsoft 365, quindi

© Acronis International GmbH, 2003-2024

attendere che l'agente cloud sincronizzi la modifica.L'agente cloud esegue automaticamente la sincronizzazione con Microsoft 365 ogni 24 ore. Per sincronizzare immediatamente la modifica, nella console di Cyber Protect selezionare l'organizzazione nella pagina di **Microsoft 365** quindi fare clic su **Aggiorna**.

Inoltre, è possibile eseguire una delle seguenti operazioni:

- Dopo aver selezionato un elemento, fare clic su **Mostra contenuto** per visualizzarne il contenuto, inclusi gli allegati. Fare clic sul nome di un file allegato per scaricarlo.
- Quando è selezionato un messaggio e-mail o un elemento di calendario, fare clic su **Invia come e-mail** per inviare l'elemento all'indirizzo e-mail specificato. È possibile selezionare il mittente e scrivere un testo da aggiungere all'elemento inoltrato.
- Solo se il backup non è crittografato, è stata usata la ricerca e selezionato un unico elemento nei risultati della ricerca, è possibile fare clic su **Mostra versioni** per selezionare la versione dell'elemento da ripristinare. È possibile selezionare qualsiasi versione di cui sia stato eseguito il backup, precedente o successiva al punto di ripristino selezionato.

8. Fare clic su **Ripristina**.
9. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.

   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.
10. In **Ripristina nelle caselle di posta**, visualizzare, modificare o specificare la casella di posta di destinazione.

    Per impostazione predefinita, viene selezionata la casella di posta originale. Se questa casella di posta non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare la casella di posta di destinazione.
11. [Solo quando si ripristinano gli elementi in una casella di posta utente o condivisa] In **Percorso** visualizzare o modificare la cartella di destinazione nella casella di posta di destinazione. Per impostazione predefinita, la cartella **Elementi ripristinati** è selezionata.

    Gli elementi delle caselle di posta di gruppo vengono sempre ripristinati nella cartella **Posta in arrivo**.
12. Fare clic su **Avvia ripristino**.
13. Selezionare una delle opzioni di sovrascrittura:
    - **Sovrascrivi gli elementi esistenti**
    - **Non sovrascrivere gli elementi esistenti**
14. Fare clic su **Procedi** per confermare la decisione.

© Acronis International GmbH, 2003-2024

Ripristino di intere caselle di posta in file di dati PST

Nota
Non è possibile ripristinare un archivio sul posto come parte di un ripristino su file PST. Per ripristinare l'archivio sul posto insieme alla casella di posta, consultare "Ripristino delle caselle postali" (pag. 624).

Per ripristinare una casella di posta

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per ripristinare una casella di posta di un utente in un file di dati PST, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare la casella di posta da ripristinare e quindi fare clic su **Ripristino**.
   - Per ripristinare una casella di posta condivisa in un file di dati PST, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare la casella di posta da ripristinare e quindi fare clic su **Ripristino**.
   - Per ripristinare una casella di posta di gruppo in un file di dati PST, espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, selezionare il gruppo la cui casella di posta si desidera ripristinare e quindi fare clic su **Ripristino**.

   È possibile cercare gli utenti e i gruppi per nome. I caratteri jolly non sono supportati.

   Se il file di dati condiviso dell'utente, del gruppo o di Outlook è stato eliminato, selezionare l'elemento nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.
4. Fare clic su **Ripristina** > **Come file PST**.
5. Impostare la password per crittografare l'archivio che contiene i file PST.
   La password deve contenere almeno un simbolo.
6. Confermare la password e fare clic su **Fine**.
7. Gli elementi di casella di posta selezionati verranno ripristinati come file di dati PST e archiviati in formato zip. La dimensione massima di un file PST è limitata a 2 GB; pertanto, se i dati in corso di ripristino superano i 2 GB, verranno suddivisi in diversi file PST. L'archivio zip sarà protetto con la password impostata.
8. L'utente riceverà un'e-mail con un link a un archivio zip contenente i file PST creati.
9. L'amministratore riceverà una notifica e-mail che segnala l'avvenuta esecuzione della procedura di ripristino.

© Acronis International GmbH, 2003-2024

Nota
Il ripristino delle caselle di posta nei file PST è un'attività che richiede tempo, perché implica il trasferimento dei dati e la loro trasformazione mediante algoritmi complessi.

Per scaricare l'archivio con i file PST e completare il ripristino

1. Eseguire una delle seguenti operazioni:
   - Per scaricare l'archivio dall'e-mail, seguire il link **Scarica file**.
     L'archivio è disponibile per il download per 24 ore. Se il link scade, ripetere la procedura di ripristino.
   - Per scaricare l'archivio dalla console di Cyber Protect:
     a. Passare a **Archivio di backup** > **File PST**.
     b. Selezionare l'ultimo archivio evidenziato.
     c. Fare clic su **Download** nel riquadro a destra.

   L'archivio verrà scaricato nella directory di download predefinita del computer.
2. Estrarre i file PST dall'archivio utilizzando la password impostata per crittografare l'archivio stesso.
3. Aprire i file PST con Microsoft Outlook.
   È normale che i file PST risultanti abbiano dimensioni molto più piccole rispetto alla casella di posta originale.

   Importante
   Non importare questi file in Microsoft Outlook utilizzando la procedura di **Importazione/Esportazione guidata**.
   Per aprire i file, fare doppio clic su di essi o fare clic sul pulsante destro del mouse e selezionare **Apri con...** > **Microsoft Outlook** nel menu contestuale.

Ripristino di elementi di caselle di posta in file PST

Nota
Non è possibile ripristinare un archivio sul posto come parte di un ripristino su file PST. Per ripristinare l'archivio sul posto insieme alla casella di posta, consultare "Ripristino delle caselle postali" (pag. 624).

Per ripristinare gli elementi di casella di posta

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:

© Acronis International GmbH, 2003-2024

- Per ripristinare gli elementi da una casella di posta utente, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente la cui casella di posta conteneva in origine gli elementi da ripristinare e quindi fare clic su **Ripristino**.
- Per ripristinare elementi da una casella di posta condivisa, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare la casella condivisa che originariamente conteneva gli elementi che si desidera ripristinare e quindi fare clic su **Ripristino**.
- Per ripristinare gli elementi da una casella di posta di gruppo, espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, selezionare il gruppo la cui casella di posta conteneva in origine gli elementi da ripristinare e quindi fare clic su **Ripristino**.
- Se la casella di posta utente, di gruppo o condivisa è stata eliminata, selezionarla nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.

È possibile cercare gli utenti e i gruppi per nome. I caratteri jolly non sono supportati.

4. Fare clic su **Ripristina** > **Messaggi e-mail**.
5. Esplorare la cartella richiesta o utilizzare la ricerca per ottenere l'elenco degli elementi richiesti.
   Sono disponibili le opzioni di ricerca seguenti. I caratteri jolly non sono supportati.
   - Per i messaggi e-mail: ricerca per oggetto, mittente, destinatario, nome dell'allegato e data.
   - Per gli eventi: ricerca per titolo e data.
   - Per le attività: ricerca per titolo e data.
   - Per i contatti: ricerca per nome, indirizzo e-mail e numero di telefono.
6. Selezionare gli elementi che si desidera ripristinare. Per poter selezionare le cartelle, fare clic sull'icona di ripristino delle cartelle:
   Inoltre, è possibile eseguire una delle seguenti operazioni:
   - Dopo aver selezionato un elemento, fare clic su **Mostra contenuto** per visualizzarne il contenuto, inclusi gli allegati. Fare clic sul nome di un file allegato per scaricarlo.
   - Quando è selezionato un messaggio e-mail o un elemento di calendario, fare clic su **Invia come e-mail** per inviare l'elemento all'indirizzo e-mail specificato. È possibile selezionare il mittente e scrivere un testo da aggiungere all'elemento inoltrato.
   - Solo se il backup non è crittografato, è stata usata la ricerca e selezionato un unico elemento nei risultati della ricerca, è possibile fare clic su **Mostra versioni** per selezionare la versione dell'elemento da ripristinare. È possibile selezionare qualsiasi versione di cui sia stato eseguito il backup, precedente o successiva al punto di ripristino selezionato.
7. Fare clic su **Ripristina come file PST**.
8. Impostare la password per crittografare l'archivio che contiene i file PST.
   La password deve contenere almeno un simbolo.
9. Confermare la password e fare clic su **FINE**.

Gli elementi di casella di posta selezionati verranno ripristinati come file di dati PST e archiviati in formato zip. La dimensione massima di un file PST è limitata a 2 GB; pertanto, se i dati in corso di

© Acronis International GmbH, 2003-2024

ripristino superano i 2 GB, verranno suddivisi in diversi file PST. L'archivio zip sarà protetto con la password impostata.

L'utente riceverà un'e-mail con un link a un archivio zip contenente i file PST creati.

L'amministratore riceverà una notifica e-mail che segnala l'avvenuta esecuzione della procedura di ripristino.

Per scaricare l'archivio con i file PST e completare il ripristino

1. Eseguire una delle seguenti operazioni:
   - Per scaricare l'archivio dall'e-mail, seguire il link **Scarica file**.
     L'archivio è disponibile per il download per 24 ore. Se il link scade, ripetere la procedura di ripristino.
   - Per scaricare l'archivio dalla console di Cyber Protect:
     a. Passare a **Archivio di backup** > **File PST**.
     b. Selezionare l'ultimo archivio evidenziato.
     c. Fare clic su **Download** nel riquadro a destra.

   L'archivio verrà scaricato nella directory di download predefinita del computer.
2. Estrarre i file PST dall'archivio utilizzando la password impostata per crittografare l'archivio stesso.
3. Aprire i file PST con Microsoft Outlook.
   È normale che i file PST risultanti abbiano dimensioni molto più piccole rispetto alla casella di posta originale.

   Importante
   Non importare questi file in Microsoft Outlook utilizzando la procedura di **Importazione/Esportazione guidata**.
   Per aprire i file, fare doppio clic su di essi o fare clic sul pulsante destro del mouse e selezionare **Apri con...** > **Microsoft Outlook** nel menu contestuale.

Ripristino di cartelle pubbliche e di elementi della cartella

Per ripristinare una cartella pubblica o gli elementi di una cartella pubblica, almeno un amministratore dell'organizzazione di Microsoft 365 deve disporre dei diritti di **Proprietario** per la cartella pubblica di destinazione. Se il ripristino non ha esito positivo e viene segnalato un errore di accesso negato, assegnare i diritti richiesti nelle proprietà della cartella di destinazione, selezionare l'organizzazione di destinazione nella console di Cyber Protect, fare clic su **Aggiorna**, quindi ripetere il ripristino.

Per ripristinare una cartella pubblica o elementi della cartella

1. Fare clic su **Microsoft 365**.

© Acronis International GmbH, 2003-2024

2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, espandere l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Espandere il nodo **Cartelle pubbliche**, selezionare **Tutte le cartelle pubbliche**, selezionare la cartella pubblica da ripristinare o quella che conteneva in origine gli elementi da ripristinare e quindi fare clic su **Ripristino**.
   - Se la cartella pubblica è stata eliminata, selezionarla nella sezione **Backup delle applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.

   È possibile cercare le cartelle pubbliche per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina dati**.
6. Esplorare la cartella richiesta o utilizzare la ricerca per ottenere l'elenco degli elementi richiesti.

   È possibile eseguire ricerche in messaggi e-mail e post per oggetto, mittente, destinatario e data. I caratteri jolly non sono supportati.
7. Selezionare gli elementi che si desidera ripristinare. Per poter selezionare le cartelle, fare clic sull'icona di ripristino delle cartelle:

   Inoltre, è possibile eseguire una delle seguenti operazioni:
   - Dopo aver selezionato un messaggio e-mail o un post, fare clic su **Mostra contenuto** per visualizzarne il contenuto, inclusi gli allegati. Fare clic sul nome di un file allegato per scaricarlo.
   - Dopo aver selezionato un messaggio e-mail o un post, fare clic su **Invia come e-mail** per inviare l'elemento all'indirizzo e-mail specificato. È possibile selezionare il mittente e scrivere un testo da aggiungere all'elemento inoltrato.
   - Solo se il backup non è crittografato, è stata usata la ricerca e selezionato un unico elemento nei risultati della ricerca, è possibile fare clic su **Mostra versioni** per selezionare la versione dell'elemento da ripristinare. È possibile selezionare qualsiasi versione di cui sia stato eseguito il backup, precedente o successiva al punto di ripristino selezionato.
8. Fare clic su **Ripristina**.
9. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.

   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.
10. In **Ripristina nella cartella pubblica**, visualizzare, modificare o specificare la cartella pubblica di destinazione.

    Per impostazione predefinita, viene selezionata la cartella originale. Se questa cartella non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare la cartella di destinazione.

© Acronis International GmbH, 2003-2024

Durante il ripristino non è possibile creare una nuova cartella pubblica. Per ripristinare una cartella pubblica in una nuova, è necessario innanzitutto creare la cartella pubblica di destinazione nell'organizzazione Microsoft 365 desiderata, quindi attendere che l'agente cloud sincronizzi la modifica.L'agente cloud esegue automaticamente la sincronizzazione con Microsoft 365 ogni 24 ore. Per sincronizzare immediatamente la modifica, nella console di Cyber Protect selezionare l'organizzazione nella pagina di **Microsoft 365** quindi fare clic su **Aggiorna**.

11. In **Percorso**, visualizzare o modificare la sottocartella di destinazione nella cartella pubblica di destinazione. Per impostazione predefinita, verrà ricreato il percorso originale.
12. Fare clic su **Avvia ripristino**.
13. Selezionare una delle opzioni di sovrascrittura:

Opzione	Descrizione
Sovrascrivi gli elementi esistenti	Tutti i file esistenti nella posizione di destinazione vengono sovrascritti.
Non sovrascrivere gli elementi esistenti	Se nella posizione di destinazione è presente un file con lo stesso nome, tale file non viene sovrascritto e il file di origine non viene salvato nella posizione di destinazione.

14. Fare clic su **Procedi** per confermare la decisione.

Protezione di file di OneDrive

Di quali elementi è possibile eseguire il backup?

È possibile eseguire il backup di un intero OneDrive o di singoli file e cartelle.

Un'opzione distinta nel piano di backup abilita il backup dei notebook OneNote.

Il backup dei file viene eseguito insieme alle autorizzazioni di condivisione. Non viene eseguito il backup dei livelli di autorizzazione avanzati (**Progettazione**, **Completo**, **Collaborazione**).

Alcuni file possono contenere informazioni sensibili. In Microsoft 365, l'accesso a tali file potrebbe essere impedito da uno dei criteri di prevenzione della perdita dei dati. Di questi file non viene eseguito il backup e nessun avviso viene visualizzato al completamento dell'operazione di backup.

Limitazioni

Il backup di contenuti di OneDrive non è supportato per le caselle di posta condivise. Per eseguire il backup di questo contenuto, convertire la casella di posta condivisa in un account utente standard e verificare che OneDrive sia abilitato per tale account.

Quali elementi è possibile ripristinare?

È possibile ripristinare un intero OneDrive o qualsiasi file o cartella di cui è stato eseguito il backup.

È possibile utilizzare la ricerca per individuare gli elementi.

© Acronis International GmbH, 2003-2024

È possibile scegliere se ripristinare le autorizzazioni condivise o lasciare che i file ereditino le autorizzazioni dalla cartella in cui vengono ripristinati.

Non vengono ripristinati i collegamenti di condivisione di file e cartelle.

Selezione di file di OneDrive

Selezionare i file come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Per selezionare file di OneDrive

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione i cui dati utente devono essere sottoposti a backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per eseguire il backup dei file di tutti gli utenti (inclusi quelli che verranno creati in futuro), espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, quindi fare clic su **Raggruppa backup**.
   - Per eseguire il backup di file di singoli utenti, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare gli utenti i cui file si desidera sottoporre a backup e quindi fare clic su **Backup**.
4. Nel pannello del piano di protezione:
   - Verificare che l'elemento **OneDrive** sia selezionato in **Cosa includere nel backup**.

     Se per alcuni degli utenti selezionati singolarmente il servizio OneDrive non è incluso nel relativo piano di Microsoft 365, non sarà possibile selezionare questa opzione.

     Se per alcuni degli utenti selezionati per il backup di gruppo il servizio OneDrive non è incluso nel loro piano di Microsoft 365, sarà possibile selezionare questa opzione, ma il piano di protezione verrà applicato soltanto a tali utenti.
   - In **Elementi di cui eseguire il backup**, eseguire una delle seguenti operazioni:
     - Mantenere l'impostazione predefinita **[Tutti]** (tutti i file).
     - Specificare i file e le cartelle di cui eseguire il backup aggiungendo i nomi o i percorsi.

       È possibile utilizzare i caratteri jolly *, ** e ?. Per ulteriori dettagli su come specificare percorsi e utilizzare i caratteri jolly, fare riferimento a "Filtri file".
     - Specificare i file e le cartelle di cui eseguire il backup scorrendo l'elenco.

       Il collegamento **Sfoglia** è disponibile solo quando si crea un piano di protezione per un singolo utente.
   - [Facoltativo] In **Elementi di cui eseguire il backup**, fare clic su **Mostra esclusioni** per specificare i file e le cartelle da ignorare durante il backup.

     L'esclusione dei file prevale sulla selezione dei file: se si specifica lo stesso file in entrambi i campi, il file verrà ignorato durante il backup.
   - [Facoltativo] Per eseguire il backup dei notebook OneNote, abilitare l'opzione **Includi OneNote**.

© Acronis International GmbH, 2003-2024

Ripristino di OneDrive e di file di OneDrive

Ripristino di un intero OneDrive

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente di cui ripristinare l'OneDrive, quindi fare clic su **Ripristino**.

   Se l'utente è stato eliminato, selezionarlo nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.

   È possibile cercare gli utenti per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.

   Nota
   Per visualizzare solo i punti di ripristino che contengono file di OneDrive, selezionare **OneDrive** in **Filtra per contenuto**.
5. Fare clic su **Ripristina** > **Intero OneDrive**.
6. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.

   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.

   Durante il ripristino non è possibile creare un nuovo OneDrive di destinazione. Per ripristinare un OneDrive su uno nuovo, è necessario innanzitutto creare un OneDrive di destinazione nell'organizzazione Microsoft 365 e quindi attendere che l'agente cloud sincronizzi la modifica. L'agente cloud esegue automaticamente la sincronizzazione con Microsoft 365 ogni 24 ore. Per sincronizzare immediatamente la modifica, nella console di Cyber Protect selezionare l'organizzazione nella pagina di **Microsoft 365** quindi fare clic su **Aggiorna**.
7. In **Ripristina nell'unità**, visualizzare, modificare o specificare l'utente di destinazione.

   Per impostazione predefinita, è selezionato l'utente originale. Se questo utente non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare l'utente di destinazione.
8. Selezionare se ripristinare o meno le autorizzazioni di condivisione dei file.
9. Fare clic su **Avvia ripristino**.
10. Selezionare una delle opzioni di sovrascrittura:

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
Sovrascrivi il file esistente se meno recente	Se nella posizione di destinazione è presente un file con lo stesso nome, e se tale file è meno recente del file di origine, il file di origine viene salvato nella posizione di destinazione e sostituisce la versione precedente.
Sovrascrivi i file esistenti	Tutti i file esistenti nella posizione di destinazione vengono sovrascritti, qualunque sia la data dell'ultima modifica.
Non sovrascrivere i file esistenti	Se nella posizione di destinazione è presente un file con lo stesso nome, tale file non viene modificato e il file di origine non viene salvato nella posizione di destinazione.

Nota
Durante il ripristino dei notebook OneNote, entrambe le opzioni **Sovrascrivi il file esistente se meno recente** e **Sovrascrivi i file esistenti** hanno come risultato la sovrascrittura dei notebook OneNote esistenti.

11. Fare clic su **Procedi** per confermare la decisione.

Ripristino di file di OneDrive

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente di cui ripristinare i file di OneDrive, quindi fare clic su **Ripristino**.
   Se l'utente è stato eliminato, selezionarlo nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.
   È possibile cercare gli utenti per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.

Nota
Per visualizzare solo i punti di ripristino che contengono file di OneDrive, selezionare **OneDrive** in **Filtra per contenuto**.

5. Fare clic su **Ripristina** > **File/cartelle**.
6. Esplorare la cartella richiesta o utilizzare la ricerca per ottenere l'elenco dei file e delle cartelle necessarie.
7. Selezionare i dati che si desidera ripristinare.
   Se il backup non è crittografato ed è stato selezionato un solo file è possibile fare clic su **Mostra versioni** per selezionare la versione del file da ripristinare. È possibile selezionare qualsiasi versione di cui sia stato eseguito il backup, precedente o successiva al punto di ripristino selezionato.

© Acronis International GmbH, 2003-2024

8. Per scaricare un file, selezionarlo e fare clic su **Download**, selezionare la posizione in cui salvare i dati e quindi fare clic su **Salva**. Altrimenti, ignorare questo passaggio.
9. Fare clic su **Ripristina**.
10. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.

    Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.

    Durante il ripristino non è possibile creare un nuovo OneDrive. Per ripristinare un file su uno nuovo, è necessario innanzitutto creare un OneDrive di destinazione nell'organizzazione Microsoft 365 desiderata, quindi attendere che l'agente cloud sincronizzi la modifica. L'agente cloud esegue automaticamente la sincronizzazione con Microsoft 365 ogni 24 ore. Per sincronizzare immediatamente la modifica, nella console di Cyber Protect selezionare l'organizzazione nella pagina di **Microsoft 365** quindi fare clic su **Aggiorna**.
11. In **Ripristina nell'unità**, visualizzare, modificare o specificare l'utente di destinazione.

    Per impostazione predefinita, è selezionato l'utente originale. Se questo utente non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare l'utente di destinazione.
12. In **Percorso**, visualizzare o modificare la cartella di destinazione nell'OneDrive dell'utente di destinazione. Per impostazione predefinita, è selezionato il percorso originale.
13. Selezionare se ripristinare o meno le autorizzazioni di condivisione dei file.
14. Fare clic su **Avvia ripristino**.
15. Selezionare una delle opzioni di sovrascrittura dei file:

Opzione	Descrizione
Sovrascrivi il file esistente se meno recente	Se nella posizione di destinazione è presente un file con lo stesso nome, e se tale file è meno recente del file di origine, il file di origine viene salvato nella posizione di destinazione e sostituisce la versione precedente.
Sovrascrivi i file esistenti	Tutti i file esistenti nella posizione di destinazione vengono sovrascritti, qualunque sia la data dell'ultima modifica.
Non sovrascrivere i file esistenti	Se nella posizione di destinazione è presente un file con lo stesso nome, tale file non viene modificato e il file di origine non viene salvato nella posizione di destinazione.

    Nota
    Durante il ripristino dei notebook OneNote, entrambe le opzioni **Sovrascrivi il file esistente se meno recente** e **Sovrascrivi i file esistenti** hanno come risultato la sovrascrittura dei notebook OneNote esistenti.

16. Fare clic su **Procedi** per confermare la decisione.

© Acronis International GmbH, 2003-2024

Protezione di siti di SharePoint Online

Di quali elementi è possibile eseguire il backup?

È possibile eseguire il backup di raccolte di siti classici, siti di gruppo (team moderno) e siti di comunicazione di SharePoint. È inoltre possibile scegliere di eseguire il backup di singoli siti secondari, elenchi e librerie.

Un'opzione distinta nel piano di backup abilita il backup dei notebook OneNote.

Durante il backup vengono *ignorati* gli elementi seguenti:

- Le impostazioni dell'**aspetto predefinito** del sito, ad eccezione di **titolo, descrizione e logo**.
- I commenti della pagina del sito e le impostazioni dei commenti della pagina (commenti **attivati**/**disattivati**).
- Le impostazioni del sito relative alle **caratteristiche del sito**.
- Pagine Web part e Web part incorporate nelle pagine wiki (a causa delle limitazioni delle API di SharePoint Online).
- File estratti — file estratti manualmente per l'editing e tutti i file creati o caricati nelle librerie, per i quali è stata abilitata l'opzione **Estrazione obbligatoria**. Per eseguire il backup di questi file, è prima necessario eseguire l'archiviazione.
- Dati esterni e tipi di colonne di metadati gestiti.
- La raccolta sito predefinita "domain-my.sharepoint.com". Si tratta della raccolta in cui risiedono tutti i file OneDrive degli utenti dell'organizzazione.
- Il contenuto del cestino.

Limitazioni

- Durante un backup, titoli e descrizioni di siti/siti secondari/elenchi/colonne vengono troncati se la descrizione o il titolo superano i 10.000 byte.
- Non è possibile eseguire il backup di versioni precedenti dei file create in SharePoint Online. Sono protette soltanto le più recenti versioni dei file.
- Non è possibile eseguire il backup della raccolta di archiviazione.
- Non è possibile eseguire il backup dei siti creati con Business Productivity Online Suite (BPOS), predecessore di Microsoft 365.
- Non è possibile eseguire il backup delle impostazioni dei siti che utilizzano il percorso gestito (ad esempio `https://<tenant>.sharepoint.com/portals/...`).
- Le impostazioni IRM (Information Rights Management) di un elenco o di una libreria possono essere ripristinate solo se IRM è abilitato nell'organizzazione Microsoft 365 di destinazione.

Quali elementi è possibile ripristinare?

Dal backup di un sito è possibile ripristinare i seguenti elementi:

© Acronis International GmbH, 2003-2024

- Intero sito
- Siti secondari
- Elenchi
- Elementi degli elenchi
- Librerie di documenti
- Documenti
- Allegati agli elementi degli elenchi
- Pagine del sito e pagine wiki

È possibile utilizzare la ricerca per individuare gli elementi.

Gli elementi vengono ripristinati all'originale o a un sito non originale. Il percorso di un elemento ripristinato è lo stesso dell'elemento originale. Se il percorso non esiste, viene creato.

È possibile scegliere se ripristinare le autorizzazioni condivise o lasciare che gli elementi ereditino le autorizzazioni dall'oggetto padre dopo il ripristino.

Quali elementi non è possibile ripristinare?

- Siti secondari basati sul modello **Visio Process Repository**.
- Elenchi dei seguenti tipi: **Elenco sondaggi**, **elenco attività**, **libreria immagini**, **collegamenti**, **calendario**, **area discussioni**, **esterno** e **fogli di calcolo importati**.
- Elenchi per i quali sono attivati più tipi di contenuto.

Selezione di dati di SharePoint Online

Selezionare i dati come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Per selezionare i dati di SharePoint Online

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione i cui dati utente devono essere sottoposti a backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per eseguire il backup di tutti i siti SharePoint classici nell'organizzazione, inclusi i siti che verranno creati in futuro, espandere il nodo **Raccolte sito**, selezionare **Tutte le raccolte di siti**, quindi fare clic su **Raggruppa backup**.
   - Per eseguire il backup di singoli siti classici, espandere il nodo **Raccolte siti**, selezionare **Tutte le raccolte di siti**, selezionare i siti di cui eseguire il backup, quindi fare clic su **Backup**.
   - Per eseguire il backup di tutti i siti di gruppo (team moderno), inclusi i siti che verranno creati in futuro, espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, quindi fare clic su **Raggruppa backup**.

© Acronis International GmbH, 2003-2024

- Per eseguire il backup di singoli siti di gruppo (team moderno), espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, selezionare i gruppi i cui siti si desidera sottoporre a backup e quindi fare clic su **Backup**.

4. Nel pannello del piano di protezione:
   - Verificare che l'elemento **Siti di SharePoint** sia selezionato in **Cosa includere nel backup**.
   - In **Elementi di cui eseguire il backup**, eseguire una delle seguenti operazioni:
     - Mantenere l'impostazione predefinita **[Tutti]** (tutti gli elementi dei siti selezionati).
     - Specificare i siti secondari, gli elenchi e le librerie di cui eseguire il backup aggiungendo i nomi o i percorsi.

       Per eseguire il backup di un sito secondario o di un elenco/libreria di siti di livello superiore, specificarne il nome visualizzato nel formato: `/nome visualizzato/**`

       Per eseguire il backup di un elenco/libreria di siti secondari, specificarne il nome visualizzato nel formato: `/nome visualizzato del sito secondario/nome visualizzato dell'elenco/**`

       I nomi visualizzati di siti secondari, elenchi e librerie sono visualizzati nella pagina relativa ai **contenuti del sito** di un sito o sito secondario di SharePoint.
     - Specificare i siti secondari di cui eseguire il backup scorrendo l'elenco.

       Il collegamento **Sfoglia** è disponibile solo quando si crea un piano di protezione per un singolo sito.
   - [Facoltativo] In **Elementi di cui eseguire il backup**, fare clic su **Mostra esclusioni** per specificare i siti secondari, gli elenchi e le librerie da ignorare durante il backup.

     L'esclusione degli elementi prevale sulla selezione degli elementi: se si specifica lo stesso sito secondario in entrambi i campi, il sito verrà ignorato durante il backup.
   - [Facoltativo] Per eseguire il backup dei notebook OneNote, abilitare l'opzione **Includi OneNote**.

Ripristino di dati di SharePoint Online

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per ripristinare i dati da un sito di gruppo (team moderno), espandere il nodo **Gruppi**, selezionare **Tutti i gruppi**, selezionare il gruppo il cui sito conteneva in origine gli elementi da ripristinare e quindi fare clic su **Ripristino**.
   - Per ripristinare i dati da un sito classico, espandere il nodo **Raccolte siti**, selezionare **Tutte le raccolte siti**, selezionare il si che conteneva in origine gli elementi da ripristinare e quindi fare clic su **Ripristino**.
   - Se il sito è stato eliminato, selezionarlo nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.

© Acronis International GmbH, 2003-2024

È possibile cercare gruppi e siti per nome. I caratteri jolly non sono supportati.

4. Selezionare un punto di ripristino.

   Nota
   Per visualizzare solo i punti di ripristino che contengono siti SharePoint, selezionare **Siti di SharePoint** in **Filtra per contenuto**.

5. Fare clic su **Ripristina file di SharePoint**.
6. Esplorare la cartella richiesta o utilizzare la ricerca per ottenere l'elenco degli elementi dati richiesti.
7. Selezionare gli elementi che si desidera ripristinare.

   Se il backup non è crittografato, è stata usata la ricerca e selezionato un unico elemento nei risultati della ricerca, è possibile fare clic su **Mostra versioni** per selezionare la versione dell'elemento da ripristinare. È possibile selezionare qualsiasi versione di cui sia stato eseguito il backup, precedente o successiva al punto di ripristino selezionato.
8. [Facoltativo] Per scaricare un elemento, selezionarlo e fare clic su **Download**, selezionare la posizione in cui salvare l'elemento e quindi fare clic su **Salva**.
9. Fare clic su **Ripristina**.
10. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.

    Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.
11. In **Ripristina nel sito**, visualizzare, cambiare o specificare il sito di destinazione.

    Durante il ripristino non è possibile creare un nuovo sito SharePoint. Per ripristinare un sito SharePoint su uno nuovo, è necessario innanzitutto creare il sito di destinazione nell'organizzazione Microsoft 365 desiderata, quindi attendere che l'agente cloud sincronizzi la modifica.L'agente cloud esegue automaticamente la sincronizzazione con Microsoft 365 ogni 24 ore. Per sincronizzare immediatamente la modifica, nella console di Cyber Protect selezionare l'organizzazione nella pagina di **Microsoft 365** quindi fare clic su **Aggiorna**.
12. Selezionare se ripristinare o meno le autorizzazioni di condivisione degli elementi ripristinati.
13. Fare clic su **Avvia ripristino**.
14. Selezionare una delle opzioni di sovrascrittura:

Opzione	Descrizione
Sovrascrivi il file esistente se meno recente	Se nella posizione di destinazione è presente un file con lo stesso nome, e se tale file è meno recente del file di origine, il file di origine viene salvato nella posizione di destinazione e sostituisce la versione precedente.
Sovrascrivi i file	Tutti i file esistenti nella posizione di destinazione vengono sovrascritti, qualunque

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
esistenti	sia la data dell'ultima modifica.
Non sovrascrivere i file esistenti	Se nella posizione di destinazione è presente un file con lo stesso nome, tale file non viene modificato e il file di origine non viene salvato nella posizione di destinazione.

Nota
Durante il ripristino dei notebook OneNote, entrambe le opzioni **Sovrascrivi il file esistente se meno recente** e **Sovrascrivi i file esistenti** hanno come risultato la sovrascrittura dei notebook OneNote esistenti.

15. Fare clic su **Procedi** per confermare la decisione.

Protezione di Microsoft 365 Teams

Di quali elementi è possibile eseguire il backup?

È possibile eseguire il backup di interi team. Nel backup verranno incluse informazioni quali nome del team, elenco dei membri del team, canali dei team e relativo contenuto, caselle di posta e riunioni del team e sito del team.

Un'opzione distinta nel piano di backup abilita il backup dei notebook OneNote.

Quali elementi è possibile ripristinare?

- Team completo
- Canali dei team
- File del canale
- Casella di posta del canale
- Cartelle e-mail nella casella di posta del team
- Messaggi e-mail nella casella di posta del team
- Riunioni
- Sito del team

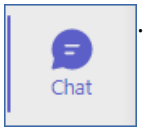
Non è possibile ripristinare le conversazioni nei canali del team, ma è possibile scaricarle come singolo file html.

Limitazioni

Non viene eseguito il backup degli elementi seguenti:

- Le impostazioni del canale generale (preferenze di moderazione) a causa di una limitazione dell'API beta di Microsoft Teams.

© Acronis International GmbH, 2003-2024

- Le impostazioni dei canali personalizzati (preferenze di moderazione) a causa di una limitazione dell'API beta di Microsoft Teams.
- Verbali delle riunioni.
- Messaggi nella sezione chat 

. Questa sezione contiene chat private individuali e chat di gruppo.
- Adesivi e complimenti.

Il backup e il ripristino sono supportati per le schede del canale seguenti:

- Word
- Excel
- PowerPoint
- PDF
- Raccolta di documenti

Selezione dei team

Selezionare i team come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Per selezionare i team

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione i cui team devono essere sottoposti a backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per eseguire il backup di tutti i team nell'organizzazione (inclusi i team che verranno creati in futuro), espandere il nodo **Team**, selezionare **Tutti i team**, quindi fare clic su **Raggruppa backup**.
   - Per eseguire il backup di singoli team, espandere il nodo **Team**, selezionare **Tutti i team**, selezionare i team da sottoporre a backup e quindi fare clic su **Backup**.

   È possibile cercare i team per nome. I caratteri jolly non sono supportati.
4. Nel pannello del piano di protezione:
   - Verificare che l'elemento **Microsoft Teams** sia selezionato in **Cosa includere nel backup**.
   - [Facoltativo] In **Tempo di conservazione** impostare le opzioni di pulizia.
   - [Facoltativo] Se si desidera crittografare il backup, abilitare l'opzione **Crittografia**, quindi impostare la password e selezionare l'algoritmo di crittografia.
   - [Facoltativo] Per eseguire il backup dei notebook OneNote, abilitare l'opzione **Includi OneNote**.

© Acronis International GmbH, 2003-2024

Ripristino di un team completo

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i team oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Team**, selezionare **Tutti i team**, selezionare il team da ripristinare, quindi fare clic su **Ripristino**.

   È possibile cercare i team per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina** > **Team completo**.

   Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.

   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.
6. In **Ripristina su team**, visualizzare il team di destinazione o selezionarne un altro.

   Per impostazione predefinita, è selezionato il team originale. Se questo team non esiste (se, ad esempio, è stata eliminata) o se è stata selezionata un'organizzazione che non contiene il team originale, è necessario selezionare un team di destinazione dall'elenco a discesa.

   È possibile ripristinare un team solo in un team esistente. Non è possibile creare i team durante le operazioni di ripristino.
7. Fare clic su **Avvia ripristino**.
8. Selezionare una delle opzioni di sovrascrittura:
   - **Sovrascrivi il contenuto esistente se meno recente**
   - **Sovrascrivi il contenuto esistente**
   - **Non sovrascrivere il contenuto esistente**

   Nota
   Durante il ripristino dei notebook OneNote, entrambe le opzioni **Sovrascrivi il contenuto esistente se meno recente** e **Sovrascrivi il contenuto esistente** hanno come risultato la sovrascrittura dei notebook OneNote esistenti.
9. Fare clic su **Procedi** per confermare la decisione.

Quando si elimina un canale nell'interfaccia grafica di Microsoft Teams, questo non viene immediatamente rimosso dal sistema. Pertanto, quando si ripristina il team completo, il nome di questo canale non potrà essere usato; al nome verrà aggiunto un suffisso.

© Acronis International GmbH, 2003-2024

Le conversazioni vengono ripristinate come singolo file html nella scheda **File** del canale. È possibile trovare tale file in una cartella denominata in base allo schema seguente: `<Nome team>_<Nome canale>_backup_conversazioni_<data di ripristino>T<ora di ripristino>Z`.

Nota
Dopo il ripristino di un team o di canali dei team, aprire Microsoft Teams, selezionare i canali ripristinati e fare clic sulle rispettive schede **File**. In caso contrario, i backup successivi dei canali non includeranno il contenuto di questa scheda, a causa di una limitazione dell'API beta di Microsoft Teams.

Ripristino dei canali dei team o di file nei canali dei team

Per ripristinare i canali dei team

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i team oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Team**, selezionare **Tutti i team**, selezionare il team di cui si desidera ripristinare i canali, quindi fare clic su **Ripristino**.
4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina** > **Canali**.
6. Selezionare i canali da ripristinare, quindi fare clic su **Ripristina**. Per selezionare un canale nel riquadro principale, selezionare la casella di controllo davanti al suo nome.
   Sono disponibili le opzioni di ricerca seguenti:
   - Per **Conversazioni**: mittente, oggetto, contenuto, lingua, nome dell'allegato, data o intervallo di date.
   - Per **File**: nome del file o nome della cartella, tipo di file, dimensione, data o intervallo di date dell'ultima modifica.

     Nota
     È inoltre possibile scaricare i file in locale, invece di ripristinarli.
7. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.
   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.
8. In **Ripristina su team**, visualizzare, modificare o specificare il team di destinazione.
   Per impostazione predefinita, è selezionato il team originale. Se questo team non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare il team di destinazione.

© Acronis International GmbH, 2003-2024

9. In **Ripristina nel canale**, visualizzare, modificare o specificare il canale di destinazione.
10. Fare clic su **Avvia ripristino**.
11. Selezionare una delle opzioni di sovrascrittura:
    - **Sovrascrivi il contenuto esistente se meno recente**
    - **Sovrascrivi il contenuto esistente**
    - **Non sovrascrivere il contenuto esistente**

    Nota
    Durante il ripristino dei notebook OneNote, entrambe le opzioni **Sovrascrivi il contenuto esistente se meno recente** e **Sovrascrivi il contenuto esistente** hanno come risultato la sovrascrittura dei notebook OneNote esistenti.
12. Fare clic su **Procedi** per confermare la decisione.

Le conversazioni vengono ripristinate come singolo file html nella scheda **File** del canale. È possibile trovare tale file in una cartella denominata in base allo schema seguente: `<Nome team>_<Nome canale>_backup_conversazioni_<data di ripristino>T<ora di ripristino>Z`.

Nota
Dopo il ripristino di un team o di canali dei team, aprire Microsoft Teams, selezionare i canali ripristinati e fare clic sulle rispettive schede **File**. In caso contrario, i backup successivi dei canali non includeranno il contenuto di questa scheda, a causa di una limitazione dell'API beta di Microsoft Teams.

Per ripristinare i file in un canale del team

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i team oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Team**, selezionare **Tutti i team**, selezionare il team di cui si desidera ripristinare i canali, quindi fare clic su **Ripristino**.
4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina** > **Canali**.
6. Selezionare il canale desiderato e quindi aprire la cartella **File**.
   Individuare gli elementi richiesti o utilizzare la ricerca per ottenere l'elenco degli elementi richiesti. Sono disponibili le opzioni di ricerca seguenti: nome del file o nome della cartella, tipo di file, dimensione, data o intervallo di date dell'ultima modifica.
7. [Facoltativo] Per scaricare un elemento, selezionarlo e fare clic su **Download**, selezionare la posizione in cui salvare l'elemento e quindi fare clic su **Salva**.
8. Selezionare gli elementi da ripristinare, quindi fare clic su **Ripristina**

© Acronis International GmbH, 2003-2024

9. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su Organizzazione di Microsoft 365 per visualizzare, modificare o specificare l'organizzazione di destinazione.
   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.
10. In **Ripristina su team**, visualizzare, modificare o specificare il team di destinazione.
    Per impostazione predefinita, è selezionato il team originale. Se questo team non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare il team di destinazione.
11. In **Ripristina nel canale**, visualizzare, modificare o specificare il canale di destinazione.
12. Selezionare se ripristinare o meno le autorizzazioni di condivisione degli elementi ripristinati.
13. Fare clic su **Avvia ripristino**.
14. Selezionare una delle opzioni di sovrascrittura:
    - **Sovrascrivi il contenuto esistente se meno recente**
    - **Sovrascrivi il contenuto esistente**
    - **Non sovrascrivere il contenuto esistente**

    Nota
    Durante il ripristino dei notebook OneNote, entrambe le opzioni **Sovrascrivi il contenuto esistente se meno recente** e **Sovrascrivi il contenuto esistente** hanno come risultato la sovrascrittura dei notebook OneNote esistenti.
15. Fare clic su **Procedi** per confermare la decisione.

Non è possibile ripristinare le singole conversazioni. Nel pannello principale è possibile soltanto sfogliare la cartella **Conversazioni** o scaricarne il contenuto come singolo file html. Per eseguire questa operazione, fare clic sull'icona per il ripristino delle cartelle , selezionare la cartella **Conversazioni** e quindi fare clic su **Download**.

È possibile effettuare una ricerca nei messaggi della cartella **Conversazione** in base a:

- Mittente
- Contenuto
- Nome dell'allegato
- Data

Ripristino della casella di posta del team

1. Fare clic su **Microsoft 365**.

© Acronis International GmbH, 2003-2024

2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i team oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Team**, selezionare **Tutti i team**, selezionare il team di cui si desidera ripristinare la casella di posta, quindi fare clic su **Ripristino**.
   È possibile cercare i team per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina** > **Messaggi e-mail**.
6. Fare clic sull'icona per il ripristino delle cartelle , selezionare la cartella della casella di posta root e quindi fare clic su **Ripristina**.

   Nota
   È anche possibile ripristinare le singole cartelle dalla casella di posta selezionata.

7. Fare clic su **Ripristina**.
8. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.
   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.
9. In **Ripristina nelle caselle di posta**, visualizzare, modificare o specificare la casella di posta di destinazione.
   Per impostazione predefinita, viene selezionata la casella di posta originale. Se questa casella di posta non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare la casella di posta di destinazione.
10. Fare clic su **Avvia ripristino**.
11. Selezionare una delle opzioni di sovrascrittura:
    - **Sovrascrivi gli elementi esistenti**
    - **Non sovrascrivere gli elementi esistenti**
12. Fare clic su **Procedi** per confermare la decisione.

Ripristino di elementi della casella di posta del team su file PST

Per ripristinare gli elementi della casella di posta di un team

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. È possibile cercare gli utenti e i gruppi per nome. I caratteri jolly non sono supportati.

© Acronis International GmbH, 2003-2024

4. Espandere il nodo **Team**, selezionare **Tutti i team**, selezionare il team la cui casella di posta conteneva originariamente gli elementi da ripristinare, quindi fare clic su **Ripristino**.
5. Fare clic su **Ripristina** > **Messaggi e-mail**.
6. Esplorare la cartella richiesta o utilizzare la ricerca per ottenere l'elenco degli elementi richiesti.
   Sono disponibili le opzioni di ricerca seguenti. I caratteri jolly non sono supportati.
   - Per i messaggi e-mail: ricerca per oggetto, mittente, destinatario, nome dell'allegato e data.
   - Per gli eventi: ricerca per titolo e data.
   - Per le attività: ricerca per titolo e data.
   - Per i contatti: ricerca per nome, indirizzo e-mail e numero di telefono.
7. Selezionare gli elementi che si desidera ripristinare. Per poter selezionare le cartelle, fare clic sull'icona di ripristino delle cartelle:
   Inoltre, è possibile eseguire una delle seguenti operazioni:
   - Dopo aver selezionato un elemento, fare clic su **Mostra contenuto** per visualizzarne il contenuto, inclusi gli allegati. Fare clic sul nome di un file allegato per scaricarlo.
   - Quando è selezionato un messaggio e-mail o un elemento di calendario, fare clic su **Invia come e-mail** per inviare l'elemento all'indirizzo e-mail specificato. È possibile selezionare il mittente e scrivere un testo da aggiungere all'elemento inoltrato.
   - Se il backup non è crittografato, è stata usata la ricerca e selezionato un unico elemento nei risultati della ricerca: fare clic su **Mostra versioni** per selezionare la versione dell'elemento. È possibile selezionare qualsiasi versione di cui sia stato eseguito il backup, precedente o successiva al punto di ripristino selezionato.
8. Fare clic su **Ripristina come file PST**.
9. Impostare la password per crittografare l'archivio che contiene i file PST.
   La password deve contenere almeno un simbolo.
10. Confermare la password e fare clic su **FINE**.

Gli elementi di casella di posta selezionati verranno ripristinati come file di dati PST e archiviati in formato zip. La dimensione massima di un file PST è limitata a 2 GB; pertanto, se i dati in corso di ripristino superano i 2 GB, verranno suddivisi in diversi file PST. L'archivio zip sarà protetto con la password impostata.

L'utente riceverà un'e-mail con un link a un archivio zip contenente i file PST creati.

L'amministratore riceverà una notifica e-mail che segnala l'avvenuta esecuzione della procedura di ripristino.

Per scaricare l'archivio con i file PST e completare il ripristino

1. Eseguire una delle seguenti operazioni:
   - Per scaricare l'archivio dall'e-mail, seguire il link **Scarica file**.
     L'archivio è disponibile per il download per 24 ore. Se il link scade, ripetere la procedura di ripristino.

© Acronis International GmbH, 2003-2024

- Per scaricare l'archivio dalla console di Cyber Protect:
  a. Passare a **Archivio di backup** > **File PST**.
  b. Selezionare l'ultimo archivio evidenziato.
  c. Fare clic su **Download** nel riquadro a destra.

  L'archivio verrà scaricato nella directory di download predefinita del computer.
2. Estrarre i file PST dall'archivio utilizzando la password impostata per crittografare l'archivio stesso.
3. In Microsoft Outlook, aprire o importare i file PST. Per ulteriori informazioni su come eseguire questa operazione, consultare la documentazione Microsoft.

Ripristino di messaggi e-mail e riunioni

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i team oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Team**, selezionare **Tutti i team**, selezionare il team di cui si desidera ripristinare i messaggi e-mail o le riunioni, quindi fare clic su **Ripristino**.
   È possibile cercare i team per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina** > **Messaggi e-mail**.
6. Individuare l'elemento richiesto o utilizzare la ricerca per ottenere l'elenco degli elementi richiesti.
   Sono disponibili le opzioni di ricerca seguenti:
   - Per i messaggi e-mail: ricerca per oggetto, mittente, destinatario e data.
   - Per le riunioni: ricerca per nome evento e data.
7. Selezionare gli elementi da ripristinare, quindi fare clic su **Ripristina**.

   Nota
   Le riunioni sono reperibili nella cartella **Calendario**.

   Inoltre, è possibile eseguire una delle seguenti operazioni:
   - Dopo aver selezionato un elemento, fare clic su **Mostra contenuto** per visualizzarne il contenuto, inclusi gli allegati. Fare clic sul nome di un file allegato per scaricarlo.
   - Dopo aver selezionato un messaggio e-mail o una riunione, fare clic su **Invia come e-mail** per inviare l'elemento all'indirizzo e-mail specificato. È possibile selezionare il mittente e scrivere un testo da aggiungere all'elemento inoltrato.
8. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.

© Acronis International GmbH, 2003-2024

Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.

9. In **Ripristina nelle caselle di posta**, visualizzare, modificare o specificare la casella di posta di destinazione.

   Per impostazione predefinita, viene selezionata la casella di posta originale. Se questa casella di posta non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare la casella di posta di destinazione.
10. Fare clic su **Avvia ripristino**.
11. Selezionare una delle opzioni di sovrascrittura:
    - **Sovrascrivi gli elementi esistenti**
    - **Non sovrascrivere gli elementi esistenti**
12. Fare clic su **Procedi** per confermare la decisione.

Ripristino di un sito del team o di elementi specifici di un sito

1. Fare clic su **Microsoft 365**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, selezionare l'organizzazione di cui ripristinare i team oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Team**, selezionare **Tutti i team**, selezionare il team di cui si desidera ripristinare il sito, quindi fare clic su **Ripristino**.

   È possibile cercare i team per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina** > **Sito del team**.
6. Individuare l'elemento richiesto o utilizzare la ricerca per ottenere l'elenco degli elementi richiesti.
7. [Facoltativo] Per scaricare un elemento, selezionarlo e fare clic su **Download**, selezionare la posizione in cui salvare l'elemento e quindi fare clic su **Salva**.
8. Selezionare gli elementi da ripristinare, quindi fare clic su **Ripristina**.
9. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Microsoft 365, fare clic su **Organizzazione di Microsoft 365** per visualizzare, modificare o specificare l'organizzazione di destinazione.

   Per impostazione predefinita, sono selezionati l'organizzazione e il team originali. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare l'organizzazione di destinazione.
10. In **Ripristina su team**, visualizzare, modificare o specificare il team di destinazione.

    Per impostazione predefinita, è selezionato il team originale. Se questo team non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare il sito di destinazione.
11. Selezionare se ripristinare o meno le autorizzazioni di condivisione degli elementi ripristinati.

© Acronis International GmbH, 2003-2024

12. Fare clic su **Avvia ripristino**.
13. Selezionare una delle opzioni di sovrascrittura:
    - **Sovrascrivi il contenuto esistente se meno recente**
    - **Sovrascrivi il contenuto esistente**
    - **Non sovrascrivere il contenuto esistente**

    Nota
    Durante il ripristino dei notebook OneNote, entrambe le opzioni **Sovrascrivi il contenuto esistente se meno recente** e **Sovrascrivi il contenuto esistente** hanno come risultato la sovrascrittura dei notebook OneNote esistenti.
14. Fare clic su **Procedi** per confermare la decisione.

Protezione di notebook OneNote

Per impostazione predefinita, i notebook OneNote sono inclusi nei backup dei file di OneDrive, Microsoft Teams e dei siti SharePoint.

Per escludere questi notebook dal backup, disabilitare l'opzione **Includi OneNote** nel rispettivo piano di backup.

Ripristino di notebook OneNote oggetto di backup

Per ulteriori informazioni su come eseguire il ripristino di un notebook OneNote oggetto di backup, fare riferimento al rispettivo argomento:

- Per i backup di OneDrive, vedere "Ripristino di un intero OneDrive" (pag. 635) o "Ripristino di file di OneDrive" (pag. 636).
- Per i backup di Microsoft Teams, vedere "Ripristino di un team completo" (pag. 644), "Ripristino dei canali dei team o di file nei canali dei team" (pag. 645) o "Ripristino di un sito del team o di elementi specifici di un sito" (pag. 651).
- Per il backup dei siti SharePoint, vedere "Ripristino di dati di SharePoint Online" (pag. 640).

Versioni supportate

- OneNote (OneNote 2016 e versioni successive)
- OneNote per Windows 10

Limitazioni e problemi noti

- I notebook OneNote salvati in OneDrive o SharePoint sono limitati a 2 GB. Non è possibile ripristinare notebook OneNote di maggiori dimensioni su destinazioni di OneDrive o SharePoint.
- Non sono supportati i notebook OneNote con gruppi di sezioni.

© Acronis International GmbH, 2003-2024

- Nei notebook di OneNote oggetto di backup che contengono sezioni con nomi non predefiniti, la prima sezione è visualizzata con il nome predefinito (ad esempio `Nuova sezione` o `Sezione senza titolo`). Ciò può incidere sull'ordine delle sezioni nei notebook con sezioni multiple.
- Durante il ripristino dei notebook OneNote, entrambe le opzioni **Sovrascrivi il contenuto esistente se meno recente** e **Sovrascrivi il contenuto esistente** hanno come risultato la sovrascrittura dei notebook OneNote esistenti.
- Quando si ripristina un intero team, il sito di un team o la cartella `Risorse del sito` del sito di un team, se è stata selezionata l'opzione **Sovrascrivi il contenuto esistente se meno recente** o l'opzione **Sovrascrivi il contenuto esistente**, il notebook OneNote predefinito di quel team non verrà sovrascritto. Il ripristino viene completato con l'avviso *Impossibile aggiornare le proprietà del file '/sites/<nome del team>/SiteAssets/<nome del notebook OneNote>'*.

Protezione delle utenze delle app di collaborazione di Microsoft 365

È possibile utilizzare il pacchetto Advanced Email Security, che offre protezione in tempo reale delle caselle di posta di Microsoft 365, Google Workspace o Open-Xchange:

- Anti-malware e anti-spam
- Scansione degli URL nelle e-mail
- Analisi DMARC
- Antiphishing
- Protezione dagli attacchi di imitazione delle identità
- Scansione degli allegati
- Neutralizzazione e ricostruzione di contenuti
- Grafico di attendibilità

È inoltre possibile abilitare le utenze per le app di collaborazione di Microsoft 365, per proteggere le applicazioni di collaborazione nel cloud di Microsoft 365 dalle minacce alla sicurezza perpetrate tramite contenuti. Queste applicazioni includono, tra le altre, OneDrive, SharePoint e Teams.

È possibile abilitare Advanced Email Security per workload o per gigabyte; la scelta incide sul modello di licensing.

Per l'onboarding di Advanced Email Security dalla console di Cyber Protect Cloud

1. Fare clic su **Dispositivi** > **Microsoft 365**.
2. Fare clic sul nodo **Utenti** e quindi sul link **Seleziona Sicurezza e-mail** in alto a destra.

Per ulteriori informazioni sul modulo Advanced Email Security, leggere la relativa scheda informativa.

Per istruzioni sulla configurazione, vedere Advanced Email Security con Perception Point.

© Acronis International GmbH, 2003-2024

Protezione dei dati di Google Workspace

Nota
Questa funzionalità non è disponibile ai tenant in modalità Conformità. Per ulteriori informazioni, consultare "Modalità Conformità" (pag. 1110).

Cosa si intende con protezione dei dati di Google Workspace?

- Backup e ripristino da cloud a cloud di dati utente di Google Workspace (caselle postali di Gmail, Calendario, Contatti, Google Drive) e di unità condivise di Google Workspace.
- Ripristino granulare di e-mail, file, contatti e altri elementi.
- Supporto per più organizzazioni di Google Workspace e ripristino tra organizzazioni.
- Autenticazione facoltativa dei file di cui è stato eseguito il backup tramite il database blockchain Ethereum. Se abilitata, l'autenticazione consente di dimostrare l'autenticità del file e l'assenza di modifiche dal momento del backup.
- Ricerca testo completo facoltativa. Se abilitata, è possibile eseguire ricerche nel contenuto dei messaggi e-mail.
- È possibile proteggere fino a 5.000 elementi (caselle di posta, Google Drive e unità condivise) per azienda senza compromettere le prestazioni.
- I dati contenuti nel backup sono compressi automaticamente e occupano meno spazio nella posizione di backup rispetto a quello che occupano nella posizione originaria. Il livello di compressione per i backup cloud-to-cloud è fisso e corrisponde al livello **Normale** dei backup non cloud-to-cloud. Per ulteriori informazioni su questi livelli, consultare "Livello di compressione" (pag. 466).

Diritti utente necessari

In Cyber Protection

In Cyber Protection è necessario avere un ruolo di amministratore dell'azienda che agisce a livello di tenant del cliente. Gli amministratori dell'azienda che agiscono a livello di unità, gli amministratori di unità e gli utenti non possono eseguire il backup o il recupero di dati di Google Workspace.

In Google Workspace

Per aggiungere l'organizzazione di Google Workspace al servizio Cyber Protection, è necessario essere registrati come amministratore con accesso API abilitato (**Sicurezza** > **Riferimento API** > **Abilita accesso API** nella console di gestione di Google).

La password dell'amministratore con privilegi elevati non viene memorizzata in nessun luogo e non è usata per eseguire backup e ripristino. La modifica di questa password in Google Workspace non compromette la funzionalità del servizio Cyber Protection.

© Acronis International GmbH, 2003-2024

Se l'amministratore con privilegi elevati che ha aggiunto l'organizzazione di Google Workspace viene eliminato da Google Workspace o assegnato a un ruolo con privilegi inferiori, i backup non verranno completati correttamente ma con un errore di "accesso negato". In questo caso, ripetere la procedura descritta in "Aggiunta di un'organizzazione Google Workspace" (pag. 656) e specificare credenziali valide per l'amministratore con privilegi elevati. Per evitare questa situazione, si consiglia di creare un utente amministratore con privilegi elevati per l'esecuzione del backup e del ripristino.

Informazioni sulla pianificazione dei backup

Poiché un agente cloud serve più clienti, stabilisce l'orario di avvio di ogni piano di protezione in modo autonomo, per garantire l'uniformità del carico durante il giorno e una qualità del servizio paritaria per tutti i clienti.

Ogni piano di protezione viene eseguito ogni giorno alla stessa ora.

L'opzione predefinita è **Una volta al giorno**. Con il pacchetto Advanced Backup è possibile pianificare un massimo di sei backup giornalieri. I backup si avviano a intervalli approssimativi che dipendono dal carico corrente dell'agente cloud, che serve più clienti in un data center. Ciò garantisce un'equa distribuzione del carico durante il giorno e un'equa qualità del servizio per tutti i clienti.

Limitazioni

- La console mostra soltanto gli utenti ai quali è stata assegnata una licenza di Google Workspace e una casella di posta o Google Drive.
- Il backup dei documenti nei formati nativi di Google viene eseguito come documenti di Office generici; questi ultimi vengono visualizzati con un'estensione differente nella console di Cyber Protect, ad esempio .docx o .pptx. Durante il ripristino, tali documenti vengono convertiti di nuovo nel loro formato originale.
- Non è possibile superare le 10 esecuzioni manuali di backup in un'ora.
- Non è possibile eseguire più di 10 operazioni di ripristino simultanee (il numero include ripristini di Microsoft 365 e di Google Workspace).
- Non è possibile ripristinare simultaneamente elementi da punti di ripristino differenti, anche se è possibile selezionare tali elementi nei risultati della ricerca.
- I backup degli account utente di Google Workspace eliminati non vengono automaticamente eliminati dal cloud storage. Il costo dello spazio di storage utilizzato da tali backup viene quindi addebitato.
- Non è possibile applicare più di un piano di backup allo stesso workload.
- Se un piano di backup singolo e un piano di backup di gruppo vengono applicati allo stesso workload, le impostazioni del piano singolo avranno priorità.

© Acronis International GmbH, 2003-2024

Registrazione

Le azioni compiute con le risorse cloud-to-cloud, come la visualizzazione del contenuto di e-mail di cui è stato eseguito il backup, il download di allegati o file, il ripristino di e-mail in caselle di posta diverse da quella originaria o il loro invio come e-mail, possono violare la privacy degli utenti. Queste azioni vengono registrate nel portale di gestione, in **Monitoraggio** > **Registro di audit**.

Aggiunta di un'organizzazione Google Workspace

Per aggiungere un'organizzazione Google Workspace al servizio Cyber Protection, è necessario un progetto personale Google Cloud dedicato. Per ulteriori informazioni su come creare e configurare questo tipo di progetto, fare riferimento a "Creazione di un progetto personale Google Cloud" (pag. 657).

Per aggiungere un'organizzazione Google Workspace utilizzando un progetto personale Google Cloud dedicato

1. Accedere alla console di Cyber Protect come amministratore aziendale.
2. Fare clic su **Dispositivi** > **Aggiungi** > **Google Workspace**.
3. Inserire l'indirizzo e-mail di un amministratore con privilegi avanzati dell'account Google Workspace.
   Per questa procedura è irrilevante che la verifica in due passaggi sia abilitata per l'account e-mail dell'amministratore con privilegi avanzati.
4. Individuare il file JSON che contiene la chiave privata dell'account del servizio creato nel progetto Google Cloud personale.
   È possibile incollare il contenuto del file come testo.
5. Fare clic su **Conferma**.

L'organizzazione di Google Workspace viene visualizzata nella scheda **Dispositivi** della console di Cyber Protect.

Suggerimenti utili

- Dopo aver aggiunto un'organizzazione Google Workspace, viene eseguito il backup dei dati dell'utente e delle unità condivise nel dominio primario e in tutti i domini secondari, se presenti. Le risorse oggetto di backup verranno visualizzate in un elenco e non saranno raggruppate in base al dominio.
- L'agente cloud esegue la sincronizzazione con Google Workspace ogni 24 ore, a partire dal momento in cui l'organizzazione è aggiunta al servizio Cyber Protection. Se un utente o un'unità condivisa vengono aggiunti o rimossi, la modifica non viene immediatamente visualizzata nella console di Cyber Protect. Per sincronizzare immediatamente la modifica, selezionare l'organizzazione nella pagina di **Google Workspace**, quindi fare clic su **Aggiorna**.

© Acronis International GmbH, 2003-2024

Per ulteriori informazioni sulla sincronizzazione delle risorse di un'organizzazione Google Workspace e la console di Cyber Protect, fare riferimento a "Individuazione delle risorse di Google Workspace" (pag. 660).

- Se è stato applicato un piano di protezione al gruppo **Tutti gli utenti** o **Tutte le unità condivise**, gli elementi appena aggiunti vengono inclusi nel backup solo dopo la sincronizzazione.
- In base alla policy di Google, quando un utente o un'unità condivisa sono stati rimossi dall'interfaccia utente grafica di Google Workspace, restano disponibili per qualche giorno tramite l'API. In questo periodo l'elemento rimosso è inattivo (mostrato in grigio) nella console di Cyber Protect e non ne viene eseguito il backup. Quando l'elemento rimosso non è più disponibile neanche tramite l'API, non sarà più visualizzato nella console di Cyber Protect. I relativi backup (se presenti) sono reperibili in **Archivi di backup** > **Backup di applicazioni cloud**.

Creazione di un progetto personale Google Cloud

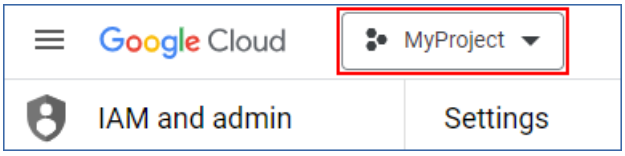
Per aggiungere un'organizzazione Google Workspace al servizio Cyber Protection utilizzando un progetto personale Google Cloud dedicato, è necessario procedere come indicato di seguito:

1. Creare un nuovo progetto Google Cloud.
2. Abilitare le API richieste per il progetto.
3. Configurare le credenziali per questo progetto:
   a. Configurare la schermata per il consenso OAuth.
   b. Creare e configurare l'account del servizio per il servizio Cyber Protection.
4. Garantire l'accesso al nuovo progetto all'account Google Workspace.

Nota
Questo argomento contiene una descrizione delle interfacce utente di terzi che possono essere soggette a modifica senza preavviso.

Per creare un nuovo progetto Google Cloud

1. Accedere a Google Cloud Platform (console.cloud.google.com) come Amministratore con privilegi avanzati.
2. Nella console di Google Cloud Platform, fare clic sul selettore dei progetti nell'angolo in a sinistra.



3. Nella schermata visualizzata, selezionare un'organizzazione e quindi fare clic su **New project**.

© Acronis International GmbH, 2003-2024

4. Specificare un nome per il nuovo progetto.
5. Fare clic su **Create**.

   Viene creato il nuovo progetto Google Cloud.

   Per abilitare le API necessarie per questo progetto

   1. Nella console di Google Cloud Platform, selezionare il nuovo progetto.
   2. Nel menu di navigazione, selezionare **APIs and services** > **Enabled APIs and services**.
   3. Una alla volta, disabilitare tutte le API abilitate per impostazione predefinita per questo progetto:
      a. Scorrere verso il basso la pagina **Enabled APIs and services**, quindi fare clic sul nome di un'API abilitata.
         Viene visualizzata la pagina **API/Service details** dell'API selezionata.
      b. Fare clic su **Disable API**, quindi confermare la selezione facendo clic su **Disable**.
      c. [Se richiesto] Confermare la selezione facendo clic su **Confirm**.
      d. Tornare a **APIs and Services** > **Enabled APIs and services** e disabilitare l'API successiva.
   4. Nel menu di navigazione, selezionare **APIs and Services** > **Library**.
   5. Una alla volta, abilitare le seguenti API nella libreria delle API:
      - Admin SDK API
      - Gmail API
      - Google Calendar API
      - Google Drive API
      - Google People API

      Utilizzare la barra di ricerca per trovare le API richieste. Per abilitare un'API, selezionarne il nome e quindi fare clic su **Enable**. Per cercare l'API successiva, tornare alla libreria delle API selezionando **APIs and services** > **Library** nel menu di navigazione.

   Per configurare la schermata per il consenso OAuth

   1. Nel menu di navigazione di Google Cloud Platform, selezionare **APIs and services** > **OAuth consent screen**.
   2. Nella finestra visualizzata, selezionare **Internal** come tipo di utente e quindi fare clic su **Create**.
   3. Nel campo **App name** specificare un nome per l'applicazione.
   4. Nel campo **User support email**, immettere l'indirizzo e-mail dell'amministratore con privilegi avanzati.
   5. Nel campo **Developer contact information**, immettere l'indirizzo e-mail dell'amministratore con privilegi avanzati.
   6. Lasciare tutti gli altri campi in bianco, quindi fare clic su **Save and continue**.
   7. Nella pagina **Scopes**, fare clic su **Save and continue** senza modificare nulla.
   8. Nella pagina **Summary**, verificare le impostazioni e quindi fare clic su **Back to dashboard**.

© Acronis International GmbH, 2003-2024

Per creare e configurare l'account del servizio per il servizio Cyber Protection

1. Nel menu di navigazione in Google Cloud Platform, selezionare **IAM & Admin** > **Service accounts**.
2. Fare clic su **Create service account**.
3. Specificare un nome per l'account del servizio.
4. [Facoltativo] Specificare una descrizione per l'account del servizio.
5. Fare clic su **Create and continue**.
6. Nei passaggi **Grant this service account access to the project** e **Grant users access to this service account** non modificare alcun campo.
7. Fare clic su **Done**.

   Viene visualizzata la pagina **Service accounts**.
8. Nella pagina **Service accounts**, selezionare il nuovo account del servizio, quindi in **Actions** fare clic su **Manage keys**.
9. In **Keys**, fare clic su **Add key** > **Create new key** e selezionare il tipo di chiave **JSON**.
10. Fare clic su **Create**.

    Un file JSON contenente la chiave privata dell'account del servizio viene automaticamente scaricata nel sistema dell'utente. Archiviare questo file in modo sicuro, perché sarà necessario per aggiungere l'organizzazione di Google Workspace al servizio Cyber Protection.

Per concedere l'accesso al nuovo progetto all'account Google Workspace

1. Nel menu di navigazione di Google Cloud Platform, selezionare **IAM & Admin** > **Service Accounts**.
2. Nell'elenco, individuare l'account del servizio creato, quindi copiare il relativo ID client visualizzato nella colonna **OAuth 2.0 Client ID**.
3. Accedere alla console di Google Admin (admin.google.com) come Amministratore con privilegi avanzati.
4. Nel menu di navigazione, selezionare **Security** > **Access and data control** > **API controls**.
5. Scorrere verso il basso la pagina **API controls**, quindi in **Domain-wide delegation** fare clic su **Manage domain-wide delegation**.

   Viene visualizzata la pagina **Domain-wide delegation**.
6. Nella pagina **Domain-wide delegation** fare clic su **Add new**.

   Viene visualizzata la pagina **Add a new client ID**.
7. Nel campo **Client ID** immettere l'ID cliente del cliente dell'account del servizio.
8. Nel campo **OAuth scopes**, copiare e incollare gli ambiti seguenti, delimitati da virgole:

   ```
   https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googleapis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleapis.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
   ```

   In alternativa, è possibile aggiungere gli ambiti su ogni riga:

© Acronis International GmbH, 2003-2024

- https://mail.google.com
- https://www.googleapis.com/auth/contacts
- https://www.googleapis.com/auth/calendar
- https://www.googleapis.com/auth/admin.directory.user.readonly
- https://www.googleapis.com/auth/admin.directory.domain.readonly
- https://www.googleapis.com/auth/drive
- https://www.googleapis.com/auth/gmail.modify

9. Fare clic su **Authorise**.

Il nuovo progetto Google Cloud può ora accedere ai dati dell'account Google Workspace. Per eseguire il backup dei dati, è necessario collegare questo progetto al servizio Cyber Protection. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Per aggiungere un'organizzazione Google Workspace utilizzando un progetto personale Google Cloud dedicato" (pag. 656).

Se è necessario revocare l'accesso del progetto Google Cloud all'account Google Workspace, e rispettivamente l'acceso del servizio Cyber Protection, eliminare il client API utilizzato dal progetto.

Per revocare l'accesso all'account Google Workspace

1. Accedere alla console di amministrazione Google (admin.google.com) con privilegi di super amministratore.
2. Nel menu di navigazione, selezionare **Security** > **Access and data control** > **API controls**.
3. Scorrere verso il basso la pagina **API controls**, quindi in **Domain-wide delegation** fare clic su **Manage domain-wide delegation**.
   Viene visualizzata la pagina **Domain-wide delegation**.
4. Nella pagina **Domain-wide delegation**, selezionare il client API utilizzato dal progetto e fare clic su **Delete**.
   Il progetto Google Cloud e il servizio Cyber Protection non potranno più accedere all'account Google Workspace né eseguire il backup dei dati che contiene.

Individuazione delle risorse di Google Workspace

Quando si aggiunge un'organizzazione Google Workspace al servizio Cyber Protection, le risorse di questa organizzazione, come le caselle di posta e i Google Drive, vengono sincronizzate con la console di Cyber Protect. Questa operazione è chiamata individuazione e viene registrata in **Monitoraggio** > **Attività**.

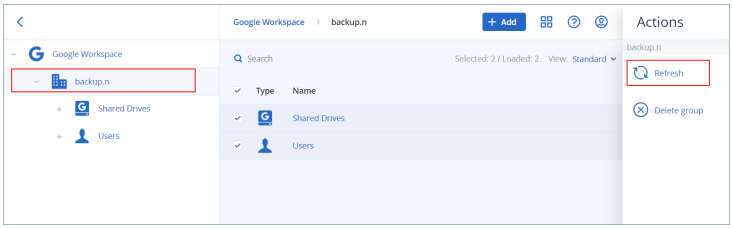
Una volta completata l'operazione di individuazione, le risorse dell'organizzazione Google Workspace sono visualizzate nella scheda **Dispositivi** > **Google Workspace** nella console di Cyber Protect, ed è possibile applicare a queste i piani di backup.

© Acronis International GmbH, 2003-2024

Una volta al giorno, viene eseguita un'operazione di individuazione automatica, per garantire che l'elenco delle risorse nella console di Cyber Protect sia sempre aggiornato. È anche possibile sincronizzare l'elenco su richiesta, avviando manualmente l'operazione di individuazione.

Per eseguire manualmente l'operazione di individuazione

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Google Workspace**.
2. Selezionare l'organizzazione Google Workspace e quindi nel pannello **Azioni**, fare clic su **Aggiorna**.



Nota
È possibile eseguire manualmente un'operazione di individuazione fino a 10 volte in un'ora. Una volta raggiunto questo numero, il numero di esecuzioni consentite viene ripristinato a una per ora, e da questo momento in poi è possibile eseguire un'esecuzione aggiuntiva ogni ora, fino a quando non viene raggiunto di nuovo il totale di 10 esecuzioni per ora.

Impostazione della frequenza dei backup di Google Workspace

Per impostazione predefinita, i backup di Google Workspace vengono eseguiti una volta al giorno e non sono disponibili ulteriori opzioni di pianificazione.

Se nel tenant è abilitato il pacchetto Advanced Backup, è possibile configurare backup più frequenti. È possibile selezionare il numero di backup quotidiani, ma non l'orario di avvio del backup. I backup si avviano automaticamente a intervalli approssimativi che dipendono dal carico corrente dell'agente cloud, che serve più clienti in un data center. Ciò garantisce un'equa distribuzione del carico durante il giorno e un'equa qualità del servizio per tutti i clienti.

Sono disponibili le seguenti opzioni.

Opzioni di pianificazione	Intervallo approssimativo tra ciascun backup
Una volta al giorno	24 ore
Due volte al giorno (predefinito)	12 ore
3 volte al giorno	8 ore
6 volte al giorno	4 ore

© Acronis International GmbH, 2003-2024

Nota
A seconda del carico sull'agente cloud e della possibile limitazione di banda sul lato Google Workspace, un backup potrebbe iniziare più tardi del previsto o richiedere più tempo per essere completato. Se il backup dura di più rispetto all'intervallo medio tra due backup, il backup successivo verrà ripianificato, il che potrebbe risultare in un numero di backup al giorno inferiore rispetto a quanto selezionato. Ad esempio, potrebbe essere possibile completare solo due backup al giorno, anche se ne sono stati selezionati sei al giorno.

Protezione dei dati di Gmail

Di quali elementi è possibile eseguire il backup?

È possibile eseguire il backup delle caselle di posta degli utenti di Gmail. Il backup di una casella postale include anche i dati del calendario e dei contatti. Facoltativamente, è possibile scegliere di eseguire il backup dei calendari condivisi.

Durante il backup vengono *ignorati* gli elementi seguenti:

- I calendari **Compleanni**, **Promemoria**, **Tasks**
- Cartelle allegate agli eventi del calendario
- La cartella **Directory** in Contatti

I seguenti elementi del calendario vengono *ignorati* a causa delle limitazioni dell'API di Google Calendar:

- Slot degli appuntamenti
- Il campo relativo alla conferenza di un evento
- L'impostazione del calendario **Notifiche di eventi di tutto il giorno**
- L'impostazione del calendario **Accetta automaticamente gli inviti** (nei calendari per sale o spazi condivisi)

I seguenti elementi del calendario vengono *ignorati* a causa delle limitazioni dell'API di Google People:

- La cartella **Altri contatti**
- I profili esterni di un contatto (**Profilo Directory**, **Profilo Google**)
- Il campo del contatto **Archivia come**

Quali elementi è possibile ripristinare?

Dal backup di una casella postale è possibile ripristinare i seguenti elementi:

© Acronis International GmbH, 2003-2024

- Caselle postali
- Cartelle e-mail (nella terminologia Google sono denominate “Etichette”. Le **Etichette** sono presentate nel software di backup come cartelle, per coerenza con la presentazione degli altri dati.)
- Messaggi e-mail
- Eventi di calendario
- Contatti

È possibile utilizzare la funzionalità di ricerca per localizzare gli elementi in un backup.

Durante il ripristino di caselle di posta e di elementi delle caselle di posta, è possibile selezionare se sovrascrivere o meno gli elementi nella posizione di destinazione.

Limitazioni

- Non è possibile ripristinare le foto dei contatti
- L’elemento del calendario **Fuori sede** viene ripristinato come evento del calendario standard, a causa delle limitazioni dell’API Google Calendar

Selezione delle caselle di posta di Gmail

Selezionare le caselle di posta come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Per selezionare caselle di posta di Gmail

1. Fare clic su **Google Workspace**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, selezionare l’organizzazione i cui dati utente devono essere sottoposti a backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per eseguire il backup delle caselle di posta di tutti gli utenti (incluse quelle che verranno create in futuro), espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, quindi fare clic su **Raggruppa backup**.
   - Per eseguire il backup di singole caselle di posta utente, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare gli utenti la cui casella di posta si desidera sottoporre a backup e quindi fare clic su **Backup**.
4. Nel pannello del piano di protezione:
   - Verificare che l’elemento **Gmail** sia selezionato in **Cosa includere nel backup**.
   - Per eseguire il backup dei calendari condivisi con gli utenti selezionati, abilitare l’opzione **Includi calendari condivisi**.
   - Decidere se è necessario poter eseguire la ricerca testo completo nei messaggi e-mail di cui è stato eseguito il backup. Per accedere all’opzione, fare clic sull'icona ingranaggio, quindi scegliere **Opzioni di backup** > **Ricerca testo completo**.

© Acronis International GmbH, 2003-2024

Ripristino di caselle postali e di elementi delle caselle postali

Ripristino delle caselle postali

1. Fare clic su **Google Workspace**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente di cui ripristinare la casella di posta, quindi fare clic su **Ripristino**.

   Se l'utente è stato eliminato, selezionarlo nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.

   È possibile cercare gli utenti e i gruppi per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.

   Nota
   Per visualizzare solo i punti di ripristino che contengono caselle di posta, selezionare **Gmail** in **Filtra per contenuto**.
5. Fare clic su **Ripristina** > **Intera casella di posta**.
6. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, fare clic su **Organizzazione di Google Workspace** per visualizzare, modificare o specificare l'organizzazione di destinazione.

   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare una nuova organizzazione di destinazione dalle organizzazioni registrate disponibili.
7. In **Ripristina nelle caselle di posta**, visualizzare, modificare o specificare la casella di posta di destinazione.

   Per impostazione predefinita, viene selezionata la casella di posta originale. Se questa casella di posta non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare la casella di posta di destinazione.

   Non è possibile creare una nuova casella di posta di destinazione durante il ripristino. Per ripristinare una casella di posta in una nuova, è innanzitutto necessario creare la casella di posta di destinazione nell'organizzazione Google Workspace desiderata, e quindi consentire all'agente cloud di sincronizzare la modifica. L'agente cloud esegue la sincronizzazione con Google Workspace ogni 24 ore. Per sincronizzare immediatamente la modifica, nella console di Cyber Protect selezionare l'organizzazione nella pagina di **Google Workspace** quindi fare clic su **Aggiorna**.
8. Fare clic su **Avvia ripristino**.
9. Selezionare una delle opzioni di sovrascrittura:

© Acronis International GmbH, 2003-2024

- **Sovrascrivi gli elementi esistenti**
- **Non sovrascrivere gli elementi esistenti**

10. Fare clic su **Procedi** per confermare la decisione.

Ripristino di elementi di casella di posta

1. Fare clic su **Google Workspace**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente la cui casella di posta conteneva in origine gli elementi da ripristinare e quindi fare clic su **Ripristino**.
   Se l'utente è stato eliminato, selezionarlo nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.
   È possibile cercare gli utenti e i gruppi per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.

   Nota
   Per visualizzare solo i punti di ripristino che contengono caselle di posta, selezionare **Gmail** in **Filtra per contenuto**.

5. Fare clic su **Ripristina** > **Messaggi e-mail**.
6. Passare alla cartella richiesta. Se il backup non è crittografato, è possibile utilizzare la ricerca per ottenere l'elenco degli elementi richiesti.
   Sono disponibili le opzioni di ricerca seguenti. I caratteri jolly non sono supportati.
   - Per i messaggi e-mail: ricerca per oggetto, mittente, destinatario, data, nome dell'allegato e contenuto del messaggio.
     Quando si effettua una ricerca per data, è possibile selezionare una data di inizio o una data di fine (entrambe comprese) oppure entrambe le date per effettuare una ricerca in un intervallo di tempo.
     La ricerca per nome dell'allegato o nel contenuto del messaggio fornisce risultati solo se l'opzione **Ricerca testo completo** è stata attivata durante il backup. Come ulteriore parametro è possibile specificare la lingua del frammento di messaggio da cercare.
   - Per gli eventi: ricerca per titolo e data.
   - Per i contatti: ricerca per nome, indirizzo e-mail e numero di telefono.
7. Selezionare gli elementi che si desidera ripristinare. Per poter selezionare le cartelle, fare clic sull'icona di ripristino delle cartelle:
   Inoltre, è possibile eseguire una delle seguenti operazioni:
   - Dopo aver selezionato un elemento, fare clic su **Mostra contenuto** per visualizzarne il contenuto, inclusi gli allegati. Fare clic sul nome di un file allegato per scaricarlo.

© Acronis International GmbH, 2003-2024

- Solo se il backup non è crittografato, è stata usata la ricerca e selezionato un unico elemento nei risultati della ricerca, è possibile fare clic su **Mostra versioni** per selezionare la versione dell'elemento da ripristinare. È possibile selezionare qualsiasi versione di cui sia stato eseguito il backup, precedente o successiva al punto di ripristino selezionato.

8. Fare clic su **Ripristina**.
9. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, fare clic su **Organizzazione di Google Workspace** per visualizzare, modificare o specificare l'organizzazione di destinazione.

   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare una nuova organizzazione di destinazione dalle organizzazioni registrate disponibili.
10. In **Ripristina nelle caselle di posta**, visualizzare, modificare o specificare la casella di posta di destinazione.

    Per impostazione predefinita, viene selezionata la casella di posta originale. Se questa casella di posta non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare la casella di posta di destinazione.
11. In **Percorso**, visualizzare o modificare la cartella di destinazione nella casella di posta di destinazione. Per impostazione predefinita, viene selezionata la cartella originale.
12. Fare clic su **Avvia ripristino**.
13. Selezionare una delle opzioni di sovrascrittura:
    - **Sovrascrivi gli elementi esistenti**
    - **Non sovrascrivere gli elementi esistenti**
14. Fare clic su **Procedi** per confermare la decisione.

Protezione di file di Google Drive

Di quali elementi è possibile eseguire il backup?

È possibile eseguire il backup di un intero Google Drive o di singoli file e cartelle. Il backup dei file viene eseguito insieme alle autorizzazioni di condivisione.

Importante
Non viene eseguito il backup degli elementi seguenti:

- La cartella **Condivisi con me**
- La cartella **Computer** (creata dal client di backup e sincronizzazione)

Limitazioni

Oltre ai formati di file specifici di Google, è supportato il backup e il ripristino di Documenti di Google, Fogli di Google e Presentazioni di Google. Altri formati specifici di Google potrebbero non essere completamente supportati o non supportati affatto. Nello specifico, i file di Disegni Google

© Acronis International GmbH, 2003-2024

vengono ripristinati come file `.svg`, i file di Google Sites vengono ripristinati come file `.txt`, i file di Google Jamboard vengono ripristinati come file `.pdf` e i file di Google My Maps vengono ignorati durante un backup.

Nota
I formati di file non specifici di Google, ad esempio `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip`, sono completamente supportati nelle attività di backup e ripristino.

Quali elementi è possibile ripristinare?

È possibile ripristinare un intero Google Drive o qualsiasi file o cartella di cui è stato eseguito il backup.

È possibile scegliere se ripristinare le autorizzazioni condivise o lasciare che i file ereditino le autorizzazioni dalla cartella in cui vengono ripristinati.

Limitazioni

- I commenti nei file non vengono ripristinati.
- Non vengono ripristinati i collegamenti di condivisione di file e cartelle.
- Non è possibile modificare le **impostazioni di sola lettura del proprietario** dei file condivisi (**Impedisci agli editor di modificare gli accessi e aggiungere nuove persone** e **Disattiva le opzioni di download, stampa e copia per commentatori/visualizzatori**) durante un ripristino.
- Non è possibile modificare la proprietà di una cartella condivisa durante un ripristino se l'opzione **Impedisci agli editor di modificare gli accessi e aggiungere nuove persone** è abilitata per la cartella. Questa impostazione impedisce all'API di Google Drive di elencare le autorizzazioni della cartella. La proprietà dei file nella cartella viene ripristinata correttamente.

Selezione di file di Google Drive

Selezionare i file come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Per selezionare file di Google Drive

1. Fare clic su **Google Workspace**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, selezionare l'organizzazione i cui dati utente devono essere sottoposti a backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per eseguire il backup dei file di tutti gli utenti (inclusi quelli che verranno creati in futuro), espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, quindi fare clic su **Raggruppa backup**.

© Acronis International GmbH, 2003-2024

- Per eseguire il backup di file di singoli utenti, espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare gli utenti i cui file si desidera sottoporre a backup e quindi fare clic su **Backup**.

4. Nel pannello del piano di protezione:
   - Verificare che l'elemento **Google Drive** sia selezionato in **Cosa includere nel backup**.
   - In **Elementi di cui eseguire il backup**, eseguire una delle seguenti operazioni:
     - Mantenere l'impostazione predefinita **[Tutti]** (tutti i file).
     - Specificare i file e le cartelle di cui eseguire il backup aggiungendo i nomi o i percorsi.
       È possibile utilizzare i caratteri jolly *, ** e ?. Per ulteriori dettagli su come specificare percorsi e utilizzare i caratteri jolly, fare riferimento a "Filtri file".
     - Specificare i file e le cartelle di cui eseguire il backup scorrendo l'elenco.
       Il collegamento **Sfoglia** è disponibile solo quando si crea un piano di protezione per un singolo utente.
   - [Facoltativo] In **Elementi di cui eseguire il backup**, fare clic su **Mostra esclusioni** per specificare i file e le cartelle da ignorare durante il backup.
     L'esclusione dei file prevale sulla selezione dei file: se si specifica lo stesso file in entrambi i campi, il file verrà ignorato durante il backup.
   - Per abilitare l'autenticazione di tutti i file selezionati per il backup, abilitare l'opzione **Autenticazione**. Per ulteriori informazioni sull'autenticazione, fare riferimento ad "Autenticazione".

Ripristino di Google Drive e di file di Google Drive

Ripristino di un intero Google Drive

1. Fare clic su **Google Workspace**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente di cui ripristinare il Google Drive, quindi fare clic su **Ripristino**.
   Se l'utente è stato eliminato, selezionarlo nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.
   È possibile cercare gli utenti per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.

   Nota
   Per visualizzare solo i punti di ripristino che contengono file di Google Drive, selezionare **Google Drive** in **Filtra per contenuto**.

5. Fare clic su **Ripristina** > **Intera unità**.

© Acronis International GmbH, 2003-2024

6. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, fare clic su **Organizzazione di Google Workspace** per visualizzare, modificare o specificare l'organizzazione di destinazione.

   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare una nuova organizzazione di destinazione dalle organizzazioni registrate disponibili.
7. In **Ripristina nell'unità**, visualizzare, modificare o specificare l'utente o l'unità condivisa di destinazione.

   Per impostazione predefinita, è selezionato l'utente originale. Se questo utente non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare l'utente o l'unità condivisa di destinazione.

   Se il backup contiene file condivisi, tali file verranno ripristinati nella cartella radice dell'unità di destinazione.
8. Selezionare se ripristinare o meno le autorizzazioni di condivisione dei file.
9. Fare clic su **Avvia ripristino**.
10. Selezionare una delle opzioni di sovrascrittura:

Opzione	Descrizione
Sovrascrivi il file esistente se meno recente	Se nella posizione di destinazione è presente un file con lo stesso nome, e se tale file è meno recente del file di origine, il file di origine viene salvato nella posizione di destinazione e sostituisce la versione precedente.
Sovrascrivi i file esistenti	Tutti i file esistenti nella posizione di destinazione vengono sovrascritti, qualunque sia la data dell'ultima modifica.
Non sovrascrivere i file esistenti	Se nella posizione di destinazione è presente un file con lo stesso nome, tale file non viene modificato e il file di origine non viene salvato nella posizione di destinazione.

11. Fare clic su **Procedi** per confermare la decisione.

Ripristino di file di Google Drive

1. Fare clic su **Google Workspace**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Utenti**, selezionare **Tutti gli utenti**, selezionare l'utente di cui ripristinare i file di Google Drive, quindi fare clic su **Ripristino**.

   Se l'utente è stato eliminato, selezionarlo nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.

   È possibile cercare gli utenti per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.

© Acronis International GmbH, 2003-2024

Nota
Per visualizzare solo i punti di ripristino che contengono file di Google Drive, selezionare **Google Drive** in **Filtra per contenuto**.

5. Fare clic su **Ripristina** > **File/cartelle**.
6. Esplorare la cartella richiesta o utilizzare la ricerca per ottenere l'elenco dei file e delle cartelle necessarie.
7. Selezionare i dati che si desidera ripristinare.
   Se il backup non è crittografato ed è stato selezionato un solo file è possibile fare clic su **Mostra versioni** per selezionare la versione del file da ripristinare. È possibile selezionare qualsiasi versione di cui sia stato eseguito il backup, precedente o successiva al punto di ripristino selezionato.
8. Per scaricare un file, selezionarlo e fare clic su **Download**, selezionare la posizione in cui salvare i dati e quindi fare clic su **Salva**. Altrimenti, ignorare questo passaggio.
9. Fare clic su **Ripristina**.
10. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, fare clic su **Organizzazione di Google Workspace** per visualizzare, modificare o specificare l'organizzazione di destinazione.
    Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare una nuova organizzazione di destinazione dalle organizzazioni registrate disponibili.
11. In **Ripristina nell'unità**, visualizzare, modificare o specificare l'utente o l'unità condivisa di destinazione.
    Per impostazione predefinita, è selezionato l'utente originale. Se questo utente non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare l'utente o l'unità condivisa di destinazione.
12. In **Percorso**, visualizzare o modificare la cartella di destinazione nel Google Drive dell'utente di destinazione o nell'unità condivisa di destinazione. Per impostazione predefinita, è selezionato il percorso originale.
13. Selezionare se ripristinare o meno le autorizzazioni di condivisione dei file.
14. Fare clic su **Avvia ripristino**.
15. Selezionare una delle opzioni di sovrascrittura dei file:

Opzione	Descrizione
Sovrascrivi il file esistente se meno recente	Se nella posizione di destinazione è presente un file con lo stesso nome, e se tale file è meno recente del file di origine, il file di origine viene salvato nella posizione di destinazione e sostituisce la versione precedente.
Sovrascrivi i file esistenti	Tutti i file esistenti nella posizione di destinazione vengono sovrascritti, qualunque sia la data dell'ultima modifica.

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
Non sovrascrivere i file esistenti	Se nella posizione di destinazione è presente un file con lo stesso nome, tale file non viene modificato e il file di origine non viene salvato nella posizione di destinazione.

16. Fare clic su **Procedi** per confermare la decisione.

Protezione di file di unità condivise

Di quali elementi è possibile eseguire il backup?

È possibile eseguire il backup di un'intera unità condivisa o di singoli file e cartelle. Il backup dei file viene eseguito insieme alle autorizzazioni di condivisione.

Importante
Non viene eseguito il backup della cartella **Condivisi con me**.

Limitazioni

- Non è possibile eseguire il backup di un'unità condivisa che non contiene membri, a causa delle limitazioni dell'API di Google Drive.
- Oltre ai formati di file specifici di Google, è supportato il backup e il ripristino di Documenti di Google, Fogli di Google e Presentazioni di Google. Altri formati specifici di Google potrebbero non essere completamente supportati o non supportati affatto. Nello specifico, i file di Disegni Google vengono ripristinati come file `.svg`, i file di Google Sites vengono ripristinati come file `.txt`, i file di Google Jamboard vengono ripristinati come file `.pdf` e i file di Google My Maps vengono ignorati durante un backup.

  Nota
  I formati di file non specifici di Google, ad esempio `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip`, sono completamente supportati nelle attività di backup e ripristino.

Quali elementi è possibile ripristinare?

È possibile ripristinare un'intera unità condivisa o qualsiasi file o cartella di cui è stato eseguito il backup.

È possibile scegliere se ripristinare le autorizzazioni condivise o lasciare che i file ereditino le autorizzazioni dalla cartella in cui vengono ripristinati.

Non vengono ripristinati gli elementi seguenti:

- Le autorizzazioni di condivisione per un file che è stato condiviso con un utente esterno all'organizzazione non vengono ripristinate se la condivisione esterna all'organizzazione è disabilitata nell'unità condivisa di destinazione.

© Acronis International GmbH, 2003-2024

- Le autorizzazioni di condivisione per un file che è stato condiviso con un utente che non è membro dell'unità condivisa di destinazione non vengono ripristinate se l'impostazione di **condivisione con persone non appartenenti all'organizzazione** è disabilitata nell'unità condivisa di destinazione.

Limitazioni

- I commenti nei file non vengono ripristinati.
- Non vengono ripristinati i collegamenti di condivisione di file e cartelle.

Selezione di file di unità condivise

Selezionare i file come descritto di seguito, quindi specificare eventuali altre impostazioni del piano di protezione come necessario.

Per selezionare file di unità condivise

1. Fare clic su **Google Workspace**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, selezionare l'organizzazione i cui dati utente devono essere sottoposti a backup. Altrimenti, ignorare questo passaggio.
3. Eseguire una delle seguenti operazioni:
   - Per eseguire il backup dei file di tutte le unità condivise (incluse quelle che verranno create in futuro), espandere il nodo **Unità condivise**, selezionare **Tutte le unità condivise**, quindi fare clic su **Raggruppa backup**.
   - Per eseguire il backup dei file di singole unità condivise, espandere il nodo **Unità condivise**, selezionare **Tutte le unità condivise**, selezionare le unità condivise di cui eseguire il backup, quindi fare clic su **Backup**.
4. Nel pannello del piano di protezione:
   - In **Elementi di cui eseguire il backup**, eseguire una delle seguenti operazioni:
     - Mantenere l'impostazione predefinita **[Tutti]** (tutti i file).
     - Specificare i file e le cartelle di cui eseguire il backup aggiungendo i nomi o i percorsi.
       È possibile utilizzare i caratteri jolly *, ** e ?. Per ulteriori dettagli su come specificare percorsi e utilizzare i caratteri jolly, fare riferimento a "Filtri file".
     - Specificare i file e le cartelle di cui eseguire il backup scorrendo l'elenco.
       Il collegamento **Sfoglia** è disponibile solo quando si crea un piano di protezione per una singola unità condivisa.
   - [Facoltativo] In **Elementi di cui eseguire il backup**, fare clic su **Mostra esclusioni** per specificare i file e le cartelle da ignorare durante il backup.
     L'esclusione dei file prevale sulla selezione dei file: se si specifica lo stesso file in entrambi i campi, il file verrà ignorato durante il backup.

© Acronis International GmbH, 2003-2024

- Per abilitare l'autenticazione di tutti i file selezionati per il backup, abilitare l'opzione **Autenticazione**. Per ulteriori informazioni sull'autenticazione, fare riferimento ad "Autenticazione".

Ripristino di unità condivise e di file di unità condivise

Ripristino di un'intera unità condivisa

1. Fare clic su **Google Workspace**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Unità condivise**, selezionare **Tutte le unità condivise**, selezionare l'utente di cui ripristinare l'unità condivisa, quindi fare clic su **Ripristino**.
   Se l'unità condivisa è stata eliminata, selezionarla nella sezione **Backup delle applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.
   È possibile cercare le unità condivise per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina** > **Entire Shared drive (Intera unità condivisa)**.
6. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, fare clic su **Organizzazione di Google Workspace** per visualizzare, modificare o specificare l'organizzazione di destinazione.
   Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare una nuova organizzazione di destinazione dalle organizzazioni registrate disponibili.
7. In **Ripristina nell'unità**, visualizzare, modificare o specificare l'utente di destinazione o l'unità condivisa di destinazione. Se si specifica un utente, i dati verranno ripristinati nel Google Drive di tale utente.
   Per impostazione predefinita, è selezionata l'unità condivisa originale. Se questa unità condivisa non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare l'utente o l'unità condivisa di destinazione.
8. Selezionare se ripristinare o meno le autorizzazioni di condivisione dei file.
9. Fare clic su **Avvia ripristino**.

© Acronis International GmbH, 2003-2024

10. Selezionare una delle opzioni di sovrascrittura:

Opzione	Descrizione
Sovrascrivi il file esistente se meno recente	Se nella posizione di destinazione è presente un file con lo stesso nome, e se tale file è meno recente del file di origine, il file di origine viene salvato nella posizione di destinazione e sostituisce la versione precedente.
Sovrascrivi i file esistenti	Tutti i file esistenti nella posizione di destinazione vengono sovrascritti, qualunque sia la data dell'ultima modifica.
Non sovrascrivere i file esistenti	Se nella posizione di destinazione è presente un file con lo stesso nome, tale file non viene modificato e il file di origine non viene salvato nella posizione di destinazione.

11. Fare clic su **Procedi** per confermare la decisione.

Ripristino di file di unità condivise

1. Fare clic su **Google Workspace**.
2. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, selezionare l'organizzazione di cui ripristinare i dati oggetto di backup. Altrimenti, ignorare questo passaggio.
3. Espandere il nodo **Unità condivise**, selezionare **Tutte le unità condivise**, selezionare l'unità condivisa che conteneva originariamente i file da ripristinare, quindi fare clic su **Ripristino**.
   Se l'unità condivisa è stata eliminata, selezionarla nella sezione **Backup delle applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.
   È possibile cercare le unità condivise per nome. I caratteri jolly non sono supportati.
4. Selezionare un punto di ripristino.
5. Fare clic su **Ripristina** > **File/cartelle**.
6. Esplorare la cartella richiesta o utilizzare la ricerca per ottenere l'elenco dei file e delle cartelle necessarie.
7. Selezionare i dati che si desidera ripristinare.
   Se il backup non è crittografato ed è stato selezionato un solo file è possibile fare clic su **Mostra versioni** per selezionare la versione del file da ripristinare. È possibile selezionare qualsiasi versione di cui sia stato eseguito il backup, precedente o successiva al punto di ripristino selezionato.
8. Per scaricare un file, selezionarlo e fare clic su **Download**, selezionare la posizione in cui salvare i dati e quindi fare clic su **Salva**. Altrimenti, ignorare questo passaggio.
9. Fare clic su **Ripristina**.
10. Se al servizio Cyber Protection sono state aggiunte più organizzazioni di Google Workspace, fare clic su **Organizzazione di Google Workspace** per visualizzare, modificare o specificare l'organizzazione di destinazione.

© Acronis International GmbH, 2003-2024

Per impostazione predefinita, è selezionata l'organizzazione originale. Se tale organizzazione non risulta più registrata al servizio Cyber Protection, è necessario specificare una nuova organizzazione di destinazione dalle organizzazioni registrate disponibili.

11. In **Ripristina nell'unità**, visualizzare, modificare o specificare l'utente di destinazione o l'unità condivisa di destinazione. Se si specifica un utente, i dati verranno ripristinati nel Google Drive di tale utente.
    Per impostazione predefinita, è selezionata l'unità condivisa originale. Se questa unità condivisa non esiste o se è stata selezionata un'organizzazione non originale, è necessario specificare l'utente o l'unità condivisa di destinazione.
12. In **Percorso**, visualizzare o modificare la cartella di destinazione nell'unità condivisa di destinazione o nel Google Drive dell'utente di destinazione. Per impostazione predefinita, è selezionato il percorso originale.
13. Selezionare se ripristinare o meno le autorizzazioni di condivisione dei file.
14. Fare clic su **Avvia ripristino**.
15. Selezionare una delle opzioni di sovrascrittura dei file:

Opzione	Descrizione
Sovrascrivi il file esistente se meno recente	Se nella posizione di destinazione è presente un file con lo stesso nome, e se tale file è meno recente del file di origine, il file di origine viene salvato nella posizione di destinazione e sostituisce la versione precedente.
Sovrascrivi i file esistenti	Tutti i file esistenti nella posizione di destinazione vengono sovrascritti, qualunque sia la data dell'ultima modifica.
Non sovrascrivere i file esistenti	Se nella posizione di destinazione è presente un file con lo stesso nome, tale file non viene modificato e il file di origine non viene salvato nella posizione di destinazione.

16. Fare clic su **Procedi** per confermare la decisione.

Autenticazione

L'autenticazione consente di dimostrare l'autenticità del file e l'assenza di modifiche dal momento del backup. L'utilizzo di questa funzionalità è consigliato per proteggere i file dei documenti legali o qualsiasi altro file che richieda una prova di autenticità.

L'autenticazione è disponibile solo per i backup di file di Google Drive e file di unità condivise di Google Workspace.

Come utilizzare l'autenticazione

Per abilitare l'autenticazione di tutti i file selezionati per il backup, abilitare l'opzione **Autenticazione** quando si crea un piano di protezione.

Durante la configurazione del ripristino, i file sottoposti ad autenticazione vengono contrassegnati con un'icona speciale ed è quindi possibile verificare l'autenticità dei file.

© Acronis International GmbH, 2003-2024

Come funziona

Durante l'esecuzione di un backup, l'agente elabora i codici hash dei file sottoposti a backup, crea un albero hash basato sulla struttura della cartella, salva l'albero nel backup e quindi invia la root dell'albero hash al servizio di autenticazione. Il servizio di autenticazione salva la root dell'albero hash nel database blockchain Ethereum per garantire che questo valore non venga modificato.

Durante la verifica dell'autenticità del file, l'agente elabora l'hash del file ed esegue il confronto con l'hash archiviato nell'albero hash all'interno del backup. Se gli hash non corrispondono, il file non è considerato autentico. Altrimenti, l'autenticità del file è garantita dall'albero hash.

Per verificare che lo stesso albero hash non sia stato compromesso, l'agente invia la root dell'albero hash al servizio di autenticazione, che lo confronta con quello archiviato nel database blockchain. Se gli hash corrispondono, viene garantita l'autenticità del file selezionato. In caso contrario, il software visualizza un messaggio che segnala la non autenticità del file.

Verifica dell'autenticità dei file con Notary Service

Se l'autenticazione è stata abilitata durante il backup, è possibile verificare l'autenticità di un file sottoposto a backup.

Per verificare l'autenticità dei file

1. Eseguire una delle seguenti operazioni:
   - Per verificare l'autenticità di un file di Google Drive, selezionare il file come descritto nei passaggi da 1 a 7 della sezione "Ripristino di file di Google Drive".
   - Per verificare l'autenticità di un file di unità condivise di Google Workspace, selezionare il file come descritto nei passaggi da 1 a 7 della sezione "Ripristino di file di unità condivise".
2. Verificare che il file selezionato sia contrassegnato dall'icona seguente: . Ciò significa che il file è autenticato.
3. Eseguire una delle seguenti operazioni:
   - Fare clic su **Verifica**.
     Il software controlla l'autenticità del file e mostra il risultato.
   - Fare clic su **Ottieni certificato**.
     In una finestra del browser Web viene visualizzato un certificato che conferma l'autenticazione del file. La finestra contiene inoltre le istruzioni per verificare manualmente l'autenticità dei file.

Ricerca nei backup cloud-to-cloud

Durante il ripristino dei dati, è possibile cercare elementi specifici di cui è stato eseguito il backup senza sfogliare l'archivio di backup.

© Acronis International GmbH, 2003-2024

Nei backup non crittografati, la ricerca è sempre disponibile. È supportata solo la ricerca avanzata (indicizzata).

La ricerca indicizzata è più veloce e offre opzioni aggiuntive quali: visualizzazione delle versioni degli elementi di cui è stato eseguito il backup, ricerca nei nomi degli allegati e ricerca testo completo nei backup di Gmail.

Nei backup crittografati è possibile abilitare anche la ricerca avanzata (indicizzata). Se non si abilita la ricerca avanzata, la ricerca di base sarà disponibile per i backup delle caselle di posta di Microsoft 365. Per tutti gli altri workload, la ricerca non sarà disponibile.

La tabella seguente riepiloga le opzioni disponibili per i backup crittografati.

Tipo di workload	Cosa convalidare	La ricerca avanzata è disabilitata	La ricerca avanzata è abilitata
Workload di Microsoft 365			
Casella di posta	Messaggi e-mail	La ricerca di base (non indicizzata) è disponibile	La ricerca avanzata (indicizzata) è disponibile
OneDrive	File/cartelle	La ricerca non è disponibile	La ricerca avanzata (indicizzata) è disponibile
Sito SharePoint	File SharePoint	La ricerca non è disponibile	La ricerca avanzata (indicizzata) è disponibile
Teams	Canali	La ricerca non è disponibile	La ricerca avanzata (indicizzata) è disponibile
	Messaggi e-mail	La ricerca di base (non indicizzata) è disponibile	La ricerca avanzata (indicizzata) è disponibile
	Sito del team	La ricerca non è disponibile	La ricerca avanzata (indicizzata) è disponibile
Workload di Google Workspace			
Casella di posta	Messaggi e-mail	La ricerca non è disponibile	La ricerca avanzata (indicizzata) è disponibile
Google Drive	File/cartelle	La ricerca non è disponibile	La ricerca avanzata (indicizzata) è disponibile
Unità condivise	File/cartelle	La ricerca non è disponibile	La ricerca avanzata (indicizzata) è disponibile

Ricerca testo completo

La ricerca a tutto testo è disponibile solo per i backup di Gmail ed è abilitata per impostazione predefinita. Questa funzionalità consente la ricerca nel corpo del testo delle e-mail di cui è stato

© Acronis International GmbH, 2003-2024

eseguito il backup. Se questa opzione è disabilitata, la ricerca è possibile solo per oggetto, mittente, destinatario e data.

Un indice di ricerca testo completo occupa tra il 10% e il 30% dello spazio di storage occupato dal backup di Gmail. Un indice senza dati di ricerca testo completo è molto più piccolo. Per risparmiare spazio di storage, disabilitare la ricerca testo completo e cancellare la parte di indice che contiene i dati della ricerca testo completo.

Indici di ricerca

Gli indici di ricerca offrono funzionalità di ricerca avanzate negli archivi di backup cloud-to-cloud.

Gli archivi vengono automaticamente indicizzati dopo ogni operazione di backup. Il processo di indicizzazione non compromette le prestazioni di backup perché l'indicizzazione e il backup sono eseguiti da componenti software differenti.

I risultati della ricerca sono disponibili e visualizzabili al completamento dell'operazione di indicizzazione, che potrebbe richiedere fino a 24 ore. L'indicizzazione del primo backup, che è completo, richiede di solito più tempo rispetto all'indicizzazione dei backup incrementali successivi.

Tutti gli indici contengono metadati che supportano la funzionalità di ricerca principale: ricerca per oggetto, mittente, destinatario o data. Gli indici dei backup di Gmail contengono dati aggiuntivi se è abilitata la ricerca a tutto testo.

Verifica della dimensione di un indice di ricerca

Gli indici di ricerca diventano più grandi con il tempo. Gli indici degli archivi di backup in cui è abilitata la ricerca a tutto testo potrebbero occupare fino al 30 percento della dimensione dell'archivio.

Per controllare la dimensione di un indice di ricerca

1. Accedere alla console di Cyber Protect come amministratore.
2. Nella scheda **Storage di backup**, fare clic su **Backup di applicazioni cloud**.
3. Controllare il valore nella colonna **Dimensione dell'indice**.

Aggiornare, ricompilare o eliminare gli indici

Per la risoluzione dei problemi relativi alla ricerca nei backup cloud-to-cloud, è possibile aggiornare, ricompilare o eliminare gli indici di ricerca.

Nota
Si consiglia di contattare il team di supporto prima di aggiornare, ricompilare o eliminare un indice.

Per aggiornare, ricompilare o eliminare un indice

© Acronis International GmbH, 2003-2024

1. Accedere alla console di Cyber Protect come amministratore.
2. Nella scheda **Storage di backup**, fare clic su **Backup di applicazioni cloud**.
   Selezionare l'archivio di cui aggiornare, ricompilare o eliminare l'indice.
   La disponibilità di queste azioni dipende dal livello e dal ruolo dell'amministratore, come indicato di seguito:

Livello dell'account	Ruolo	Può aggiornare un indice	Può ricompilare un indice	Può eliminare un indice
Tenant Partner	Amministratore società	+	+	+
	Amministratore Cyber della protezione	+	-	-
	Amministratore della protezione	+	-	-
	Amministratore di sola lettura della protezione	-	-	-
Tenant cliente	Amministratore società	+	-	-
	Amministratore della protezione	+	-	-
	Amministratore di sola lettura della protezione	-	-	-
Unità	Amministratore unità	+	-	-
	Amministratore della protezione	+	-	-
	Amministratore di sola lettura della protezione	-	-	-

3. Nel pannello **Azioni**, selezionare l'azione da eseguire:
   - **Aggiorna indice**: vengono controllati i punti di ripristino nell'archivio e aggiunti gli indici mancanti.
   - **Ricompila indice**: vengono eliminati gli indici di tutti i punti di ripristino nell'archivio, quindi gli indici vengono creati di nuovo.
   - **Elimina indice**: vengono eliminati gli indici di tutti i punti di ripristino nell'archivio.
4. [Per archivi criptati] Specificare la password di crittografia, quindi fare clic su **OK**.
5. Selezionare l'ambito dell'azione, quindi fare clic su **OK**.
   A seconda dell'archivio e dell'azione selezionata, sono disponibili una o più delle seguenti opzioni:
   - **Solo metadati**
   - **Solo contenuto**
   - **Ricerca metadati e ricerca**

© Acronis International GmbH, 2003-2024

Abilitazione della ricerca avanzata nei backup crittografati

Quando si crea un piano di backup per il backup cloud-to-cloud crittografato, è possibile abilitare la ricerca avanzata (indicizzata).

Se non si abilita la ricerca avanzata, la ricerca di base sarà disponibile per i backup delle caselle di posta di Microsoft 365. Per tutti gli altri workload, la ricerca non sarà disponibile. Per ulteriori informazioni sulle opzioni disponibili, consultare "Ricerca nei backup cloud-to-cloud" (pag. 676).

Nota
Questa funzionalità è disponibile in alcuni data center selezionati e potrebbe non essere accessibile a tutti i clienti.

Per abilitare la ricerca nei backup crittografati

1. Quando si crea un piano di backup, abilitare l'opzione **Crittografia**.
2. Specificare la password per la crittografia e confermarla.
3. Selezionare la casella di controllo **Consentire la ricerca avanzata nei backup crittografati**.
4. Fare clic su **Fine**.

Nota
Non è possibile disabilitare la crittografia o modificare la password di crittografia in un secondo momento. Per creare un backup non crittografato o modificare la password di crittografia, creare un nuovo piano di backup.

Abilitazione o disabilitazione della ricerca avanzata nei piani esistenti

È possibile modificare un piano esistente per il backup crittografato per abilitare o disabilitare la ricerca avanzata (indicizzata).

Se non si abilita la ricerca avanzata, la ricerca di base sarà disponibile per i backup delle caselle di posta di Microsoft 365. Per tutti gli altri workload, la ricerca non sarà disponibile. Per ulteriori informazioni sulle opzioni disponibili, consultare "Ricerca nei backup cloud-to-cloud" (pag. 676).

Nei backup non crittografati, la ricerca avanzata è sempre disponibile. Questa opzione non può essere disabilitata.

Per abilitare o disabilitare la ricerca avanzata nei backup crittografati

1. Quando si modifica un piano di backup in cui è abilitata la crittografia, fare clic sull'icona ingranaggio nell'angolo in alto a destra.
2. Nella scheda **Opzioni di ricerca**, attivare o disattivare l'opzione come necessario.
3. Fare clic su **Fine**.
4. Fare clic su **Salva impostazioni**.

© Acronis International GmbH, 2003-2024

Nota
Se si riattiva la ricerca avanzata, tutti gli archivi creati da questo piano di backup vengono di nuovo indicizzati. Questa operazione potrebbe richiedere molto tempo.

Disabilitazione della ricerca a tutto testo per i backup di Gmail

La ricerca a tutto testo è disponibile solo per i backup di Gmail ed è abilitata per impostazione predefinita. Questa funzionalità consente la ricerca nel corpo del testo delle e-mail di cui è stato eseguito il backup. Se questa opzione è disabilitata, la ricerca è possibile solo per oggetto, mittente, destinatario e data.

Potrebbe essere necessario disabilitare la ricerca a tutto testo se occorre ridurre la dimensione dell'indice di ricerca.

Per disabilitare la ricerca a tutto testo

1. Quando si crea o si modifica un piano di backup, fare clic sull'icona ingranaggio nell'angolo in alto a destra.
2. Nella scheda **Ricerca a tutto testo**, disabilitare l'opzione.
3. Fare clic su **Fine**.
4. [Quando si crea un piano] Fare clic su **Applica**.
5. [Quando si modifica un piano] Fare clic su **Salva impostazioni**.

Nota
Se si riattiva la ricerca a tutto testo, tutti gli archivi creati da questo piano di backup vengono di nuovo indicizzati. Questa operazione potrebbe richiedere molto tempo.

Protezione per Oracle Database

Nota
Questa funzionalità è disponibile con il pacchetto Advanced Backup.

La protezione per Oracle Database è descritta in un altro documento disponibile all'indirizzo https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf

Protezione di SAP HANA

Nota
Questa funzionalità è disponibile con il pacchetto Advanced Backup.

La protezione per SAP HANA è descritta in un altro documento disponibile all'indirizzo https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf

© Acronis International GmbH, 2003-2024

Protezione dei dati di MySQL e MariaDB

Un backup application-aware consente di proteggere i dati di MySQL e MariaDB. Tale backup raccoglie i metadati dell'applicazione e consente il ripristino granulare a livello di istanza, database o tabella.

Nota
Il backup application-aware dei dati MySQL o MariaDB è disponibile con il pacchetto Advanced Backup.

Per proteggere con il backup application-aware un sistema fisico o una virtual machine che esegue istanze di MySQL o MariaDB, è necessario che su tale sistema sia installato l'Agente per MySQL/MariaDB. L'Agente per MySQL/MariaDB è incluso nel pacchetto con l'Agente per Linux (64-bit) e quindi può essere installato solo su sistemi operativi Linux a 64 bit. Vedere "Sistemi operativi e ambienti supportati" (pag. 23).

Per scaricare il file di installazione dell'Agente per Linux (64-bit)

1. Accedere alla console di Cyber Protect.
2. Fare clic sull'icona dell'account nell'angolo in alto a destra, quindi selezionare **Download**.
3. Fare clic su **Agente per Linux (64 bit)**.

   Il file di installazione viene scaricato nel sistema. Per installare l'agente, procedere come descritto in "Installazione degli agenti di protezione in Linux" (pag. 80) o in "Installazione o disinstallazione automatica in Linux" (pag. 106). Accertarsi di aver selezionato l'Agente per MySQL/MariaDB, trattandosi di un componente facoltativo.

   Per ripristinare database e tabelle in un'istanza live, l'Agente per MySQL/MariaDB richiede un archivio temporaneo in cui operare. Per impostazione predefinita, viene utilizzata la directory `/tmp`. È possibile modificare tale directory impostando la variabile di ambiente `ACRONIS_MYSQL_RESTORE_DIR`.

Limitazioni

- Non sono supportati i cluster MySQL o MariaDB.
- Non sono supportate le istanze MySQL o MariaDB in esecuzione nei contenitori Docker.
- Non sono supportate le istanze MySQL o MariaDB in esecuzione nei sistemi operativi che utilizzano file system BTRFS.
- I database di sistema (`sys`, `mysql`, `information-schema` e `performance_schema`) e i database che non contengono tabelle non possono essere ripristinati su istanze live. Durante il ripristino dell'intera istanza, questi database possono essere tuttavia ripristinati come file.
- Il ripristino è supportato solo su istanze di destinazione con versione uguale o successiva all'istanza di cui è stato eseguito il backup, con le limitazioni seguenti:

© Acronis International GmbH, 2003-2024

- Non è supportato il ripristino dalle istanze di MySQL 5.x alle istanze di MySQL 8.x.
- Il ripristino a una versione successiva a MySQL 5.x (incluse le versioni minori) è supportato solo tramite il ripristino dell'intera istanza come file. Prima di tentare il ripristino, consultare la guida ufficiale all'upgrade della versione di MySQL di destinazione, ad esempio la guida all'upgrade di MySQL 5.7.

- Il ripristino dai backup archiviati nella Secure Zone non è supportato.
- Database e tabelle non possono essere ripristinati dall'Agente per MySQL/MariaDB se questo è eseguito in un sistema sul quale è installato AppArmor. È tuttavia possibile ripristinare un'istanza come file, oppure l'intero sistema.
- Non è supportato il ripristino in database di destinazione che sono stati configurati con collegamenti simbolici. È possibile ripristinare i database oggetto di backup come nuovi database, modificandone il nome.

Problemi noti

Se si riscontrano problemi durante il ripristino di dati da condivisioni Samba protette da password, disconnettersi dalla console di Cyber Protect e quindi eseguire una nuova connessione. Selezionare il punto di ripristino desiderato e quindi fare clic su **Database MySQL/MariaDB**. Non fare clic su **Intera macchina** né su **File/cartelle**.

Configurare un backup application-aware

Prerequisiti

- Sul sistema selezionato deve essere in esecuzione almeno un'istanza di MySQL o MariaDB.
- Sul sistema in cui è in esecuzione l'istanza di MySQL o MariaDB, l'agente di protezione deve essere avviato nell'utente root.
- Il backup application-aware è disponibile solo quando l'opzione **Intera macchina** è selezionata come origine del backup nel piano di protezione.
- L'opzione di backup **Settore per settore** deve essere disabilitata nel piano di protezione. In caso contrario, non sarà possibile ripristinare i dati dell'applicazione.

Per configurare un backup application-aware

1. Nella console di Cyber Protect, selezionare uno o più sistemi nei quali sono in esecuzione le istanze di MySQL o MariaDB.
   È possibile avere una o più istanze su ciascun sistema.
2. Creare un piano di protezione con il modulo Backup abilitato.
3. In **Cosa includere nel backup**, selezionare **Intera macchina**.
4. Fare clic su **Backup applicazione**, quindi abilitare l'opzione accanto a **MySQL/MariaDB Server**.
5. Selezionare come specificare le istanze di MySQL o MariaDB:

© Acronis International GmbH, 2003-2024

- **Per tutti i workload**

  Utilizzare questa opzione se si eseguono istanze con configurazioni identiche su più server. Per tutte le istanze verranno utilizzati gli stessi parametri di connessione e credenziali di accesso.
- **Per workload specifici**

  Utilizzare questa opzione per specificare i parametri di connessione e le credenziali di accesso per ogni istanza.

6. Fare clic su **Aggiungi istanza** per configurare i parametri di connessione e le credenziali di accesso.
   a. Selezionare il tipo di connessione, quindi specificare quanto segue:
      - [Per il socket TCP] Indirizzo IP e porta.
      - [Per il socket Unix] Percorso del socket.
   b. Specificare le credenziali di un account utente che dispone dei privilegi seguenti per l'istanza:
      - `FLUSH_TABLES` o `RELOAD` per tutti i database e le tabelle (`*.*`)
      - `SELECT` per `information_schema.tables`
   c. Fare clic su **OK**.
7. Fare clic su **Fine**.

Ripristino dei dati da un backup application-aware

Da un backup application-aware è possibile ripristinare istanze, database e tabelle di MySQL o MariaDB. È anche possibile ripristinare l'intero server sul quale sono in esecuzione le istanze, o i file e le cartelle che su di esso risiedono.

La tabella seguente riepiloga tutte le opzioni di ripristino.

Cosa convalidare	Ripristina come	Ripristina in
Server MySQL Server MariaDB	Intera macchina	Sistema* sul quale è installato l'Agente per Linux
Server MySQL Server MariaDB	File o cartelle	Sistema* sul quale è installato l'Agente per Linux
Istanza	File	Sistema* sul quale è installato l'Agente per MySQL/MariaDB
Database	Stesso database Nuovo database	Sistema* sul quale è installato l'Agente per MySQL/MariaDB • Istanza originale • Altra istanza • Database originale

© Acronis International GmbH, 2003-2024

Cosa convalidare	Ripristina come	Ripristina in
		• Nuovo database
Tabella	Stessa tabella Nuova tabella	Sistema* sul quale è installato l'Agente per MySQL/MariaDB • Istanza originale • Altra istanza • Database originale • Tabella originale • Nuova tabella

* Dal punto di vista del backup, una virtual machine contenente un agente viene considerata come un sistema fisico.

Ripristino dell'intero server

Per maggiori informazioni su come ripristinare l'intero server sul quale sono in esecuzione le istanze MySQL o MariaDB, fare riferimento a "Ripristino di una macchina" (pag. 507).

Ripristino di istanze

Da un backup application-aware è possibile ripristinare istanze di MySQL o MariaDB come file.

Per ripristinare un'istanza

1. Nella console di Cyber Protect, selezionare il sistema che conteneva in origine i dati da recuperare.
2. Fare clic su **Ripristino**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.

   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Eseguire una delle seguenti operazioni:
   - Se la posizione di backup è il cloud o un archivio condiviso (a cui possono accedere altri agenti), fare clic su **Seleziona macchina** e selezionare un sistema online con l'Agente per MySQL/MariaDB, quindi scegliere un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda **Archivio di backup**.

   Il sistema scelto per sfogliare una delle azioni di cui sopra diventa un sistema di destinazione per il recupero.
4. Fare clic su **Ripristina** > **Database MySQL/MariaDB**.
5. Selezionare l'istanza da ripristinare, quindi fare clic su **Ripristina come file**.
6. In **Percorso**, selezionare la directory in cui verranno ripristinati i file.
7. Fare clic su **Avvia ripristino**.

© Acronis International GmbH, 2003-2024

Ripristino di database

Da un backup application-aware è possibile ripristinare i database in istanze live di MySQL o MariaDB.

1. Nella console di Cyber Protect, selezionare il sistema che conteneva in origine i dati da recuperare.
2. Fare clic su **Ripristino**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.

   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Eseguire una delle seguenti operazioni:

   - Se la posizione di backup è il cloud o un archivio condiviso (a cui possono accedere altri agenti), fare clic su **Seleziona macchina** e selezionare un sistema online con l'Agente per MySQL/MariaDB, quindi scegliere un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda **Archivio di backup**.

   Il sistema scelto per sfogliare una delle azioni di cui sopra diventa un sistema di destinazione per il recupero.
4. Fare clic su **Ripristina** > **Database MySQL/MariaDB**.
5. Fare clic sul nome dell'istanza desiderata per esaminare in dettaglio i database che contiene.
6. Selezionare uno o più database da ripristinare.
7. Fare clic su **Ripristina**.
8. Fare clic su **Istanza MySQL/MariaDB di destinazione** per specificare i parametri di connessione e le credenziali di accesso per l'istanza di destinazione.
   - Verificare l'istanza nella quale ripristinare i dati. Per impostazione predefinita è selezionata l'istanza originale.
   - Specificare le credenziali di un account utente che dispone dell'accesso all'istanza di destinazione. A questo account utente devono essere assegnati i seguenti privilegi per tutti i database e le tabelle (`*.*`):
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Fare clic su **OK**.
9. Verificare il database di destinazione.

   Per impostazione predefinita, è selezionato il database originale.

© Acronis International GmbH, 2003-2024

Per ripristinare un database come nuovo database, fare clic sul nome del database di destinazione e modificarlo. Questa azione è disponibile solo se si intende ripristinare un singolo database.

10. In **Sovrascrivi database esistenti**, selezionare la modalità di sovrascrittura.
    Per impostazione predefinita, è abilitata la sovrascrittura, quindi il database oggetto di backup sostituirà il database di destinazione che ha lo stesso nome.
    Se la sovrascrittura è disabilitata, durante l'operazione di ripristino il database oggetto di backup verrà ignorato e non sostituirà il database di destinazione che ha lo stesso nome.
11. Fare clic su **Avvia ripristino**.

Ripristino di tabelle

Da un backup application-aware è possibile ripristinare le tabelle in istanze live di MySQL o MariaDB.

1. Nella console di Cyber Protect, selezionare il sistema che conteneva in origine i dati da recuperare.
2. Fare clic su **Ripristino**.
3. Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.
   Se il sistema è offline, i punti di ripristino non vengono visualizzati. Eseguire una delle seguenti operazioni:
   - Se la posizione di backup è il cloud o un archivio condiviso (a cui possono accedere altri agenti), fare clic su **Seleziona macchina** e selezionare un sistema online con l'Agente per MySQL/MariaDB, quindi scegliere un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda **Archivio di backup**.

   Il sistema scelto per sfogliare una delle azioni di cui sopra diventa un sistema di destinazione per il recupero.
4. Fare clic su **Ripristina** > **Database MySQL/MariaDB**.
5. Fare clic sul nome dell'istanza desiderata per esaminare in dettaglio i database che contiene.
6. Fare clic sul nome del database desiderato per esaminare in dettaglio le tabelle che contiene.
7. Selezionare una o più tabelle da ripristinare.
8. Fare clic su **Ripristina**.
9. Fare clic su **Istanza MySQL/MariaDB di destinazione** per specificare i parametri di connessione e le credenziali di accesso per l'istanza di destinazione.
   - Verificare l'istanza nella quale ripristinare i dati. Per impostazione predefinita è selezionata l'istanza originale.
   - Specificare le credenziali di un account utente che dispone dell'accesso all'istanza di destinazione. A questo account utente devono essere assegnati i seguenti privilegi per tutti i database e le tabelle (`*.*`):

© Acronis International GmbH, 2003-2024

- INSERT
- CREATE
- DROP
- LOCK_TABLES
- ALTER
- SELECT

- Fare clic su **OK**.

10. Verificare la tabella di destinazione.

    Per impostazione predefinita, è selezionata la tabella originale.

    Per ripristinare una tabella come nuova tabella, fare clic sul nome della tabella di destinazione e modificarlo. Questa azione è disponibile solo se si intende ripristinare una singola tabella.
11. In **Sovrascrivi tabelle esistenti** selezionare la modalità di sovrascrittura.

    Per impostazione predefinita, è abilitata la sovrascrittura, quindi la tabella oggetto di backup sostituirà la tabella di destinazione che ha lo stesso nome.

    Se la sovrascrittura è disabilitata, durante l'operazione di ripristino la tabella oggetto di backup verrà ignorata e non sostituirà la tabella di destinazione che ha lo stesso nome.
12. Fare clic su **Avvia ripristino**.

Recupero delle routine archiviate

Quando si recupera un'intera istanza di MySQL, le routine archiviate vengono recuperate automaticamente.

Quando si recupera un singolo database in un'istanza non originale o lo si recupera come nuovo database, le routine archiviate non vengono recuperate automaticamente. È possibile recuperarle manualmente, esportandole in un file SQL e aggiungendole al database recuperato.

Per esportare le routine archiviate e aggiungerle a un database recuperato

1. Sul sistema con l'istanza originale di MySQL, aprire il Terminal.
2. Eseguire il seguente comando per esportare le routine archiviate.
3. ```
   mysqldump -p [source_database_name] --routines --no-create-info --no-data > [exported_db_routines.sql]
   ```
4. Sulla macchina in cui è stato recuperato il database, aprire il client della riga di comando MySQL.
5. Eseguire i seguenti comandi per aggiungere le routine al database recuperato.

   ```
   mysql>  use [recovered_database_name];
   ```

   ```
   mysql>  source [path_to_exported_db_routines.sql];
   ```


© Acronis International GmbH, 2003-2024
   ```

Protezione di siti Web e di server di hosting

Protezione di siti Web

Come conseguenza di un accesso non autorizzato o di un attacco malware, un sito Web può subire gravi danni. In caso di danni, per riportare il sito allo stato di integrità precedente all'attacco, è indispensabile disporre del backup del sito.

Perché è necessario eseguire il backup di un sito Web?

Il sito Web deve essere accessibile tramite SFTP o protocollo SSH. Non è necessario installare un'agente, ma è sufficiente aggiungere un sito Web come descritto più avanti in questa sezione.

Di quali elementi è possibile eseguire il backup?

È possibile eseguire il backup degli elementi indicati di seguito:

- **File di contenuti del sito Web**
  Tutti i file accessibili all'account specificato per la connessione tramite SFTP o SSH.
- **Database collegati (se presenti) ospitati su server MySQL.**
  Tutti i database accessibili all'account MySQL specificato.

Se il sito Web utilizza dei database, è consigliabile eseguire il backup dei file e dei database, per poterli ripristinare entrambi a uno stato coerente.

Limitazioni

- L'unica posizione di backup disponibile per il backup del sito Web è l'archivio nel cloud.
- È possibile applicare diversi piani di protezione a un sito Web, ma solo uno fra questi può essere eseguito con una pianificazione. Gli altri piani dovranno essere avviati manualmente.
- L'unica opzione di backup disponibile è "Nome file di backup".
- I piani di protezione del sito web non vengono mostrati nella scheda **Gestione** > **Piani di protezione**.

Backup di un sito Web

Per aggiungere un sito Web

1. Fare clic su **Dispositivi** > **Aggiungi**.
2. Fare clic su **Sito Web**.
3. Configurare le seguenti impostazioni di accesso per il sito Web:
   - In **Nome del sito Web**, creare e digitare un nome per il sito Web. Tale nome viene visualizzato nella console di Cyber Protect.

© Acronis International GmbH, 2003-2024

- In **Host**, specificare il nome dell'host o l'indirizzo IP che verrà utilizzato per accedere al sito Web tramite SFTP o SSH. Ad esempio, `mio.server.com` o `10.250.100.100`.
- In **Porta**, specificare il numero della porta.
- In **Nome utente** e **Password**, specificare le credenziali dell'account che verrà utilizzato per accedere al sito Web tramite SFTP o SSH.

  Importante
  Verrà eseguito il backup dei soli file accessibili all'account specificato.

  Al posto di una password è possibile specificare la chiave SSH privata. In questo caso, selezionare la casella di controllo **Utilizza la chiave privata SSH al posto della password** e specificare la chiave.

4. Fare clic su **Avanti**.
5. Se il sito Web utilizza database MySQL, configurare le impostazioni di accesso per i database. In caso contrario, fare clic su **Ignora**.
   a. In **Tipo di connessione**, selezionare la modalità di accesso ai database dal cloud:
      - **Tramite SSH dall'host** - È possibile accedere ai database tramite l'host specificato al passaggio 3.
      - **Connessione diretta** - È possibile accedere direttamente ai database. Selezionare questa impostazione solo se i database sono accessibili da Internet.
   b. In **Host**, specificare il nome o l'indirizzo IP dell'host nel quale viene eseguito il server MySQL.
   c. In **Porta**, specificare il numero di porta della connessione TCP/IP al server. Il numero di porta predefinito è 3306.
   d. In **Nome utente** e **Password** immettere le credenziali dell'account MySQL.

      Importante
      Verrà eseguito il backup dei soli database accessibili all'account specificato.

   e. Fare clic su **Crea**.

   Il sito web viene visualizzo nella console di Cyber Protect in **Dispositivi** > **Siti web**.

Per modificare le impostazioni di connessione

1. In **Dispositivi** > **Siti Web**, selezionare il sito Web.
2. Fare clic su **Dettagli**.
3. Fare clic sull'icona a forma di matita accanto alle impostazioni di connessione al sito Web o al database.
4. Apportare le modifiche necessarie e fare clic su **Salva**.

Per creare un piano di protezione per siti web

1. In **Dispositivi** > **Siti Web**, selezionare uno o più siti Web.
2. Fare clic su **Proteggi**.

© Acronis International GmbH, 2003-2024

3. [Facoltativo] Abilitare il backup dei database.

   Se risultano selezionati vari database, il backup dei database è disabilitato per impostazione predefinita.
4. [Facoltativo] Modificare le regole di conservazione.
5. [Facoltativo] Abilitare la crittografia dei backup.
6. [Facoltativo] Fare clic sull'icona ingranaggio per modificare l'opzione **Nome file di backup**.
   L'operazione ha senso in due casi:
   - Se l'utente ha effettuato il backup di tale sito Web e vuole proseguire la sequenza dei backup esistente
   - Se l'utente vuole visualizzare un nome personalizzato nella scheda **Archivio di backup**
7. Fare clic su **Applica**.

È possibile modificare, revocare ed eliminare i piani di protezione per i siti web seguendo lo stesso procedimento indicato per i sistemi. Queste operazioni sono descritte in "Operazioni con piani di protezione".

Ripristino di un sito Web

Per ripristinare un sito Web

1. Eseguire una delle seguenti operazioni:
   - In **Dispositivi** > **Siti Web**, selezionare il sito Web da ripristinare, quindi fare clic su **Ripristino**.
     È possibile cercare i siti Web per nome. I caratteri jolly non sono supportati.
   - Se il sito web è stato eliminato, selezionarlo nella sezione **Backup di applicazioni cloud** della scheda Archivio di backup, quindi fare clic su **Mostra backup**.
     Per ripristinare un sito Web eliminato, è necessario aggiungere il sito di destinazione come un dispositivo.
2. Selezionare il punto di ripristino.
3. Fare clic su **Ripristina** e selezionare gli elementi che si desidera ripristinare: **Intero sito Web**, **Database** (se presenti) o **File/Cartelle**.
   Per assicurare uno stato omogeneo al sito web, si consiglia di recuperare sia i file sia i database, in qualsiasi ordine.
4. In funzione della scelta effettuata, seguire una delle procedure descritte di seguito.

Per ripristinare il sito Web intero

1. In **Ripristina nel sito Web**, visualizzare o modificare il sito Web di destinazione.
   Per impostazione predefinita, è selezionato il sito Web originale. Se questo non esiste, l'utente dovrà selezionare il sito Web di destinazione.
2. Selezionare se ripristinare o meno le autorizzazioni di condivisione degli elementi ripristinati.
3. Fare clic su **Avvia ripristino** e confermare l'azione.

Per ripristinare i database

© Acronis International GmbH, 2003-2024

1. Selezionare i database che si desidera ripristinare.
2. Per scaricare un database come file, fare clic su **Download**, selezionare la posizione in cui salvare il file e fare clic su **Salva**. Altrimenti, ignorare questo passaggio.
3. Fare clic su **Ripristina**.
4. In **Ripristina nel sito Web**, visualizzare o modificare il sito Web di destinazione.
   Per impostazione predefinita, è selezionato il sito Web originale. Se questo non esiste, l'utente dovrà selezionare il sito Web di destinazione.
5. Fare clic su **Avvia ripristino** e confermare l'azione.

Per ripristinare le cartelle o i file di un sito Web

1. Selezionare i file/cartelle che si desidera ripristinare.
2. Per salvare un file, fare clic su **Download**, selezionare la posizione di salvataggio e fare clic su **Salva**. Altrimenti, ignorare questo passaggio.
3. Fare clic su **Ripristina**.
4. In **Ripristina nel sito Web**, visualizzare o modificare il sito Web di destinazione.
   Per impostazione predefinita, è selezionato il sito Web originale. Se questo non esiste, l'utente dovrà selezionare il sito Web di destinazione.
5. Selezionare se ripristinare o meno le autorizzazioni di condivisione degli elementi ripristinati.
6. Fare clic su **Avvia ripristino** e confermare l'azione.

Protezione di server di hosting su Web

È possibile proteggere i server di web hosting basati su Linux che eseguono i pannelli di controllo Plesk, cPanel, DirectAdmin, VirtualMin o ISPManager. I server che eseguono pannelli di controllo di web hosting di altri vendor sono protetti come workload standard.

Quote

I server che eseguono i pannelli di controllo Plesk, cPanel, DirectAdmin, VirtualMin o ISPManager sono considerati server di web hosting. Ogni server di web hosting di cui è stato eseguito il backup consuma la quota **Server di web hosting**. Se tale quota è disabilitata o se il surplus della quota viene superato, verrà assegnata una quota come indicato di seguito, oppure i backup avranno esito negativo.

- Se il server è fisico, viene usata la quota **Server**. Se tale quota è disabilitata o se il surplus della quota viene superato, il backup ha esito negativo.
- Se il server è virtuale, viene usata la quota **Macchine virtuali**. Se tale quota è disabilitata o se il surplus della quota viene superato, il backup ha esito negativo.

Integrazioni per DirectAdmin, cPanel e Plesk

Gli amministratori di web hosting che usano DirectAdmin, Plesk o cPanel possono integrare tali pannelli di controllo con il servizio Cyber Protection per ottenere numerose funzionalità utili, tra cui:

© Acronis International GmbH, 2003-2024

- Esecuzione dell'intero backup del server di web hosting nel cloud storage, con backup del disco
- Ripristino dell'intero server, inclusi tutti i siti web e gli account
- Esecuzione del ripristino granulare e del download di account, siti web, singoli file, caselle di posta o database
- Esecuzione del ripristino self-service dei propri dati per rivenditori e clienti

Per eseguire l'integrazione, è necessario utilizzare un'estensione del servizio Cyber Protection. Per informazioni dettagliate, fare riferimento alle guide all'integrazione corrispondenti:
- Guida all'integrazione di DirectAdmin
- Guida all'integrazione di WHM e cPanel
- Guida all'integrazione di Plesk

Operazioni speciali con le macchine virtuali

Esecuzione di una macchina virtuale da un backup (Ripristino istantaneo)

È possibile eseguire una macchina virtuale da un backup del disco contenente un sistema operativo. Questa operazione, nota anche come ripristino istantaneo, consente di allestire un server virtuale in pochi secondi. I dischi virtuali sono emulati direttamente dal backup, pertanto non consumano spazio sul datastore (archivio). Lo spazio di archiviazione è necessario soltanto per conservare le modifiche apportate ai dischi virtuali.

Si consiglia di lasciare in funzione questa virtual machine temporanea per un massimo di tre giorni. In seguito, è possibile rimuoverla completamente o convertirla in una macchina virtuale normale (finalizzarla) senza interruzione di attività.

Fintanto che esiste la macchina virtuale temporanea, non è possibile applicare le regole di conservazione al backup utilizzato da tale macchina. È possibile proseguire l'esecuzione dei backup della sistema originale.

Esempi di utilizzo

- **Disaster Recovery**
  Portare immediatamente online una copia del sistema guasto.
- **Prova di un backup**
  Eseguire il sistema dal backup e accertarsi che l'OS e le applicazioni guest funzionino correttamente.
- **Accesso ai dati dell'applicazione**
  Durante l'esecuzione del sistema, utilizzare gli strumenti di gestione nativi dell'applicazione per accedere ed estrarre i dati richiesti.

© Acronis International GmbH, 2003-2024

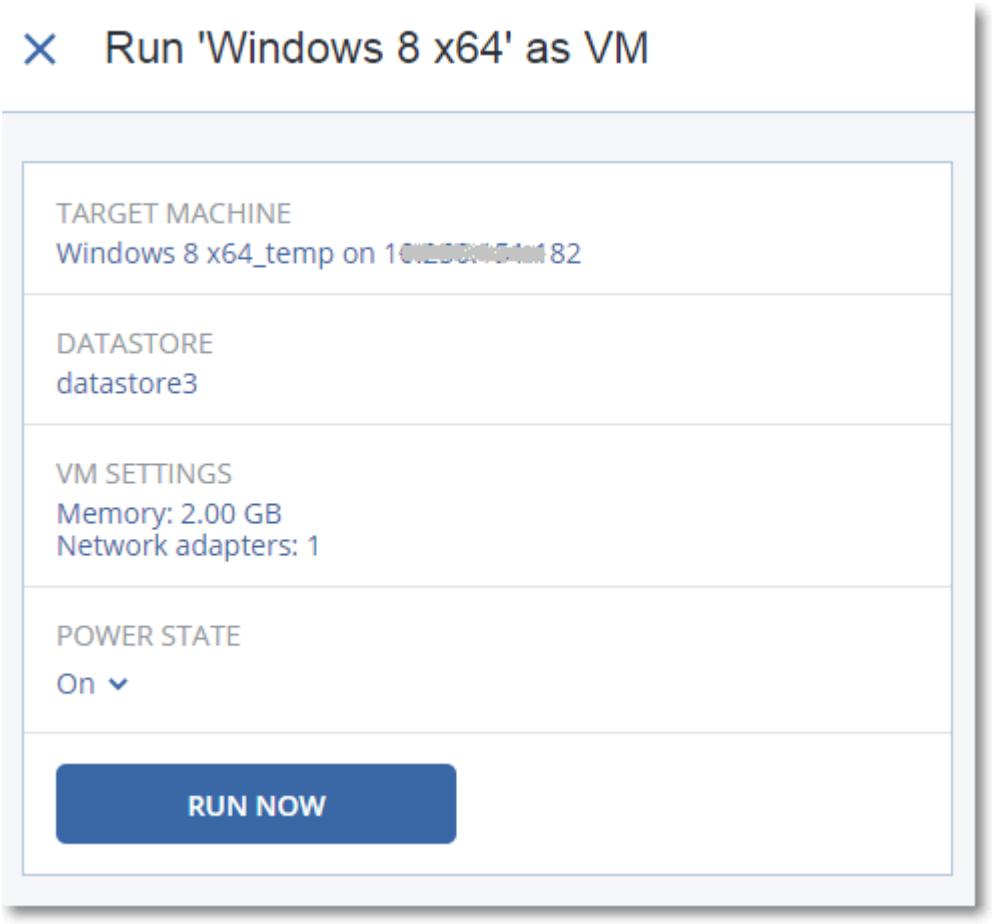
Prerequisiti

- Almeno un Agente per VMware o Agente per Hyper-V deve essere registrato nel servizio Cyber Protection.
- Il backup può essere archiviato in una cartella di rete o in una cartella locale del sistema in cui è installato l'Agente per VMware o l'Agente per Hyper-V. Se viene selezionata una cartella di rete, questa deve essere accessibile dal sistema. È possibile anche eseguire una macchina virtuale da un backup archiviato nell'archivio nel cloud, ma le prestazioni saranno più lente perché questa operazione comporta un'intensa attività di accesso casuale durante la lettura del backup.
- Il backup deve contenere un intero sistema o tutti i volumi necessari per l'avvio del sistema operativo.
- È possibile utilizzare sia i backup di macchine fisiche sia quelli di macchine virtuali. Non è possibile utilizzare i backup dei *contenitori* di Virtuozzo.
- I backup che contengono i volumi logici Linux (LVM) devono essere creati con l'Agente per VMware o l'Agente per Hyper-V. La macchina virtuale deve essere dello stesso tipo della macchina originale (ESXi o Hyper-V).

Esecuzione del sistema

1. Eseguire una delle seguenti operazioni:
   - Selezionare un sistema di cui è stato eseguito il backup e fare clic su **Ripristino**, quindi selezionare un punto di ripristino.
   - Selezionare un punto di ripristino nella scheda Archivio di backup.
2. Fare clic su **Esegui come MV**.
   Il software seleziona automaticamente l'host e altri parametri obbligatori.

© Acronis International GmbH, 2003-2024



3. [Facoltativo] Fare clic su **Macchina di destinazione**, quindi cambiare il tipo di macchina virtuale (ESXi o Hyper-V), l'host o il nome della macchina virtuale.
4. [Facoltativo] Fare clic su **Datastore** per ESXi o su **Percorso** per Hyper-V, quindi selezionare il datastore per la macchina virtuale.

   I cambiamenti ai dischi virtuali si accumulano durante l'esecuzione del sistema. Accertarsi che il datastore selezionato disponga di sufficiente spazio libero. Se si prevede di mantenere le modifiche apportate rendendo permanente la macchina virtuale, selezionare un datastore adatto all'esecuzione della macchina in produzione.
5. [Facoltativo] Fare clic su **Impostazioni MV** per cambiare le dimensioni della memoria e le connessioni di rete della macchina virtuale.
6. [Facoltativo] Selezionare lo stato di alimentazione della MV (**Attivo**/**Disattivato**).
7. Fare clic su **Esegui ora**.

Come risultato, il sistema viene visualizzato nell'interfaccia web con una delle seguenti icone: o

. Non è possibile selezionare tali macchine virtuali per il backup.

© Acronis International GmbH, 2003-2024

Nota
È possibile eseguire l'operazione Esegui come macchina virtuale (Ripristino istantaneo) con i backup in Microsoft Azure. Questa operazione causa tuttavia un significativo traffico in uscita, che viene addebitato sulla fattura dell'abbonamento Microsoft Azure. In genere, il traffico in uscita per un sistema Windows eseguito da un backup di Microsoft Azure è pari approssimativamente a 5 GB, dall'attivazione della virtual machine al login.

Eliminazione della macchina

Non si consiglia di eliminare una virtual machine temporanea direttamente in vSphere/Hyper-V, poiché ciò potrebbe causare la presenza di artefatti nell'interfaccia web. Inoltre il backup da cui era in esecuzione la macchina potrebbe restare bloccato per un certo periodo di tempo (non può essere eliminato in base alla regole di conservazione).

Per eliminare una macchina virtuale in esecuzione da un backup

1. Nella scheda **Tutti i dispositivi**, selezionare un sistema in esecuzione da un backup.
2. Fare clic su **Elimina**.

La macchina viene rimossa dall'interfaccia Web. Viene inoltre rimossa dall'inventario e dal datastore (archivio) vSphere o Hyper-V. Tute le modifiche apportate ai dati durante l'esecuzione della macchina andranno perse.

Finalizzazione del sistema

Durante l'esecuzione di una macchina virtuale da un backup, il contenuto dei dischi virtuali viene estratto direttamente da tale backup. Pertanto, la macchina diventerà inaccessibile o subirà danni se viene persa la connessione alla posizione di backup o all'agente di protezione.

È possibile scegliere di rendere permanente questa macchina, ossia di ripristinarne tutti i dischi virtuali, nonché le modifiche apportate durante l'esecuzione della macchina, nel datastore in cui sono archiviate tali modifiche. Questo processo è denominato finalizzazione.

L'esecuzione della finalizzazione non comporta tempi di inattività del sistema. La macchina virtuale *non* viene spenta durante la finalizzazione.

La posizione dei dischi virtuali finali viene definita nei parametri dell'operazione **Esegui come MV** (**Datastore** per ESXi o **Percorso** per Hyper-V). Prima di avviare la finalizzazione, verificare che lo spazio libero, le funzionalità di condivisione e le prestazioni del datastore siano idonee all'esecuzione della macchina in produzione.

Nota
La finalizzazione non è supportata per Hyper-V in esecuzione su Windows Server 2008/2008 R2 e Microsoft Hyper-V Server 2008/2008 R2, perché in queste versioni di Hyper-V non è presente l'API necessaria.

Per finalizzare un sistema in esecuzione da un backup

© Acronis International GmbH, 2003-2024

1. Nella scheda **Tutti i dispositivi**, selezionare un sistema in esecuzione da un backup.
2. Fare clic su **Finalizza**.
3. [Facoltativo] Specificare un nuovo nome per il sistema.
4. [Facoltativo] Cambiare la modalità di provisioning del disco. L'impostazione predefinita è **Thin**.
5. Fare clic su **Finalizza**.

Il nome del sistema cambia immediatamente. L'avanzamento del ripristino viene mostrato nella scheda **Attività**. Al termine del ripristino, l'icona cambia e diventa l'icona di una macchina virtuale normale.

Informazioni sulla finalizzazione

Finalizzazione e normale ripristino a confronto

Il processo di finalizzazione risulta più lento di un normale ripristino per le ragioni seguenti:

- Durante una finalizzazione, l'agente accede in modo casuale alle varie componenti del backup. Quando si esegue il ripristino di un intero sistema, l'agente legge i dati dal backup in modo sequenziale.
- Se durante la finalizzazione la macchina virtuale è in esecuzione, l'agente legge i dati dal backup con più frequenza, per far sì che entrambi i processi avvengano simultaneamente. Durante un normale ripristino, la macchina virtuale viene arrestata.

Finalizzazione di sistemi in esecuzione dai backup nel cloud

A causa dell'accesso intensivo ai dati di backup, la velocità della finalizzazione dipende molto dalla larghezza di banda di rete della connessione tra la posizione di backup e l'agente. La finalizzazione dei backup posizionati nel cloud risulterà più lenta rispetto a quella dei backup locali. Se la connessione Internet è molto lenta o instabile, la finalizzazione di un sistema eseguito da un backup nel cloud potrebbe anche non riuscire. Se è possibile scegliere e si ha intenzione di eseguire la finalizzazione, si consiglia di eseguire le virtual machine dai backup locali.

Nota
La velocità della finalizzazione dipende dal fatto che l'agente sia connesso o meno a un host VMware ESXi o vCenter, come descritto nel passaggio 3 di "Configurazione dell'appliance virtuale" (pag. 139). La connessione a un VMware vCenter può rallentare l'operazione di finalizzazione a causa delle specifiche delle API VMware. Per accelerare la finalizzazione, utilizzare un Agente per VMware distinto per eseguire l'operazione **Esegui come MV** seguita dalla finalizzazione, durante la quale l'agente viene connesso a un host ESXi invece che a un vCenter.

Lavorare in VMware vSphere

Questa sezione descrive le operazioni specifiche degli ambienti VMware vSphere.

© Acronis International GmbH, 2003-2024

Replica di macchine virtuali

La replica è disponibile soltanto per le macchine virtuali VMware ESXi.

La replica è il processo di creazione di una copia esatta di una macchina virtuale, che viene costantemente sincronizzata con la macchina originale. Eseguendo la replicazione di una macchina virtuale critica, l'utente avrà sempre a disposizione una copia della macchina pronta per essere avviata.

La replica può essere avviata manualmente o nell'ambito della pianificazione specificata dall'utente. La prima replica è completa (copia l'intera macchina). Tutte le repliche successive sono incrementali e vengono eseguite con Changed Block Tracking a condizione che questa opzione non sia disabilitata.

Confronto tra replica e backup

Diversamente da quanto accade nel caso dei backup pianificati, una copia conserva soltanto l'ultimo stato della macchina virtuale. Una copia consuma spazio del datastore, mentre i backup possono essere conservati in archivi meno onerosi.

Tuttavia, l'avvio della copia è molto più rapido rispetto a un ripristino e rispetto all'esecuzione di una macchina virtuale da un backup. Una volta attivata la copia, la sua velocità di funzionamento è superiore a quella di una MV eseguita da un backup e non carica l'Agente per VMware.

Esempi di utilizzo

- **Creazione di copie di macchine virtuali in un sito remoto.**
  La replica consente di resistere meglio a errori totali o parziali dei datacenter, grazie alla clonazione delle macchine virtuali da un sito primario a un sito secondario. In genere il sito secondario è ubicato in una struttura remota che probabilmente non sarà influenzata da fattori ambientali, infrastrutturali o di altro tipo, che potrebbero causare gli errori nel sito primario.
- **Creazione di copie di macchine virtuali in un unico sito (da un host/datastore a un altro).**
  La replica sul posto può essere utilizzata in scenari di elevata disponibilità e di ripristino di emergenza.

Possibili utilizzi di una copia

- **Prova copia**
  La copia verrà accesa per effettuare il testing. Utilizzare il client vSphere o altri strumenti per verificare il corretto funzionamento della copia. Durante il testing, la replica viene sospesa.
- **Failover in una copia**
  Il failover è una transizione del carico di lavoro dalla macchina virtuale originale alla sua copia. Durante il failover, la replica viene sospesa.
- **Backup della copia**
  Sia il backup che la replica richiedono l'accesso a dischi virtuali e influiscono dunque sulle prestazioni dell'host che esegue la macchina virtuale. Se si desidera avere sia la copia che il

© Acronis International GmbH, 2003-2024

backup di una macchina virtuale, evitando nel contempo di caricare ulteriormente l'host di produzione, eseguire una copia della macchina su un host diverso e impostare i backup della copia.

Limitazioni

- Non è possibile eseguire copie dei seguenti tipi di macchine virtuali:
  - Macchine a tolleranza d'errore eseguite su ESXi 5.5 e versioni precedenti.
  - Macchine in esecuzione da backup
  - Copie di macchine virtuali
- Alcune modifiche hardware, come l'aggiunta o la rimozione di una scheda di interfaccia di rete (NIC) dall'host ESXi, comportano la modifica degli ID interni dell'host. Questa modifica ha effetto sui piani di replica delle VM. Dopo la modifica, è necessario ricreare i piani di replica delle VM nei quali l'host ESXi è selezionato come origine o destinazione. Altrimenti, i piani di replica delle VM non vengono eseguiti correttamente.

Creazione di un piano di replica

È necessario creare un piano di replica individuale per ciascuna macchina. Non è possibile applicare un piano esistente ad altre macchine.

Per creare un piano di replica

1. Selezionare una macchina virtuale per la replicazione.
2. Fare clic su **Replica**.
   Viene visualizzato un nuovo modello di piano di replica.
3. [Facoltativo] Per modificare il nome del piano di replica, fare clic sul nome predefinito.
4. Fare clic su **Macchina di destinazione** e procedere nel seguente modo:
   a. Indicare se si desidera creare una nuova copia o utilizzare una copia esistente della macchina originale.
   b. Selezionare l'host ESXi e specificare il nome della nuova copia oppure selezionare una copia esistente.
      Il nome predefinito della nuova replica è **[Nome macchina originale]_replica**.
   c. Fare clic su **OK**.
5. [Solo in caso di replica in una nuova macchina] Fare clic su **Datastore**, quindi selezionare il datastore per la macchina virtuale.
6. [Facoltativo] Fare clic su **Pianificazione** per cambiare la pianificazione della replica.
   Per impostazione predefinita, le replicazioni vengono eseguite giornalmente dal lunedì al venerdì. È possibile selezionare la data e l'ora in cui eseguire la replica.
   Per cambiare la frequenza delle replicazioni, spostare l'interruttore e specificare la pianificazione.
   È inoltre possibile eseguire le seguenti operazioni:

© Acronis International GmbH, 2003-2024

- Impostare un intervallo di date per l'entrata in vigore della pianificazione. Selezionare la casella di controllo **Esegui il piano in un intervallo di date** e specificare l'intervallo di date.
- Disabilitare la pianificazione. In questo caso, la replica può essere avviata manualmente.

7. [Facoltativo] Fare clic sull'icona ingranaggio per modificare le opzioni di replica.
8. Fare clic su **Applica**.
9. [Facoltativo] Per eseguire il piano manualmente, fare clic su **Esegui ora** nel riquadro del piano.

In seguito all'esecuzione di un piano di replica, la copia della macchina virtuale viene visualizzata nell'elenco **Tutti i dispositivi** con la seguente icona:

Prova di una copia

Per preparare una copia per la prova

1. Selezionare una copia da provare.
2. Fare clic su **Prova copia**.
3. Fare clic su **Avvia test**.
4. Indicare se connettere la copia avviata a una rete. Per impostazione predefinita, la copia non è connessa a una rete.
5. [Facoltativo] Se si sceglie di connettere la copia alla rete, selezionare la casella di controllo **Interrompi macchina virtuale originale** per interrompere la macchina originale prima di avviare la copia.
6. Fare clic su **Avvia**.

Per interrompere la prova di una copia

1. Selezionare una copia di cui è in corso la prova.
2. Fare clic su **Prova copia**.
3. Fare clic su **Interrompi test**.
4. Confermare la propria decisione.

Failover in una copia

Per eseguire il failover di una macchina a una copia

1. Selezionare una copia in cui eseguire il failover.
2. Fare clic su **Azioni copia**.
3. Fare clic su **Failover**.
4. Indicare se connettere la copia avviata a una rete. Per impostazione predefinita, la copia sarà connessa alla stessa rete della macchina originale.

© Acronis International GmbH, 2003-2024

5. [Facoltativo] Se si sceglie di connettere la copia alla rete, deselezionare la casella di controllo **Interrompi macchina virtuale originale** per mantenere online la macchina originale.
6. Fare clic su **Avvia**.

Mentre la copia si trova in stato di failover, è possibile scegliere una delle seguenti azioni:

- **Interrompi failover**
  Interrompe il failover se il problema della macchina originale è risolto. La copia verrà spenta. L'attività di replica verrà ripresa.
- **Eseguire un failover permanente alla copia**
  Questa operazione istantanea rimuove il flag "copia" dalla macchina virtuale, rendendo impossibile la replica. Per riprendere la replica, modificare il relativo piano selezionando questa macchina come origine.
- **Failback**
  Eseguire il failback se si è attuato il failover al sito che non è destinato a operazioni continue. La copia verrà ripristinata all'originale o a una macchina virtuale nuova. Una volta completato il ripristino alla macchina originale, questa verrà accesa e sarà riavviata la replica. Se si sceglie di riprendere la replica in una nuova macchina, modificare il relativo piano selezionando tale macchina come origine.

Arresto failover

Per interrompere un failover

1. Selezionare una copia che si trovi in stato di failover.
2. Fare clic su **Azioni copia**.
3. Fare clic su **Interrompi failover**.
4. Confermare la propria decisione.

Esecuzione di un failover permanente

Per eseguire un failover permanente

1. Selezionare una copia che si trovi in stato di failover.
2. Fare clic su **Azioni copia**.
3. Fare clic su **Failover permanente**.
4. [Facoltativo] Cambiare il nome della macchina virtuale.
5. [Facoltativo] Selezionare la casella di controllo **Interrompi macchina virtuale originale**.
6. Fare clic su **Avvia**.

Failback

Per eseguire il failback da una copia

© Acronis International GmbH, 2003-2024

1. Selezionare una copia che si trovi in stato di failover.
2. Fare clic su **Azioni copia**.
3. Fare clic su **Failback da copia**.
   Il software seleziona automaticamente il sistema originale come macchina di destinazione.
4. [Facoltativo] Fare clic su **Macchina di destinazione** e procedere nel seguente modo:
   a. Selezionare se eseguire il failback in una macchina nuova o una già esistente.
   b. Selezionare l'host ESXi e specificare il nome della nuova macchina oppure selezionare una macchina esistente.
   c. Fare clic su **OK**.
5. [Facoltativo] Durante il failback in una nuova macchina, è inoltre possibile effettuare le seguenti operazioni:
   - Fare clic su **Datastore** per selezionare il datastore per la macchina virtuale.
   - Fare clic su **Impostazioni MV** per cambiare la dimensione della memoria, il numero di processori e le connessioni di rete della macchina virtuale.
6. [Facoltativo] Fare clic su **Opzioni di ripristino** per modificare le opzioni di failback.
7. Fare clic su **Avvia ripristino**.
8. Confermare la propria decisione.

Opzioni di replica

Per modificare le opzioni di replica, fare clic sull'icona ingranaggio accanto al nome del piano di replica, quindi scegliere **Opzioni di replica**.

Changed Block Tracking (CBT)

Questa opzione è simile all'opzione di backup "Changed Block Tracking (CBT)".

Provisioning disco

Questa opzione consente di definire le impostazioni di provisioning del disco per la copia.

L'impostazione predefinita è: **Thin provisioning**.

Sono disponibili i seguenti valori: **Thin provisioning**, **Thick provisioning**, **Mantenere l'impostazione originale**.

Gestione degli errori

Questa opzione è simile all'opzione di backup "Gestione degli errori".

Comandi pre/post

Questa opzione è simile all'opzione di backup "Comandi pre/post".

© Acronis International GmbH, 2003-2024

Servizio Copia Shadow del volume per macchine virtuali

Questa opzione è simile all'opzione di backup "Servizio Copia Shadow del volume per macchine virtuali".

Opzioni di failback

Per modificare le opzioni relative al failback, fare clic su **Opzioni di ripristino** durante la configurazione del failback.

Gestione degli errori

Questa opzione è simile all'opzione di ripristino "Gestione degli errori".

Prestazioni

Questa opzione è simile all'opzione di ripristino "Prestazioni".

Comandi pre/post

Questa opzione è simile all'opzione di ripristino "Comandi pre/post".

Gestione energetica MV

Questa opzione è simile all'opzione di ripristino "Gestione energetica MV".

Raccolta dei dati di replica iniziali

Per velocizzare la replica a una posizione remota e risparmiare larghezza di banda di rete, è possibile eseguire la raccolta dei dati di copia.

Importante
Per eseguire la raccolta dei dati di replica, l'Agente per VMware (appliance virtuale) deve essere in esecuzione sull'host ESXi di destinazione.

Per raccogliere i dati di replica iniziali

1. Eseguire una delle seguenti operazioni:
   - Se la macchina virtuale originaria può essere spenta, spegnerla e saltare al passaggio 4.
   - Se la macchina virtuale originaria non può essere spenta, continuare con il passaggio successivo.
2. Creare un piano di replica.

   Quando viene creato il piano, in **Macchina di destinazione** selezionare **Nuova replica** e l'host ESXi che ospita la macchina originaria.
3. Eseguire una sola volta il piano.

   Nell'host ESXi originario viene creata una replica.
4. Esportare i file della macchina virtuale (o di replica) in un'unità disco esterna.

© Acronis International GmbH, 2003-2024

a. Collegare l'unità disco esterna alla macchina in cui viene eseguito il client vSphere.
b. Collegare il client vSphere al server vCenter o all'host ESXi originario.
c. Selezionare la replica appena creata nell'inventario.
d. Fare clic su **File** > **Esportazione** > **Esportazione modello OVF**.
e. In **Directory**, specificare la cartella sull'unità disco esterna.
f. Fare clic su **OK**.

5. Trasferire l'unità disco nella posizione remota.
6. Importare la replica nell'host ESXi di destinazione.
   a. Collegare l'unità disco esterna alla macchina in cui viene eseguito il client vSphere.
   b. Collegare il client vSphere al vCenter o ESXi di destinazione.
   c. Fare clic su **File** > **Distribuisci modello OVF**.
   d. In **Distribuisci da file o URL**, specificare il modello esportato nel passaggio 4.
   e. Completare la procedura di importazione.
7. Modificare il piano di replica creato nel passaggio 2. In **Macchina di destinazione**, selezionare **Copia esistente**, quindi selezionare la copia importata.

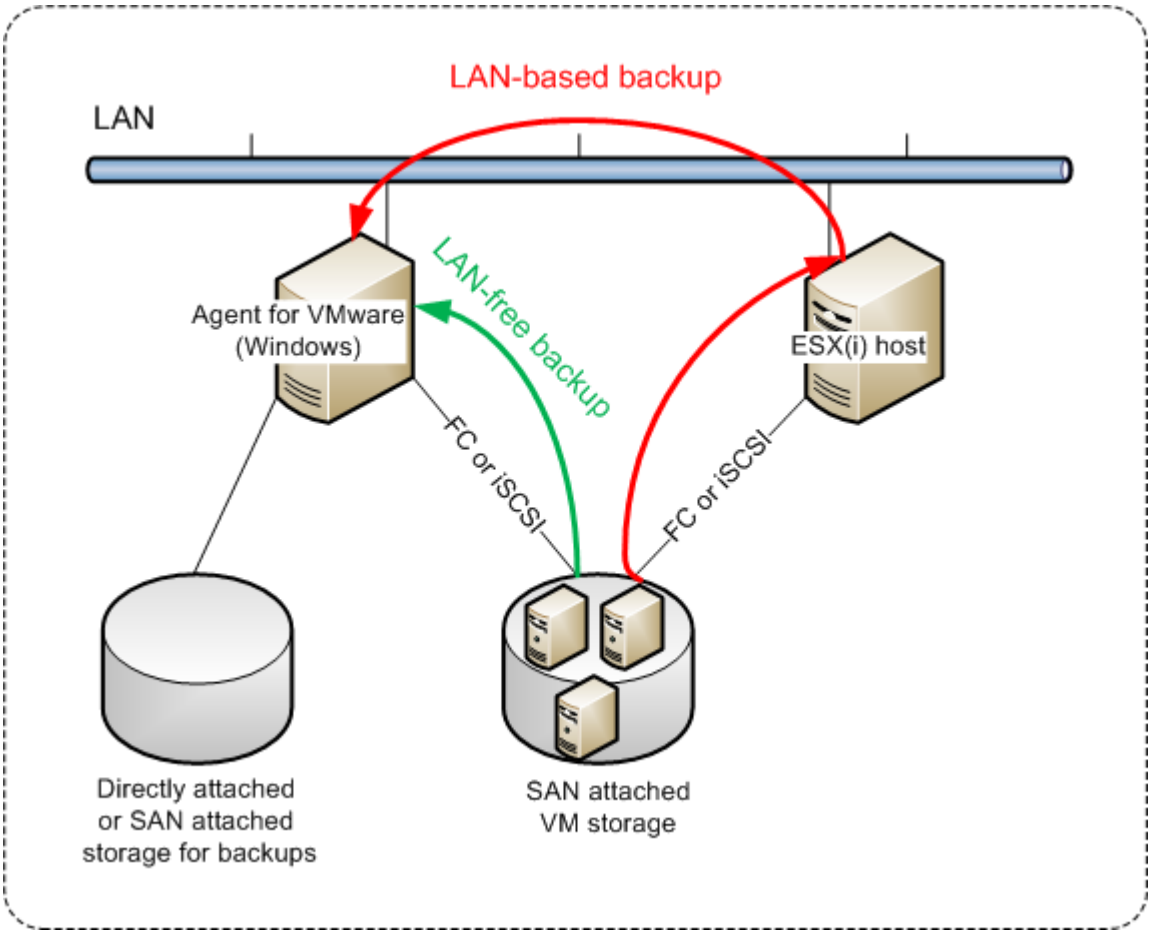
A questo punto, il software prosegue con l'aggiornamento della replica. Tutte le repliche saranno incrementali.

Agente per VMware - Backup senza LAN

Se ESXi utilizza un SAN attached storage, installare l'agente su una macchina connessa alla stessa SAN. L'agente eseguirà il backup delle macchine virtuali direttamente dall'archivio, anziché tramite l'host ESXi e la LAN. Questa funzionalità è chiamata backup senza LAN.

Il diagramma di seguito illustra un backup basato su LAN e uno senza LAN. L'accesso senza LAN alle macchine virtuali è disponibile se si dispone di una SAN (Storage Area Network) Fibre Channel (FC) o iSCSI. Per eliminare completamente il trasferimento dei dati del backup tramite la LAN, archiviare i backup su un disco locale della macchina dell'agente o in un archivio collegato a una SAN.

© Acronis International GmbH, 2003-2024



Per abilitare l'accesso diretto a un datastore da parte di un agente

1. Installare l'Agente per VMware su una macchina Windows che dispone dell'accesso di rete al vCenter Server.
2. Collegare il numero di unità logica (LUN) che ospita il datastore alla macchina. Considerare quando segue:
   - Utilizzare lo stesso protocollo (iSCSI o FC) usato per la connessione del datastore a ESXi.
   - L'unità LUN *non deve* essere inizializzata e deve apparire come disco "offline" in **Gestione disco**. Se Windows inizializza la LUN, questa potrebbe subire danni e non essere leggibile da VMware vSphere.

Di conseguenza, l'agente utilizzerà la modalità di trasporto SAN per accedere ai dischi virtuali: ad esempio, leggerà i settori LUN raw su iSCSI/FC senza riconoscere il file system VMFS (che Windows non è in grado di individuare).

Limitazioni

- In vSphere 6.0 e versioni successive, l'agente non può utilizzare la modalità di trasporto SAN se alcuni dei dischi MV sono collocati in un volume virtuale VMware (VVol), mentre altri non lo sono. Il backup di tali macchine virtuali non andrà a buon fine.
- Il backup delle macchine virtuali crittografate, introdotte in VMware vSphere 6.5, verrà eseguito via LAN, anche se per l'agente è stata configurata la modalità di trasporto SAN. L'agente eseguirà

© Acronis International GmbH, 2003-2024

il fallback sul trasporto NBD poiché VMware non supporta il trasporto SAN per l'esecuzione di backup di dischi virtuali crittografati.

Esempio

Se si utilizza una SAN iSCSI, configurare l'iniziatore iSCSI sulla macchina che esegue Windows in cui è installato l'Agente per VMware.

Per configurare il criterio SAN

1. Accedere come amministratore e aprire il prompt dei comandi, quindi digitare `diskpart` e premere **Invio**.
2. Digitare `san` e premere **Invio**. Assicurarsi che sia visualizzato il **criterio SAN: Tutto non in linea**
3. Se è impostato un altro valore per il criterio SAN:
   a. Digitare `san policy=offlineall`.
   b. Premere **Invio**.
   c. Per verificare che l'impostazione sia stata applicata correttamente, eseguire il passaggio 2.
   d. Riavviare la macchina.

Per configurare un iniziatore iSCSI

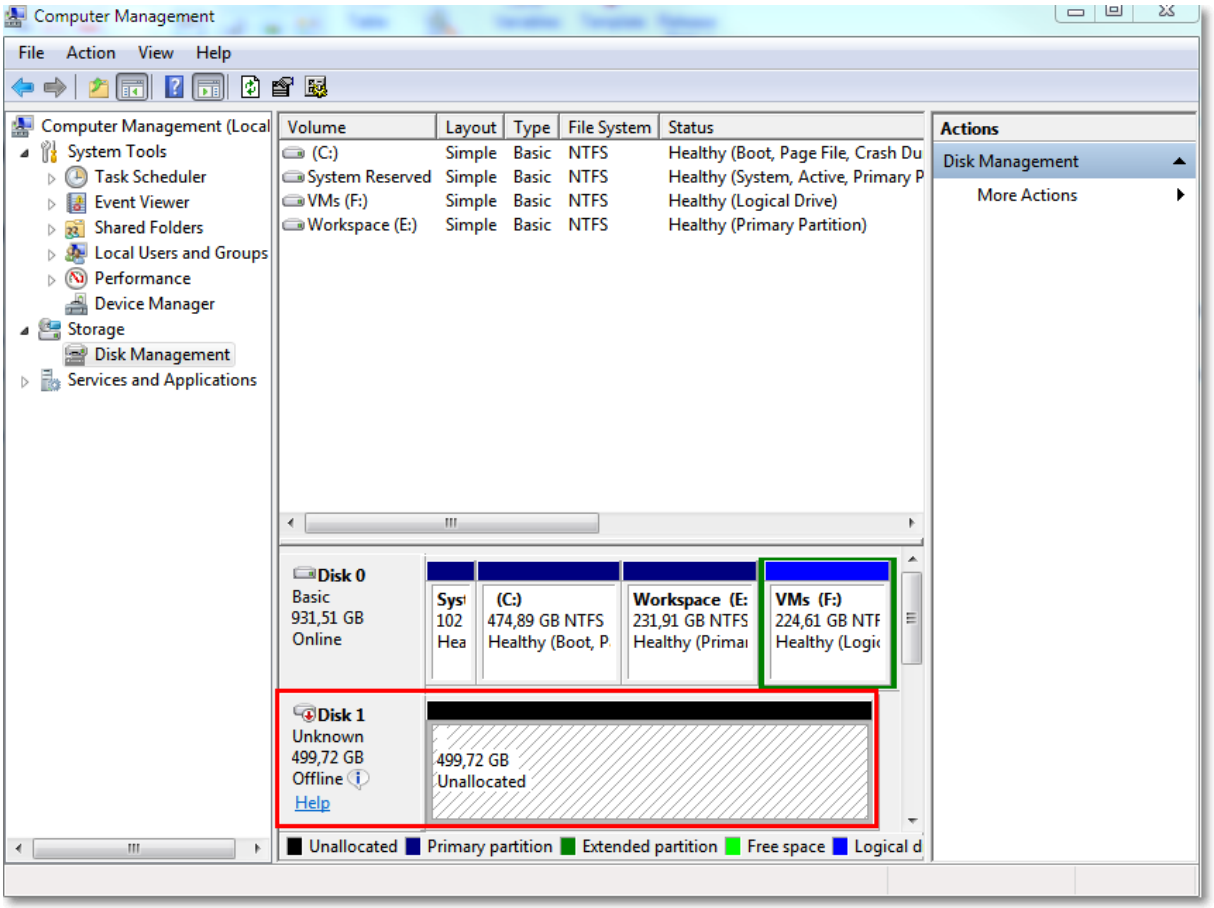
1. Aprire **Pannello di controllo** > **Strumenti di amministrazione** > **Iniziatore iSCSI**.

   Nota
   Per trovare l'applet **Strumenti di amministrazione**, potrebbe essere necessario cambiare la visualizzazione **Pannello di controllo** su un'impostazione diversa da **Home** o **Categoria**, oppure utilizzare la ricerca.

2. Se è la prima volta che Microsoft iSCSI Initiator viene avviato, confermare che si desidera avviare il servizio Microsoft iSCSI Initiator.
3. Nella scheda **Destinazioni**, digitare il nome completo di dominio (FQDN) o l'indirizzo IP del dispositivo SAN di destinazione e fare clic su **Connessione rapida**.
4. Selezionare la LUN che ospita il datastore e fare clic su **Connettere**.
   Se la LUN non viene visualizzata, accertarsi che la zonizzazione nella destinazione iSCSI abiliti la macchina che esegue l'agente per l'accesso alla LUN. La macchina deve essere aggiunta all'elenco degli iniziatori iSCSI nella destinazione.
5. Fare clic su **OK**.

La LUN SAN dovrebbe essere visualizzata in **Gestione del disco**, come illustrato nella cattura di schermata seguente.

© Acronis International GmbH, 2003-2024



Utilizzo di un archivio collegato localmente

È possibile collegare un disco aggiuntivo a un Agente per VMware (Virtual Appliance) in modo tale che l'agente possa eseguire il backup in questo archivio collegato localmente. Questo approccio limita il traffico di rete tra l'agente e la posizione di backup.

Un'appliance virtuale in esecuzione nello stesso host o cluster delle macchine virtuali di cui viene eseguito il backup può accedere direttamente ai datastore in cui risiede la macchina. Ciò significa che l'appliance può collegare i dischi oggetto di backup tramite il trasporto HotAdd; di conseguenza il traffico di backup è diretto da un disco locale a un altro. Se il datastore è connesso come **Disco/LUN** e non come **NFS**, il backup non richiede l'utilizzo della LAN. In presenza di un datastore NFS, il traffico di rete avviene tra il datastore e l'host.

L'utilizzo di un archivio collegato localmente implica che l'agente esegue sempre il backup nello stesso sistema. Se più agenti sono in funzione in vSphere e uno o più di questi utilizza archivi collegati localmente, è necessario associare manualmente ognuno di essi a tutti i sistemi da sottoporre a backup. Altrimenti, se i sistemi vengono ridistribuiti tra gli agenti dal server di gestione, i backup di un sistema potrebbero essere dispersi in archivi diversi.

È possibile aggiungere l'archiviazione a un agente già in funzione o durante la distribuzione dell'agente da un modello OVF.

Per collegare un archivio a un agente già in funzione

© Acronis International GmbH, 2003-2024

1. Nell'inventario di VMware vSphere, fare clic con il pulsante destro dela mouse sull'Agente per VMware (Virtual Appliance).
2. Aggiungere il disco modificando le impostazioni della macchina virtuale. La dimensione del disco deve essere almeno 10 GB.

   Attenzione!
   Prestare attenzione quando si aggiunge un disco già esistente. Una volta creato l'archivio, tutti i dati contenuti precedentemente sul disco andranno perduti.

3. Passare alla console dell'appliance virtuale. Il collegamento **Crea archivio** è disponibile nella parte inferiore della schermata. In caso contrario, fare clic su **Aggiorna**.
4. Fare clic sul collegamento **Crea archivio**, selezionare il disco e specificare un'etichetta. La lunghezza dell'etichetta è limitata a 16 caratteri a causa delle restrizioni del file system.

Per selezionare un archivio collegato localmente come destinazione di backup

- Quando si crea un piano di protezione, in **Dove eseguire il backup** selezionare **Cartelle locali**, quindi digitare la lettera corrispondente all'archivio collegato localmente, ad esempio **D:**.

Nota
Un archivio collegato localmente (LAS, Locally Attached Storage) è progettato per ambienti relativamente piccoli con un singolo agente (appliance virtuale). Abbiamo testato unità LAS con dimensioni massime di 5 TB. È possibile collegare dischi più grandi a proprio rischio, tenendo presente che tali configurazioni non sono supportate. Si consiglia di utilizzare altri tipi di storage per dati di backup superiori ai 5 TB. Ad esempio, è possibile creare e collegare un disco virtuale VMware a qualsiasi virtual machine casuale e crearvi una condivisione di rete che verrà quindi utilizzata come destinazione di backup al posto di un LAS.

Associazione delle macchine virtuali

Questa sezione fornisce una panoramica del modo in cui il servizio Cyber Protection organizza il funzionamento di più agenti con VMware vCenter.

L'algoritmo di distribuzione di seguito funziona sia per gli appliance virtuali che per gli agenti installati in Windows.

Algoritmo di distribuzione

Le macchine virtuali vengono distribuite in modo uniforme fra gli Agenti per VMware. Per modo uniforme, si intende che ogni agente gestisce un numero uguale di macchine. La quantità di spazio di archiviazione occupato da una macchina virtuale non viene calcolato.

Tuttavia, quando si sceglie un agente per una macchina, il software prova a ottimizzare le prestazioni generali del sistema. In particolare, il software considera la posizione dell'agente e della macchina virtuale. Viene privilegiato un agente ospitato sullo stesso host. Se non è presente alcun agente sullo stesso host, viene privilegiato un agente dello stesso cluster.

© Acronis International GmbH, 2003-2024

Quando una macchina virtuale viene assegnata a un agente, tutti i backup di questa macchina verranno delegati a questo agente.

Ridistribuzione

La ridistribuzione avviene ogni volta che l'equilibrio stabilito si interrompe, o più precisamente, quando lo squilibrio del carico tra gli agenti raggiunge il 20%. Questo si può verificare quando una macchina o un agente viene aggiunto o rimosso, o una macchina migra a un host o cluster diverso, o se si associa manualmente una macchina a un agente. Se ciò accade, il server Cyber Protection ridistribuisce i sistemi utilizzando lo stesso algoritmo.

Per esempio, si realizza che sono necessari più agenti per aiutare con la produttività e distribuire un appliance virtuale aggiuntivo sul cluster. Il servizio Cyber Protection assegna i sistemi più idonei al nuovo agente. Il carico dei vecchi agenti si ridurrà.

Quando si rimuove un agente dal servizio Cyber Protection, i sistemi assegnati all'agente vengono distribuiti tra gli agenti rimanenti. Tuttavia, ciò non accade se un agente risulta danneggiato o se viene eliminato manualmente da vSphere. La ridistribuzione verrà avviata solo dopo aver rimosso l'agente dall'interfaccia Web.

Visualizzazione dei risultati della distribuzione

È possibile visualizzare il risultato della distribuzione automatica:

- nella colonna **Agente** disponibile per ogni macchina virtuale alla sezione **Tutti i dispositivi**
- nella sezione **Macchine virtuali assegnate** del pannello **Dettagli**, quando viene selezionato un agente in **Impostazioni** > sezione **Agenti**

Associazione manuale

L'associazione Agente per VMware consente di escludere una macchina virtuale da questo processo di distribuzione specificando l'agente che deve sempre eseguire il backup di questa macchina. Il bilanciamento generale viene mantenuto, ma sarà possibile passare la macchina specifica a un agente diverso solo se l'agente originale viene rimosso.

Per associare una macchina a un agente

1. Selezionare la macchina.
2. Fare clic su **Dettagli**.
   Nella sezione **Agente assegnato**, il software mostra l'agente che gestisce la macchina correntemente selezionata.
3. Fare clic su **Modifica**.
4. Selezionare **Manuale**.
5. Selezionare l'agente a cui associare la macchina.
6. Fare clic su **Salva**.

Per annullare l'associazione di una macchina a un agente

© Acronis International GmbH, 2003-2024

1. Selezionare la macchina.
2. Fare clic su **Dettagli**.

   Nella sezione **Agente assegnato**, il software mostra l'agente che gestisce la macchina correntemente selezionata.
3. Fare clic su **Modifica**.
4. Selezionare **Automatica**.
5. Fare clic su **Salva**.

Disabilitazione dell'assegnazione automatica per un agente

È possibile disabilitare l'assegnazione automatica per un Agente per VMware, al fine di escluderlo dal processo di distribuzione, specificando l'elenco di sistemi di cui l'agente deve eseguire il backup. Il bilanciamento complessivo verrà mantenuto tra gli altri agenti.

Non è possibile disabilitare l'assegnazione automatica per un agente se non sono presenti altri agenti registrati o se l'assegnazione automatica è stata disabilitata per tutti gli altri agenti.

Per disabilitare l'assegnazione automatica per un agente

1. Fare clic su **Impostazioni** > **Agenti**.
2. Selezionare l'Agente per VMware per cui disabilitare l'assegnazione automatica.
3. Fare clic su **Dettagli**.
4. Disabilitare l'opzione **Assegnazione automatica**.

Esempi di utilizzo

- L'associazione manuale risulta utile se si desidera che il backup di uno specifico sistema (di grandi dimensioni) venga eseguito dall'Agente per VMware (Windows) tramite Fibre Channel, mentre il backup degli altri sistemi viene eseguito tramite appliance virtuali.
- È necessario associare le MV a un agente se questo dispone di un archivio collegato localmente.
- Disabilitando l'assegnazione automatica è possibile garantire che un determinato sistema venga sottoposto a backup in modo prevedibile in base alla pianificazione specificata. L'agente che esegue solo il backup di una MV non può risultare impegnato nel backup di altre MV durante l'orario pianificato.
- Disabilitare l'assegnazione automatica è utile in presenza di più host ESXi separati a livello geografico. Se si disabilita l'assegnazione automatica e poi si associano le VM su ogni host all'agente in esecuzione sullo stesso host, è possibile assicurarsi che l'agente non esegua mai il backup delle macchine in esecuzione negli host ESXi remoti, risparmiando traffico di rete.

Esecuzione automatica degli script di pre blocco e post sblocco

Con Strumenti VMware è possibile eseguire automaticamente gli script di pre blocco e post sblocco sulle virtual machine di cui è eseguito il backup in modalità agentless. Pertanto, ad esempio, è

© Acronis International GmbH, 2003-2024

possibile eseguire script di disattivazione e creare backup compatibili con l'applicazione per virtual machine che eseguono applicazioni non compatibili con VSS.

Prerequisiti

Gli script pre blocco e post sblocco devono essere posizionati in una cartella specifica nella virtual machine.

- Per le virtual machine Windows, la posizione di questa cartella dipende dalla versione ESXi dell'host.

  Ad esempio, per le virtual machine eseguite in un host ESXi 6.5, tale cartella è `C:\Program Files\VMware\VMware Tools\backupScripts.d\`. È necessario creare manualmente la cartella `backupScripts.d`. L'archiviazione di altri tipi di file in questa cartella può causare l'instabilità di Strumenti VMware.

  Per ulteriori informazioni sulla posizione degli script pre blocco e post sblocco di altre versioni di ESXi, fare riferimento alla documentazione VMware.
- Per le virtual machine Linux, copiare gli script nelle directory `/usr/sbin/pre-freeze-script` e `/usr/sbin/post-thaw-script`, rispettivamente. Gli script in `/usr/sbin/pre-freeze-script` vengono eseguiti quando si crea una snapshot e quelli in `/usr/sbin/post-thaw-script` vengono eseguiti quando la snapshot viene finalizzata. Gli script devono essere eseguibili dall'utente di Strumenti VMware.

Per eseguire in modalità automatica gli script di pre blocco e post sblocco

1. Verificare che Strumenti VMware sia installato nella virtual machine.
2. Nella virtual machine, posizionare gli script personalizzati nella cartella richiesta.
3. Nel piano di protezione per questo sistema, abilitare l'opzione **Servizio Copia Shadow del volume per virtual machine**.

   Viene così creata una snapshot VMware con l'opzione **Quiesce guest file system** abilitata, che a sua volta attiverà gli script pre blocco e post sblocco all'interno della virtual machine.

Non è necessario eseguire script di disattivazione nelle virtual machine che eseguono applicazioni compatibili con VSS, quali Microsoft SQL Server o Microsoft Exchange. Per creare backup compatibili con l'applicazione per questi sistemi, nel piano di protezione abilitare l'opzione **Servizio Copia Shadow del volume per virtual machine**.

Supporto per la migrazione di virtual machine

Questa sezione contiene informazioni sulla migrazione delle virtual machine in un ambiente vSphere, inclusa la migrazione tra host ESXi che fanno parte di un cluster vSphere.

vMotion consente di trasferire lo stato e la configurazione di una virtual machine a un altro host, mentre i dischi del sistema rimangono nella stessa posizione in uno storage condiviso. Storage VMotion consente di spostare i dischi di una virtual machine da un datastore a un altro.

- La migrazione con vMotion, incluso con Storage vMotion, non è supportata per virtual machine che eseguono l'Agente per VMware (appliance virtuale), e viene automaticamente disabilitata.

© Acronis International GmbH, 2003-2024

Questa virtual machine viene aggiunta all'elenco **VM overrides** nella configurazione del cluster vSphere.

- Quando si avvia il backup di una virtual machine, la migrazione con vMotion, incluso con Storage vMotion, viene automaticamente disabilitata. Questa virtual machine viene temporaneamente aggiunta all'elenco **VM overrides** nella configurazione del cluster vSphere. Al termine del backup, le impostazioni di **VM overrides** vengono automaticamente ripristinate allo stato precedente.
- Non è possibile avviare il backup di una virtual machine mentre è in corso la migrazione con vMotion, incluso con Storage vMotion. Il backup di questo sistema verrà avviato al termine della migrazione.

Gestione di ambienti di virtualizzazione

È possibile visualizzare gli ambienti vSphere, Hyper-V e Virtuozzo nelle rispettive presentazioni native. Una volta che l'agente corrispondente è installato e registrato, la scheda **VMware**, **Hyper-V** o **Virtuozzo** viene visualizzata in **Dispositivi**.

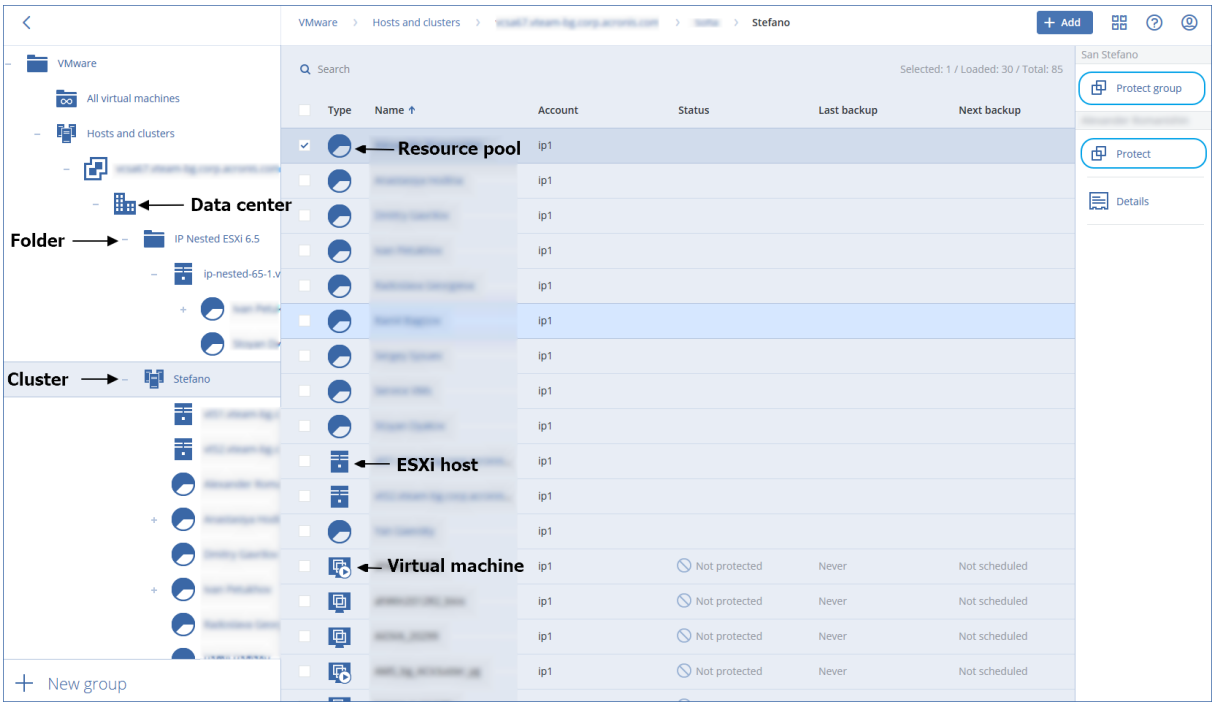
Nella scheda **VMware** è possibile eseguire il backup dei seguenti oggetti dell'infrastruttura vSphere:

- Datacenter
- Cartella
- Cluster
- Host ESXi
- Pool di risorse

Ognuno degli oggetti dell'infrastruttura funziona come un oggetto di gruppo per macchine virtuali. Quando si applica un piano di protezione a uno qualsiasi di questi oggetti di gruppo, viene eseguito il backup di tutte le macchine virtuali che esso contiene. È possibile eseguire il backup dei sistemi del gruppo selezionato facendo clic su **Proteggi**, oppure dei sistemi del gruppo padre in cui è incluso il gruppo selezionato facendo clic su **Proteggi gruppo**.

Ad esempio, è stato selezionato il cluster Stefano e quindi il pool di risorse che si trova al suo interno. Facendo clic su **Proteggi**, viene eseguito il backup di tutte le macchine virtuali incluse nel pool di risorse selezionato. Facendo clic su **Proteggi gruppo**, viene eseguito il backup di tutte le virtual machine incluse nel cluster Stefano.

© Acronis International GmbH, 2003-2024



La scheda **VMware** consente di cambiare le credenziali di accesso per il vCenter Server o per l'host ESXi autonomo senza reinstallare l'agente.

Per cambiare le credenziali di accesso per il server vCenter o per l'host ESXi

1. In **Dispositivi**, fare clic su **VMware**.
2. Fare clic su **Host e cluster**.
3. Nell'elenco **Host e cluster** (a destra dell'albero **Host e Cluster**), selezionare il vCenter Server o l'host ESXi autonomo specificati durante l'installazione dell'Agente per VMware.
4. Fare clic su **Dettagli**.
5. In **Credenziali**, fare clic sul nome utente.
6. Specificare le nuove credenziali di accesso e fare clic su **OK**.

Visualizzazione dello stato del backup stato nel client vSphere

Nel client vSphere, è possibile visualizzare lo stato del backup e l'ora dell'ultimo backup di una macchina virtuale.

Queste informazioni sono visualizzate nel riepilogo della macchina virtuale (**Riepilogo** > **Attributi personalizzati/Annotazioni/Note**, a seconda del tipo di client e versione di vSphere). È inoltre possibile abilitare le colonne **Ultimo backup** e **Stato backup** nella scheda **Macchine Virtuali** per ogni host, data center, cartella, pool di risorse o per l'intero vCenter Server.

Per fornire tali attributi, l'Agente per VMware deve avere i seguenti privilegi, oltre a quelli descritti nella sezione "Agente per VMware: privilegi necessari":

© Acronis International GmbH, 2003-2024

- **Globale** > **Gestire attributi personalizzati**
- **Globale** > **Impostare attributo personalizzato**

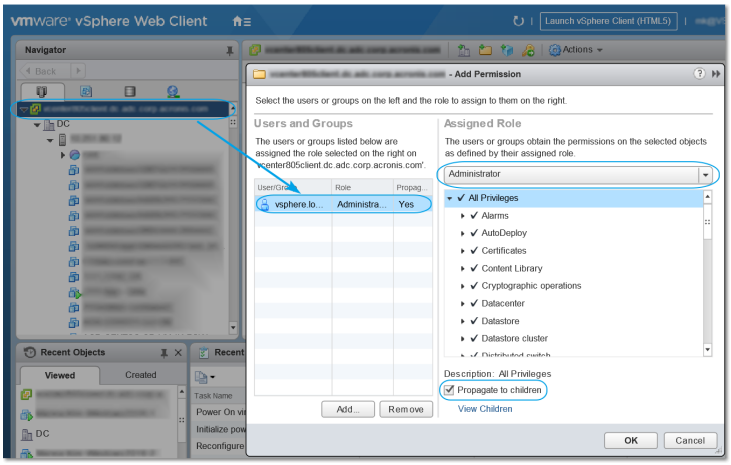
Privilegi necessari per l'Agente per VMware

Per eseguire qualsiasi operazione con oggetti vCenter quali macchine virtuali, host ESXi, cluster, vCenter e altri, l'Agente per VMware si autentica sull'host vCenter o ESXi utilizzando le credenziali vSphere fornite dall'utente. L'account vSphere, utilizzato per la connessione a vSphere dall'Agente per VMware, deve disporre dei privilegi richiesti a tutti i livelli dell'infrastruttura vSphere, ad iniziare dal livello vCenter.

Specificare l'account vSphere con i privilegi richiesti nel corso dell'installazione o della configurazione dell'Agente per VMware. Per modificare l'account in un momento successivo, fare riferimento a "Gestione di ambienti di virtualizzazione" (pag. 712).

Per assegnare le autorizzazioni a un utente vSphere al livello vCenter

1. Accedere al client web vSphere.
2. Fare clic con il pulsante destro del mouse su vCenter e quindi su **Aggiungi autorizzazione**.
3. Selezionare o aggiungere un nuovo utente con il ruolo richiesto (il ruolo deve includere tutte le autorizzazioni richieste indicate nella tabella seguente).
4. Selezionare l'opzione di **propagazione ai figli**.



Oggetto	Privilegio	Operazione			
		Backup di una VM	**Ripristino in una nuova VM**	**Ripristino in una VM esistente**	**Esegui MV dal backup**
Operazioni crittografiche (inizia con vSphere 6.5)	**Aggiungi disco**	+*			

© Acronis International GmbH, 2003-2024

	Accesso diretto	+*			
Datastore	**Allocazione dello spazio**		+	+	+
	Esplorazione del datastore				+
	Configurazione del datastore	+	+	+	+
	Operazioni file di basso livello				+
Globale	**Licenze**	+	+	+	+
	Disabilitazione dei metodi	+	+	+	
	Abilitazione dei metodi	+	+	+	
	Gestire attributi personalizzati	+	+	+	
	Impostare l'attributo personalizzato	+	+	+	
Host > **Configurazione**	**Configurazione della partizione di archiviazione**				+
Host > **Operazioni locali**	**Creazione VM**				+
	Eliminazione VM				+
	Riconfigurazione VM				+
Rete	**Assegnazione della rete**		+	+	+
Risorsa	**Assegnazione della MV al pool di risorse**		+	+	+
Macchina virtuale > **Configurazione**	**Aggiunta di un disco esistente**	+	+		+
	Aggiunta di un disco nuovo		+	+	+
	Aggiunta o rimozione di un dispositivo		+		+
	Avanzato	+	+	+	
	Modifica del conto CPU		+		

© Acronis International GmbH, 2003-2024

	Monitoraggio modifiche disco	+		+	
	Assegnazione disco	+		+	
	Memoria		+		
	Rimozione di un disco	+	+	+	+
	Rinomina		+		
	Impostazione annotazione				+
	Impostazioni		+	+	+
Macchina virtuale -> **Operazioni guest**	**Esecuzione programma operazioni guest**	+**			
	Query operazioni guest	+**			
	Modifiche operazioni guest	+**			
Macchina virtuale > **Interazione**	**Acquisisci ticket controllo guest** (in vSphere 4.1 e 5.0)				+
	Configurazione supporto CD		+	+	
	Gestione di sistemi operativi guest da parte di VIX API (in vSphere 5.1 e versioni successive)				+
	Spegnimento			+	+
	Accensione		+	+	+
Macchina virtuale > **Inventario**	**Creazione da esistente**		+	+	+
	Crea nuovo		+	+	+
	Registra				+
	Rimuovi		+	+	+
	Annulla registrazione				+
Macchina virtuale > **Provisioning**	**Consenso accesso disco**		+	+	+
	Consenso accesso disco sola lettura	+		+	

© Acronis International GmbH, 2003-2024

	Consenso download macchina virtuale	+	+	+	+
Macchina virtuale > **Stato** **Macchina virtuale** > **Gestione snapshot** (vSphere 6.5 e successive)	**Creazione snapshot**	+		+	+
	Rimozione snapshot	+		+	+
vApp	**Aggiungi macchina virtuale**				+

* Questo privilegio è obbligatorio solo per i backup di macchine criptate.

** Questo privilegio è obbligatorio solo per i backup compatibili con l'applicazione.

Backup di sistemi Hyper-V in cluster

In un cluster Hyper-V, è possibile effettuare la migrazione delle macchine virtuali tra i nodi dei cluster. Seguire queste raccomandazioni per configurare il backup corretto dei sistemi Hyper-V in cluster:

1. Un sistema deve essere disponibile per il backup a prescindere dal nodo su cui viene effettuata la sua migrazione. Per garantire che un Agente per Hyper-V possa accedere a un sistema su qualunque nodo, è necessario eseguire il servizio agente con un account utente di dominio con privilegi di amministrazione su ciascun nodo del cluster.
   Si consiglia di specificare tale account per il servizio dell'agente durante l'installazione dell'Agente per Hyper-V.
2. Installare l'Agente per Hyper-V su ogni nodo del cluster.
3. Registrare tutti gli agenti al servizio Cyber Protection.

Disponibilità elevata di un sistema ripristinato

Quando si ripristinano dischi di cui è stato eseguito il backup in una macchina virtuale Hyper-V *esistente*, la proprietà Disponibilità elevata del sistema rimane così com'è.

Quando si ripristinano dischi di cui è stato eseguito il backup in una macchina virtuale Hyper-V *nuova*, il sistema derivante non sarà a disponibilità elevata. È considerato come sistema di riserva e normalmente è spento. Per utilizzare il sistema nell'ambiente di produzione, è possibile configurarlo per la Disponibilità elevata dallo snap-in **Gestione cluster di failover**.

© Acronis International GmbH, 2003-2024

Limitare il numero totale di macchine virtuali di cui viene eseguito il backup simultaneo

Nell'opzione di backup **Pianificazione** è possibile limitare il numero di virtual machine il cui backup viene eseguito simultaneamente per piano di protezione.

Quando un agente esegue più piani nello stesso momento, il numero di sistemi il cui backup viene eseguito simultaneamente si somma. Questa sovrapposizione può influire negativamente sulle prestazioni di backup e sovraccaricare l'host e lo storage della virtual machine. Per evitare questo problema, è possibile configurare una limitazione a livello di agente.

Per limitare il numero di backup eseguiti simultaneamente a livello di agente

Agente per VMware (Windows)

1. Nel sistema con l'agente, creare un nuovo documento di testo e aprirlo in un editor di testo.
2. Copiare e incollare nel file le righe seguenti.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Sostituire `00000001` con il valore esadecimale del limite che si desidera impostare.
   Ad esempio, `00000001` è 1 e `0000000A` è 10.
4. Salvare il documento come **limit.reg**.
5. Eseguire il file come amministratore.
6. Confermare che si desidera modificare il registro di Windows.
7. Riavviare l'agente.
   a. Nel menu **Start** fare clic su **Esegui**.
   b. Digitare **cmd**, quindi fare clic su **OK**.
   c. Nella riga di comando eseguire i comandi seguenti:

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

Agente per Hyper-V

1. Nel sistema con l'agente, creare un nuovo documento di testo e aprirlo in un editor di testo.
2. Copiare e incollare nel file le righe seguenti.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
```


© Acronis International GmbH, 2003-2024

```
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Sostituire `00000001` con il valore esadecimale del limite che si desidera impostare.
   Ad esempio, `00000001` è 1 e `0000000A` è 10.
4. Salvare il documento come **limit.reg**.
5. Eseguire il file come amministratore.
6. Confermare che si desidera modificare il registro di Windows.
7. Riavviare l'agente.
   a. Nel menu **Start** fare clic su **Esegui**.
   b. Digitare **cmd**, quindi fare clic su **OK**.
   c. Nella riga di comando eseguire i comandi seguenti:

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

Appliance virtuali

Questa procedura si applica ad Agente per VMware (appliance virtuale), Agente per Scale Computing, Agente per Virtuozzo Hybrid Infrastructure e Agente per oVirt.

1. Nella console dell'appliance virtuale, premere CTRL+MAIUSC+F2 per aprire l'interfaccia a riga di comando.
2. Aprire il file `/etc/Acronis/MMS.config` in un editor di testo.
3. Individuare la sezione seguente:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Sostituire `10` con il numero massimo di backup simultanei che si desidera impostare.
5. Salvare il file.
6. Riavviare l'agente utilizzando il comando `reboot`.

Migrazione della macchina

È possibile eseguire la migrazione della macchina ripristinando i relativi backup in una macchina non originale.

La tabella seguente riepiloga le opzioni di migrazione disponibili.

© Acronis International GmbH, 2003-2024

Tipo di macchina di cui è stato eseguito il backup	Destinazioni di ripristino disponibili							
	Macchina fisica	Macchina virtuale ESXi	Macchina virtuale Hyper-V	Virtuozzo		Macchina virtuale Virtuozzo Hybrid Infrastructure	Virtual machine Scale Computing HC3	Virtual machine RHV/oVirt
				Macchina virtuale	Container			
Macchina fisica	+	+	+	-	-	+	+*	+
Macchina virtuale VMware ESXi	+	+	+	-	-	+	+*	+
Macchina virtuale Hyper-V	+	+	+	-	-	+	+*	+
Macchina virtuale Virtuozzo	+	+	+	+	-	+	+*	+
Contenitore Virtuozzo	-	-	-	-	+	-	-	-
Macchina virtuale Virtuozzo Hybrid Infrastructure	+	+	+	-	-	+	+*	+
Virtual machine Scale Computing HC3	+	+	+	-	-	+	+	+
Virtual machine Red Hat Virtualization/oVirt	+	+	+	-	-	+	+*	+

*Se Secure Boot è abilitato nel sistema di origine, la VM ripristinata non sarà in grado di avviarsi a meno che Secure Boot non venga disabilitato nella console della VM dopo il ripristino.

© Acronis International GmbH, 2003-2024

Nota
Non è possibile ripristinare le macchine virtuali MacOS su host Hyper-V, perché Hyper-V non supporta MacOS. È invece possibile ripristinare le macchine virtuali MacOS su un host VMware installato su hardware Mac.

Per ulteriori informazioni su come eseguire le operazioni di migrazione, consultare gli argomenti seguenti:

- Per le migrazioni da fisico a virtuale (P2V), consultare "Da macchina fisica a macchina virtuale" (pag. 509).
- Per le migrazioni da virtuale a virtuale (V2V), consultare "Ripristino di una macchina virtualeÈ possibile ripristinare le macchine virtuali dai rispettivi backup.Non è possibile ripristinare i backup nella console di Cyber Protect per i tenant in modalità Conformità. Per ulteriori informazioni su come ripristinare questi backup, consultare "Ripristino dei backup per i tenant in modalità Conformità" (pag. 1).PrerequisitiDurante il ripristino in una macchina virtuale, questa deve essere arrestata. Per impostazione predefinita, il software interrompe la macchina senza preavviso. Una volta completato il ripristino, l'utente dovrà avviare la macchina manualmente. Questo comportamento può essere modificato utilizzando l'opzione di ripristino della Gestione dell'alimentazione delle VM (fare clic su Opzioni di ripristino > Gestione energetica MV).ProceduraEseguire una delle seguenti operazioni:Selezionare un sistema di cui è stato eseguito il backup e fare clic su Ripristino, quindi selezionare un punto di ripristino.Selezionare un punto di ripristino nella scheda Archivio di backup.Fare clic su Ripristina > Intera macchina.Se si desidera eseguire il ripristino in una macchina fisica, selezionare Macchina fisica in Ripristina in. Altrimenti, ignorare questo passaggio.Il ripristino in una macchina fisica è possibile solo se la configurazione del disco della macchina di destinazione corrisponde esattamente alla configurazione del disco nel backup.In questo caso, procedere al passaggio 4 in "Macchina fisica". In caso contrario, è preferibile eseguire la migrazione V2P con l'uso di supporti di avvio. [Facoltativo] Per impostazione predefinita, il software seleziona automaticamente il sistema originale come macchina di destinazione. Per eseguire il ripristino in un'altra macchina virtuale, fare clic su Macchina di destinazione ed eseguire le seguenti operazioni:Selezionare l'hypervisor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 o oVirt).Solo le macchine virtuali Virtuozzo possono essere ripristinate in Virtuozzo. Per ulteriori informazioni sulla migrazione V2V, fare riferimento a "Migrazione del sistema".Selezionare se eseguire il ripristino di un sistema nuovo o uno già esistente.Selezionare l'host e specificare il nome del nuovo sistema oppure selezionare una macchina di destinazione esistente.Fare clic su OK.Configurare le opzioni di ripristino aggiuntive necessarie.[Non disponibile per Virtuozzo Hybrid Infrastructure e Scale Computing HC3] Per selezionare il datastore per la virtual machine, fare clic su Datastore per ESXi o su Percorso per Hyper-V e Virtuozzo, oppure su Dominio di archiviazione per Red Hat Virtualization (oVirt), quindi selezionare il datastore (archivio) per la virtual machine.Fare clic su Mappatura disco per visualizzare il datastore (archivio), l'interfaccia e la modalità di provisioning per ogni disco virtuale. È possibile modificare queste impostazioni, a meno che non sia in corso il ripristino di un contenitore Virtuozzo o una macchina virtuale Virtuozzo Hybrid Infrastructure.In Virtuozzo Hybrid Infrastructure è possibile selezionare soltanto

© Acronis International GmbH, 2003-2024

la policy di archiviazione dei dischi di destinazione. A tal fine, selezionare il disco di destinazione desiderato e fare clic su Modifica. Nel pannello visualizzato, fare clic sull'icona ingranaggio, selezionare la policy di archiviazione, quindi fare clic su Fine.La sezione dedicata alla mappatura consente anche di scegliere singoli dischi per il ripristino.[Disponibile per VMware ESXi, Hyper-V e Virtuozzo] Per cambiare la dimensione della memoria, il numero di processori e le connessioni di rete della virtual machine fare clic su Impostazioni VM.[Per Virtuozzo Hybrid Infrastructure] Per cambiare la dimensione della memoria, il numero di processori della virtual machine, selezionare Versione.[Disponibile soltanto per i sistemi Windows nei quali è installato un agente di protezione] Abilitare l'opzione Ripristino sicuro per verificare che i dati ripristinati siano privi di malware. Per ulteriori informazioni sul funzionamento del ripristino sicuro, consultare "Ripristino sicuro" (pag. 1).Fare clic su Avvia ripristino.Quando si esegue il ripristino in una macchina virtuale esistente, confermare che si desidera sovrascrivere i dischi.L'avanzamento del ripristino viene mostrato nella scheda Attività." (pag. 1).

- Per le migrazioni da virtuale a fisico (V2P), consultare "Ripristino di una macchina virtualeÈ possibile ripristinare le macchine virtuali dai rispettivi backup.Non è possibile ripristinare i backup nella console di Cyber Protect per i tenant in modalità Conformità. Per ulteriori informazioni su come ripristinare questi backup, consultare "Ripristino dei backup per i tenant in modalità Conformità" (pag. 1).PrerequisitiDurante il ripristino in una macchina virtuale, questa deve essere arrestata. Per impostazione predefinita, il software interrompe la macchina senza preavviso. Una volta completato il ripristino, l'utente dovrà avviare la macchina manualmente. Questo comportamento può essere modificato utilizzando l'opzione di ripristino della Gestione dell'alimentazione delle VM (fare clic su Opzioni di ripristino > Gestione energetica MV).ProceduraEseguire una delle seguenti operazioni:Selezionare un sistema di cui è stato eseguito il backup e fare clic su Ripristino, quindi selezionare un punto di ripristino.Selezionare un punto di ripristino nella scheda Archivio di backup.Fare clic su Ripristina > Intera macchina.Se si desidera eseguire il ripristino in una macchina fisica, selezionare Macchina fisica in Ripristina in. Altrimenti, ignorare questo passaggio.Il ripristino in una macchina fisica è possibile solo se la configurazione del disco della macchina di destinazione corrisponde esattamente alla configurazione del disco nel backup.In questo caso, procedere al passaggio 4 in "Macchina fisica". In caso contrario, è preferibile eseguire la migrazione V2P con l'uso di supporti di avvio. [Facoltativo] Per impostazione predefinita, il software seleziona automaticamente il sistema originale come macchina di destinazione. Per eseguire il ripristino in un'altra macchina virtuale, fare clic su Macchina di destinazione ed eseguire le seguenti operazioni:Selezionare l'hypervisor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 o oVirt).Solo le macchine virtuali Virtuozzo possono essere ripristinate in Virtuozzo. Per ulteriori informazioni sulla migrazione V2V, fare riferimento a "Migrazione del sistema".Selezionare se eseguire il ripristino di un sistema nuovo o uno già esistente.Selezionare l'host e specificare il nome del nuovo sistema oppure selezionare una macchina di destinazione esistente.Fare clic su OK.Configurare le opzioni di ripristino aggiuntive necessarie.[Non disponibile per Virtuozzo Hybrid Infrastructure e Scale Computing HC3] Per selezionare il datastore per la virtual machine, fare clic su Datastore per ESXi o su Percorso per Hyper-V e Virtuozzo, oppure su Dominio di archiviazione per Red Hat Virtualization (oVirt), quindi selezionare il datastore (archivio) per la virtual machine.Fare clic su Mappatura disco per visualizzare il datastore (archivio), l'interfaccia e

© Acronis International GmbH, 2003-2024

la modalità di provisioning per ogni disco virtuale. È possibile modificare queste impostazioni, a meno che non sia in corso il ripristino di un contenitore Virtuozzo o una macchina virtuale Virtuozzo Hybrid Infrastructure.In Virtuozzo Hybrid Infrastructure è possibile selezionare soltanto la policy di archiviazione dei dischi di destinazione. A tal fine, selezionare il disco di destinazione desiderato e fare clic su Modifica. Nel pannello visualizzato, fare clic sull'icona ingranaggio, selezionare la policy di archiviazione, quindi fare clic su Fine.La sezione dedicata alla mappatura consente anche di scegliere singoli dischi per il ripristino.[Disponibile per VMware ESXi, Hyper-V e Virtuozzo] Per cambiare la dimensione della memoria, il numero di processori e le connessioni di rete della virtual machine fare clic su Impostazioni VM.[Per Virtuozzo Hybrid Infrastructure] Per cambiare la dimensione della memoria, il numero di processori della virtual machine, selezionare Versione.[Disponibile soltanto per i sistemi Windows nei quali è installato un agente di protezione] Abilitare l'opzione Ripristino sicuro per verificare che i dati ripristinati siano privi di malware. Per ulteriori informazioni sul funzionamento del ripristino sicuro, consultare "Ripristino sicuro" (pag. 1).Fare clic su Avvia ripristino.Quando si esegue il ripristino in una macchina virtuale esistente, confermare che si desidera sovrascrivere i dischi.L'avanzamento del ripristino viene mostrato nella scheda Attività." (pag. 1) e "Ripristino di dischi mediante i supporti di avvio" (pag. 514).

Migrazione tramite un supporto di avvio

In alternativa alla migrazione dei sistemi eseguita nella console di Cyber Protect, è possibile ripristinare un sistema utilizzando un supporto di avvio.

Si consiglia l'utilizzo di un supporto di avvio nei casi seguenti:

- Esecuzione di una migrazione non supportata in modalità nativa.
  Ad esempio, utilizzare un supporto di avvio per ripristinare un sistema fisico o una virtual machine non Virtuozzo come virtual machine Virtuozzo in un host Virtuozzo.
- Esecuzione della migrazione di un sistema Linux contenente volumi logici (LVM).
  Utilizzare Agente per Linux o il supporto di avvio per creare il backup, quindi utilizzare il supporto di avvio per il ripristino del backup.
- Fornitura di driver per hardware specifici di importanza critica per l'avviabilità del sistema.
  Creare un supporto di avvio che possa utilizzare i driver necessari. Per ulteriori informazioni, consultare "Generatore di supporti riavviabili" (pag. 726).

Backup di virtual machine Microsoft Azure e Amazon EC2

Per eseguire il backup di una virtual machine Microsoft Azure o Amazon EC2, installare un agente di protezione sul sistema. Le operazioni di backup e ripristino sono le stesse utilizzate per le macchine fisiche. Tuttavia la macchina verrà conteggiata come virtuale quando vengono impostate le quote per il numero di macchine.

La differenza con un sistema fisico è che le virtual machine Microsoft Azure e Amazon EC2 non possono essere inizializzate da un supporto di avvio. Se è necessario eseguire il ripristino su una nuova virtual machine Microsoft Azure o Amazon EC2, seguire la procedura descritta di seguito.

© Acronis International GmbH, 2003-2024

Nota
La procedura di ripristino seguente si applica solo ai backup di sistemi che contengono tutti i driver necessari per l'esecuzione nativa in Microsoft Azure (backup creati per una VM Azure, un sistema Hyper-V locale, o il sistema di origine Windows Server 2016 e versioni successive). Per eseguire un ripristino tra piattaforme, consultare questo articolo della Knowledge Base.

Per ripristinare un sistema come virtual machine Microsoft Azure o Amazon EC2

1. Creare una nuova virtual machine da un'immagine/modello in Microsoft Azure o Amazon EC2. La nuova macchina deve avere la stessa configurazione del disco della macchina da ripristinare.
2. Installare l'Agente per Windows o l'Agente per Linux sulla nuova macchina.
3. Ripristinare la macchina di cui è stato eseguito il backup come descritto in "Macchina fisica". Quando si configura il ripristino, selezionare il nuovo sistema come una macchina di destinazione.

Creazione di un supporto di avvio per recuperare i sistemi operativi

Il supporto di avvio è un supporto CD, DVD, unità flash USB o altro dispositivo rimovibile che consente di eseguire l'agente di protezione in un ambiente Linux o in un Ambiente di preinstallazione Windows/Ambiente ripristino Windows (WinPE/WinRE), senza l'intervento di un sistema operativo. Lo scopo principale del supporto di avvio è ripristinare un sistema operativo che non è in grado di avviarsi.

Nota
Il supporto di avvio non supporta le unità ibride.

Qual è la differenza tra un supporto di avvio personalizzato e uno pronto all'uso?

Utilizzando Generatore di supporti riavviabili, è possibile creare un supporto di avvio personalizzato (basato su Linux o su WinPE) per computer Windows, Linux o macOS. Nel supporto di avvio personalizzato Linux e in quello WinPE/WinRE, è possibile configurare impostazioni aggiuntive quali la registrazione automatica, le impostazioni di rete o le impostazioni del server proxy. Il supporto di avvio personalizzato WinPE/WinRE consente di aggiungere anche altri driver.

In alternativa, è possibile scaricare un supporto di avvio pronto all'uso (solo per Linux). Il supporto di avvio pronto all'uso potrà essere utilizzato solo per le operazioni di ripristino e per accedere alla funzionalità Universal Restore.

© Acronis International GmbH, 2003-2024

Qual è la differenza tra un supporto di avvio basato su Linux o uno basato su WinPE?

Basato su Linux

I supporti di avvio basati su Linux contengono un agente di protezione basato sul kernel Linux. L'agente è in grado di avviare ed eseguire operazioni su qualsiasi hardware compatibile con PC, compresi sistemi bare-metal e sistemi con file system corrotti o non supportati.

Basato su WinPE/WinRE

Il supporto di avvio basato su WinPE contiene un sistema Windows minimo chiamato Ambiente Preinstallazione di Windows (WinPE) e il plug-in Cyber Protection per WinPE, ovvero una versione modificata dell'agente di protezione in grado di avviarsi nell'ambiente di preinstallazione. Il supporto di avvio basato su WinRE utilizza l'Ambiente ripristino Windows e non richiede l'istallazione di pacchetti Windows aggiuntivi.

WinPE si è dimostrato la soluzione di avvio più pratica in ambienti estesi con componenti hardware eterogenei.

Vantaggi:

- L'utilizzo di Cyber Protection in Ambiente preinstallazione di Windows offre più funzionalità rispetto all'uso di supporti di avvio basati su Linux. Quando si esegue l'avvio in WinPE di componenti hardware PC compatibili è possibile utilizzare non solo l'agente di protezione, ma anche i comandi e gli script di PE e altri plug-in aggiunti a PE dall'utente.
- Il supporto di avvio basato su PE agevola la risoluzione dei problemi dei supporti di avvio correlati a Linux, ad esempio il supporto per alcuni controller RAID o limitato ad alcuni livelli di array RAID. I supporti basati su WinPE 2.x e versioni successive abilitano il caricamento dinamico dei driver dei dispositivi necessari.

Limitazioni:

- Un supporto basato su versioni di WinPE precedenti alla 4.0 non è in grado di eseguire l'avvio su macchine che utilizzano Unified Extensible Firmware Interface (UEFI).

Creazione di un supporto di avvio fisico

È fortemente consigliabile creare e testare il supporto di avvio non appena si inizia a utilizzare il backup del disco. Inoltre, una buona prassi consiste nel ricreare il supporto dopo ciascun aggiornamento importante dell'agente di protezione.

È possibile ripristinare Windows o Linux utilizzando lo stesso supporto. Per ripristinare macOS, creare un supporto separato su un sistema che esegue macOS.

Per creare un supporto di avvio fisico in Windows o Linux

© Acronis International GmbH, 2003-2024

1. Creare un file ISO del supporto di avvio personalizzato o scaricare il file ISO pronto l'uso.
   Per creare un file ISO personalizzato, utilizzare "Generatore di supporti riavviabili" (pag. 726).
   Per scaricare il file ISO pronto all'uso, nella console di Cyber Protect selezionare un sistema e quindi fare clic su **Ripristina** > **Altri metodi di ripristino** > **Scarica immagine ISO**.
2. [Facoltativo] Nella console di Cyber Protect, generare un token di registrazione. Il token di registrazione viene visualizzato automaticamente quando si scarica un file ISO pronto all'uso.
   Tale token consente al supporto di avvio di accedere al cloud storage senza richiedere l'immissione di login e password.
3. Creare un supporto di avvio fisico in uno dei modi indicati di seguito:
   - Masterizzare il file ISO utilizzando un CD/DVD.
   - Creare un'unità flash USB di avvio utilizzando il file ISO e uno degli strumenti gratuiti disponibili online.
     Utilizzare `ISO to USB` o `RUFUS` se è necessario avviare un sistema UEFI, `Win32DiskImager` per un sistema BIOS. In Linux è ragionevole utilizzare l'utilità `dd`.

   Per le virtual machine, connettere il file ISO come unità CD/DVD al sistema che si desidera ripristinare.

Per creare un supporto di avvio fisico in macOS

1. Su un sistema in cui è installato l'Agente per Mac, fare clic su **Applicazioni** > **Generatore di supporti di ripristino**.
2. Il software mostra il supporto rimovibile connesso. Selezionare il supporto che si desidera trasformare in supporto di avvio.

   Attenzione!
   Tutti i dati contenuti nel disco andranno perduti.

3. Fare clic su **Crea**.
4. Attendere che il software crei il supporto di avvio.

Generatore di supporti riavviabili

Il Generatore di supporti di avvio è uno strumento dedicato che consente la creazione di supporti di avvio. È installato come componente facoltativo nel sistema in cui è installato l'agente di protezione.

Perché utilizzare Generatore di supporti riavviabili?

Il supporto di avvio pronto all'uso che è possibile scaricare nella console di Cyber Protect è basato su un kernel Linux. A differenza di Windows PE, non consente l'inserimento rapido di driver personalizzati.

Generatore di supporti riavviabili consente di creare immagini dei supporti di avvio WinPE o Linux personalizzate.

© Acronis International GmbH, 2003-2024

32 o 64 bit?

Generatore di supporti riavviabili consente di creare supporti di avvio con componenti a 32 bit e a 64 bit. Nella maggior parte dei casi è necessario un supporto a 64 bit per avviare un sistema che utilizza UEFI (Unified Extensible Firmware Interface).

Supporto di avvio basato su Linux

Per creare un supporto di avvio basato su Linux

1. Avviare **Generatore di supporti riavviabili**.
2. In **Tipo di supporto di avvio**, selezionare **predefinito (supporto basato su Linux)**.
3. Selezionare la modalità di rappresentazione dei volumi e delle risorse di rete:
   - Un supporto di avvio con una rappresentazione dei volumi in stile Linux visualizza i volumi come, ad esempio, hda1 e sdb2. Il supporto tenta di ricostruire le periferiche MD e i volumi logici (LVM) prima di iniziare un ripristino.
   - Un supporto di avvio con una rappresentazione dei volumi in stile Windows visualizza i volumi come, ad esempio, C: e D:. Fornisce accesso ai volumi dinamici (LDM).
4. [Facoltativo] Specificare i parametri del kernel Linux. Diversi parametri multipli con spazi.
   Ad esempio, per poter selezionare una modalità di visualizzazione per l'agente di avvio ogni volta che viene avviato il supporto, digitare: **vga=ask**. Per ulteriori informazioni sui parametri disponibili, fare riferimento a "Parametri del kernel" (pag. 728).
5. [Facoltativo] Selezionare la lingua del supporto di avvio.
6. [Facoltativo] Selezionare la modalità di avvio (BIOS o UEFI) utilizzata da Windows dopo il ripristino.
7. Selezionare il componente da collocare nel supporto, ovvero l'agente di avvio Cyber Protection.
8. [Facoltativo] Specificare la durata del timeout per il menu di avvio. Se questa impostazione non viene configurata, il caricatore attende che l'utente selezioni se avviare il sistema operativo (se presente) o il componente.
9. [Facoltativo] Per automatizzare le operazioni dell'agente di avvio, selezionare la casella di controllo **Utilizza lo script seguente**. Quindi, selezionare uno degli script e specificarne i parametri. Per ulteriori informazioni sugli script, fare riferimento a "Script nel supporto di avvio" (pag. 730).
10. [Facoltativo] Selezionare il modo in cui registrare il supporto di avvio nel servizio Cyber Protection all'avvio. Per ulteriori informazioni sulle impostazioni di registrazione, fare riferimento a "Registrare il supporto di avvio" (pag. 739).
11. Specificare le impostazioni di rete delle schede di rete del sistema avviato oppure conservare la configurazione DHCP automatica.
12. [Facoltativo] Se è abilitato un server proxy nella rete, specificare il nome host o l'indirizzo IP e la porta.
13. Selezionare il tipo di file del supporto di avvio creato:

© Acronis International GmbH, 2003-2024

- Immagine ISO
- File ZIP

14. Specificare un nome file per il file del supporto di avvio.
15. Verificare le impostazioni nella schermata di riepilogo e fare clic su **Procedi**.

Parametri del kernel

È possibile specificare uno o più parametri del kernel Linux che verranno applicati automaticamente all'avvio del supporto di avvio. In genere, questi parametri vengono utilizzati in caso di problemi con l'utilizzo dei supporti di avvio. Di norma, questo campo andrebbe lasciato vuoto.

È inoltre possibile specificare ognuno di questi parametri premendo F11 dal menu di avvio.

Parametri

Se si specificano più parametri, bisogna separarli con lo spazio.

- **acpi=off**
  Disabilita ACPI (Advanced Configuration and Power Interface). Questo parametro può essere utilizzato quando si verificano problemi con una particolare configurazione hardware.
- **noapic**
  Disabilita APIC (Advanced Programmable Interrupt Controller). Questo parametro può essere utilizzato quando si verificano problemi con una particolare configurazione hardware.
- **vga=ask**
  Richiede la modalità video da utilizzare tramite l'interfaccia grafica del supporto di avvio. Senza il parametro **vga**, la modalità video è rilevata automaticamente.
- **vga=** *mode_number*
  Specifica la modalità video da utilizzare tramite l'interfaccia grafica del supporto di avvio. Il numero della modalità è espresso dal valore *mode_number* nel formato esadecimale, ad esempio: **vga=0x318**
  La risoluzione dello schermo e il numero di colori che corrispondono a un numero di modalità possono variare a seconda del sistema. Si consiglia di utilizzare per primo il parametro **vga=ask** per assegnare un valore a *mode_number*.
- **quiet**
  Disabilita la visualizzazione dei messaggi di avvio durante il caricamento del kernel di Linux, ed esegue la console di gestione dopo il caricamento del kernel.
  Questo parametro è specificato in modo implicito quando si crea il supporto di avvio, ma può essere eliminato dal menu di avvio.
  Senza questo parametro, verranno visualizzati tutti i messaggi della fase di avvio del sistema, seguiti da un prompt dei comandi. Per avviare la console di gestione dal prompt dei comandi, eseguire l'istruzione: **/bin/product**
- **nousb**
  Disabilita il caricamento del sottosistema USB (Universal Serial Bus).

© Acronis International GmbH, 2003-2024

- **nousb2**

  Disabilita il supporto USB 2.0. I dispositivi USB 1.1 funzionano ancora con questo parametro. Questo parametro permette di utilizzare alcune unità USB in modalità USB 1.1 nel caso in cui non dovessero funzionare in modalità USB 2.0.
- **nodma**

  Disabilita l'accesso diretto alla memoria (DMA) per tutti i dischi rigidi IDE. Impedisce al kernel di bloccarsi con alcuni dispositivi hardware.
- **nofw**

  Disabilita il supporto dell'interfaccia FireWire (IEEE1394).
- **nopcmcia**

  Disabilita il rilevamento dell'hardware PCMCIA.
- **nomouse**

  Disabilita il supporto per il mouse.
- *module_name* **=off**

  Disabilita il modulo il cui nome è specificato da *module_name*. Ad esempio, per disabilitare l'uso del modulo SATA, specificare: **sata_sis=off**
- **pci=bios**

  Forza l'utilizzo del PCI BIOS invece di accedere direttamente alle periferiche hardware. Questo parametro può essere utilizzato se il computer ha un bridge host PCI non standard.
- **pci=nobios**

  Disabilita l'utilizzo del PCI BIOS; sono consentiti solo i metodi per l'accesso diretto all'hardware. Questo parametro può essere utilizzato quando il supporto di avvio non parte, situazione che potrebbe essere provocata dal BIOS.
- **pci=biosirq**

  Utilizza chiamate PCI BIOS per richiamare la tabella di routing di interrupt. Questo parametro può essere utilizzato se il kernel non è in grado di allocare richieste di interrupt (IRQ) o se si rilevano bus PCI secondari sulla scheda madre.

  Queste chiamate potrebbero non funzionare correttamente su alcune macchine. Tuttavia, potrebbe essere il solo modo per ottenere la tabella di routing di interrupt.
- **LAYOUTS=en-US, de-DE, fr-FR, ...**

  Specifica i layout tastiera da utilizzare tramite l'interfaccia utente grafica del supporto di avvio.

  Se il parametro non è specificato, è possibile utilizzare solo due layout: Inglese (USA) e il layout che corrisponde alla lingua selezionata nel menu di avvio del supporto.

  È possibile specificare uno dei seguenti layout:

  Belga: **be-BE**

  Ceco: **cz-CZ**

  Inglese: **en-GB**

  Inglese (USA): **en-US**

  Francese: **fr-FR**

  Francese (Svizzera): **fr-CH**

© Acronis International GmbH, 2003-2024

Tedesco: **de-DE**
Tedesco (Svizzera): **de-CH**
Italiano: **it-IT**
Polacco: **pl-PL**
Portoghese: **pt-PT**
Portoghese (Brasiliano): **pt-BR**
Russo: **ru-RU**
Serbo (Cirillico): **sr-CR**
Serbo (Latino): **sr-LT**
Spagnolo: **es-ES**
Quando si lavora con un supporto di avvio, usare CTRL + MAIUSC per scorrere i layout disponibili.

Script nel supporto di avvio

Affinché il supporto di avvio esegua un insieme di operazioni predefinito, è possibile specificare uno script durante la creazione del supporto in Generatore di supporti riavviabili. Pertanto, ogni volta che il sistema viene avviato dal supporto, verrà eseguito lo script specificato e l'interfaccia utente non verrà mostrata.

È possibile selezionare uno degli script predefiniti o crearne uno personalizzato, seguendo le convenzioni sulla creazione di script.

Script predefiniti

Generatore di supporti riavviabili offre gli script predefiniti seguenti:

- Ripristino da cloud storage (**cloud_intero_pc**)
- Ripristino da una condivisione di rete (**condivisione_intero_pc**)

Gli script sono posizionati nelle seguenti cartelle nel sistema in cui è installato Generatore di supporti riavviabili:

- In Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- In Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Ripristino dall'archiviazione cloud

In Generatore di supporti riavviabili, specificare i parametri seguenti per lo script:

1. Il nome del file di backup.
2. [Facoltativo] Una password utilizzata dallo script per accedere ai backup crittografati.

Ripristino da una condivisione di rete

In Generatore di supporti riavviabili, specificare i parametri seguenti per lo script:

© Acronis International GmbH, 2003-2024

- Il percorso della condivisione di rete.
- Il nome utente e la password per la condivisione di rete.
- Il nome del file di backup. Per individuare il nome del file di backup
  a. Nella console di Cyber Protect, passare a **Archivio di backup** > **Posizioni**.
  b. Selezionare la condivisione di rete (fare clic su **Aggiungi posizione** se la condivisione non è in elenco).
  c. Selezionare il backup.
  d. Fare clic su **Dettagli**. Il nome del file viene visualizzato in **Nome file di backup**.
- [Facoltativo] Una password utilizzata dallo script per accedere ai backup crittografati.

Script personalizzati

Importante
Per creare gli script personalizzati è necessario avere familiarità con il linguaggio dei comandi Bash e JavaScript Object Notation (JSON). Se non si conosce Bash, un buon posto per impararlo è http://www.tldp.org/LDP/abs/html. La specifica JSON è disponibile all'indirizzo http://www.json.org

File di uno script

Lo script deve essere posizionato nelle seguenti directory nella macchina in cui è installato il Generatore di supporti riavviabili:

- In Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- In Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Lo script deve consistere di almeno tre file:

- **<script_file>.sh** - un file con lo script Bash. Quando si crea lo script, usare solo un set limitato di comandi shell, reperibili all'indirizzo https://busybox.net/downloads/BusyBox.html. È possibile utilizzare i seguenti comandi:
  - `acrocmd` - l'utility della riga di comando per il backup e il ripristino
  - `product` - il comando che avvia l'interfaccia del Generatore di supporti avviabili

  Questo file e qualsiasi file aggiuntivo incluso nello script (ad esempio, utilizzando il comando dot) devono essere posizionati nella sottocartella **bin**. Nello script, specificare i percorsi dei file aggiuntivi come **/ConfigurationFiles/bin/<some_file>**.
- **autostart** - un file per l'avvio di **<script_file>.sh**. I contenuti del file devono essere come segue:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - un file JSON contenente quanto segue:

© Acronis International GmbH, 2003-2024

- Il nome e la descrizione dello script da visualizzare nel Generatore di supporti riavviabili.
- I nomi delle variabili di script da configurare tramite il Generatore di supporti riavviabili.
- I parametri di controllo che saranno visualizzati nel Generatore di supporti riavviabili per ciascuna variabile.

Struttura di autostart.json

Oggetto di livello superiore

Coppia		Obbligatorio	Descrizione
Nome	**Tipo di valore**		
`displayName`	string	Sì	Nome dello script da visualizzare nel Generatore di supporti riavviabili.
`description`	string	No	Descrizione dello script da visualizzare nel Generatore di supporti riavviabili.
`timeout`	number	No	Tempo scaduto (in secondi) per il menu di avvio prima di far partire lo script. Se la coppia non è specificata, il tempo scaduto sarà di 10 secondi.
`variables`	oggetto	No	Qualsiasi variabile per **<script_file>.sh** che si desidera configurare tramite il Generatore di supporti riavviabili. Il valore deve essere un set delle coppie seguenti: l'identificante della stringa di una variabile e l'oggetto di una variabile (vedere la tabella sottostante).

Oggetto variabile

Coppia		Obbligatorio	Descrizione
Nome	**Tipo di valore**		
`displayName`	string	Sì	Il nome della variabile usato in **<script_file>.sh**.
`type`	string	Sì	Il tipo di controllo visualizzato nel Generatore di supporti riavviabili. Questo controllo è utilizzato per configurare il valore della variabile. Per tutti i tipi supportati, vedere la tabella sottostante.

© Acronis International GmbH, 2003-2024

`description`	string	Sì	L'etichetta di controllo è visualizzata sopra il controllo nel Generatore di supporti riavviabili.
`default`	stringa se il `type` è `string`, `multiString`, `password` o `enum` numero se il `type` è `number`, `spinner` o `checkbox`	No	Il valore predefinito per il controllo. Se la coppia non è specificata, il valore predefinito sarà una strina vuota o uno zero, in base al tipo di controllo. Il valore predefinito per una casella di controllo può essere `0` (lo stato cancellato) o `1` (lo stato selezionato).
`order`	number (non negativo)	Sì	L'ordine di controllo nel Generatore di supporti riavviabili. Maggiore è il valore, minore è il controllo relativo ad altri controlli definiti in **autostart.json**. Il valore iniziale deve essere `{0}`.
`min` (solo per `spinner`)	number	No	Il valore minimo del controllo in una casella di selezione. Se la coppia non è specificata, il valore sarà `0`.
`max` (solo per `spinner`)	number	No	Il valore massimo del controllo in una casella di selezione. Se la coppia non è specificata, il valore sarà `100`.
`step` (solo per `spinner`)	number	No	Il valore di passaggio del controllo in una casella di selezione. Se la coppia non è specificata, il valore sarà `1`.
`items` (solo per `enum`)	array di stringhe	Sì	I valori di un elenco a discesa.
`required` (per `string`, `multiString`, `password` ed `enum`)	number	No	Specifica se il valore del controllo può essere vuoto (`0`) o no (`1`). Se la coppia non è specificata, il valore di controllo può essere vuoto.

Tipo di Controllo

Nome	Descrizione
`string`	Una casella di testo senza vincoli di una sola riga usata per inserire o modificare stringhe corte.

© Acronis International GmbH, 2003-2024

`multiString`	Una casella di testo senza vincoli di una sola riga usata per inserire o modificare stringhe lunghe.
`password`	Una casella di testo senza vincoli di una sola riga usata per inserire password in modo sicuro.
`number`	Una casella di testo solo numerica di una sola riga usata per inserire o modificare numeri.
`spinner`	Una casella di testo solo numerica di una sola riga usata per inserire o modificare numeri, con una casella di controllo. Chiamata anche casella di controllo.
`enum`	Un elenco a discesa standard con un set fisso di valori predeterminati.
`checkbox`	Una casella di controllo con due stati - stato cancellato o stato selezionato.

Il campione sottostante **autostart.json** contiene tutti i tipi possibili di controllo che possono essere usati per configurare variabili per **<script_file>.sh**.

```
{
        "displayName": "Autostart script name",
        "description": "This is an autostart script description.",
        "variables": {
                "var_string": {
                        "displayName": "VAR_STRING",
                        "type": "string", "order": 1,
                        "description": "This is a 'string' control:", "default": "Hello,
world!"
                },
                "var_multistring": {
                        "displayName": "VAR_MULTISTRING",
                        "type": "multiString", "order": 2,
                        "description": "This is a 'multiString' control:",
                        "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
                },
                "var_number": {
                        "displayName": "VAR_NUMBER",
                        "type": "number", "order": 3,
```


© Acronis International GmbH, 2003-2024

```
                "description": "This is a 'number' control:", "default": 10
            },
            "var_spinner": {
                "displayName": "VAR_SPINNER",
                "type": "spinner", "order": 4,
                "description": "This is a 'spinner' control:",
                "min": 1, "max": 10, "step": 1, "default": 5
            },
            "var_enum": {
                "displayName": "VAR_ENUM",
                "type": "enum", "order": 5,
                "description": "This is an 'enum' control:",
                "items": ["first", "second", "third"], "default": "second"
            },
            "var_password": {
                "displayName": "VAR_PASSWORD",
                "type": "password", "order": 6,
                "description": "This is a 'password' control:", "default": "qwe"
            },
            "var_checkbox": {
                "displayName": "VAR_CHECKBOX",
                "type": "checkbox", "order": 7,
                "description": "This is a 'checkbox' control", "default": 1
            }
        }
}
```

Supporto di avvio basato su WinPE e WinRE

È possibile creare immagini WinRE senza alcuna preparazione aggiuntiva, oppure creare immagini WinPE dopo aver installato Windows Automated Installation Kit (AIK) oppure Windows Assessment and Deployment Kit (ADK).

© Acronis International GmbH, 2003-2024

Immagini WinRE

La creazione di immagini WinRE è supportata per i seguenti sistemi operativi:

- Windows 7 (64 bit)
- Windows 8 (32 bit e 64 bit)
- Windows 8.1 (32 bit e 64 bit)
- Windows 10 (32 bit e 64 bit)
- Windows 11 (64 bit)
- Windows Server 2012 (64 bit)
- Windows Server 2016 (64 bit)
- Windows Server 2019 (64 bit)
- Windows Server 2022 (64 bit)

Immagini WinPE

Dopo l'installazione di Windows Automated Installation Kit (AIK) o di Windows Assessment and Deployment Kit (ADK), Generatore di supporti riavviabili supporta le distribuzioni di WinPE basate sui seguenti kernel:

- Windows Vista (PE 2.0)
- Windows Vista SP1 e Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) con o senza supplemento per Windows 7 SP1 (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

Il Generatore di supporti riavviabili supporta sia le distribuzioni di WinPE a 32 bit che a 64 bit. Le distribuzioni di WinPE a 32 bit possono funzionare anche su hardware a 64 bit. Tuttavia, è necessaria una distribuzione a 64 bit per eseguire l'avvio di una macchina che utilizza Unified Extensible Firmware Interface (UEFI).

Nota
Il funzionamento delle immagini di PE basate su WinPE 4 e versione successiva richiede circa 1 GB di RAM.

Creazione di un supporto di avvio WinPE o WinRE

Generatore di supporti riavviabili fornisce due metodi per l'integrazione di Cyber Protection con WinPE e WinRE:

© Acronis International GmbH, 2003-2024

- Creazione di un file ISO da zero, con il plug-in Cyber Protection.
- Aggiunta del plug-in Cyber Protection a un file WIM per qualsiasi utilizzo futuro (creazione manuale di ISO, aggiunta di altri strumenti all'immagine e così via).

Per creare un supporto di avvio WinPE o WinRE

1. Eseguire Generatore di supporti riavviabili nel sistema in cui è installato l'agente di protezione.
2. In **Tipo di supporto di avvio**, selezionare **Windows PE** o **Windows PE (64 bit)**. Un supporto a 64 bit è necessario per eseguire l'avvio su macchine che utilizzano UEFI (Unified Extensible Firmware Interface).
3. Specificare il sottotipo di supporto di avvio: **WinRE** oppure **WinPE**.
   La creazione di supporti di avvio WinRE non richiede l'installazione di alcun pacchetto aggiuntivo.
   Per creare un supporto WinPE a 64 bit, è necessario scaricare Windows Automated Installation Kit (AIK) oppure Windows Assessment and Deployment Kit (ADK). Per creare un supporto WinPE a 32 bit, oltra a scaricare i kit AIK o ADK, è necessario attenersi alla seguente procedura:
   a. Fare clic su **Scarica il plug-in per WinPE (32 bit)**.
   b. Salvare il plug-in in **%PROGRAM_FILES%\BackupClient\BootableComponents\WinPE32**.
4. [Facoltativo] Selezionare la lingua del supporto di avvio.
5. [Facoltativo] Selezionare la modalità di avvio (BIOS o UEFI) utilizzata da Windows dopo il ripristino.
6. Specificare le impostazioni di rete delle schede di rete del sistema avviato oppure conservare la configurazione DHCP automatica.
7. [Facoltativo] Selezionare il modo in cui registrare il supporto di avvio nel servizio Cyber Protection all'avvio. Per ulteriori informazioni sulle impostazioni di registrazione, fare riferimento a "Registrare il supporto di avvio" (pag. 739).
8. Specificare i driver di Windows da aggiungere al supporto di avvio.
   Quando si avvia un sistema in Windows PE o in Windows RE, i driver possono aiutare ad accedere al dispositivo in cui è posizionato il backup. Aggiungere driver a 32 bit se si utilizza una distribuzione a 32 bit di WinPE o WinRE o driver a 64 bit se si utilizza una distribuzione a 64 bit di WinPE o WinRE.
   Per aggiungere i driver:
   - Fare clic su **Aggiungi** e specificare il percorso del file .inf necessario per i controller SCSI, RAID, SATA, la scheda di rete, l'unità a nastro o altro dispositivo corrispondente.
   - Ripetere questa procedura per ogni driver da includere nel supporto WinPE o WinRE risultante.
9. Selezionare il tipo di file del supporto di avvio creato:
   - Immagine ISO
   - Immagine WIM
10. Specificare il percorso completo del file di immagine risultante, incluso il nome del file.
11. Verificare le impostazioni nella schermata di riepilogo e fare clic su **Procedi**.

Per creare un'immagine PE (file ISO) dal file WIM risultante

© Acronis International GmbH, 2003-2024

- Sostituire il file boot.wim predefinito che si trova nella cartella Windows PE con il nuovo file WIM appena creato. Per l'esempio precedente, digitare:

```
copy c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Usare lo strumento **Oscdimg**. Per l'esempio precedente, digitare:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

Attenzione!
Non copiare e incollare questo esempio. Digitare il comando manualmente. In caso contrario l'operazione avrà esito negativo.

Preparazione: WinPE 2.x e 3.x

Per creare o modificare le immagini di PE 2.x o 3.x, installare Bootable Media Builder e Windows Automated Installation Kit (AIK) nello stesso sistema.

Per preparare un sistema

1. Scaricare il file di immagine AIK dal sito web di Microsoft, come segue:
   - Per Windows Vista (PE 2.0): https://www.microsoft.com/it-it/download/details.aspx?id=10333
   - Per Windows Vista SP1 e Windows Server 2008 (PE 2.1): https://www.microsoft.com/it-it/download/details.aspx?id=9085
   - Per Windows 7 (PE 3.0): https://www.microsoft.com/it-it/download/details.aspx?id=5753
     Per Windows 7 SP1 (PE 3.1) è necessario anche il supplemento AIK disponibile su https://www.microsoft.com/it-it/download/details.aspx?id=5188
2. Masterizzare il file di immagine su un disco DVD o su una chiavetta USB.
3. Dal file di immagine, installare quanto segue:
   - Microsoft .NET Framework (NETFXx86 o NETFXx64, a seconda dell'hardware)
   - MSXML (Microsoft XML parser)
   - Windows AIK
4. Installare il Generatore di supporti di avvio nello stesso computer.

Preparazione: WinPE 4.0 e versioni successive

Per poter creare o modificare immagini PE 4 o successive, installare Bootable Media Builder e Windows Assessment and Deployment Kit (ADK) sullo stesso sistema.

Per preparare un sistema

1. Scaricare il programma di installazione ADK dal sito web Microsoft.
   Sono supportate le seguenti versioni di Windows:
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)

© Acronis International GmbH, 2003-2024

- Windows 8,1 (PE 5,0)
- Windows 8 (PE 4.0)

2. Installare Windows Assessment and Deployment Kit.
3. Installare Bootable Media Builder.

Registrare il supporto di avvio

Per accedere ai backup nel cloud storage, è necessario registrare il supporto di avvio nel servizio Cyber Protection. È possibile preconfigurare la registrazione durante la creazione del supporto di avvio. Se la registrazione non è preconfigurata, è possibile registrare il supporto dopo averlo utilizzato per avviare un sistema.

Per preconfigurare la registrazione nel servizio Cyber Protection

1. In Generatore di supporti riavviabili passare a **Registrazione del supporto di avvio**.
2. In **URL del servizio**, specificare l'indirizzo del servizio Cyber Protection.
3. [Facoltativo] In **Nome visualizzato**, specificare un nome per il sistema avviato.
4. Per impostare la registrazione automatica nel servizio Cyber Protection, selezionare la casella di controllo **Registra automaticamente il supporto di avvio**, quindi selezionare il livello di registrazione automatica:
   - **Chiedi il token di registrazione all'avvio**
     Sarà necessario immettere il token ogni volta che il sistema viene avviato dal supporto di avvio.
   - **Usa il token seguente**
     Il sistema verrà registrato automaticamente ogni volta che viene avviato da questo supporto di avvio.

Per registrare il supporto di avvio dopo averlo utilizzato per l'avvio di un sistema

1. Avviare la macchina dal supporto di avvio.
2. Nella finestra di avvio, fare clic su **Registra supporto**.
3. In **Server**, specificare l'indirizzo del servizio Cyber Protection.
4. Inserire il token di registrazione nel campo **Token di registrazione**.
5. Fare clic su **Registra**.

Impostazioni di rete

Durante la creazione del supporto di avvio, è possibile preconfigurare le connessioni di rete che verranno utilizzate dall'agente di avvio. È possibile preconfigurare i parametri seguenti:

- Indirizzo IP
- Subnet mask
- Gateway

© Acronis International GmbH, 2003-2024

- Server DNS
- Server WINS

Dopo l'avvio dell'agente di avvio su un sistema, la configurazione viene applicata alla scheda di interfaccia di rete (NIC) del sistema stesso. Se le impostazioni non sono state preconfigurate, l'agente utilizza la configurazione automatica DHCP.

È inoltre possibile configurare manualmente le impostazioni di rete quando l'agente di avvio è in esecuzione del sistema.

Preconfigurazione di più connessioni di rete

È possibile preconfigurare le impostazioni TCP/IP di un massimo di dieci schede di interfaccia di rete. Per garantire che a ogni NIC vengano assegnate le impostazioni appropriate, creare il supporto sul server per il quale il supporto stesso è personalizzato. Quando si seleziona una NIC esistente nella finestra della procedura guidata, le relative impostazioni vengono selezionate e salvate sul supporto. Viene salvato sul supporto anche l'indirizzo MAC di ogni NIC esistente.

È possibile modificare queste impostazioni, ad eccezione dell'indirizzo MAC, oppure configurare le impostazioni di una NIC inesistente.

Quando l'agente di avvio si avvia sul server, recupera l'elenco delle NIC disponibili, che è ordinato in base agli slot occupati dalle NIC; quelle più vicine al processore compaiono per prime.

L'agente avviabile assegna a ogni NIC nota le impostazioni appropriate, identificando le schede in base al loro indirizzo MAC. Dopo la configurazione delle NIC con indirizzo MAC noto, alle NIC restanti vengono assegnate le impostazioni definite dall'utente per le NIC non esistenti, iniziando dalla NIC non assegnata che figura per prima nell'elenco.

È possibile personalizzare il supporto di avvio di qualsiasi sistema, non solo per quello su cui viene creato il supporto. A tal fine, configurare le NIC in base all'ordine dello slot occupato su tale macchina: NIC1 occupa lo slot più vicino al processore, NIC2 lo slot successivo e così via. Quando l'agente di avvio si avvia sul sistema in questione, non troverà alcuna NIC con indirizzo MAC noto e configurerà le NIC nello stesso ordine utilizzato dall'utente.

Esempio

L'agente avviabile può utilizzare una delle schede di rete per la comunicazione con la console di gestione nella rete produttiva. Per tale connessione può essere utilizzata la configurazione automatica. I dati di ripristino dimensionabili possono essere trasferiti attraverso la seconda NIC, inclusa nella rete di backup dedicata con le impostazioni TCP/IP statiche.

Connessione a un sistema avviato da un supporto di avvio

Connessione locale

Per operare direttamente sulla macchina avviata dal supporto di avvio, fare clic su **Gestisci questa macchina localmente** nella finestra di avvio.

© Acronis International GmbH, 2003-2024

Dopo aver avviato un sistema da un supporto di avvio, il terminale del sistema visualizza una finestra di avvio con gli indirizzi IP ricevuti dal DHCP o impostati in base ai valori preconfigurati.

Configurazione delle impostazioni di rete

Per modificare le impostazioni di rete per una sessione corrente, fare clic su **Configura rete** nella finestra di avvio. La finestra **Impostazioni di rete** visualizzata consentirà di configurare le impostazioni di rete di ogni scheda di rete (NIC) del sistema.

Le modifiche effettuate durante una sessione andranno perdute dopo il riavvio del sistema.

Aggiunta di VLAN

Nella finestra **Impostazioni di rete**, è possibile aggiungere reti locali virtuali (VLAN). Utilizzare questa funzionalità per accedere a una posizione di backup inclusa in una VLAN specifica.

Le VLAN sono utilizzate principalmente per dividere una rete locale in segmenti. Una NIC (scheda di interfaccia di rete) connessa a una porta di *accesso* dello switch ha sempre accesso alla VLAN specificata nella configurazione della porta. Una NIC connessa a una porta *trunk* dello switch può accedere alle VLAN consentite nella configurazione della porta solo se si specificano le VLAN nelle impostazioni di rete.

Per abilitare l'accesso a una VLAN tramite una porta trunk

1. Fare clic su **Aggiungi VLAN**.
2. Selezionare le NIC che forniscono accesso alla rete locale che include la VLAN richiesta.
3. Specificare l'identificatore della VLAN.

Dopo aver fatto clic su **OK**, nell'elenco delle schede di rete verrà visualizzata una nuova voce.

Per rimuovere una VLAN, fare clic sulla voce della VLAN richiesta e selezionare **Rimuovi VLAN**.

Operazioni locali con un supporto di avvio

Le operazioni che è possibile eseguire con il supporto di avvio sono simili a quelle di ripristino che vengono eseguite con un sistema operativo in esecuzione. Sussistono tuttavia le differenze indicate di seguito:

1. In un supporto di avvio in cui il volume è rappresentato in stile Windows, il volume ha la stessa lettera di unità visualizzata in Windows. Ai volumi che non hanno lettere di unità in Windows (come il volume Riservato per il sistema) vengono assegnate lettere disponibili nell'ordine della loro sequenza sul disco.

   Se il supporto di avvio non è in grado di rilevare il sistema operativo Windows o ne rileva più di uno, a tutti i volumi, inclusi quelli senza lettere di unità, vengono assegnate le lettere disponibili nell'ordine della loro sequenza sul disco. Per questa ragione le lettere dei volumi possono essere diverse da quelle visualizzate in Windows. Ad esempio, l'unità D: del supporto di avvio potrebbe corrispondere all'unità E: in Windows.

© Acronis International GmbH, 2003-2024

Nota
È consigliabile assegnare ai volumi nomi univoci.

2. In un supporto di avvio in cui il volume è rappresentato in stile Linux, i dischi e i volumi locali vengono visualizzati come se fossero smontati (sda1, sda2...).
3. Non è possibile pianificare le attività. Se occorre ripetere un'operazione, è necessario configurarla dall'inizio.
4. La durata del registro è limitata alla sessione corrente. È possibile salvare l'intero registro o le voci di registro filtrate in un file.

Impostazione di una modalità di visualizzazione

Quando si avvia un sistema da un supporto di avvio Linus, viene rilevata automaticamente una modalità video in base alla configurazione hardware (specifiche del monitor e della scheda grafica). Se la modalità video viene rilevata in maniera non corretta, effettuare le seguenti operazioni:

1. Nel menu di avvio, premere F11.
2. Nella riga di comando inserire **vga=ask** e quindi proseguire con l'avvio.
3. Dall'elenco delle modalità video supportate, scegliere quella appropriata immettendo il relativo numero (per esempio **318**), quindi premere **Invio**.

Per non effettuare questa procedura ogni volta che viene eseguito l'avvio di una determinata configurazione hardware, creare nuovamente il supporto di avvio con il numero di modalità appropriato (nel precedente esempio **vga=0x318**) specificato nel campo **Parametri del kernel**.

Ripristino con supporto di avvio in locale

1. Avviare il sistema dal supporto di avvio.
2. Fare clic su **Gestisci questa macchina localmente**.
3. Fare clic su **Ripristina**.
4. In **Cosa ripristinare**, fare clic su **Selezionare i dati**.
5. Selezionare il file di backup dal quale eseguire il ripristino.
6. Nel pannello in basso a sinistra, selezionare le unità/i volumi o i file/le cartelle da ripristinare, quindi fare clic su **OK**.
7. Configurare le regole di sovrascrittura.
8. Configurare le esclusioni dal ripristino.
9. Configurare le opzioni di ripristino.
10. Verificare la correttezza delle impostazioni, quindi fare clic su **OK**.

© Acronis International GmbH, 2003-2024

Operazioni remoto con un supporto di avvio

Nota
Questa funzionalità è disponibile con il pacchetto Advanced Backup.

Per visualizzare il supporto di avvio nella console di Cyber Protect, è innazitutto necessario eseguire la registrazione come descritto in "Registrare il supporto di avvio" (pag. 739).

Una volta completata la registrazione del supporto nella console di Cyber Protect, questo verrà visualizzato nella scheda **Dispositivi** > **Supporto di avvio**. Un supporto di avvio viene eliminato dalla scheda se è stato offline per più di 30 giorni.

È possibile gestire il supporto di avvio nella console di Cyber Protect. Ad esempio, è possibile ripristinare i dati, riavviare o arrestare il sistema avviato con il support, oppure visualizzare informazioni, attività e avvisi relativi al supporto.

Importante
Non è possibile aggiornare il supporto di avvio da remoto, nella scheda **Impostazioni** > **Agenti** nella console di Cyber Protect.

Per aggiornare il supporto di avvio, crearne uno nuovo come descritto nella sezione "Generatore di supporti riavviabili" (pag. 726). In alternativa, scaricare il supporto pronto all'uso facendo clic sull'icona dell'account, quindi su > **Download** > **Supporto di avvio** nella console di Cyber Protect.

Per ripristinare file o cartelle con un supporto di avvio da remoto

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Supporto di avvio**.
1. Selezionare il supporto da utilizzare per il recupero dei dati.
2. Fare clic su **Ripristino**.
3. Selezionare la posizione e quindi il backup desiderato. Tenere presente che i backup vengono filtrati in base alla posizione.
4. Selezionare il punto di ripristino e fare clic su **Ripristina file/cartelle**.
5. Esplorare la cartella richiesta o utilizzare la barra di ricerca per ottenere l'elenco dei file e delle cartelle necessari.

   La ricerca è indipendente dalla lingua.

   È possibile utilizzare uno o più caratteri jolly (* e ?). Per ulteriori dettagli sull'utilizzo dei caratteri jolly, fare riferimento a "Filtri file (Inclusioni/Esclusioni)" (pag. 468).
6. Selezionare i file da ripristinare, quindi fare clic su **Ripristina**.
7. In **Percorso**, selezionare la destinazione del ripristino.
8. [Facoltativo] Per una configurazione di ripristino avanzata, fare clic su **Opzioni di ripristino**. Per ulteriori informazioni, fare riferimento a "Opzioni di ripristino" (pag. 528).
9. Fare clic su **Avvia ripristino**.

© Acronis International GmbH, 2003-2024

10. Selezionare una delle opzioni di sovrascrittura dei file:
    - **Sovrascrivi i file esistenti**
    - **Sovrascrivi il file esistente se meno recente**
    - **Non sovrascrivere i file esistenti**

    Scegliere se riavviare il sistema automaticamente.
11. Fare clic su **Procedi** per avviare il ripristino. L'avanzamento del ripristino viene mostrato nella scheda **Attività**.

Per ripristinare dischi, volumi o interi sistemi con un supporto di avvio da remoto

1. Nella scheda **Dispositivi**, passare al gruppo **Supporto di avvio**, quindi selezionare il supporto da utilizzare per il recupero dei dati.
2. Fare clic su **Ripristino**.
3. Selezionare la posizione e quindi il backup desiderato. Tenere presente che i backup vengono filtrati in base alla posizione.
4. Selezionare il punto di ripristino e fare clic su **Ripristina** > **Intera macchina**.

   Se necessario, configurare il sistema di destinazione e il mapping del volume come descritto in "Ripristino di sistemi fisiciIn questa sezione viene descritto il ripristino delle macchine fisiche mediante l'utilizzo dell'interfaccia Web.Utilizzare supporti di avvio anziché l'interfaccia Web se occorre ripristinare:Un sistema che esegue macOSUn sistema di un tenant in modalità ConformitàDa qualsiasi sistema operativo a bare metal o a un sistema offlineLa struttura dei volumi logici (volumi creati da Logical Volume Manager su Linux). Il supporto consente di ricreare la struttura del volume logico in modo automatico.Non è possibile ripristinare i backup del disco di sistemi Mac con processori Intel su Mac con processori Apple Silicon, e viceversa. È possibile ripristinare file e cartelle.Ripristino con riavvioIl ripristino di un sistema operativo e di volumi crittografati con BitLocker richiede un riavvio. È possibile scegliere se riavviare il sistema automaticamente o assegnare lo stato Richiesta interazione. Il sistema operativo ripristinato va online automaticamente.I backup dei volumi crittografati vengono ripristinati come non crittografati.Per il ripristino di volumi crittografati con BitLocker non deve essere presente un volume non crittografato nello stesso sistema; tale volume deve disporre di almeno un 1 GB di spazio disponibile. Se una delle condizioni non viene soddisfatta, il ripristino avrà esito negativo.Per il ripristino di un volume di sistema crittografato non è richiesta alcuna azione aggiuntiva. Per ripristinare un volume crittografato non di sistema, è necessario per prima cosa bloccarlo, ad esempio aprendo un file che risiede su tale volume. In caso contrario, il ripristino continuerà senza riavvio e il volume ripristinato potrebbe non essere riconosciuto da Windows.Se il ripristino non riesce e il riavvio del sistema genera l'errore Impossibile acquisire il file dalla partizione, provare a disabilitare l'avvio protetto. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a Disabilitare l'avvio protetto nella documentazione Microsoft.Per ripristinare una macchina fisicaSelezionare il sistema di cui è stato eseguito il backup.Fare clic su Ripristino.Selezionare un punto di ripristino. Notare che i punti di ripristino vengono filtrati in base alla posizione.Se il sistema è offline, i punti di ripristino non vengono visualizzati. Eseguire una delle seguenti operazioni:Se la posizione di backup è il cloud o un

© Acronis International GmbH, 2003-2024

archivio condiviso (a cui possono accedere altri agenti), fare clic su Seleziona macchina e selezionare una macchina di destinazione che sia online, quindi selezionare un punto di ripristino.Selezionare un punto di ripristino nella scheda Archivio di backup.Ripristinare il sistema come descritto in "Ripristino di dischi mediante i supporti di avvio".Fare clic su Ripristina > Intera macchina.Il software esegue automaticamente la mappatura dei dischi dal backup ai dischi della macchina di destinazione.Per eseguire il ripristino in un'altra macchina fisica, fare clic su Macchina di destinazione, quindi selezionare un sistema di destinazione che sia online.Se non si è soddisfatti del risultato della mappatura o se tale operazione non ha avuto esito positivo, fare clic su Mappatura volume per ripetere la mappatura dei dischi in modalità manuale.La sezione dedicata alla mappatura consente anche di scegliere singoli dischi o volumi per il ripristino. È possibile passare in rassegna i vari dischi e volumi in ripristino tramite il collegamento Passa a... nell'angolo in alto a destra.[Disponibile soltanto per i sistemi Windows nei quali è installato un agente di protezione] Abilitare l'opzione Ripristino sicuro per verificare che i dati ripristinati siano privi di malware. Per ulteriori informazioni sul funzionamento del ripristino sicuro, consultare "Ripristino sicuro" (pag. 1).Fare clic su Avvia ripristino.Confermare che si desidera sovrascrivere i dischi con le versioni di cui si è eseguito il backup. Scegliere se riavviare il sistema automaticamente.L'avanzamento del ripristino viene mostrato nella scheda Attività." (pag. 1).

5. Per una configurazione di ripristino avanzata, fare clic su **Opzioni di ripristino**. Per ulteriori informazioni, fare riferimento a "Opzioni di ripristino" (pag. 528).
6. Fare clic su **Avvia ripristino**.
7. Confermare che si desidera sovrascrivere i dischi con le versioni di cui si è eseguito il backup. Scegliere se riavviare il sistema automaticamente.
8. L'avanzamento del ripristino viene mostrato nella scheda **Attività**.

Per riavviare il sistema avviato da remoto

1. Nella scheda **Dispositivi**, passare al gruppo **Supporto di avvio**, quindi selezionare il supporto da utilizzare per il recupero dei dati.
2. Fare clic su **Riavvia**.
3. Confermare di voler riavviare il sistema avviato con il supporto di avvio.

Per arrestare il sistema avviato da remoto

1. Nella scheda **Dispositivi**, passare al gruppo **Supporto di avvio**, quindi selezionare il supporto da utilizzare per il recupero dei dati.
2. Fare clic su **Arresta**.
3. Confermare di voler arrestare il sistema avviato con il supporto di avvio.

Per visualizzare informazioni sul supporto di avvio

1. Nella scheda **Dispositivi**, passare al gruppo **Supporto di avvio**, quindi selezionare il supporto da utilizzare per il recupero dei dati.
2. Fare clic su **Dettagli**, **Attività** o **Avvisi** per visualizzare le informazioni corrispondenti.

© Acronis International GmbH, 2003-2024

Per eliminare il supporto di avvio da remoto

1. Nella scheda **Dispositivi**, passare al gruppo **Supporto di avvio**, quindi selezionare il supporto da utilizzare per il recupero dei dati.
2. Fare clic su **Elimina** per eliminare il supporto di avvio dalla console di Cyber Protect.
3. Confermare di voler eliminare il supporto di avvio.

Startup Recovery Manager

Startup Recovery Manager è un componente di avvio che risiede nel disco rigido. Con Startup Recovery Manager è possibile avviare l'utilità di ripristino avviabile senza utilizzare un supporto di avvio distinto.

Se si verifica un errore, riavviare il sistema, attendere la visualizzazione del messaggio **Premere F11 per AcronisStartup Recovery Manager**, quindi premere F11 o selezionare Startup Recovery Manager dal menu di avvio (se si utilizza il caricatore di avvio GRUB). Startup Recovery Manager viene avviato ed è possibile eseguire il ripristino.

Limitazioni

- [Non applicabile se GRUB è installato nel record di avvio principale] L'attivazione di Startup Recovery Manager sovrascrive il record di avvio principale (MBR) con il proprio codice di avvio. Di conseguenza, potrebbe essere necessario riattivare qualsiasi caricatore di avvio di terza parte dopo l'attivazione.
- [Non applicabile a GRUB] Prima di attivare Startup Recovery Manager in Linux, si consiglia di installare il caricatore di avvio nel record di avvio della partizione radice o nel record di avvio delle partizioni /boot invece di installarlo nel record di avvio principale. Altrimenti, riconfigurare manualmente il caricatore di avvio dopo l'attivazione.

Attivazione di Startup Recovery Manager

Per abilitare il prompt all'avvio **Premere F11 per Acronis Startup Recovery Manager** (o aggiungere la voce **Startup Recovery Manager** al menu GRUB), è necessario attivare Startup Recovery Manager.

Nota
L'attivazione di Startup Recovery Manager su un sistema con volume di sistema non crittografato richiede almeno 100 MB di spazio libero su tale sistema. Il ripristino con riavvio richiede ulteriori 100 MB di spazio libero.

Per attivare Startup Recovery Manager su un sistema con volume crittografato con BitLocker, tale sistema richiede almeno un volume non crittografato con almeno 500 MB di spazio libero. Il ripristino con riavvio richiede ulteriori 500 MB di spazio libero.

Se Startup Recovery Manager non è attivato, le operazioni di backup che creano i backup One-click Recovery non riescono.

© Acronis International GmbH, 2003-2024

Per attivare Startup Recovery Manager

Su un sistema Windows o Linux con agente

1. Nella console di Cyber Protect, selezionare il sistema su cui attivare Startup Recovery Manager.
2. Fare clic su **Dettagli**.
3. Abilitare l'opzione **Startup Recovery Manager**.

Su un sistema senza agente

1. Avviare il sistema utilizzando un supporto di avvio.
2. Nell'interfaccia grafica del supporto di avvio, fare clic su **Strumenti** > **Attiva Startup Recovery Manager**.
3. Selezionare **Attiva**.
4. Fare clic su **OK**.
5. Nella scheda **Dettagli**, controllare la riga **Risultato** per verificare che l'attivazione sia riuscita, quindi fare clic su **Chiudi**.

Disattivazione di Startup Recovery Manager

La disattivazione disabilita il prompt all'avvio **Prememere F11 per Acronis Startup Recovery Manager** (o rimuove l'elemento **Startup Recovery Manager** dal menu GRUB).

Se Startup Recovery Manager non è attivato, è comunque possibile recuperare un sistema che non riesce ad avviarsi utilizzando un supporto di avvio separato.

Nota
Se Startup Recovery Manager non è attivato, le operazioni di backup che creano i backup One-click Recovery non riescono.

Per disattivare Startup Recovery Manager

Su un sistema Windows o Linux con agente

1. Nella console di Cyber Protect, selezionare il sistema su cui disattivare Startup Recovery Manager.
2. Fare clic su **Dettagli**.
3. Disabilitare l'opzione **Startup Recovery Manager**.

Su un sistema senza agente

1. Avviare il sistema utilizzando un supporto di avvio.
2. Nell'interfaccia grafica del supporto di avvio, fare clic su **Strumenti** > **Disattiva Startup Recovery Manager**.
3. Selezionare **Disattiva**.
4. Fare clic su **OK**.

© Acronis International GmbH, 2003-2024

5. Nella scheda **Dettagli**, controllare la riga **Risultato** per verificare che la disattivazione sia riuscita, quindi fare clic su **Chiudi**.

© Acronis International GmbH, 2003-2024

Implementazione del disaster recovery

Nota
- Questa funzionalità non supporta le posizioni di backup di Microsoft Azure.

Informazioni su Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) è un componente di Cyber Protection che fornisce servizi DRaaS (Disaster Recovery as-a-Service). Cyber Disaster Recovery Cloud rappresenta una soluzione rapida e stabile per avviare copie esatte dei sistemi nel sito cloud e per trasferire i carichi di lavoro dai sistemi originali danneggiati ai server di ripristino nel cloud in caso di errore umano o calamità naturale.

È possibile impostare e configurare il disaster recovery secondo le modalità seguenti:

- Creare un piano di protezione che include il modulo di disaster recovery e applicarlo ai dispositivi. Ciò configurerà automaticamente l'infrastruttura di disaster recovery. Vedere Creare un piano di protezione di disaster recovery.
- Configurare manualmente l'infrastruttura cloud di disaster recovery e controllare ogni fase. Vedere "Configurazione dei server di ripristino" (pag. 796).

Funzionalità principali

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

- Gestisci il servizio Cyber Disaster Recovery Cloud da un'unica console
- Estende al cloud un massimo di 23 reti locali, utilizzando un tunnel VPN sicuro
- Stabilisci la connessione al sito cloud senza distribuire alcuna appliance VPN[1] (modalità solo cloud)
- Stabilisci la connessione da punto a sito ai siti cloud e locale
- Proteggi le macchine utilizzando i server di ripristino nel cloud
- Proteggi applicazioni e appliance utilizzando i server primari nel cloud
- Esegui attività di disaster recovery automatiche per i backup crittografati
- Esegui failover di prova nella rete isolata
- Utilizza i runbook per allestire l'ambiente di produzione nel cloud

[1] [Disaster Recovery] Una macchina virtuale speciale che abilita la connessione tra la rete locale e il sito nel cloud tramite un tunnel VPN sicuro. L'appliance VPN viene distribuita nel sito locale.

© Acronis International GmbH, 2003-2024

Requisiti software

Sistemi operativi supportati

La protezione tramite server di ripristino è stata testata con i sistemi operativi seguenti:

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.x, 21.x
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2019 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2022 - tutte le opzioni di installazione, ad eccezione di Nano Server

Il software può funzionare con altri sistemi operativi Windows e distribuzioni Linux, ma ciò non è garantito.

Nota
La protezione tramite server di ripristino è stata testata per le VM Microsoft Azure che eseguono i sistemi operativi seguenti:

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2019 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2022 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Ubuntu Server 20.04 LTS - Gen2 (Canonical) Per ulteriori informazioni su come accedere alla console del server di ripristino, consultare https://kb.acronis.com/content/71616.

Piattaforme di virtualizzazione supportate

La protezione delle macchine virtuali con un server di ripristino è stata testata con le piattaforme di virtualizzazione seguenti:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V

© Acronis International GmbH, 2003-2024

- Windows Server 2016 con Hyper-V - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2019 con Hyper-V – tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2022 con Hyper-V – tutte le opzioni di installazione, ad eccezione di Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Virtual machine basate su Kernel (KVM) – solo guest (HVM) completamente virtualizzati. Non sono supportati i guest paravirtualizzati (PV).
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

L'appliance VPN è stata testata con le piattaforme di virtualizzazione seguenti:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Windows Server 2016 con Hyper-V - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2019 con Hyper-V – tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2022 con Hyper-V – tutte le opzioni di installazione, ad eccezione di Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Il software può funzionare con altre versioni e piattaforme di virtualizzazione, ma ciò non è garantito.

Limitazioni

Cyber Disaster Recovery Cloud non supporta le seguenti piattaforme e configurazioni:

1. Piattaforme non supportate:
   - Agenti per Virtuozzo
   - macOS
   - I sistemi operativi desktop di Windows non sono supportati a causa dei termini del prodotto di Microsoft.
   - Azure Edition per Windows Server

     Azure Edition è una versione speciale di Windows Server progettata specificamente per funzionare sia come virtual machine (VM) IaaS di Azure in Azure, sia come VM su un cluster Azure Stack HCI. A differenza delle edizioni Standard e Datacenter, Azure Edition non dispone della licenza per funzionare su hardware bare metal, Hyper-V client di Windows, Hyper-V server di Windows, hypervisor di terze parti o su cloud di terze parti.

© Acronis International GmbH, 2003-2024

2. Configurazioni non supportate:

   Microsoft Windows

   - I dischi dinamici non sono supportati
   - I sistemi operativi desktop di Windows non sono supportati a causa dei termini del prodotto di Microsoft.
   - Il servizio Active Directory con replica FRS non è supportato
   - I supporti rimovibili senza formattazione GPT o (i cosiddetti "superfloppy") non sono supportati

   Linux

   - File system senza una tabella di partizione
   - I workload Linux il cui backup è stato eseguito con un agente da un SO guest e che hanno volumi con le seguenti configurazioni avanzate di Logical Volume Manager (LVM): volumi con striping, volumi con mirroring, volumi RAID 0, RAID 4, RAID 5, RAID 6 o RAID 10.

   Nota
   I workload con più sistemi operativi installati non sono supportati.

3. Tipi di backup non supportati:
   - I punti di ripristino con protezione continua dei dati (CDP) non sono compatibili.

     Importante
     Se si crea un server di ripristino da un backup dotato di un punto di ripristino CDP, durante il failback o la creazione di un server di ripristino, i dati contenuti nel punto di ripristino CDP andranno perduti.

   - Non è possibile utilizzare backup contenenti dati forensi per la creazione di server di ripristino.

Un server di ripristino è dotato di una sola interfaccia di rete. Se il sistema originale presenta più interfacce di rete, solo una verrà emulata.

I server cloud non sono crittografati.

Versione in trial di Cyber Disaster Recovery Cloud

È possibile utilizzare una versione in trial di Acronis Cyber Disaster Recovery Cloud per un periodo di 30 giorni. In questa versione, Disaster Recovery presenta le seguenti limitazioni per i tenant partner:

- I server di ripristino e primari non possono accedere a una rete Internet pubblica. Non è possibile assegnare indirizzi IP pubblici ai server.
- La VPN IPsec multisito non è disponibile.

© Acronis International GmbH, 2003-2024

Limitazioni durante l'utilizzo di Geo-redundant Cloud Storage

Geo-redundant Cloud Storage fornisce una posizione secondaria per i dati di backup. La posizione secondaria si trova in una regione geograficamente distinta dalla posizione primaria dello storage. La separazione geografica tra le regioni garantisce che, in caso di un'emergenza che colpisca una delle regioni e renda irrecuperabili i dati dei backup, l'altra regione non subisca conseguenze, evitando così interruzioni operative.

Importante
Il servizio Disaster Recovery non è supportato se la posizione dello storage di backup viene trasferita dalla posizione primaria alla posizione secondaria con geo-ridondanza.

Compatibilità di Disaster Recovery con il software di crittografia

Disaster Recovery è compatibile con i seguenti software di crittografia a livello del disco:

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

Nota
- Per i workload con crittografia a livello del disco, si consiglia di installare l'agente di protezione nel sistema operativo guest del workload e di eseguire backup con agente.
- I backup agentless di workload crittografati non supportano le attività di failover e failback.

Per ulteriori informazioni sulla compatibilità di Cyber Protection con i software di crittografia, consultare "Compatibilità con il software di crittografia" (pag. 42).

Punti di calcolo

In Disaster Recovery, i punti di calcolo vengono utilizzati per i server primari e per i server di ripristino, durante il failover di prova e il failover di produzione. I punti di calcolo riflettono le risorse di elaborazione utilizzate per l'esecuzione dei server (virtual machine) nel cloud.

Il consumo di punti di calcolo durante il disaster recovery dipende dai parametri del server e dalla durata dell'intervallo di tempo in cui il server è nella condizione di failover. Più è potente il server e più è lungo l'intervallo di tempo, maggiore sarà il volume di punti di calcolo consumati. A un volume più elevato di punti di calcolo consumati corrisponde un prezzo più alto.

© Acronis International GmbH, 2003-2024

L'addebito per tutti i server in esecuzione in Acronis Cloud viene conteggiato in base ai punti di calcolo consumati e alla preferenza configurata e indipendentemente dallo stato in cui si trovano (acceso o spento).

I server di ripristino nello stato Standby non consumano punti di calcolo e il relativo addebito non avviene in base ai punti di calcolo.

Nella tabella sottostante è visualizzato un esempio che mostra otto server nel cloud con diverse preferenze e i corrispondenti punti di calcolo consumati all'ora. È possibile modificare le versioni dei server nella scheda **Dettagli**.

Tipo	CPU	RAM	Punti di calcolo
F1	1 vCPU	2 GB	1
F2	1 vCPU	4 GB	2
F3	2 vCPU	8 GB	4
F4	4 vCPU	16 GB	8
F5	8 vCPU	32 GB	16
F6	16 vCPU	64 GB	32
F7	16 vCPU	128 GB	64
F8	16 vCPU	256 GB	128

Utilizzando le informazioni nella tabella, sarà facile stimare quanti punti di calcolo verranno consumati da un server (virtual machine).

Ad esempio, proteggendo con il modulo Disaster Recovery una virtual machine con 4 vCPU* con 16 GB di RAM e una virtual machine con 2 vCPU con 8 GB di RAM, la prima virtual machine consumerà 8 punti di calcolo l'ora e la seconda virtual machine 4 punti di calcolo l'ora. Se entrambe le virtual machine sono in failover, il consumo totale sarà di 12 punti di calcolo l'ora, ovvero 288 punti di calcolo per l'intera giornata (12 punti di calcolo x 24 ore = 288 punti di calcolo).

*vCPU indica un'unità di elaborazione fisica centrale (CPU) assegnata a una virtual machine; si tratta di un'entità dipendente dal tempo.

Nota
Se viene raggiunto il surplus della quota relativa ai **Punti di calcolo**, tutti i server primari e di ripristino vengono spenti. Non sarà possibile utilizzare questi server fino all'inizio del periodo di fatturazione successivo, o fino a quando non viene incrementata la quota. Per impostazione predefinita, il periodo di fatturazione corrisponde a un mese di calendario.

© Acronis International GmbH, 2003-2024

Configurazione della funzionalità di disaster recovery

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

Per configurare la funzionalità di disaster recovery

1. Configurare il tipo di connessione al sito cloud:
   - Connessione da punto a sito
   - Connessione Open VPN da sito a sito
   - Connessione VPN IPsec multisito
   - Modalità solo cloud
2. Creare un piano di protezione con il modulo di backup abilitato e selezionare l'intera macchina o sistema e i volumi di avvio per il backup. Per creare un server di ripristino è necessario creare almeno un piano di protezione.
3. Applicare il piano di protezione ai server locali da proteggere.
4. Creare i server di ripristino per ognuno dei server locali da proteggere.
5. Eseguire un failover di prova per verificarne il funzionamento.
6. [Facoltativo] creare i server primari per la replica dell'applicazione.

Viene configurata la funzionalità di disaster recovery per proteggere i server locali.

In caso di necessità, è possibile eseguire il failover del carico di lavoro nei server di ripristino nel cloud. È necessario creare almeno un punto di ripristino prima che sia possibile eseguire il failover sui server di ripristino. Dopo aver ripristinato il sito locale da un'emergenza, è possibile trasferire di nuovo il workload nel sito locale eseguendo il failback. Per ulteriori informazioni sul processo di failback, fare riferimento a "Prerequisiti" (pag. 810) e "Prerequisiti" (pag. 814).

Creare un piano di protezione di disaster recovery

Creare un piano di protezione che include il modulo Disaster Recovery e applicarlo ai dispositivi.

Per impostazione predefinita, durante la creazione di un nuovo piano di protezione il modulo Disaster Recovery è disabilitato. Dopo aver abilitato la funzionalità di disaster recovery e applicato il piano ai dispositivi, viene creata l'infrastruttura della rete cloud, che include un *server di ripristino* per ogni dispositivo protetto. Il *server di ripristino* è una virtual machine nel cloud che è una copia del dispositivo selezionato. Per ognuno dei dispositivi selezionati, verrà creato un server di ripristino con impostazioni predefinite nello stato Standby (virtual machine non in esecuzione). La dimensione del server di ripristino è automatica e dipende dalla CPU e dalla RAM del dispositivo protetto. Viene creata in modalità automatica anche l'infrastruttura di rete cloud: Reti e gateway VPN nel sito cloud, ai quali verranno connessi i server di ripristino.

© Acronis International GmbH, 2003-2024

Se si revoca, elimina o disabilita il modulo Disaster Recovery di un piano di protezione, i server di ripristino e le reti cloud non vengono automaticamente eliminate. È possibile rimuovere l'infrastruttura di disaster recovery manualmente, se necessario.

Nota

- Dopo aver configurato il disaster recovery, sarà possibile eseguire il failover di prova o di produzione da qualsiasi punto di ripristino generato dopo la creazione del server di ripristino per il dispositivo. I punti di ripristino generati prima che i dispositivi vengano protetti con la funzionalità di disaster recovery (ad esempio prima della creazione del server di ripristino) non possono essere utilizzati per il failover.
- Non è possibile abilitare un piano di protezione di disaster recovery se non è possibile individuare l'indirizzo IP di un dispositivo, come nel caso in cui viene eseguito il backup agentless delle virtual machine e a queste non viene assegnato un indirizzo IP.
- Quando si applica un piano di protezione, nel sito cloud vengono assegnati le stesse reti e gli stessi indirizzi IP. Per la connessione VPN IPsec è necessario che i segmenti di rete del cloud e dei siti locali non si sovrappongano. Se si configura una connessione VPN IPsec multisito, e se il piano di protezione viene applicato a uno o più dispositivi in un secondo momento, sarà anche necessario aggiornare le reti cloud e riassegnare gli indirizzi IP dei server cloud. Per ulteriori informazioni, consultare "Riassegnazione di indirizzi IP" (pag. 786).

Per creare un piano di protezione di disaster recovery

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare i sistemi da proteggere.
3. Fare clic su **Proteggi**, quindi su **Crea piano**.
   Viene visualizzato il piano di protezione con le impostazioni predefinite.
4. Configurare le opzioni di backup.
   Per utilizzare la funzionalità di disaster recovery, il piano deve eseguire il backup dell'intero sistema, o solo dei dischi necessari per l'avvio e per fornire i servizi necessari, in un archivio nel cloud.
5. Abilitare il modulo di Disaster recovery facendo clic sull'interruttore accanto al nome del modulo.
6. Fare clic su **Crea**.
   Il piano viene creato e applicato ai sistemi selezionati.

Passaggi successivi

- È possibile modificare la configurazione predefinita del server di ripristino. Per ulteriori informazioni, consultare "Configurazione dei server di ripristino" (pag. 796).
- È possibile modificare la configurazione di rete predefinita. Per ulteriori informazioni, consultare "Configurazione della connessione" (pag. 759).
- È possibile visualizzare più informazioni sui parametri predefiniti del server di ripristino e sull'infrastruttura di rete cloud. Per ulteriori informazioni, consultare "Modifica dei parametri predefiniti del server di ripristino" (pag. 757) e "Infrastruttura di rete cloud" (pag. 758).

 © Acronis International GmbH, 2003-2024

Modifica dei parametri predefiniti del server di ripristino

Quando si crea e applica un piano di protezione di disaster recovery, viene creato un server di ripristino con parametri predefiniti. I parametri predefiniti possono essere modificati in un secondo momento.

Nota
Tale server viene creato solo se non esiste. Eventuali server di ripristino esistenti non vengono né modificati né ricreati.

Per modificare i parametri predefiniti del server di ripristino

1. Passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare un dispositivo e fare clic su **Disaster Recovery**.
3. Modificare i parametri predefiniti del server di ripristino.
   I parametri del server di ripristino sono descritti nella tabella seguente.

Server di ripristino **parametro**	**Impostazione predefinita** **valore**	**Descrizione**
CPU e RAM	auto	Il numero di CPU virtuali e la dimensione della RAM del server di ripristino. Le impostazioni predefinite verranno determinate automaticamente alla configurazione di CPU e RAM del dispositivo originale.
Rete cloud	auto	Specificare la rete cloud alla quale viene connesso il server. Per informazioni su come sono configurate le reti cloud, vedere Infrastruttura di rete cloud.
Indirizzo IP in rete di produzione	auto	L'indirizzo IP che avrà il server nella rete di produzione. Per impostazione predefinita, viene configurato l'indirizzo IP del sistema originale.
Indirizzo IP di prova	disattivato	Il test dell'indirizzo IP consente di eseguire il failover di prova nella rete di prova isolata e di connettersi al server di ripristino tramite RDP o SSH durante un failover di prova. Nella modalità failover di prova, il gateway VPN sostituisce l'indirizzo IP di prova con l'indirizzo IP di produzione utilizzando il protocollo NAT. Se non è specificato un indirizzo IP di prova, per accedere al server durante un failover di prova sarà possibile utilizzare esclusivamente la console.

© Acronis International GmbH, 2003-2024

Accesso Internet	Abilitato	Il server di ripristino potrà accedere a Internet durante un failover reale o di prova. Per impostazione predefinita, la porta TCP 25 non è autorizzata alle connessioni in uscita.
Utilizza indirizzo pubblico	disattivato	Se dispone di un indirizzo IP pubblico, il server di ripristino è disponibile anche da Internet durante un failover reale o di prova. Se non viene utilizzato un indirizzo IP pubblico, il server sarà disponibile solo nella rete di produzione. Per utilizzare un indirizzo IP pubblico, è necessario abilitare l'accesso a Internet. L'indirizzo IP pubblico verrà visualizzato dopo aver completato la configurazione. Per impostazione predefinita, la porta TCP 443 è aperta per le connessioni in entrata.
Imposta soglia RPO	disattivato	La soglia RPO definisce l'intervallo di tempo massimo consentito tra l'ultimo punto di ripristino e l'ora corrente. È possibile impostare il valore tra 15–60 minuti, 1–24 ore, 1–14 giorni.

Infrastruttura di rete cloud

L'infrastruttura di rete cloud è costituita dal gateway VPN nel sito cloud e dalle reti cloud alle quali verranno connessi i server di ripristino.

Nota
L'applicazione di un piano di protezione di disaster recovery creare un'infrastruttura di rete cloud di ripristino solo se non esiste. Le reti cloud esistenti non possono essere modificate o ricreate.

Il sistema controlla gli indirizzi IP dei dispositivi e se non sono presenti reti cloud adatte a un indirizzo IP, crea automaticamente reti cloud idonee. Se sono già disponibili reti cloud per le quali gli indirizzi IP dei server di ripristino sono adatti, le reti cloud esistenti non verranno modificate o ricreate.

- Se non sono presenti reti cloud o se la configurazione di disaster recovery viene impostata per la prima volta, le reti cloud verranno create con gli intervalli massimi raccomandati da IANA per l'uso privato (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) in base all'intervallo di indirizzi IP dei dispositivi in uso. È possibile limitare la rete modificando la maschera di rete.
- Se sono presenti dispositivi su più reti locali, la rete nel sito cloud può diventare un superinsieme di reti locali. È possibile riconfigurare le reti nella sezione **Connessione**. Vedere "Gestione delle reti" (pag. 779).
- Se è necessario configurare la connessione Open VPN da sito a sito, scaricare e configurare l'appliance VPN. Vedere "Configurazione di una Open VPN da sito a sito" (pag. 770).Verificare che

© Acronis International GmbH, 2003-2024

gli intervalli delle reti cloud corrispondano agli intervalli della rete locale connessa all'appliance VPN.

- Per modificare la configurazione di rete predefinita fare clic sul collegamento **Vai a Connessione** nel modulo Disaster Recovery del piano di protezione oppure passare a **Disaster Recovery** > **Connessione**.

Configurazione della connessione

In questa sezione vengono illustrati alcuni concetti sulla rete, necessari per comprendere il funzionamento di Cyber Disaster Recovery Cloud. Viene spiegato come configurare diversi tipi di connessione al sito cloud, in base alle diverse esigenze. Infine, viene illustrato come gestire le reti nel cloud, le impostazioni dell'appliance VPN, e il gateway VPN.

Concetti sulla rete

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

Cyber Disaster Recovery Cloud consente di definire i seguenti tipi di connessione al sito cloud:

- **Modalità solo cloud**

  Questo tipo di connessione non richiede la distribuzione di un'appliance VPN nel sito locale.

  Le reti locali e cloud operano come reti indipendenti. Questo tipo di connessione implica il failover di tutti i server protetti del sito locale o il failover parziale dei server indipendenti che non hanno necessità di comunicare con il sito locale.

  È possibile accedere ai server cloud nel sito cloud tramite VPN da punto a sito e indirizzi IP pubblici, se assegnati.
- **Connessione Open VPN da sito a sito**

  Questo tipo di connessione richiede la distribuzione di un'appliance VPN nel sito locale.

  Una connessione Open VPN da sito a sito consente di estendere le reti al sito cloud, mantenendo gli indirizzi IP.

  Il sito locale viene connesso al cloud tramite un tunnel VPN sicuro. Si tratta di una connessione adatta in presenza di server altamente dipendenti nel sito locale, come un server web e un server per database. In caso di failover parziale, nel momento in cui uno di questi server viene ricreato nel sito site mentre l'altro resta nel sito locale, i server potranno comunque comunicare uno con l'altro tramite il tunnel VPN.

  È possibile accedere ai server cloud nel sito cloud tramite rete locale, VPN da punto a sito e indirizzi IP pubblici, se assegnati.
- **Connessione VPN IPsec multisito**

  Questo tipo di connessione richiede un dispositivo VPN locale che supporti IPsec IKE v2.

© Acronis International GmbH, 2003-2024

Quando si avvia la configurazione della connessione VPN IPsec multisito, Cyber Disaster Recovery Cloud crea automaticamente un gateway VPN cloud con un indirizzo IP pubblico.

Con la connessione VPN IPsec multisito, i siti locali vengono connessi al sito cloud tramite un tunnel VPN IPsec sicuro.

Questo tipo di connessione è adatta agli scenari di Disaster Recovery in cui sono presenti uno o più siti locali che ospitano workload critici o servizi fortemente dipendenti.

In caso di failover parziale di uno dei server, questo server viene ricreato nel sito cloud mentre gli altri restano nel sito locale; i server potranno comunque comunicare uno con l'altro tramite il tunnel VPN IPsec.

In caso di failover parziale di uno dei server, questo server viene ricreato nel sito cloud mentre gli altri restano nel sito locale; i server potranno comunque comunicare uno con l'altro tramite il tunnel VPN IPsec.

- **Accesso VPN remoto da punto a sito**

  Un accesso VPN remoto sicuro da punto a sito al cloud e ai workload del sito locale dall'esterno, utilizzando il dispositivo endpoint.

  Per l'accesso al sito locale, questo tipo di connessione richiede la distribuzione di un'appliance VPN nel sito locale.

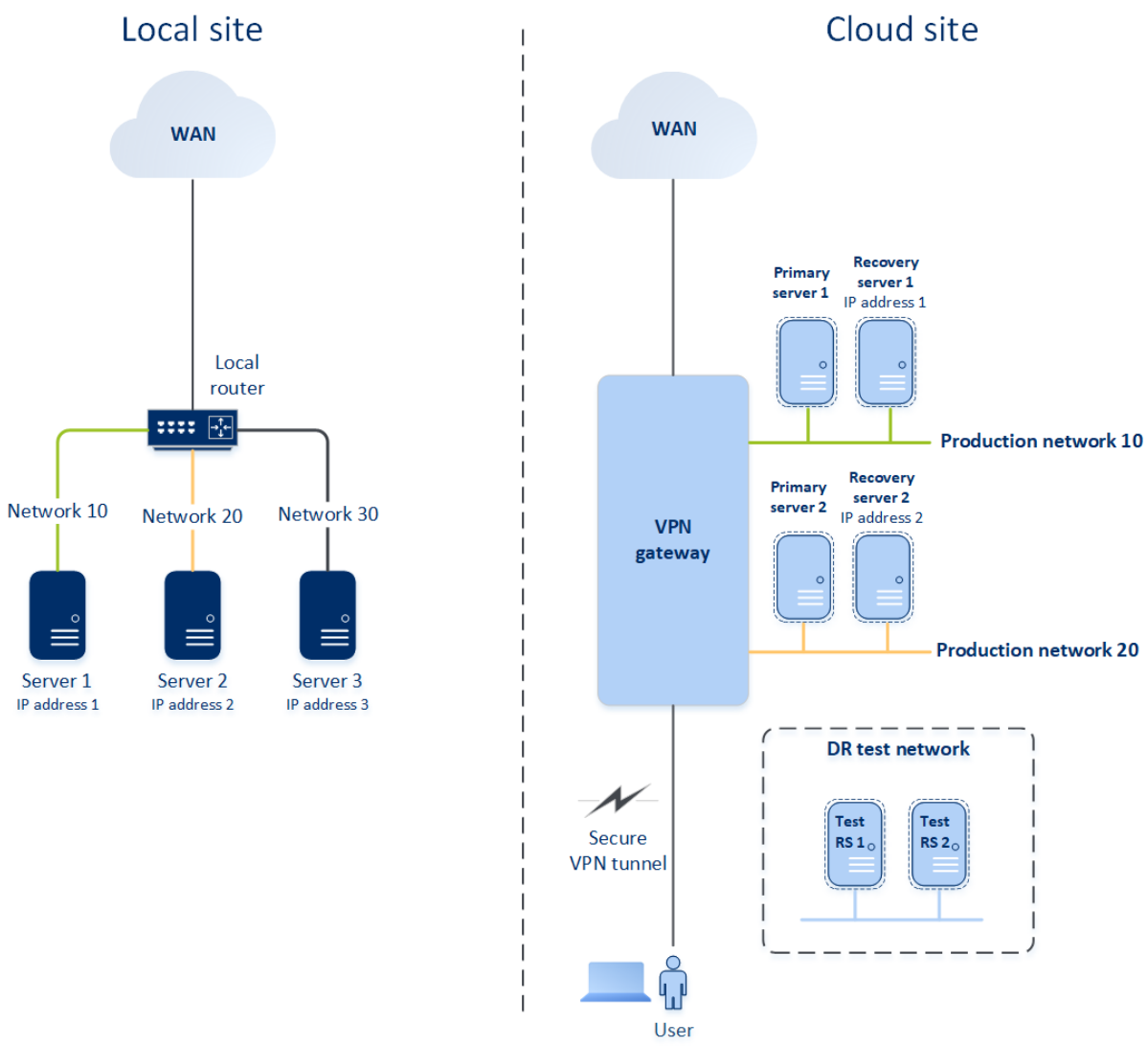
Modalità solo cloud

La connessione in modalità solo cloud non richiede la distribuzione di un'appliance VPN nel sito locale. Ciò significa che si avranno due reti indipendenti: una nel sito locale e un'altra nel sito cloud. Il routing viene eseguito con il router nel sito cloud.

Come funziona il routing

Nel caso in cui venga stabilita la modalità di connessione solo in cloud, il routing viene eseguito tramite il router sul sito in cloud, in modo che i server di diverse reti cloud possano comunicare fra loro.

© Acronis International GmbH, 2003-2024



Connessione Open VPN da sito a sito

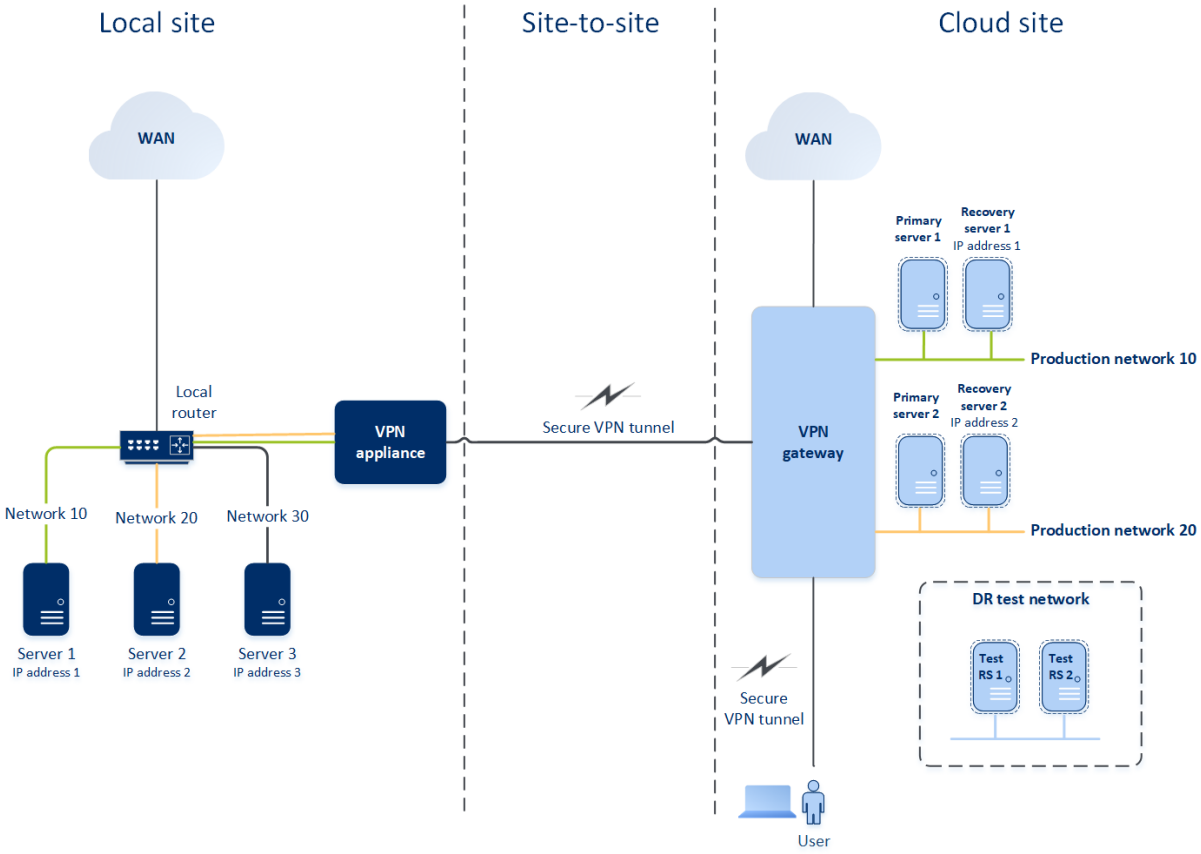
Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Per comprendere il funzionamento della rete in Cyber Disaster Recovery Cloud, verrà considerata una situazione in cui sono presenti tre reti, ognuna con un sistema nel sito locale. Nell'esempio verrà configurata la protezione per le due reti, che denomineremo Rete 10 e Rete 20.

Il diagramma sottostante mostra il sito locale che ospita i sistemi e il sito cloud in cui vengono avviati i server cloud in caso di emergenza.

La soluzione Cyber Disaster Recovery Cloud consente di eseguire il failover di tutti i workload dei sistemi danneggiati nel sito locale sui server cloud nel cloud. È possibile proteggere un massimo di 23 reti con Cyber Disaster Recovery Cloud.

© Acronis International GmbH, 2003-2024



Per stabilire una comunicazione Open VPN da sito a sito tra i siti locali e cloud vengono utilizzati un'**appliance VPN** e un **gateway VPN**. Quando si avvia la configurazione della connessione Open VPN site-to-site nella console di Cyber Protect, il gateway VPN viene distribuito automaticamente nel sito cloud. Successivamente, è necessario distribuire l'appliance VPN nel sito locale, aggiungere le reti da proteggere e registrare l'appliance nel cloud. Cyber Disaster Recovery Cloud crea una replica della rete locale nel cloud. Tra l'appliance VPN e il gateway VPN viene stabilito un tunnel VPN sicuro. che rappresenta l'estensione della rete locale nel cloud. Viene eseguito il bridging tra le reti di produzione nel cloud e le reti locali. I server locali e nel cloud possono comunicare tramite questo tunnel VPN come se fossero tutti nello stesso segmento Ethernet. Viene avviato il routing con il router locale.

È necessario creare un server di ripristino nel sito cloud per ogni macchina di origine da proteggere. Tale server rimane in modalità **Standby** fino a quando non si verifica un evento di failover. In caso di emergenza, se si avvia il processo di failover in **modalità di produzione**, il server di ripristino che rappresenta la copia esatta del sistema protetto viene avviato nel cloud. A tale server può essere assegnato lo stesso indirizzo IP del sistema di origine e potrà essere avviato nello stesso segmento Ethernet. Il server potrà essere utilizzato come sempre, senza che gli utenti notino alcun cambiamento.

È inoltre possibile avviare un processo di failover in **modalità di prova**. In questa modalità, la macchina di origine resta in funzione e al contempo rispettivo il server di ripristino, con lo stesso indirizzo IP, viene avviato nel cloud. Per evitare conflitti tra indirizzi IP, nel cloud viene creata una rete virtuale speciale, definita **rete di prova**. Tale rete è isolata per evitare la duplicazione

© Acronis International GmbH, 2003-2024

dell'indirizzo IP della macchina di origine in un segmento Ethernet. Per accedere al server di ripristino in modalità failover di prova, è necessario assegnare l'**Indirizzo IP di prova** al server di ripristino al momento della sua creazione. Gli altri parametri del server di ripristino che è possibile specificare vengono illustrati nelle rispettive sezioni, più avanti.

Come funziona il routing

Nel caso in cui venga stabilita una connessione da sito a sito, il routing tra le reti cloud viene eseguito con il router locale. Il server VPN non esegue il routing tra i server cloud posizionati in reti cloud diverse. Se il server cloud di una rete deve comunicare con un server di un'altra rete cloud, il traffico passa nel tunnel VPN verso il router locale presso il sito locale. A quel punto, il router locale effettua il routing verso un'altra rete e torna attraverso il tunnel al server di destinazione sul sito in cloud.

Gateway VPN

Il principale componente che consente la comunicazione tra i siti locali e cloud è il **gateway di VPN**. Si tratta di una virtual machine nel cloud, nella quale è installato un software speciale, con una configurazione di rete specifica. Il gateway VPN offre le seguenti funzioni:

- Connette il segmento Ethernet della rete locale e della rete di produzione al cloud, in modalità L2.
- Fornisce le regole iptables e ebtables.
- Funge da router predefinito e da NAT per i sistemi nelle reti di prova e di produzione.
- Funge da server DHCP. Tutti i sistemi nelle reti di produzione e prova ottengono la configurazione di rete (indirizzi IP, impostazioni DNS) tramite DHCP. Un dato server cloud ottiene sempre lo stesso indirizzo IP dal server DHCP. Nel caso in cui sia necessario configurare impostazioni DNS personalizzate, contattare il supporto tecnico.
- Funge da DNS di caching.

Configurazione di rete del gateway VPN

Il gateway VPN presenta diverse interfacce di rete:

- Interfaccia esterna, connessa a Internet
- Interfacce di produzione, connesse alle reti di produzione
- Interfaccia di prova, connessa alla rete di prova

Inoltre, si aggiungono due interfacce virtuali per le connessioni da punto a sito e da sito a sito.

Quando il gateway VPN viene distribuito e inizializzato, vengono creati i bridge: uno per l'interfaccia esterna e uno per le interfacce del client e di produzione. Sebbene il bridge client-produzione e l'interfaccia di prova utilizzino gli stessi indirizzi IP, il gateway VPN può instradare correttamente i pacchetti utilizzando uno specifico metodo.

© Acronis International GmbH, 2003-2024

Appliance VPN

L'**appliance VPN** è una virtual machine nel sito locale, nella quale è installato Linux e un software speciale, con una specifica configurazione di rete. Consente la comunicazione tra i siti locali e cloud.

Server di ripristino

Un **server di ripristino** è una replica virtuale del sistema di origine, basato sui backup dei server protetti archiviati nel cloud. I server di ripristino sono utilizzati per trasferire i carichi di lavoro dai server originali in caso di emergenza.

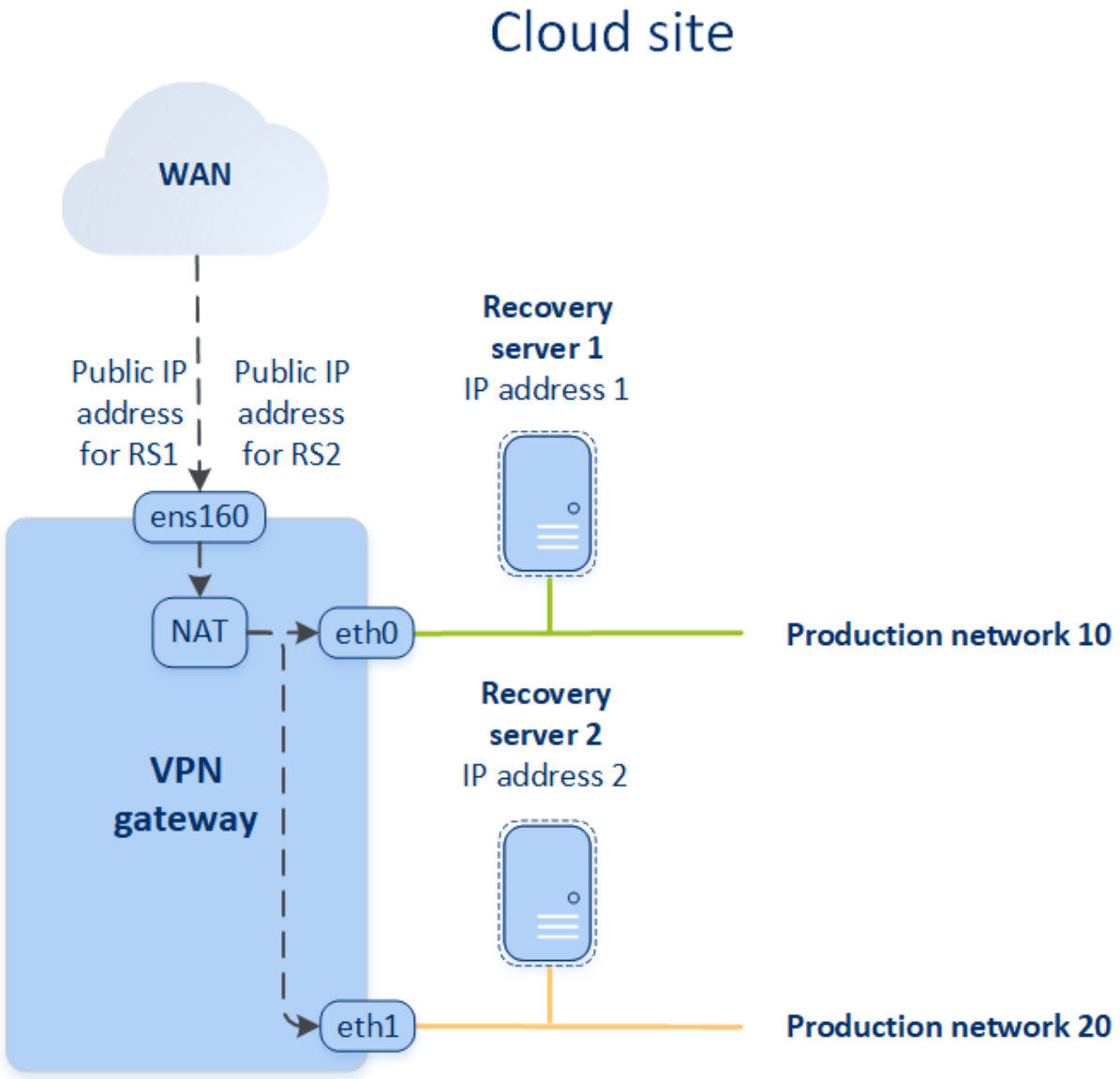
Durante la creazione di un server di ripristino è necessario specificare i seguenti parametri di rete:

- **Rete cloud** (necessario): una rete cloud alla quale viene connesso il server di ripristino.
- **Indirizzo IP nella rete di produzione** (necessario): un indirizzo IP con il quale viene avviata la macchina virtuale per un server di ripristino. Tale indirizzo è usato sia nella rete di produzione che in quella di prova. Prima dell'avvio, la macchina virtuale viene configurata per l'acquisizione dell'indirizzo IP tramite DHCP.
- **Indirizzo IP di prova** (facoltativo): un indirizzo IP utilizzato per accedere a un server di ripristino dalla rete client-produzione durante il failover di prova, per impedire che l'indirizzo IP di produzione venga duplicato sulla stessa rete. Questo indirizzo IP è diverso da quello della rete di produzione. I server del sito locale possono raggiungere i server di ripristino durante il failover di prova tramite l'indirizzo IP di prova, mentre l'accesso nella direzione contraria non è disponibile. L'accesso a Internet dal server di ripristino della rete di prova è disponibile se l'opzione **Accesso Internet** è stata selezionata durante la creazione del server di ripristino.
- **Indirizzo IP pubblico** (facoltativo): un indirizzo IP utilizzato per accedere a un server di ripristino da Internet. Se il server non dispone di un indirizzo IP pubblico, potrà essere raggiunto solo dalla rete locale.
- **Accesso Internet** (facoltativo): consente a un server di ripristino di accedere a Internet (sia in produzione sia nel failover di prova).

Assegnazione indirizzo IP di prova

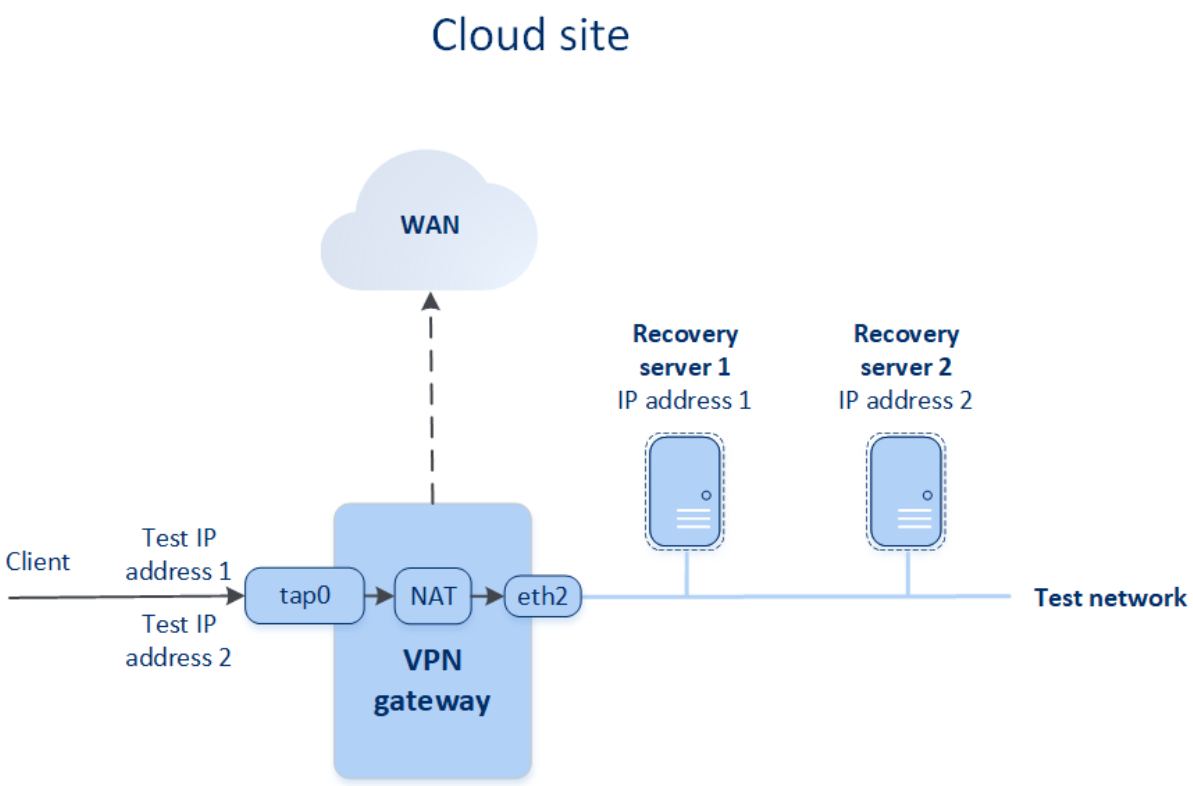
Se durante la creazione del server di ripristino viene assegnato un indirizzo IP pubblico, il server di ripristino sarà disponibile da Internet tramite tale indirizzo IP. Quando un pacchetto proveniente da Internet arriva con l'indirizzo IP pubblico di destinazione, il gateway VPN lo associa nuovamente al rispettivo indirizzo IP di produzione utilizzando NAT, quindi lo invia al server di ripristino corrispondente.

© Acronis International GmbH, 2003-2024



Se durante la creazione del server di ripristino viene assegnato un indirizzo IP di prova, il server di ripristino sarà disponibile nella rete di prova tramite tale indirizzo IP. Quando si esegue il failover di prova, il sistema di origine resta in funzione mentre il server di ripristino con lo stesso indirizzo IP viene avviato nella rete di prova nel cloud. Non si verifica alcun conflitto tra indirizzi IP poiché la rete di prova è isolata. I server di ripristino della rete di prova sono raggiungibili tramite i propri indirizzi IP di prova, che vengono riassociati agli indirizzi IP di produzione tramite NAT.

© Acronis International GmbH, 2003-2024



Per ulteriori informazioni sulle reti Open VPN da sito a sito, consultare "Open VPN site-to-site - Informazioni aggiuntive" (pag. 192).

Server primari

Un **server primario** è una virtual machine che, rispetto al server di ripristino, non dispone di un sistema connesso nel sito locale. I server primari sono utilizzati per proteggere un'applicazione tramite replica, o per eseguire diversi servizi ausiliari, ad esempio un server web.

In genere, un server primario viene utilizzato per la replica dei dati in tempo reale tra i server che eseguono le principali applicazioni. La replica viene configurata dall'utente, che a tal fine utilizza gli strumenti propri dell'applicazione. Ad esempio, è possibile configurare la replica di Active Directory o di SQL tra i server locali e il server primario.

In alternativa, è possibile includere un server primario in un gruppo di disponibilità AlwaysOn o in un gruppo di disponibilità dei database.

Entrambi questi metodi richiedono un'approfondita conoscenza dell'applicazione e i diritti di amministrazione sulla stessa. Un server primario consuma costantemente le risorse di elaborazione e lo spazio per l'archivio di ripristino di emergenza rapido. La manutenzione richiesta sul lato utente prevede il monitoraggio della replica, l'installazione degli aggiornamenti software e il backup. Tra i vantaggi, offre la riduzione degli obiettivi RPO e RTO e un carico minimo sull'ambiente di produzione, rispetto al backup dei server completi nel cloud.

I server primari sono avviati sempre ed esclusivamente nella rete di produzione e presentano i seguenti parametri di rete:

© Acronis International GmbH, 2003-2024

- **Rete cloud** (necessario): una rete cloud alla quale viene connesso il server primario.
- **Indirizzo IP nella rete di produzione** (necessario): un indirizzo IP assegnato al server primario nella rete di produzione. Per impostazione predefinita, viene configurato il primo indirizzo IP libero della rete di produzione.
- **Indirizzo IP pubblico** (facoltativo): un indirizzo IP utilizzato per accedere a un server primario da Internet. Se il server non dispone di un indirizzo IP pubblico, potrà essere raggiunto solo dalla rete locale e non da Internet.
- **Accesso Internet** (facoltativo): consente a un server primario di accedere a Internet.

Connessione VPN IPsec multisito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

La connessione VPN IPsec multisito viene usata per connettere un singolo sito locale o più siti locali a Cyber Disaster Recovery Cloud tramite una connessione VPN IPsec L3.

Si tratta di un tipo di connessione utile per situazioni di Disaster Recovery in presenza di uno dei seguenti scenari d'uso:

- è presente un sito locale che ospita workload critici;
- sono presenti più siti locali che ospitano workload critici, ad esempio uffici in diverse località;
- si utilizzano siti software di terze parti o siti di provider di servizi gestiti, e la connessione a questi avviene tramite un tunnel VPN IPsec.

Per stabilire la comunicazione VPN IPsec multisito tra il sito locale e il sito cloud viene utilizzato il **gateway VPN**. Quando si avvia la configurazione della connessione VPN IPsec multisito nella console di Cyber Protect, il gateway VPN viene distribuito automaticamente nel sito cloud. Configurare i segmenti della rete cloud e verificare non si sovrappongano ai segmenti delle reti locali. Tra i siti locali e il sito cloud viene stabilito un tunnel VPN sicuro. I server locali e nel cloud possono comunicare tramite questo tunnel VPN come se fossero tutti nello stesso segmento Ethernet.

È necessario creare un server di ripristino nel sito cloud per ogni macchina di origine da proteggere. Tale server rimane in modalità **Standby** fino a quando non si verifica un evento di failover. In caso di emergenza, se si avvia il processo di failover in **modalità di produzione**, il server di ripristino che rappresenta la copia esatta del sistema protetto viene avviato nel cloud. Il server potrà essere utilizzato come sempre, senza che gli utenti notino alcun cambiamento.

È inoltre possibile avviare un processo di failover in **modalità di prova**. In questa modalità, il sistema di origine resta in funzione e al contempo il rispettivo il server di ripristino viene avviato nel cloud in una rete virtuale speciale creta nel cloud come **rete di prova**. Tale rete è isolata per evitare la duplicazione degli indirizzi IP del sistema di origine negli altri segmenti della rete cloud.

© Acronis International GmbH, 2003-2024

Gateway VPN

Il principale componente che consente la comunicazione tra i siti locali e il sito cloud è il **gateway VPN**. Si tratta di una macchina virtuale nel cloud, nella quale è installato un software speciale, con una configurazione di rete specifica. Il gateway VPN offre le seguenti funzioni:

- Connette i segmenti Ethernet della rete locale e della rete di produzione al cloud, in modalità IPsec L3.
- Funge da router predefinito e da NAT per i sistemi nelle reti di prova e di produzione.
- Funge da server DHCP. Tutti i sistemi nelle reti di produzione e prova ottengono la configurazione di rete (indirizzi IP, impostazioni DNS) tramite DHCP. Un dato server cloud ottiene sempre lo stesso indirizzo IP dal server DHCP.
  È inoltre possibile impostare una configurazione DNS personalizzata. Per ulteriori informazioni, consultare "Configurazione di server DNS personalizzati" (pag. 787).
- Funge da DNS di caching.

Come funziona il routing

Il routing tra le reti cloud viene eseguito con il router sul sito cloud, in modo che i server di diverse reti cloud possano comunicare fra loro.

Accesso VPN remoto da punto a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

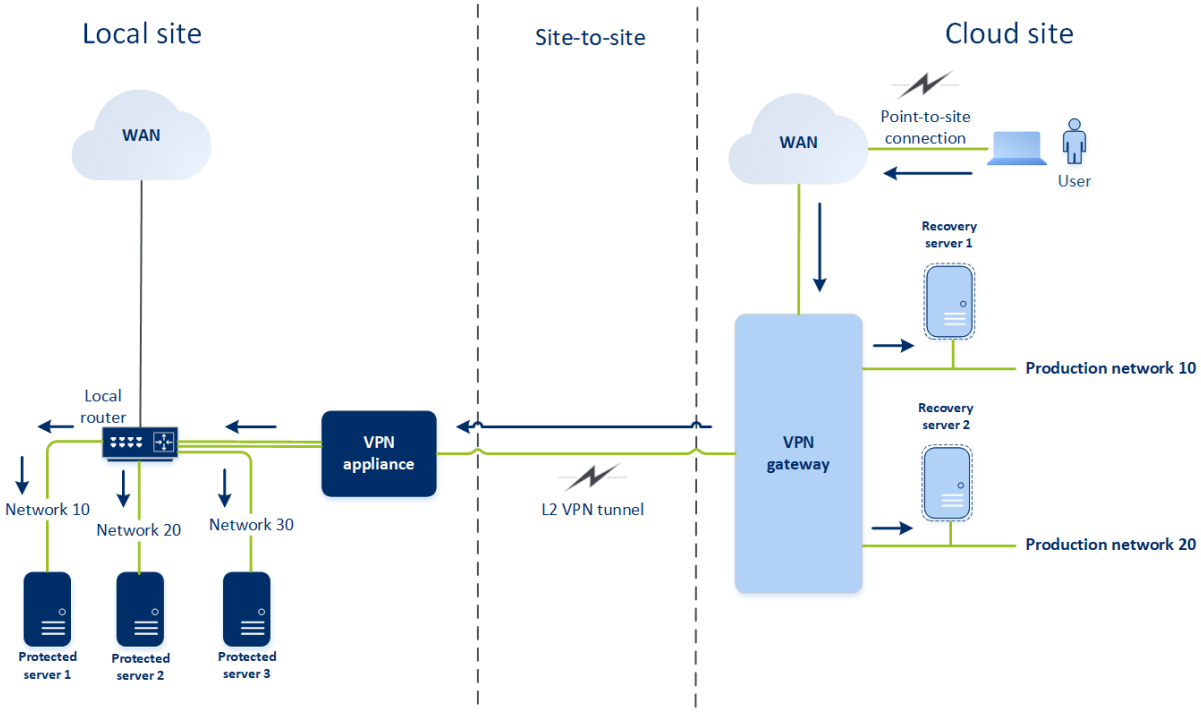
Una connessione da punto a sito è una connessione sicura dall'esterno che usa i dispositivi endpoint (ad esempio un computer o laptop) per collegarsi al cloud e ai siti locali tramite una VPN. Sarà disponibile dopo aver stabilito la connessione Open VPN al sito Cyber Disaster Recovery Cloud. Questo tipo di connessione è utile nei seguenti casi:

- In molte aziende, i servizi aziendali e le risorse web sono disponibili solo tramite la rete aziendale. La connessione da punto a sito consente di connettersi in sicurezza al sito locale.
- In caso di emergenza, quando un carico di lavoro viene trasferito al sito cloud e la rete locale non è attiva, potrebbe essere necessario accedere direttamente ai server cloud. Ciò è possibile tramite la connessione da punto a sito al sito cloud.

Per la connessione da punto a sito al sito locale, è necessario installare l'appliance VPN nel sito locale, configurare la connessione da sito a sito, e quindi la connessione da punto a sito al sito locale. Ciò consentirà al personale da remoto di accedere alla rete aziendale tramite la VPN L2.

Lo schema seguente mostra il sito locale, il sito cloud e le comunicazioni tra i server evidenziate in verde. Il tunnel VPN L2 connette i siti cloud e locale. Quando un utente stabilisce una connessione da punto a sito, le comunicazioni al sito locale avvengono tramite il sito cloud.

© Acronis International GmbH, 2003-2024



La configurazione da punto a sito utilizza i certificati per autenticare il client VPN. Per l'autenticazione sono utilizzate credenziali utente aggiuntive. Notare quanto segue relativamente alla connessione da punto a sito al sito locale:

- Gli utenti devono utilizzare le proprie credenziali Cyber Protect Cloud per autenticarsi al client VPN. Devono avere un ruolo utente di "Amministratore dell'azienda" o "Cyber Protection".
- Se la configurazione Open VPN è stata rigenerata, è necessario fornire la configurazione aggiornata a tutti gli utenti che utilizzano la connessione da punto a sito al sito cloud.

Eliminazione automatica degli ambienti del cliente non utilizzati dal sito cloud

Il servizio Disaster Recovery monitora l'utilizzo degli ambienti del cliente creati per il disaster recovery, eliminandoli automaticamente se non utilizzati.

Per stabilire se il tenant del cliente è attivo, vengono applicati i criteri indicati di seguito:

- Al momento, è presente almeno un server cloud o è stato presente uno o più server cloud negli ultimi sette giorni.

  OPPURE

- L'opzione **Accesso VPN al sito locale** è abilitata e il tunnel Open VPN da sito a sito è stabilito, oppure sono presenti dati segnalati dall'appliance VPN per gli ultimi 7 giorni.

Tutti gli altri tenant vengono considerati inattivi. Per questi tenant, il sistema esegue le attività indicate di seguito:

© Acronis International GmbH, 2003-2024

- Elimina il gateway VPN insieme a tutte le risorse cloud correlate al tenant.
- Annulla la registrazione dell'appliance VPN.

Esegue il rollback dei tenant inattivi, riportandoli allo stato precedente alla configurazione della connessione.

Configurazione della connessione iniziale

In questa sezione vengono descritti alcuni scenari di connessione.

Configurazione della modalità solo cloud

Per configurare una connessione in modalità solo cloud

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Selezionare **Solo cloud** e fare clic su **Configura**.
   In questo modo, il gateway VPN e la rete cloud con l'indirizzo e la maschera definiti verranno distribuiti nel sito cloud.

Per comprendere come gestire le reti nel cloud e configurare le impostazioni del gateway VPN, fare riferimento a "Gestione di reti cloud".

Configurazione di una Open VPN da sito a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Requisiti per l'appliance VPN

Requisiti di sistema

- 1 CPU
- 1 GB RAM
- 8 GB di spazio su disco

Porte

- TCP 443 (in uscita) - per la connessione VPN
- TCP 80 (in uscita) - per l'aggiornamento automatico dell'appliance

Verificare che i firewall e gli altri componenti del sistema di sicurezza della rete consentano le connessioni attraverso queste porte e qualsiasi indirizzo IP.

Configurazione di una connessione Open VPN da sito a sito

L'appliance VPN estende la rete locale al cloud tramite un tunnel VPN sicuro. Questo tipo di connessione viene spesso definita connessione S2S, ovvero da sito a sito. È possibile attenersi alla

© Acronis International GmbH, 2003-2024

procedura seguente o guardare il tutorial video.

Per configurare una connessione tramite l'appliance VPN

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Selezionare **Connessione Open VPN da sito a sito** quindi fare clic su **Configura**.
   Il sistema avvia la distribuzione del gateway VPN nel cloud. L'operazione richiede alcuni minuti. Nel frattempo, è possibile procedere al passaggio successivo.

   Nota
   Il gateway VPN viene fornito senza costi aggiuntivi. Verrà eliminato se la funzionalità di disaster recovery non viene utilizzata o se, ad esempio, né il server primario né quello di ripristino saranno presenti nel cloud per sette giorni.

3. Nella sezione **Appliance VPN**, fare clic su **Download e distribuzione**. A seconda della piattaforma di virtualizzazione in uso, scaricare l'appliance VPN per VMware vSphere o per Microsoft Hyper-V.
4. Distribuire l'appliance e connetterla alle reti di produzione.
   In vSphere, verificare che le opzioni **Modalità promiscua** e **Forged Transmits** siano abilitate e impostare su **Accetta** tutti i commutatori virtuali che connettono l'appliance VPN alle reti di produzione. Per accedere a queste impostazioni, nel client vSphere, selezionare l'host > **Riepilogo** > **Rete**, quindi selezionare il commutatore > **Modifica impostazioni...** > **Sicurezza**.
   In Hyper-V, creare una macchina virtuale di tipo **Generation 1** con 1024 MB di memoria. Si consiglia inoltre di abilitare l'opzione **Memoria dinamica** per il sistema. Una volta creata la macchina virtuale, passare a **Impostazioni** > **Hardware** > **Adattatore di rete** > **Funzionalità avanzate** e selezionare la casella di controllo **Abilita lo spoofing degli indirizzi MAC**.
5. Accendere l'appliance.
6. Aprire la console dell'appliance e accedere con il nome utente e la password "admin/admin".
7. [Facoltativo] Modificare la password.
8. [Facoltativo] Modificare le impostazioni di rete se necessario. Definire l'interfaccia che verrà utilizzata come WAN per la connessione Internet.
9. Registrare l'appliance nel servizio Cyber Protection usando le credenziali dell'amministratore dell'azienda.
   Tali credenziali vengono utilizzate solo una volta per recuperare il certificato. L'URL del data center è predefinito.

   Nota
   Se per l'account è stata configurata l'autenticazione a due fattori, verrà chiesto di inserire il codice TOTP. Se l'autenticazione a due fattori è abilitata ma non configurata per l'account, non è possibile registrare l'appliance VPN. È necessario innanzitutto aprire la pagina di login della console di Cyber Protect e completare la configurazione dell'autenticazione a due fattori per l'account. Per ulteriori dettagli sull'autenticazione a due fattori, consultare il Manuale dell'amministratore del portale di gestione.

© Acronis International GmbH, 2003-2024

Una volta completata la configurazione, l'appliance verrà visualizzata con lo stato **In linea**. L'appliance si connette al gateway VPN e inizia a fornire informazioni sulle reti da tutte le interfacce attive al servizio Cyber Disaster Recovery Cloud. Le interfacce vengono visualizzate nella console di Cyber Protect, in base alle informazioni raccolte dall'appliance VPN.

Configurazione di una connessione VPN IPsec multisito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile configurare una connessione VPN IPsec multisito nei due modi seguenti:

- dalla scheda **Disaster Recovery** > **Connessione**;
- applicando un piano di protezione a uno o più dispositivi e quindi passando in modo manuale dalla connessione Open VPN da sito a sito creata automaticamente a una connessione VPN IPsec multisito, quindi configurando le impostazioni VPN IPsec multisito e riassegnando gli indirizzi IP.

Per configurare una connessione VPN IPsec multisito dalla scheda Connessione

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Nella sezione **Connessione VPN multisito**, fare clic su **Configura**.
   Il gateway VPN viene distribuito nel sito cloud.
3. Configurare le impostazioni VPN IPsec multisito.

Per configurare una connessione VPN IPsec multisito da un piano di protezione

1. Nella console di Cyber Protect, passare a **Dispositivi**.
2. Applicare un piano di protezione a uno o più dispositivi dell'elenco.
   Le impostazioni del server di ripristino e dell'infrastruttura cloud vengono automaticamente configurate per la connessione Open VPN da sito a sito.
3. Passare a **Disaster Recovery** > **Connessione**.
4. Fare clic su **Mostra proprietà**.
5. Fare clic su **Passa a VPN IPsec multisito**.
6. Configurare le impostazioni VPN IPsec multisito.
7. Riassegnare gli indirizzi IP della rete cloud e dei server cloud.

Configurare le impostazioni di VPN IPsec multisito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Dopo aver configurato una VPN IPsec multisito, è necessario configurare le impostazioni del sito cloud e dei siti locali nella scheda **Disaster Recovery** > **Connessione**.

© Acronis International GmbH, 2003-2024

Prerequisiti

- La connessione VPN IPsec multisito è configurata. Per ulteriori informazioni su come configurare la connessione VPN IPsec multisito, vedere "Configurazione di una connessione VPN IPsec multisito" (pag. 772).
- Ogni gateway VPN IPsec locale ha un proprio indirizzo IP pubblico.
- La rete cloud deve essere dotata di un numero sufficiente di indirizzi IP per i server cloud che sono copie dei sistemi protetti (nella rete di produzione), e per i server di ripristino (con uno o due indirizzi IP a seconda delle esigenze).
- [Se si utilizza il firewall tra i siti locali e il sito cloud] È necessario consentire i seguenti protocolli IP e porte UDP sui siti locali: Protocollo IP ID 50 (ESP), Porta UDP 500 (IKE) e porta UDP 4500.
- La configurazione NAT-T nei siti locali è disabilitata.

Per configurare una connessione VPN IPsec multisito

1. Aggiungere una o più reti al sito cloud.
   a. Fare clic su **Aggiungi rete**.

      Nota
      Quando si aggiunge una rete cloud, verrà aggiunta automaticamente una rete di test corrispondente, con lo stesso indirizzo e maschera di rete, per l'esecuzione dei failover di prova. I server cloud nella rete di prova avranno gli stessi indirizzi IP della rete di produzione cloud. Se è necessario accedere a un server cloud dalla rete di produzione durante un failover di prova, assegnare un secondo indirizzo IP di prova al momento della creazione del server di ripristino.

   b. Nel campo **Indirizzo di rete**, digitare l'indirizzo IP della rete.
   c. Nel campo **Maschera di rete**, digitare la maschera della rete.
   d. Fare clic su **Aggiungi**.
2. Configurare le impostazioni di ogni sito locale da connettere al sito cloud, seguendo le raccomandazioni per i siti locali. Per ulteriori informazioni su queste raccomandazioni, consultare "Raccomandazioni generiche per i siti locali" (pag. 774).
   a. Fare clic su **Aggiungi Connessione**.
   b. Inserire un nome per il gateway VPN locale.
   c. Inserire l'indirizzo IP pubblico del gateway VPN locale.
   d. [Facoltativo] Inserire una descrizione per il gateway VPN locale.
   e. Fare clic su **Avanti**.
   f. Nel campo **Chiave precondivisa**, digitare la chiave precondivisa oppure fare clic su **Genera una chiave precondivisa** per utilizzare un valore generato automaticamente.

© Acronis International GmbH, 2003-2024

Nota
È necessario utilizzare la stessa chiave precondivisa per i gateway VPN locale e cloud.

g. Fare clic su **Impostazioni di sicurezza IPsec/IKE** per configurare tali impostazioni. Per ulteriori informazioni sulle impostazioni che è possibile configurare, vedere "Impostazioni di sicurezza IPsec/IKE" (pag. 775).

Nota
È possibile utilizzare le impostazioni predefinite, che vengono compilate automaticamente, oppure utilizzare valori personalizzati. Sono supportate solo le connessioni con protocollo IKEv2. L'**Azione all'avvio** predefinita quando si stabilisce la VPN è **Aggiungi** (il gateway VPN locale inizializza la connessione), ma è possibile modificarla in **Avvia** (il gateway VPN cloud inizializza la connessione) oppure in **Indirizza** (adatta ai firewall che supportano le opzioni di routing).

h. Configurare i **Criteri di rete**.
I criteri di rete specificano le reti alle quali si connette la VPN IPsec. Digitare l'indirizzo IP e la maschera della rete utilizzando il formato CIDR. I segmenti di rete locali e cloud non devono sovrapporsi.

i. Fare clic su **Salva**.

Raccomandazioni generiche per i siti locali

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Durante la configurazione dei siti locali per la connessione VPN IPsec multisito, tenere conto delle seguenti raccomandazioni:

- Per ogni fase IKE, impostare almeno uno dei valori configurati nel sito cloud per i seguenti parametri: Algoritmo di crittografia, Algoritmo hash, Numeri del gruppo Diffie-Hellman.
- Abilitare Perfect Forward Secrecy con almeno uno dei valori dei numeri del gruppo Diffie-Hellman configurato nel sito cloud per IKE Phase 2.
- Configurare lo stesso valore per la **Permanenza** di IKE Phase 1 e IKE Phase 2, come nel sito cloud.
- Le configurazioni con attraversamento NAT (NAT-T) non sono supportate. Disabilitare la configurazione NAT-T nel sito locale. Altrimenti, non sarà possibile negoziare l'ulteriore incapsulamento UDP.
- Configurando l'**Azione all'avvio** si definisce il lato che inizializza la connessione. Il valore predefinito **Aggiungi** indica che il sito locale inizializza la connessione e che il sito cloud attende l'inizializzazione della connessione. Cambiare il valore in **Avvio** per fare in modo che sia il sito cloud a inizializzare la connessione, oppure in **Indirizza** per fare in modo che entrambi i lati possano inizializzare la connessione (quest'opzione è adatta ai firewall che supportano l'opzione di routing).

© Acronis International GmbH, 2003-2024

Per ulteriori informazioni ed esempi di configurazione per diverse soluzioni, consultare:

- Questa serie di articoli della Knowledge Base
- Questo tutorial video

Impostazioni di sicurezza IPsec/IKE

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

La tabella seguente include informazioni dettagliate sui parametri di sicurezza IPsec/IKE.

Parametro	Descrizione
Algoritmo di crittografia	L'algoritmo di crittografia da utilizzare per garantire che i dati non siano visualizzabili quando in transito. Per impostazione predefinita, tutti gli algoritmi sono selezionati. È necessario configurare almeno uno degli algoritmi selezionati nel dispositivo gateway locale per ogni fase IKE.
Algoritmo di hash	L'algoritmo di hash da utilizzare per verificare l'integrità e l'autenticità dei dati. Per impostazione predefinita, tutti gli algoritmi sono selezionati. È necessario configurare almeno uno degli algoritmi selezionati nel dispositivo gateway locale per ogni fase IKE.
Numeri del gruppo Diffie-Hellman	I numeri del gruppo Diffie-Hellman definiscono la sicurezza delle chiavi utilizzate nel processo IKE (Internet Key Exchange). I numeri di gruppo più elevati sono più sicuri ma richiedono più tempo per l'elaborazione della chiave. Per impostazione predefinita, tutti i gruppi sono selezionati. È necessario configurare almeno uno dei gruppi selezionati nel dispositivo gateway locale per ogni fase IKE.
Permanenza (in secondi)	Il valore della permanenza determina la durata di un'istanza di connessione con un insieme di chiavi di crittografia/autenticazione per i pacchetti utente, dalla riuscita della negoziazione alla scadenza. Intervallo per la fase 1: 900-28800 secondo con valore predefinito 28800. Intervallo per la fase 2: 900-3600 secondi con

© Acronis International GmbH, 2003-2024

Parametro	Descrizione
	valore predefinito 3600. La permanenza nella fase 2 deve essere inferiore alla permanenza nella fase 1. La connessione viene nuovamente negoziata tramite il canale di reimpostazione delle chiavi prima della sua scadenza; consultare **Tempo di margine di reimpostazione di nuova chiave**. Se il lato locale e quello remoto entrano in conflitto sulla durata della permanenza, sul lato con la permanenza più lunga si avrà un accumulo di connessioni sostituite. Vedere anche **Tempo di margine di reimpostazione di nuova chiave** e **Fuzz di reimpostazione della chiave**.
Tempo di margine di reimpostazione della chiave (secondi)	Il tempo di margine in secondi prima della scadenza della connessione o del canale di reimpostazione della chiave, durante il quale il lato locale della connessione VPN tenta di negoziare una sostituzione. Il tempo esatto di reimpostazione della chiave viene selezionato in maniera casuale in base al valore di **Fuzz di reimpostazione della nuova chiave.** È rilevante solo a livello locale, non è necessario che il valore sia concordato con il lato remoto. Intervallo: 900-3600 secondi. Il valore predefinito è 3600.
Intervallo della finestra di riproduzione (pacchetti)	Dimensione della finestra di riproduzione IPsec per questa connessione. Il valore predefinito -1 utilizza il valore configurato con il comando charon.replay_window nel file strongswan.conf. Valori superiori a 32 sono supportati solo quando si utilizza il backend Netlink. Il valore 0 disabilita la protezione della riproduzione IPsec.
Fuzz di reimpostazione della chiave (%)	Valore che indica la percentuale massima di aumento casuale dei valori di marginbyte, marginpacket e margintime per randomizzare gli intervalli di reimpostazione della chiave (importante per gli host con molte connessioni). Il valore del fuzz di reimpostazione della chiave può superare 100%. Il valore di marginTYPE, dopo

© Acronis International GmbH, 2003-2024

Parametro	Descrizione
	l'aumento casuale, non deve superare il valore di lifeTYPE, in cui TYPE indica il tipo di byte, packet o time. Il valore 0% disabilita la randomizzazione. È rilevante solo a livello locale, non è necessario che il valore sia concordato con il lato remoto.
Timeout DPD (secondi)	Il periodo di tempo dopo il quale si verifica un timeout DPD (Dead Peer Detection). È possibile specificare un valore pari a 30 o superiore. Il valore predefinito è 30.
Azione timeout DPD	L'azione da intraprendere dopo il verificarsi del timeout DPD. **Riavvia** - Riavvia la sessione quando si verifica il timeout DPD. **Cancella** - Termina la sessione quando si verifica il timeout DPD. **Nessuna** - Non intraprende nessuna azione quando si verifica il timeout DPD.
Azione all'avvio	Determina il lato che inizializza la connessione e definisce il tunnel della connessione VPN. **Aggiungi** - Il gateway VPN locale che inizializza la connessione. **Avvia** - Il gateway VPN cloud che inizializza la connessione. **Indirizza** - Adatta ai gateway VPN che supportano l'opzione di indirizzamento. Il tunnel viene attivato solo quando c'è traffico inizializzato dal gateway VPN locale o dal gateway VPN cloud.

Raccomandazioni per la disponibilità dei Servizi di dominio Active Directory

Se i workload protetti devono eseguire l'autenticazione in un controller di dominio, è consigliabile disporre di un'istanza del controller di dominio Active Directory nel sito di disaster recovery.

Controller di dominio Active Directory per la connessione Open VPN L2

Con la connessione Open VPN L2, gli indirizzi IP dei workload protetti vengono conservati nel sito cloud durante un failover di prova o un failover di produzione. Pertanto, durante un failover di prova o un failover di produzione, il controller di dominio Active Directory avrà lo stesso indirizzo IP del sito locale.

© Acronis International GmbH, 2003-2024

Un DNS personalizzato consente di definire il proprio server DNS personalizzato per tutti i server cloud. Per ulteriori informazioni, consultare "Configurazione di server DNS personalizzati" (pag. 787).

Controller di dominio Active Directory per la connessione VPN IPsec L3

Con la connessione VPN IPsec L3, gli indirizzi IP dei workload protetti non vengono conservati nel sito cloud. Pertanto, prima di eseguire un failover di produzione, è consigliabile disporre di un'istanza aggiuntiva dedicata del controller di dominio Active Directory come server primario nel sito cloud.

Per un'istanza dedicata del controller di dominio Active Directory, configurato come server primario nel sito cloud, sono raccomandate le operazioni indicate di seguito.

- Disattivare Windows Firewall.
- Registrare il server primario al servizio Active Directory.
- Accertarsi che il server primario disponga dell'accesso a Internet.
- Aggiungere la funzionalità Active Directory.

Un DNS personalizzato consente di definire il proprio server DNS personalizzato per tutti i server cloud. Per ulteriori informazioni, consultare "Configurazione di server DNS personalizzati" (pag. 787).

Configurazione dell'accesso VPN remoto da punto a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Se è necessario connettersi al sito locale da remoto, è possibile configurare la connessione da punto a sito al sito locale. È possibile attenersi alla procedura seguente o guardare il tutorial video.

Prerequisiti

- La connessione Open VPN da sito a sito è configurata.
- L'appliance VPN è installata nel sito locale.

Per configurare la connessione da punto a sito al sito locale

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Abilitare l'opzione **Accesso VPN al sito locale**.
4. Verificare che l'utente che desidera stabilire la connessione da punto a sito al sito locale disponga di:
   - un account utente in Cyber Protect Cloud. Queste credenziali sono utilizzate per l'autenticazione nel client VPN. In caso contrario, creare un account utente in Cyber Protect

© Acronis International GmbH, 2003-2024

Cloud.

- un ruolo utente di "Amministratore dell'azienda" o "Cyber Protection".

5. Configurazione del cliente OpenVPN:
   a. Scaricare il client OpenVPN versione 2.4.0 o successive dalla posizione seguente https://openvpn.net/community-downloads/.
   b. Installare il client OpenVPN sul sistema dal quale connettersi al sito locale.
   c. Fare clic su **Scarica configurazione per OpenVPN**. Il file di configurazione è valido per gli utenti dell'organizzazione con il ruolo utente "Amministratore società" o "Cyber Protection".
   d. Importare la configurazione scaricata in OpenVPN.
   e. Accedere al client OpenVPN con le credenziali utente Cyber Protect Cloud (vedere il precedente passaggio 4).
   f. [Facoltativo] Se l'autenticazione a due fattori viene abilitata per l'organizzazione, è necessario fornire il codice TOTP temporaneo.

Importante
Se è stata abilitata l'autenticazione a due fattori per l'account, è necessario rigenerare il file di configurazione e rinnovarlo per i client OpenVPN esistenti. Gli utenti devono accedere nuovamente a Cyber Protect Cloud per configurare l'autenticazione a due fattori per i propri account.

Gli utenti potranno collegarsi ai sistemi sul sito locale.

Gestione della rete

In questa sezione vengono descritti alcuni esempi di gestione della rete.

Gestione delle reti

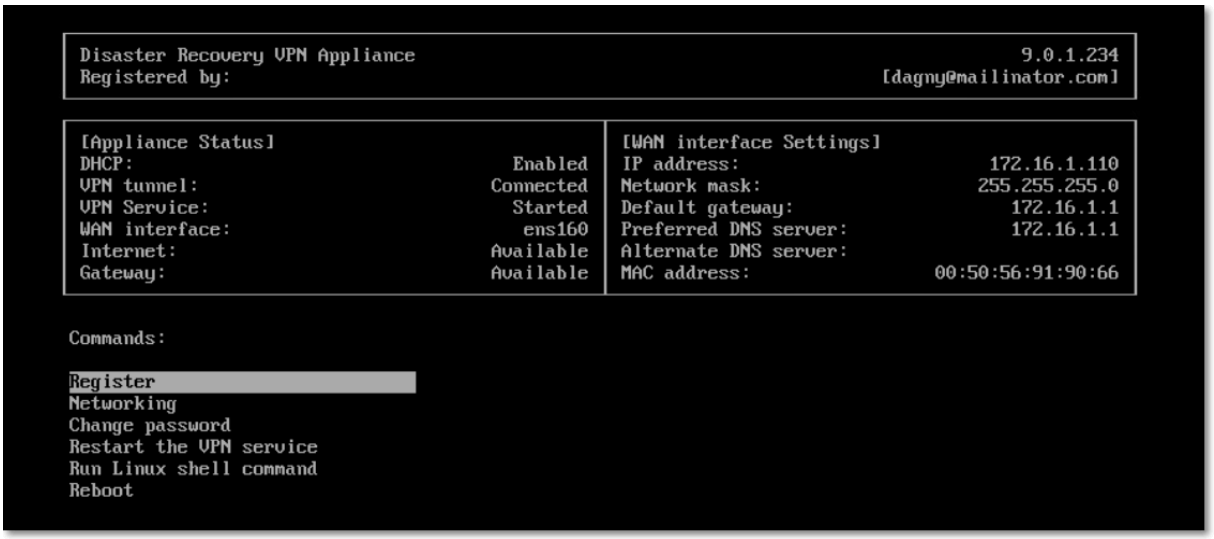
Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

Connessione Open VPN da sito a sito

Per aggiungere una rete al sito locale ed estenderla al cloud

1. Nell'appliance VPN, configurare la nuova interfaccia di rete con la rete locale che si desidera estendere al cloud.
2. Accedere alla console dell'appliance VPN.
3. Nella sezione della **rete**, configurare le impostazioni di rete della nuova interfaccia.

© Acronis International GmbH, 2003-2024



L'appliance VPN inizia a fornire informazioni sulle reti da tutte le interfacce attive al servizio Cyber Disaster Recovery Cloud. Le interfacce vengono visualizzate nella console di Cyber Protect, in base alle informazioni raccolte dall'appliance VPN.

Per eliminare una rete estesa al cloud

1. Accedere alla console dell'appliance VPN.
2. Nella sezione della **rete**, selezionare l'interfaccia da eliminare e quindi fare clic su **Elimina impostazioni di rete**.
3. Confermare l'operazione.

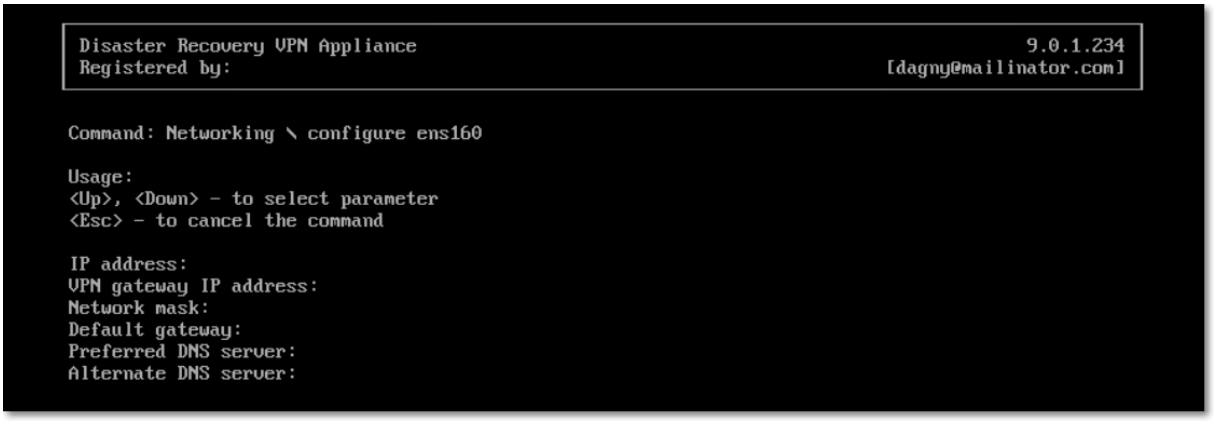
L'estensione della rete locale al cloud tramite un tunnel VPN sicuro verrà eliminata. Tale rete funzionerà come segmento cloud indipendente. Se l'interfaccia è utilizzata per il passaggio del traffico da/verso il sito cloud, tutte le connessioni di rete da/verso il sito cloud verranno disconnesse.

Per modificare i parametri di rete

1. Accedere alla console dell'appliance VPN.
2. Nella sezione della **rete**, selezionare l'interfaccia da modificare.
3. Fare clic su **Modifica impostazioni di rete**.
4. Selezionare una delle due opzioni:
   - Per la configurazione automatica tramite DHCP, fare clic su **Uso del DHCP**. Confermare l'operazione.
   - Per la configurazione manuale della rete, fare clic su **Configurazione dell'indirizzo IP statico**. Le seguenti impostazioni sono disponibili per la modifica:
     - **Indirizzo IP**: l'indirizzo IP dell'interfaccia nella rete locale.
     - **Indirizzo IP del gateway VPN**: lo speciale indirizzo IP riservato al segmento della rete cloud per l'appropriato funzionamento del servizio Cyber Disaster Recovery Cloud.
     - **Maschera di rete**: maschera di rete della rete locale.

© Acronis International GmbH, 2003-2024

- **Gateway predefinito**: gateway predefinito sul sito locale.
- **Server DNS preferito**: server DNS primario sul sito locale.
- **Server DNS alternativo**: server DNS secondario sul sito locale.



- Apportare le modifiche necessarie e confermarle facendo clic su Invio.

Modalità solo cloud

È possibile avere un massimo di 23 reti nel cloud.

Per aggiungere una nuova rete cloud

1. Passare a **Disaster Recovery** > **Connessione**.
2. In **Sito cloud**, fare clic su **Aggiungere una rete cloud**.
3. Definire i parametri della rete cloud: indirizzo e maschera. Al termine, fare clic su **Fine**.

La rete cloud aggiuntiva, con l'indirizzo e la maschera definiti, verranno creati nel sito cloud.

Per eliminare una rete cloud

Nota
Non è possibile eliminare una rete cloud se contiene anche un solo un server cloud. Eliminare innanzitutto il server cloud e quindi eliminare la rete.

1. Passare a **Disaster Recovery** > **Connessione**.
2. In **Sito cloud**, fare clic sull'indirizzo di rete che si desidera eliminare.
3. Fare clic su **Elimina** e confermare l'operazione.

Per modificare i parametri della rete cloud

1. Passare a **Disaster Recovery** > **Connessione**.
2. In **Sito cloud**, fare clic sull'indirizzo di rete che si desidera modificare.
3. Fare clic su **Modifica**.
4. Modificare l'indirizzo e la maschera della rete, quindi fare clic su **Fine**.

© Acronis International GmbH, 2003-2024

Nuova configurazione dell'indirizzo IP

Affinché le prestazioni di disaster recovery siano adeguate, gli indirizzi IP assegnati ai server locale e cloud devono essere coerenti. In caso di incoerenza o mancata corrispondenza tra gli indirizzi IP, in **Disaster Recovery** > **Connessione** verrà visualizzato un punto esclamativo accanto alla rete corrispondente.

Di seguito sono elencate alcune delle cause note di incoerenza tra indirizzi IP:

1. Un server di ripristino è stato migrato da una rete all'altra oppure la maschera di rete della rete cloud è stata modificata. Di conseguenza, i server cloud ottengono gli indirizzi IP da reti alle quali non sono connessi.
2. Il tipo di connessione è stato modificato da Senza Connessione da sito a sito in Connessione da sito a sito. Di conseguenza, un server locale risulta collocato in una rete diversa da quella creata per il sito di ripristino nel sito cloud.
3. Il tipo di connessione è stato modificato da Open VPN da sito a sito in VPN IPsec multisito, o da VPN IPsec multisito in Open VPN da sito a sito. Per ulteriori informazioni su questo scenario, vedere Passaggio da una connessione a un'altra e Riassegnazione di indirizzi IP.
4. Modifica dei seguenti parametri di rete nel sito dell'appliance VPN:
   - Aggiunta di un'interfaccia tramite le impostazioni di rete
   - Modifica manuale della maschera di rete tramite le impostazioni dell'interfaccia
   - Modifica della maschera di rete tramite DHCP
   - Modifica dell'indirizzo e della maschera di rete tramite le impostazioni dell'interfaccia
   - Modifica dell'indirizzo e della maschera di rete tramite DHCP

   Come conseguenza delle azioni sopra elencate, la rete nel sito cloud può diventare un sottoinsieme o soprainsieme della rete locale, oppure l'interfaccia dell'appliance VPN può fornire le stesse impostazioni di rete per diverse interfacce.

Per risolvere i problemi delle impostazioni di rete

1. Fare clic sulla rete che richiede una nuova configurazione dell'indirizzo IP.
   Viene visualizzato l'elenco dei server presenti nella rete selezionata, con il relativo stato e gli indirizzi IP. I server le cui impostazioni di rete non sono coerenti sono contrassegnati da un punto esclamativo.
2. Per modificare le impostazioni di rete per un server fare clic su **Vai al server**. Per modificare le impostazioni di rete per tutti i server contemporaneamente, fare clic su **Modifica** nella sezione di notifica.
3. Modificare gli indirizzi IP come necessario definendoli nei campi **Nuovo IP** e **Nuovo IP di prova**.
4. Al termine, fare clic su **Conferma**.

Spostare i server in una rete adatta

Quando si crea un piano di protezione di disaster recovery e si applica ai dispositivi selezionati, il sistema controlla gli indirizzi IP dei dispositivi e se non sono presenti reti cloud adatte all'indirizzo IP,

© Acronis International GmbH, 2003-2024

crea automaticamente reti cloud idonee. Per impostazione predefinita vengono configurate con gli intervalli massimi raccomandati da IANA per l'uso privato (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). È possibile limitare la rete modificando la maschera di rete.

Nel caso in cui i dispositivi selezionati siano presenti su più reti locali, la rete nel sito cloud può diventare un superinsieme di reti locali. In questo caso, per riconfigurare le reti cloud:

1. Fare clic sulla rete cloud che richiede la riconfigurazione della dimensione della rete e quindi su **Modifica**.
2. Riconfigurare la dimensione della rete con le impostazioni corrette.
3. Creare altre le reti necessarie.
4. Fare clic sull'icona della notifica accanto al numero dei dispositivi connessi alla rete.
5. Fare clic su **Passare a una rete adatta**.
6. Selezionare i server da spostare sulle reti adatte, quindi fare clic su **Sposta**.

Gestione delle impostazioni dell'appliance VPN

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Nella console di Cyber Protect (**Disaster Recovery** > **Connessione**) è possibile:

- Scaricare i file di registro.
- Annullare la registrazione dell'appliance (se è necessario ripristinare le impostazioni dell'appliance VPN o passare alla modalità di connessione solo cloud).

Per accedere a queste impostazioni, fare clic sull'**i**cona nella sezione **Appliance VPN**.

Nella console dell'appliance VPN è possibile:

- Modificare la password dell'appliance.
- Visualizzare/modificare le impostazioni di rete e definire l'interfaccia che verrà utilizzata come WAN per la connessione Internet.
- Registrare/modificare l'account di registrazione (ripetendo la registrazione).
- Riavviare il servizio VPN.
- Riavviare l'appliance VPN.
- Eseguire il comando della shell Linux (solo per operazioni avanzate di soluzione dei problemi).

Reinstallazione del gateway VPN

Se si verifica un problema con il gateway VPN che non si riesce a risolvere, è possibile reinstallarlo. I possibili problemi includono:

© Acronis International GmbH, 2003-2024

- Il gateway VPN è nello stato **Errore**.
- Il gateway VPN è nello stato **In sospeso** da molto tempo.
- Lo stato del gateway VPN è impossibile da determinare da molto tempo.

La procedura di reinstallazione del gateway VPN include le seguenti azioni automatiche: eliminazione completa della virtual machine del gateway VPN esistente, installazione di una nuova virtual machine dal modello e applicazione delle impostazioni del gateway VPN precedente sulla nuova virtual machine.

Prerequisiti:

È necessario configurare uno dei tipi di connessione al sito cloud.

Per reinstallare il gateway VPN

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic sull'icona ingranaggio del gateway VPN e selezionare **Reinstalla gateway VPN**.
3. Nella finestra di dialogo **Reinstalla gateway VPN**, inserire il login.
4. Fare clic su **Reinstalla**.

Abilitazione e disabilitazione della connessione da sito a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile abilitare la connessione da sito a sito nei seguenti casi:

- Se è necessario che i server cloud nel sito cloud comunichino con i server del sito locale.
- Dopo un failover nel cloud, l'infrastruttura locale viene ripristinata e si desidera eseguire il failback dei server nel sito locale.

Per abilitare la connessione da sito a sito

1. Passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**, quindi abilitare l'opzione **Connessione da sito a sito**.

Viene abilitata la connessione VPN da sito a sito tra i siti locale e cloud. Il servizio Cyber Disaster Recovery Cloud ottiene le impostazioni di rete dall'appliance VPN ed estende le reti locali al sito cloud.

Se non è necessario che i server cloud nel sito cloud comunichino con i server del sito locale, è possibile disabilitare la connessione da sito a sito.

Per disabilitare la connessione da sito a sito

1. Passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**, quindi disabilitare l'opzione **Connessione da sito a sito**.

© Acronis International GmbH, 2003-2024

Il sito locale verrà scollegato dal sito cloud.

Passaggio al tipo di connessione da sito a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile passare con facilità da una connessione Open VPN da sito a sito a una connessione VPN IPsec multisito, e viceversa.

Quando si modifica il tipo di connessione, le connessioni VPN attive vengono eliminate, mentre vengono conservate le configurazioni della rete e dei server cloud. È tuttavia necessario riassegnare gli indirizzi IP delle reti e dei server cloud.

La tabella seguente confronta le caratteristiche di base della connessione Open VPN da sito a sito e della connessione VPN IPsec multisito.

	Open VPN da sito a sito	VPN IPsec multisito
Supporto per il sito locale	Singolo	Singolo, multiplo
Modalità Gateway VPN	L2 Open VPN	L3 IPsec VPN
Segmenti di rete	Estende la rete locale alla rete cloud	I segmenti delle reti locali e delle reti cloud non devono sovrapporsi
Supporta l'accesso da punto a sito al sito locale	Sì	No
Supporta l'accesso da punto a sito al sito cloud	Sì	Sì
Richiede un elemento dell'offerta IP pubblico	No	Sì

Per passare da una connessione Open VPN da sito a sito a una connessione VPN IPsec multisito

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Fare clic su **Passa a VPN IPsec multisito**.
4. Fare clic su **Riconfigura**.
5. Riassegnare gli indirizzi IP della rete cloud e dei server cloud.
6. Configurare le impostazioni della connessione IPsec multisito.

Per passare da una connessione VPN IPsec multisito a una connessione Open VPN da sito a sito

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Fare clic su **Passa a Open VPN da sito a sito**.
4. Fare clic su **Riconfigura**.
5. Riassegnare gli indirizzi IP della rete cloud e dei server cloud.
6. Configurare le impostazioni della connessione da sito a sito.

Riassegnazione di indirizzi IP

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È necessario riassegnare gli indirizzi IP delle reti cloud e dei server cloud per poter completare la configurazione nei casi indicati di seguito:

- Il tipo di connessione è stato modificato da Open VPN da sito a sito in VPN IPsec multisito, o al contrario.
- Dopo aver applicato un piano di protezione (se la connessione VPN IPsec multisito è configurata).

Per riassegnare l'indirizzo IP di una rete cloud

1. Nella scheda **Connessione**, fare clic sull'indirizzo IP della rete cloud.
2. Nel menu a comparsa **Rete**, fare clic su **Modifica**.
3. Digitare il nuovo indirizzo e la nuova maschera di rete.
4. Fare clic su **Fine**.

Dopo aver riassegnato l'indirizzo IP di una rete cloud, è necessario riassegnare i server cloud che appartengono alla rete cloud riassegnata.

Per riassegnare l'indirizzo IP di un server

1. Nella scheda **Connessione**, fare clic sull'indirizzo IP del server nella rete cloud.
2. Nel menu a comparsa **Server**, fare clic su **Modifica indirizzo IP**.
3. Nel menu a comparsa **Modifica indirizzo IP**, digitare il nuovo indirizzo IP del server, o utilizzare l'indirizzo IP generato automaticamente che fa parte della rete cloud riassegnata.

   Nota
   Cyber Disaster Recovery Cloud assegna automaticamente gli indirizzi IP dalla rete cloud a tutti i server cloud che erano parte della rete cloud prima della riassegnazione dell'indirizzo IP di rete. È possibile utilizzare gli indirizzi IP suggeriti per riassegnare in una sola volta gli indirizzi IP di tutti i server cloud.

4. Fare clic su **Conferma**.

© Acronis International GmbH, 2003-2024

Configurazione di server DNS personalizzati

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Quando si configura una connessione, Cyber Disaster Recovery Cloud crea l'infrastruttura della rete cloud. Il server DHCP cloud assegna automaticamente i server DNS predefiniti ai server di ripristino e ai server primari; è tuttavia possibile modificare le impostazioni predefinite e configurare server DNS personalizzati. Le nuove impostazioni DNS verranno applicate al momento della successiva richiesta inviata al server DHCP.

Prerequisiti:

È necessario configurare uno dei tipi di connessione al sito cloud.

Per configurare un server DNS personalizzato

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Fare clic su **Impostazioni predefinite (fornite dal sito cloud)**.
4. Selezionare **Server personalizzati**.
5. Digitare l'indirizzo IP del server DNS.
6. [Facoltativo] Se si desidera aggiungere un altro server DNS, fare clic su **Aggiungi** e digitare l'indirizzo IP del server DNS.

   Nota
   Dopo aver aggiunto i server DNS personalizzati, è possibile aggiungere anche i server DNS predefiniti. In questo modo, se i server DNS non sono disponibili Cyber Disaster Recovery Cloud utilizzerà i server DNS predefiniti.

7. Fare clic su **Fine**.

Eliminazione di server DNS personalizzati

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile eliminare i server DNS dall'elenco dei server DNS personalizzati.

Prerequisiti:

I server DNS personalizzati sono configurati.

© Acronis International GmbH, 2003-2024

Per eliminare un server DNS personalizzato

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Fare clic su **Server personalizzati**.
4. Fare clic sull'icona di eliminazione accanto al server DNS.

   Nota
   L'operazione di eliminazione è disabitata quando è disponibile un solo server DNS personalizzato. Per eliminare tutti i server DNS personalizzati, selezionare **Impostazioni predefinite (fornite dal sito cloud)**.

5. Fare clic su **Fine**.

Configurazione del routing locale

Oltre alle reti locali estese al cloud tramite l'appliance VPN, possono essere presenti altre reti locali non registrate nell'appliance VPN ma contenenti server che devono comunicare con i server cloud. Per stabilire la connessione tra questi server locali e i server cloud, è necessario configurare le impostazioni del routing locale.

Per configurare il routing locale

1. Passare a **Disaster Recovery**>**Connessione**.
2. Fare clic su **Mostra proprietà**, quindi su **Routing locale**.
3. Specificare le reti locali nella notazione CIDR.
4. Fare clic su **Salva**.

I server delle reti locali specificate potranno ora comunicare con i server cloud.

Consentire il traffico DHCP su L2 VPN

Se i dispositivi nel sito locale dell'utente ottengono i propri indirizzi IP da un server DHCP, è possibile proteggere tale server DHCP con la funzionalità di Disaster Recovery, eseguirne il failover nel cloud e quindi consentire che il traffico DHCP venga eseguito su L2 VPN. In questo modo, il server DHCP verrà eseguito nel cloud, ma continuerà ad assegnare gli indirizzi IP ai dispositivi locali.

Prerequisiti:

È necessario configurare il tipo di connessione al sito cloud Site-to-site L2 VPN.

Per consentire il traffico DHCP tramite la connessione L2 VPN

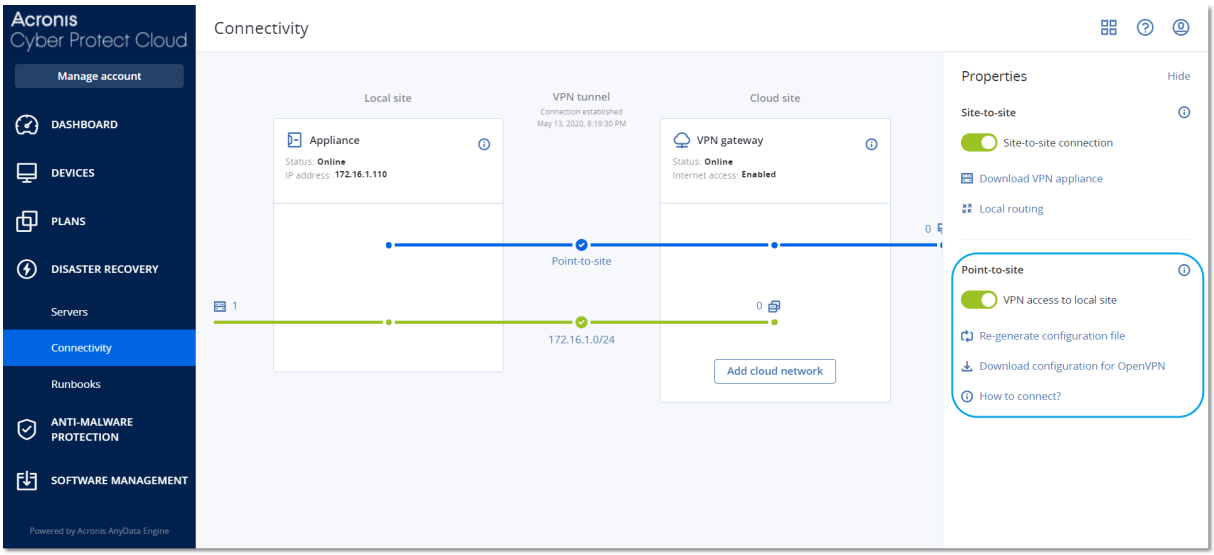
1. Passare alla scheda **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Abilitare l'opzione **Consente il traffico DHCP su L2 VPN**.

© Acronis International GmbH, 2003-2024

Gestione delle impostazioni di connessioni da punto a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**, quindi fare clic su **Mostra proprietà** nell'angolo in alto a destra.



Accesso VPN al sito locale

Questa opzione viene utilizzata per gestire l'accesso VPN al sito locale. È abilitata per impostazione predefinita. Se viene disabilitata, l'accesso da punto a sito al sito locale non verrà consentito.

Scarica configurazione per OpenVPN

Questa opzione consente di scaricare il file di configurazione del client OpenVPN. Il file è necessario per stabilire una connessione da punto a sito con il sito cloud.

Rigenera file di configurazione

Questa opzione consente di rigenerare il file di configurazione del client OpenVPN.

L'operazione è necessaria nei seguenti casi:

- Se si sospetta che il file di configurazione sia danneggiato.
- Se l'autenticazione a due fattori è stata abilitata per l'account dell'utente.

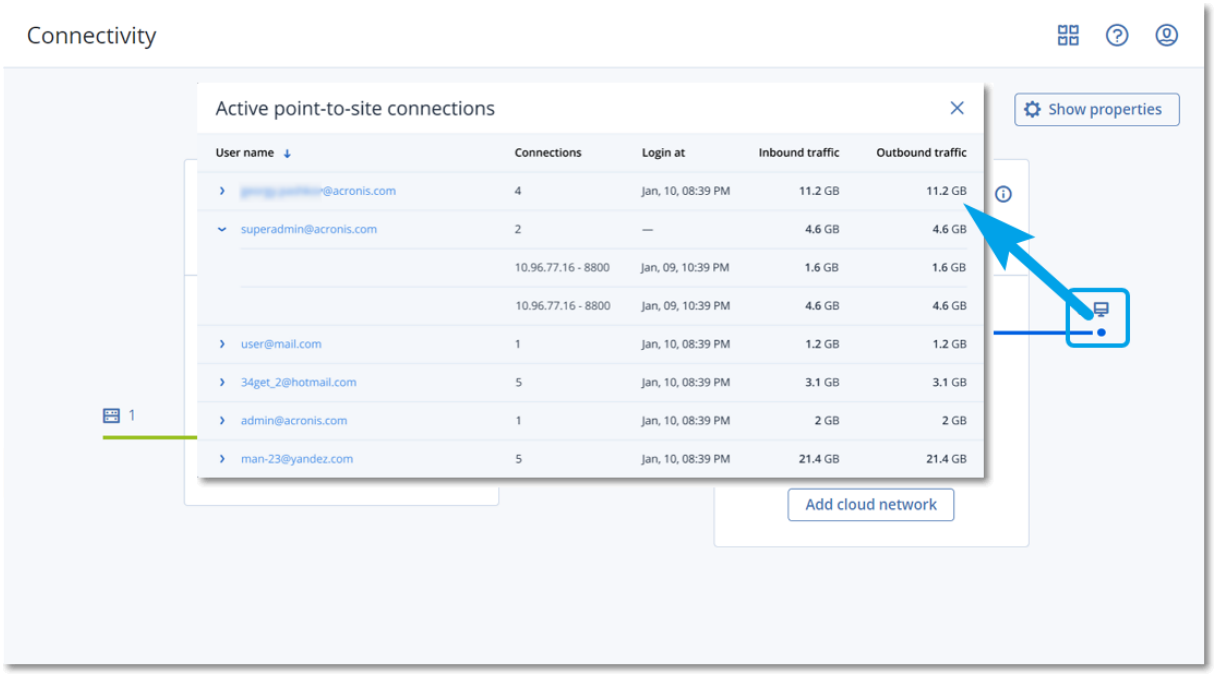
Non appena completato l'aggiornamento del file di configurazione, non sarà più possibile connettersi utilizzando il file di configurazione precedente. Accertarsi di distribuire il nuovo file agli utenti autorizzati all'uso della connessione da punto a sito.

© Acronis International GmbH, 2003-2024

Connessioni da punto a sito attive

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Tutte le connessioni attive da punto a sito sono visualizzate in **Disaster Recovery** > **Connessione**. Fare clic sull'icona del sistema sulla linea blu **Da punto a sito** per visualizzare informazioni dettagliate sulle connessioni attive da punto a sito raggruppate in base al nome dell'utente.



Lavorare con i registri

Disaster Recovery acquisisce i registri dall'appliance VPN e dal gateway VPN. Questi registri vengono salvati come file txt e quindi compressi in un archivio zip. È possibile scaricare ed estrarre l'archivio e utilizzare le informazioni per attività di soluzione dei problemi o di monitoraggio.

L'elenco seguente descrive i file di registro contenuti nell'archivio zip e le informazioni che contengono.

`dnsmasq.config.txt` - Il file contiene informazioni sulla configurazione del servizio che fornisce gli indirizzi DNS e DHCP.

`dnsmsq.leases.txt` - Il file contiene informazioni sulle assegnazioni dell'indirizzo DHCP corrente.

`dnsmasq_log.txt` - Il file contiene i registri del servizio dnsmasq.

`ebtables.txt` - Il file contiene informazioni sulle tabelle del firewall.

`free.txt` - Il file contiene informazioni sulla memoria disponibile.

© Acronis International GmbH, 2003-2024

`ip.txt` - Il file contiene i registri derivanti dalla configurazione delle interfacce di rete, inclusi i nomi che possono essere utilizzati nella configurazione delle impostazioni di **Acquisizione pacchetti di rete**.

`NetworkManager_log.txt` - Il file contiene i registri derivanti dal servizio NetworkManager.

`NetworkManager_status.txt` - Il file contiene informazioni sullo stato del servizio NetworkManager.

`openvpn@p2s_log.txt` - Il file contiene i registri derivanti dal servizio OpenVPN.

`openvpn@p2s_status.txt` - Il file contiene informazioni sullo stato dei tunnel VPN.

`ps.txt` - Il file contiene informazioni sui processi attualmente in esecuzione nel gateway VPN o nell'appliance VPN.

`resolf.conf.txt` - Il file contiene informazioni sulla configurazione dei server DNS.

`routes.txt` - Il file contiene informazioni sulle route di networking.

`uname.txt` - Il file contiene informazioni sulla versione corrente del kernel del sistema operativo.

`uptime.txt` - Il file contiene informazioni sulla lunghezza del periodo durante il quale non è avvenuto alcun riavvio del sistema operativo.

`vpnserver_log.txt` - Il file contiene registri derivanti dal servizio VPN.

`vpnserver_status.txt` - Il file contiene informazioni sullo stato del server VPN.

Per ulteriori informazioni sui file di registro specifici per la connessione VPN IPsec, vedere "File di registro della VPN IPsec multisito" (pag. 795).

Scaricare i registri dell'appliance VPN

È possibile scaricare ed estrarre l'archivio che contiene i registri dell'appliance VPN, e utilizzare le informazioni per attività di soluzione dei problemi o di monitoraggio.

Per scaricare i registri dell'appliance VPN

1. Nella pagina **Connessione**, fare clic sull'icona ingranaggio accanto all'appliance VPN.
2. Fare clic su **Scarica registro**.
3. [Facoltativo] Selezionare **Acquisizione pacchetti di rete** e configurare le impostazioni. Per ulteriori informazioni, consultare "Acquisizione di pacchetti di rete" (pag. 792).
4. Fare clic su **Fine**.
5. Non appena l'archivio zip è pronto per il download, fare clic su **Scarica registro** e salvarlo in locale.

Scaricare i registri del gateway VPN

È possibile scaricare ed estrarre l'archivio che contiene i registri del gateway VPN, e utilizzare le informazioni per attività di soluzione dei problemi o di monitoraggio.

Per scaricare i registri del gateway VPN

© Acronis International GmbH, 2003-2024

1. Nella pagina **Connessione**, fare clic sull'icona ingranaggio accanto al gateway VPN.
2. Fare clic su **Scarica registro**.
3. [Facoltativo] Selezionare **Acquisizione pacchetti di rete** e quindi configurare le impostazioni. Per ulteriori informazioni, consultare "Acquisizione di pacchetti di rete" (pag. 792).
4. Fare clic su **Fine**.
5. Non appena l'archivio zip è pronto per il download, fare clic su **Scarica registro** e salvarlo in locale.

Acquisizione di pacchetti di rete

Per risolvere i problemi e analizzare la comunicazione tra il sito di produzione locale e un server primario o di ripristino, è possibile scegliere di acquisire i pacchetti di rete dal gateway VPN o dall'appliance VPN.

Dopo aver raccolto 32.000 pacchetti di rete o raggiunto il limite temporale, l'acquisizione dei pacchetti di rete si arresta e i risultati vengono scritti in un file .libpcap che viene aggiunto all'archivio zip dei registri.

La tabella seguente fornisce più informazioni sulle impostazioni configurabili dall'utente di **Acquisizione pacchetti di rete**.

Impostazione	Descrizione
Nome interfaccia di rete	L'interfaccia di rete sulla quale acquisire i pacchetti di rete. Se si desidera acquisire i pacchetti di rete su tutte le interfacce di rete, selezionare **Qualsiasi**.
Limite di tempo (in secondi)	Il limite di tempo per l'acquisizione dei pacchetti di rete. È possibile impostare un valore massimo di 1.800.
Filtro	Un filtro ulteriore da applicare ai pacchetti di rete acquisiti. È possibile inserire una stringa contenente protocolli, porte, direzioni e le rispettive combinazioni, separate da uno spazio, come: "and", "or", "not", " (", ") ", "src", "dst", "net", "host", "port", "ip", "tcp", "udp", "icmp", "arp" e "esp". Per utilizzare le parentesi, circoscriverle entro spazi. È anche possibile inserire indirizzi IP e indirizzi di rete, ad esempio "icmp or arp" e "port 67 or 68". Per ulteriori informazioni sui valori che è possibile inserire, vedere la guida in linea di Linux tpcdump.

Soluzione dei problemi della configurazione VPN IPsec

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

© Acronis International GmbH, 2003-2024

Durante la configurazione o l'utilizzo della connessione VPN IPsec possono verificarsi alcuni problemi.

Ulteriori informazioni sui problemi riscontrati sono disponibili nel file di registro IPsec; è anche possibile consultare l'argomento Soluzione dei problemi di configurazione di VPN IPsec per possibili soluzioni ad alcuni dei problemi più comuni.

Soluzione dei problemi di configurazione di VPN IPsec

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

La tabella seguente illustra i problemi più comuni riscontrati durante la configurazione di VPN IPsec, e indica come risolverli.

Problema	Possibile soluzione
Viene visualizzato il seguente messaggio di errore: **Errore di negoziazione IKE Phase 1. Verificare le impostazioni di IPsec IKE nel cloud e nei siti locali.**	Fare clic su **Riprova** e verificare se viene visualizzato un messaggio di errore più specifico. Ad esempio, un messaggio di errore più specifico può indicare una mancata corrispondenza di un algoritmo o una chiave precondivisa errata. **Nota** Per ragioni di sicurezza, alla connessione VPN IPsec si applicano le seguenti limitazioni: • IKEv1 è stato deprecato in RFC8247 e non è più supportato a causa di rischi alla sicurezza. Sono supportate solo le connessioni con protocollo IKEv2. • I seguenti algoritmi di crittografia non sono considerati sicuri e pertanto non sono supportati: DES e 3DES. • I seguenti algoritmi di hash non sono considerati sicuri e pertanto non sono supportati: SHA1 e MD5. • Il numero 2 dei numeri del gruppo Diffie-Hellman non è considerato sicuro pertanto non è supportato.
La connessione tra il sito locale personale e il sito cloud permane nello stato **Connessione in corso**.	Verificare quanto segue: • Che la porta UDP 500 sia aperta (quando è in uso un firewall). • La connessione tra il sito locale e il sito cloud. • La correttezza dell'indirizzo IP del sito locale.

© Acronis International GmbH, 2003-2024

Problema	Possibile soluzione
La connessione tra il sito locale personale e il sito cloud permane nello stato **In attesa di connessione**.	Questo stato è visualizzato quando l'**Azione all'avvio** del sito cloud è impostata su **Aggiungi**, indicando che il sito cloud è in attesa che il sito locale inizializzi la connessione. Inizializzare la connessione dal sito locale.
La connessione tra il sito locale personale e il sito cloud permane nello stato **In attesa di traffico**.	Questo stato è visualizzato quando l'**Azione all'avvio** del sito cloud è impostata su **Indirizza**. Se si è in attesa della connessione dal sito locale, attenersi alla seguente procedura: • Dal sito locale, provare a effettuare il ping della virtual machine nel sito cloud. Si tratta di un comportamento standard necessario per stabilire un tunnel per alcuni servizi, ad esempio Cisco ASA. Modalità Indirizza • Verificare che il sito locale stabilisca un tunnel impostando l'**Azione all'avvio** del sito locale su **Avvia**.
La connessione tra il sito locale personale e il sito cloud è stabilita, ma uno o più dei criteri di rete non sono attivi.	Questo problema può essere dovuto ai seguenti motivi: • Il mapping di rete nel sito IPsec cloud è differente dal mapping di rete del sito locale. Verificare che i mapping di rete e la sequenza dei criteri di rete nei siti locale e cloud corrispondano in modo esatto. • Questo stato è corretto quando l'**Azione all'avvio** del sito locale e/o del sito cloud è impostata su **Indirizza** (ad esempio, nei dispositivi Cisco ASA), e al momento non è presente alcun traffico. È possibile provare a effettuare il ping per verificare che il tunnel sia stato stabilito. Se il ping non funziona, controllare il mapping di rete nel sito locale e nel sito cloud.
Desidero riavviare una connessione IPsec specifica.	Per riavviare una connessione IPsec specifica: 1. Nella schermata **Disaster Recovery** > **Connessione**, fare clic sulla connessione IPsec. 2. Fare clic su **Disabilita connessione**. 3. Fare di nuovo clic sulla connessione IPsec. 4. Fare clic su **Abilita connessione**.

© Acronis International GmbH, 2003-2024

Download dei file di registro della connessione VPN IPsec

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Ulteriori informazioni sulla connessione IPsec sono disponibili nel file di registro nel server VPN. I file di registro sono compressi in un archivio .zip che è possibile scaricare e decomprimere.

Prerequisiti

La connessione VPN IPsec multisito è configurata.

Per scaricare l'archivio .zip con i file di registro

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic sull'icona ingranaggio accanto al gateway VPN del sito cloud.
3. Fare clic su **Scarica registro**.
4. Fare clic su **Fine**.
5. Non appena l'archivio zip è pronto per il download, fare clic su **Scarica registro** e salvarlo in locale.

File di registro della VPN IPsec multisito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

L'elenco seguente descrive i file di registro della VPN IPsec contenuti nell'archivio zip e le informazioni che contengono.

- `ip.txt` - Il file contiene i registri derivanti dalla configurazione delle interfacce di rete. Devono essere visualizzati due indirizzi IP: l'indirizzo IP pubblico e l'indirizzo IP locale. Se nel registro non sono visibili questi due indirizzi IP, c'è un problema. Contattare il team di supporto.

  Nota
  La maschera dell'indirizzo IP pubblico deve essere 32.

- `swanctl-list-loaded-config.txt` - Il file contiene informazioni su tutti i siti IPsec.

  Se nel file non è presente uno dei siti, la configurazione IPsec non è stata applicata. Provare ad aggiornare e a salvare la configurazione, oppure contattare il team di supporto.
- `swanctl-list-active-sas.txt` - Il file contiene le connessioni e i criteri che sono nello stato attivo o in connessione.

© Acronis International GmbH, 2003-2024

Configurazione dei server di ripristino

In questa sezione vengono descritti i concetti di failover e failback, la creazione di un server di ripristino e le operazioni di disaster recovery.

Creazione di un server di ripristino

Per creare un server di ripristino che sarà una copia del workload dell'utente, seguire la procedura descritta di seguito. È anche possibile guardare il video tutorial che mostra il processo.

Importante
Quando si esegue un failover, è possibile selezionare solo punti di ripristino creati dopo la creazione del server di ripristino.

Prerequisiti

- Al sistema originale da proteggere deve essere applicato un piano di protezione. Questo piano deve eseguire il backup dell'intero sistema, o solo dei dischi necessari per l'avvio e per fornire i servizi necessari, in un archivio nel cloud.
- È necessario configurare uno dei tipi di connessione al sito cloud.

Per creare un server di ripristino

1. Nella scheda **Tutti i dispositivi** selezionare il sistema da proteggere.
2. Fare clic su **Disaster Recovery** e quindi su **Crea server di ripristino**.
3. Selezionare il numero di core virtuali e la dimensione della RAM.

   Nota
   Sono visibili i punti di calcolo per ogni opzione. Questo numero riflette il costo orario dell'esecuzione del server di ripristino. Per ulteriori informazioni, consultare "Punti di calcolo" (pag. 753).

4. Specificare la rete cloud alla quale viene connesso il server.
5. Selezionare l'opzione **DHCP**.

Opzione DHCP	Descrizione
Fornito dal sito cloud	Impostazione predefinita. L'indirizzo IP del server verrà fornito da un server DHCP configurato automaticamente nel cloud.
Personalizzato	L'indirizzo IP del server verrà fornito dal server DHCP dell'utente nel cloud.

6. [Facoltativo] Specificare l'**indirizzo MAC**.
   L'indirizzo MAC è un identificatore univoco assegnato alla scheda di rete del server. Se si utilizza un DHCP personalizzato, è possibile configurarlo in modo che assegni sempre uno specifico

© Acronis International GmbH, 2003-2024

indirizzo IP a uno specifico indirizzo MAC. Ciò garantisce che il server di ripristino disponga sempre dello stesso indirizzo IP. È possibile eseguire applicazioni che hanno licenze che sono state registrate con l'indirizzo MAC.

7. Specificare l'indirizzo IP che avrà il server nella rete di produzione. Per impostazione predefinita, viene configurato l'indirizzo IP del sistema originale.

   Nota
   Se si utilizza un server DHCP, aggiungere questo indirizzo IP all'elenco di esclusione del server per evitare che l'indirizzo IP entri in conflitto.
   Se si utilizza un server DHCP personalizzato, è necessario specificare lo stesso indirizzo IP specificato in **Indirizzo IP in rete di produzione** nella configurazione del server DHCP. In caso contrario, il failover di prova non funzionerà correttamente e il server non sarà raggiungibile tramite un indirizzo IP pubblico.

8. [Facoltativo] Selezionare la casella di controllo **Indirizzo IP di prova** e quindi specificare l'indirizzo IP.
   In questo modo sarà possibile eseguire il failover di prova nella rete di prova isolata e connettersi al server di ripristino tramite RDP o SSH durante un failover di prova. Nella modalità failover di prova, il gateway VPN sostituisce l'indirizzo IP di prova con l'indirizzo IP di produzione utilizzando il protocollo NAT.
   Se la casella di controllo non è selezionata, per accedere al server durante un failover di prova sarà possibile utilizzare esclusivamente la console.

   Nota
   Se si utilizza un server DHCP, aggiungere questo indirizzo IP all'elenco di esclusione del server per evitare che l'indirizzo IP entri in conflitto.

   È possibile selezionare uno degli indirizzi IP proposti oppure digitarne uno differente.

9. [Facoltativo] Selezionare la casella di controllo **Accesso Internet**.
   In questo modo il server di ripristino potrà accedere a Internet durante un failover reale o di prova. Per impostazione predefinita, la porta TCP 25 è aperta per le connessioni in uscita verso gli indirizzi IP pubblici.
10. [Facoltativo] Impostare la **Soglia RPO**.
    La soglia RPO definisce l'intervallo di tempo massimo consentito tra l'ultimo punto di ripristino idoneo per un failover e l'ora corrente. È possibile impostare il valore tra 15–60 minuti, 1–24 ore, 1–14 giorni.
11. [Facoltativo] Selezionare la casella di controllo **Utilizza indirizzo IP pubblico**.
    Se dispone di un indirizzo IP pubblico, il server di ripristino è disponibile anche da Internet durante un failover reale o di prova. Se la casella di controllo non è selezionata, il server sarà disponibile solo nella rete di produzione.
    L'opzione **Utilizza indirizzo IP pubblico** richiede l'abilitazione dell'opzione **Accesso Internet**.

© Acronis International GmbH, 2003-2024

L'indirizzo IP pubblico verrà visualizzato dopo aver completato la configurazione. Per impostazione predefinita, la porta TCP 443 è aperta per le connessioni in entrata verso gli indirizzi IP pubblici.

Nota
Se si deseleziona la cartella di controllo **Utilizza indirizzo IP pubblico** o si elimina il server di ripristino, il relativo indirizzo IP pubblico non viene riservato.

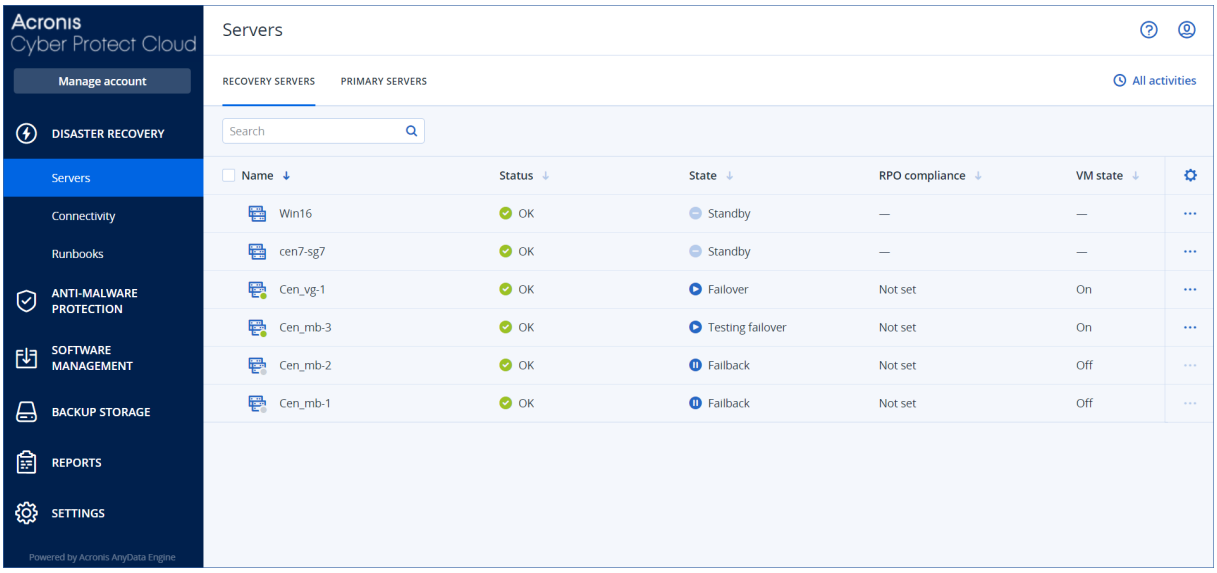
12. [Facoltativo] [Se i backup del sistema selezionato sono crittografati utilizzando la crittografia come proprietà del sistema], specificare la password che verrà automaticamente utilizzata al momento della creazione della virtual machine per il server di ripristino a partire dal backup crittografato.
    a. Fare clic su **Specificare**, quindi inserire la password per il backup crittografato e definire un nome per le credenziali.
       Per impostazione predefinita nell'elenco viene visualizzato il backup più recente.
    b. [Facoltativo] Per visualizzare tutti i backup, selezionare **Mostra tutti i backup**.
    c. Fare clic su **Fine**.

Nota
Poiché la password specificata viene archiviata in un archivio di credenziali sicuro, il salvataggio delle password potrebbe generare un conflitto con gli obblighi di conformità.

13. [Facoltativo] Modificare il nome del server di ripristino.
14. [Facoltativo] Immettere una descrizione per il server di ripristino.
15. [Facoltativo] Fare clic sulla scheda **Regole del firewall cloud** per modificare le regole predefinite del firewall. Per ulteriori informazioni, consultare "Impostazione delle regole del firewall per server cloud" (pag. 824).
16. Fare clic su **Crea**.

Il server di ripristino viene visualizzato nella scheda **Disaster Recovery** > **Server** > **Server di ripristino** della console di Cyber Protect. È anche possibile visualizzarne le impostazioni selezionando il sistema originale e facendo clic su **Disaster Recovery**.

© Acronis International GmbH, 2003-2024



Funzionamento del processo di failover

Failover di produzione

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Dal momento della creazione, un server di ripristino rimane in modalità **Standby**. La virtual machine corrispondente non esiste fino a quando non viene avviato il failover. Prima di avviare un processo di failover, è necessario creare almeno un backup dell'immagine del disco (con volume avviabile) del sistema originale.

All'avvio del processo di failover, selezionare il punto di ripristino (backup) del sistema originale dal quale verrà creata la virtual machine con i parametri predefiniti. L'operazione di failover utilizza la funzionalità di esecuzione della macchina virtuale da un backup. Il server di ripristino entra nello stato di transizione denominato **Finalizzazione**. Il processo implica il trasferimento dei dischi virtuali del server dallo storage di backup (storage ad accesso infrequente) allo storage di disaster recovery (storage ad accesso frequente).

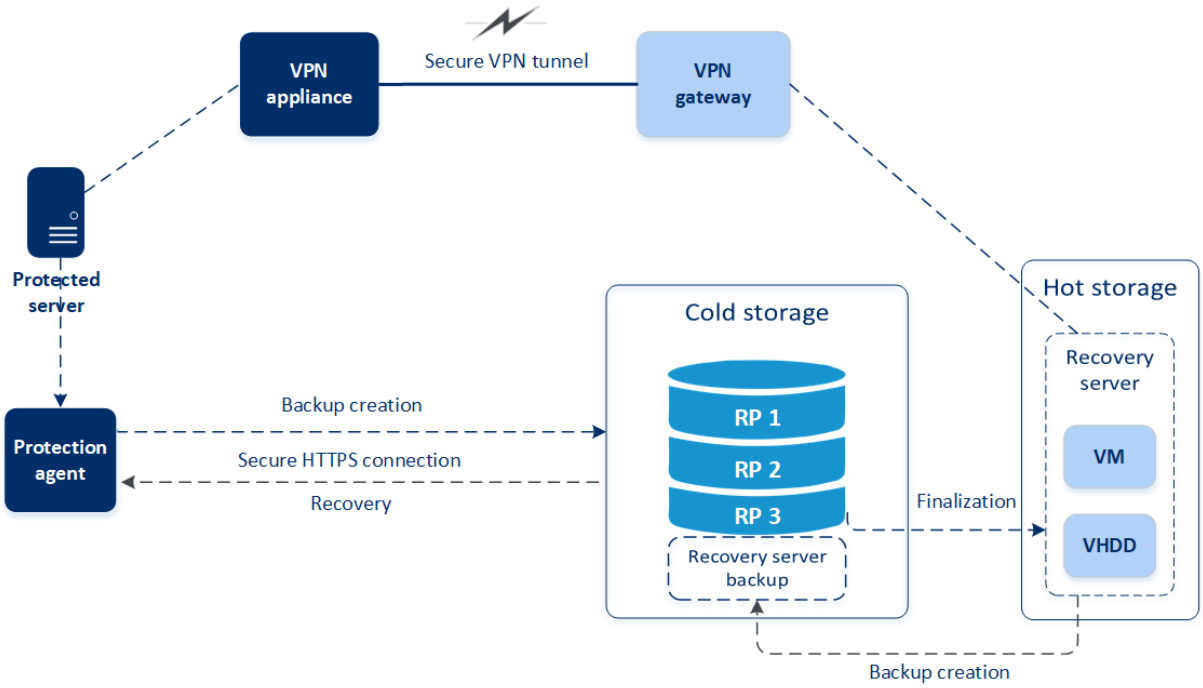
Nota
Durante la **Finalizzazione**, il server è accessibile e funzionale, sebbene con prestazioni inferiori al normale. È possibile aprire la console del server facendo clic sul link **La console è pronta**. Il link è disponibile nella colonna **Stato VM** della schermata **Disaster Recovery** > **Server**, e nella vista **Dettagli** del server.

Una volta completata la **Finalizzazione**, le prestazioni del server torneranno alla normalità. Lo stato del server passa a **Failover**. Il workload viene trasferito dal sistema originale al server di ripristino nel sito cloud.

© Acronis International GmbH, 2003-2024

Se il server di ripristino include un agente di protezione, il servizio agente viene arrestato per evitare interferenze, ad esempio l'avvio di un backup o la creazione di report di stato non aggiornati nel componente di backup.

Il diagramma sottostante mostra i processi di failover e failback.



Prova failover

Durante un **failover di prova**, la macchina virtuale non viene finalizzata. Ciò significa che l'agente legge il contenuto dei dischi virtuali direttamente dal backup, ovvero accede in modo casuale alle varie parti del backup; per questa ragione le prestazioni dell'agente potrebbero essere inferiori rispetto a quelle normali. Per ulteriori informazioni sul processo di failover di prova, fare riferimento a "Esecuzione di un failover di prova" (pag. 800).

Failover di prova automatizzato

Quando è configurato il failover di prova automatizzato, questo viene eseguito una volta al mese, senza interazione manuale. Per ulteriori informazioni, consultare "Failover di prova automatizzato" (pag. 803) e "Configurazione del failover di prova automatizzato" (pag. 803).

Esecuzione di un failover di prova

Eseguire un failover di prova significa avviare un server di ripristino in una VLAN di prova che è isolata rispetto alla rete di produzione. È possibile sottoporre a prova diversi server di ripristino alla volta e controllarne le interazioni. Nella rete di prova, i server comunicano tramite i propri indirizzi IP di produzione, ma non possono inizializzare le connessioni TCP o UDP ai workload della rete locale.

© Acronis International GmbH, 2003-2024

Durante un failover di prova, la virtual machine (server di ripristino) non viene finalizzata. L'agente legge il contenuto dei dischi virtuali direttamente dal backup e accede in modo casuale alle varie componenti del backup. Ciò può rallentare le prestazioni del server di ripristino nello stato di failover di prova rispetto alle prestazioni normali.

Sebbene il failover di prova sia un'attività facoltativa, è consigliabile eseguirla con regolarità, scegliendo la frequenza più idonea in termini di costi e sicurezza. Una procedura raccomandata è la creazione di un runbook, ovvero un insieme di istruzioni che descrive come allestire l'ambiente di produzione nel cloud.

Importante
È necessario creare un server di ripristino in anticipo, per proteggere i dispositivi da situazioni di emergenza.

È possibile eseguire il failover solo da punti di ripristino creati dopo la creazione del server di ripristino del dispositivo.

È necessario creare almeno un punto di ripristino prima che sia possibile eseguire il failover su un server di ripristino. Il numero massimo di punti di ripristino supportati è 100.

Per eseguire un failover di prova

1. Selezionare il sistema originale o il server di ripristino da sottoporre a prova.
2. Fare clic su **Disaster Recovery**.
   Viene visualizzata la descrizione del server di ripristino.
3. Fare clic su **Failover**.
4. Selezionare il tipo di failover **Prova failover**.
5. Selezionare il punto di ripristino (backup) e fare clic su **Avvia**.
6. Se il backup selezionato è crittografato utilizzando la crittografia come proprietà del sistema:
   a. Inserire la password di crittografia per il set di backup.

      Nota
      La password viene salvata solo temporaneamente e utilizzata solo per l'operazione di failover di prova corrente. La password viene automaticamente eliminata dall'archivio delle credenziali se il failover di prova viene interrotto o completato.

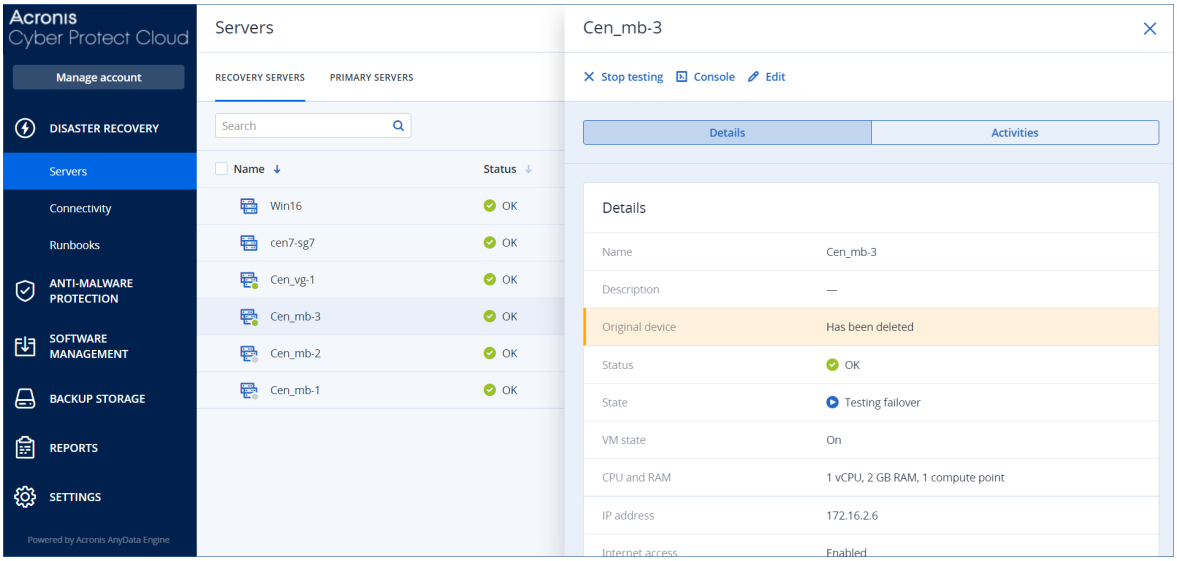
   b. [Facoltativo] Per salvare la password per il set di backup e utilizzarla nelle operazioni di failover successive, selezionare la casella di controllo **Archivia la password in un archivio delle credenziali protetto...** e, nel campo **Nome credenziali**, inserire un nome per le credenziali.

© Acronis International GmbH, 2003-2024

Importante
La password verrà archiviata in un archivio delle credenziali protetto e verrà applicata automaticamente nelle successive operazioni di failover. Tenere presente che il salvataggio delle password potrebbe generare un conflitto con gli obblighi di conformità.

c. Fare clic su **Fine**.

All'avvio del server di ripristino, lo stato passa a **Prova failover in corso**.



7. Verificare il funzionamento del server di ripristino con uno dei metodi seguenti:
   - In **Disaster Recovery** > **Server**, selezionare il server di ripristino e quindi fare clic su **Console**.
   - Eseguire la connessione al server di ripristino tramite RDP o SSH e l'indirizzo IP di prova specificato al momento della creazione del server stesso. Provare la connessione dall'interno e dall'esterno della rete di produzione, come descritto in "Connessione da punto a sito".
   - Eseguire uno script nel server di ripristino.
     Lo script può verificare la schermata di accesso, l'avvio corretto delle applicazioni, la connessione a Internet e la capacità degli altri sistemi di connettersi al server di ripristino.
   - Se il server di ripristino può accedere a Internet e a un indirizzo IP pubblico, è possibile utilizzare TeamViewer.
8. Una volta completata la prova, fare clic su **Interrompi test**.
   Il server di ripristino si arresta. Tutte le modifiche apportare al server di ripristino durante il failover di prova non vengono conservate.

Nota
Le azioni **Avvia server** e **Arresta server** non sono applicabili alle operazioni di failover di prova, sia nei runbook sia quando si avvia manualmente un failover di prova. Se si tenta di eseguire questo tipo di azione, questa non avrà esito positivo e si riceverà il seguente messaggio di errore:
Non riuscita: L'azione non è applicabile allo stato del server corrente.

© Acronis International GmbH, 2003-2024

Failover di prova automatizzato

Con il failover di prova automatizzato, il server di ripristino viene testato automaticamente una volta al mese, senza interazione manuale.

Il failover di prova automatizzato consiste delle parti seguenti:

1. creare una virtual machine dall'ultimo punto di ripristino
2. acquisire uno screenshot della virtual machine
3. analizzare se il sistema operativo della virtual machine si avvia in modo corretto
4. inviare una notifica sullo stato del failover di prova

Nota
Il failover di prova automatizzato consuma dei punti di calcolo.

È possibile configurare il failover di prova automatizzato nelle impostazioni del server di ripristino. Per ulteriori informazioni, consultare "Configurazione del failover di prova automatizzato" (pag. 803).

Tenere presente che in rari casi, il failover di prova automatizzato può essere ignorato e potrebbe non essere come pianificato. Ciò accade perché il failover di produzione ha una priorità più elevata rispetto al failover di prova automatizzato, perciò le risorse hardware (CPU e RAM) allocate al failover di prova potrebbero essere temporaneamente limitate per garantire che ci siano sufficienti risorse per eseguire simultaneamente un failover di produzione.

Se, per qualsiasi motivo, un failover di prova viene ignorato, viene visualizzato un avviso.

Nota
Il failover del test automatizzato non riesce se i backup del sistema originale sono crittografati utilizzando la crittografia come proprietà del sistema, e la password di crittografia non è specificata durante la creazione del server di ripristino. Per ulteriori informazioni su come specificare la password di crittografia, consultare "Creazione di un server di ripristino" (pag. 796).

Configurazione del failover di prova automatizzato

Configurando un failover di prova automatizzato è possibile provare il server di ripristino ogni mese, senza eseguire alcuna azione manuale.

Per configurare il failover di prova automatizzato

1. Nella console, passare a **Disaster Recovery** > **Server** > **Server di ripristino** e selezionare il server di ripristino.
2. Fare clic su **Modifica**.
3. Nella sezione **Failover di prova automatizzato**, nel campo **Pianificazione**, selezionare **Ogni mese**.

© Acronis International GmbH, 2003-2024

4. [Facoltativo] In **Timeout screenshot**, modificare il valore predefinito del periodo di tempo massimo (in minuti) entro il quale il sistema tenta l'esecuzione del failover di prova automatizzato.
5. [Facoltativo] Per salvare il valore **Timeout screenshot** come predefinito e compilarlo in modo automatico quando viene abilitato il failover di prova automatizzato per gli altri server di ripristino, selezionare **Imposta come timeout predefinito**.
6. Fare clic su **Salva**.

Visualizzazione dello stato del failover di prova automatizzato

È possibile visualizzare i dettagli di un failover di prova automatizzato completato, come stato, ora di inizio, ora di fine, durata, e lo screenshot della virtual machine.

Per visualizzare lo stato del failover di prova automatizzato di un server di ripristino

1. Nella console, passare a **Disaster Recovery** > **Server** > **Server di ripristino** e selezionare il server di ripristino.
2. Nella sezione **Failover di prova automatizzato**, controllare i dettagli dell'ultimo failover di prova automatizzato.
3. [Facoltativo] Dare clic su **Mostra screenshot** per visualizzare lo screenshot della virtual machine.

Disabilitazione del failover di prova automatizzato

È possibile disabilitare il failover di prova automatizzato per risparmiare risorse o se non è necessario eseguire il failover di prova automatizzato per un determinato server di ripristino.

Per disabilitare il failover di prova automatizzato

1. Nella console, passare a **Disaster Recovery** > **Server** > **Server di ripristino** e selezionare il server di ripristino.
2. Fare clic su **Modifica**.
3. Nella sezione **Failover di prova automatizzato**, nel campo **Pianificazione**, selezionare **Mai**.
4. Fare clic su **Salva**.

Esecuzione di un failover

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Il failover è il processo tramite il quale un carico di lavoro locale viene archiviato nel cloud. Il termine definisce anche lo stato del carico di lavoro che rimane nel cloud.

Quando si avvia un failover, il server di ripristino viene avviato nella rete di produzione. Per evitare interferenze e problemi imprevisti, verificare che il workload originale non sia online e che non sia possibile accedervi tramite VPN.

© Acronis International GmbH, 2003-2024

Per evitare l'interferenza del backup nello stesso archivio cloud, revocare manualmente il piano di protezione dal workload che è attualmente nello stato **Failover**. Per ulteriori informazioni su come revocare i piani, vedere Revoca di un piano di protezione.

Importante
È necessario creare un server di ripristino in anticipo, per proteggere i dispositivi da situazioni di emergenza.

È possibile eseguire il failover solo da punti di ripristino creati dopo la creazione del server di ripristino del dispositivo.

È necessario creare almeno un punto di ripristino prima che sia possibile eseguire il failover su un server di ripristino. Il numero massimo di punti di ripristino supportati è 100.

È possibile attenersi alle istruzioni seguenti o guardare il tutorial video.

Per eseguire un failover

1. Verificare che il sistema originale non sia disponibile in rete.
2. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Server** > **Server di ripristino** e selezionare il server di ripristino.
3. Fare clic su **Failover**.
4. Selezionare il tipo di failover **Failover di produzione**.
5. Selezionare il punto di ripristino (backup) e fare clic su **Avvia**.
6. [Se il backup selezionato è crittografato utilizzando la crittografia come proprietà del sistema]
   a. Inserire la password di crittografia per il set di backup.

      Nota
      La password viene salvata temporaneamente e utilizzata solo per l'operazione di failover corrente. La password viene automaticamente eliminata dall'archivio delle credenziali una volta completata l'operazione di failover e non appena il server torna nello stato di **standby**.

   b. [Facoltativo] Per salvare la password per il set di backup e utilizzarla nelle operazioni di failover successive, selezionare la casella di controllo **Archivia la password in un archivio delle credenziali protetto...** e, nel campo **Nome credenziali**, inserire un nome per le credenziali.

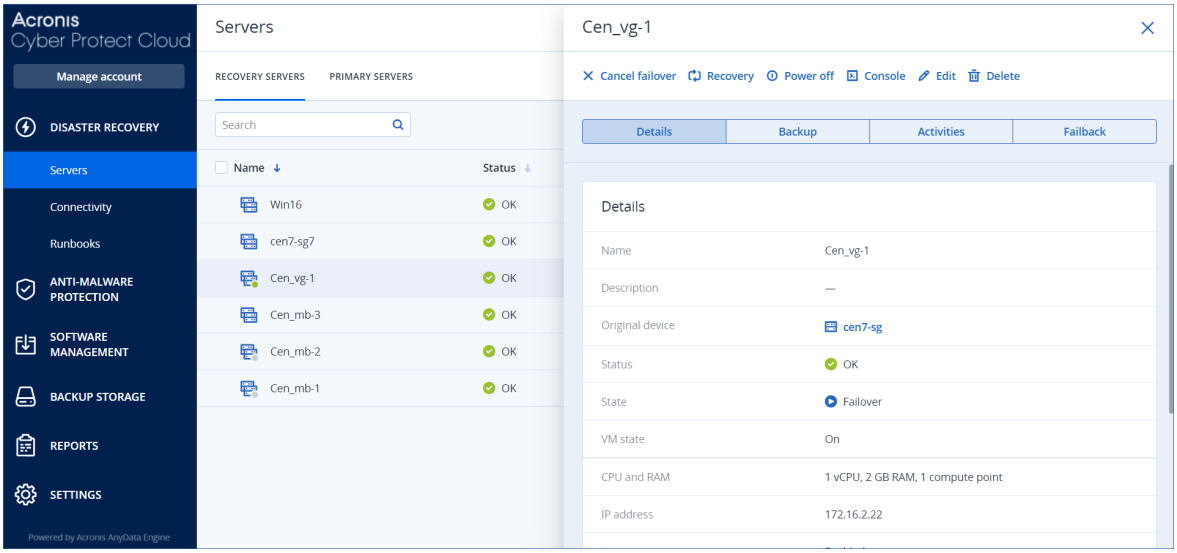
      Importante
      La password verrà archiviata in un archivio delle credenziali protetto e verrà applicata automaticamente nelle successive operazioni di failover. Tenere presente che il salvataggio delle password potrebbe generare un conflitto con gli obblighi di conformità.

   c. Fare clic su **Fine**.

   All'avvio del server di ripristino, lo stato passa a **Finalizzazione**, e dopo qualche tempo a **Failover**.

© Acronis International GmbH, 2003-2024

Importante
È fondamentale comprendere che il server è disponibile sia nello stato **Finalizzazione** che nello stato **Failover**. Durante la **Finalizzazione**, il server è accessibile facendo clic sul link **La console è pronta**. Il link è disponibile nella colonna **Stato VM** della schermata **Disaster Recovery** > **Server**, e nella vista **Dettagli** del server. Per ulteriori dettagli, consultare "Funzionamento del processo di failover" (pag. 799).



7. Verificare che il server di ripristino sia avviato visualizzandone la console. Fare clic su **Disaster Recovery** > **Server**, selezionare il server di ripristino e quindi fare clic su **Console**.
8. Verificare che sia possibile accedere al server di ripristino utilizzando l'indirizzo IP di produzione specificato al momento della creazione del server stesso.

Dopo la finalizzazione del server di ripristino, viene automaticamente creato un nuovo piano di protezione, che sarà applicato al server. Tale piano di protezione si basa sul piano di protezione utilizzato per la creazione del server di ripristino, pur se con alcune limitazioni: Del piano, ad esempio, è possibile modificare solo la pianificazione e le regole di conservazione. Per ulteriori informazioni, fare riferimento a "Backup dei server cloud".

Se si desidera annullare il failover, selezionare il server di ripristino e fare clic su **Annulla failover**. Tutte le modifiche apportate a partire dal momento del failover andranno perse, ad eccezione dei backup del server di ripristino. Il server di ripristino ritornerà in stato di **Standby**.

Se si desidera eseguire il failback, selezionare il server di ripristino e fare clic su **Failback**.

Come eseguire il failover di server utilizzando il server DNS locale

Se nel sito locale vengono utilizzati i server DNS per la risoluzione dei nomi dei sistemi, successivamente a un failover i server di ripristino corrispondenti ai sistemi che si affidano al server DNS non riusciranno a comunicare, perché i server DNS utilizzati nel cloud sono diversi. Per impostazione predefinita, i server DNS del sito cloud vengono utilizzati per i server cloud appena

© Acronis International GmbH, 2003-2024

creati. Nel caso in cui sia necessario applicare impostazioni DNS personalizzate, contattare il supporto tecnico.

Come eseguire il failover di un server DHCP

Nell'infrastruttura locale, il server DHCP può essere collocato su un host Windows o Linux. Quando viene eseguito il failover di questo host nel sito cloud, si verifica un problema di duplicazione del server DHCP, perché anche il gateway VPN nel cloud esegue il ruolo DHCP. Per risolvere il problema, eseguire una delle seguenti operazioni:

- Se è stato eseguito solo il failover dell'host DHCP nel cloud, mentre i server locali rimanenti sono ancora nel sito locale, è necessario accedere all'host DHCP nel cloud e disattivare il server DHCP ospitato. In questo modo non si avranno conflitti e solo il gateway VPN funzionerà come server DHCP.
- Se i server cloud hanno già ottenuto gli indirizzi IP dall'host DHCP, è necessario accedere all'host DHCP nel cloud e disattivare il server DHCP ospitato.È necessario accedere ai server cloud e rinnovare l'assegnazione DHCP per assegnare i nuovi indirizzi IP allocati dal server DHCP corretto ospitato nel gateway VPN.

Nota
Le istruzioni non sono valide quando il server DHCP nel cloud è configurato con l'opzione **DHCP personalizzato** e alcuni dei server di ripristino o primari ottengono il proprio indirizzo IP da questo server DHCP.

Funzionamento del processo di failback

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Il failback è il processo con il quale un workload archiviato nel cloud viene riportato in un sistema fisico o in una virtual machine nel sito locale. È possibile eseguire il failback in un server di ripristino nello stato di **Failover**, e continuare a utilizzare il server nel sito locale.

È possibile eseguire il failover automatizzato in un sistema di destinazione fisico o virtuale nel sito locale. Durante il processo di failback, è possibile trasferire i dati di backup nel sito locale mentre la virtual machine nel cloud resta in esecuzione. Questa tecnologia aiuta a ridurre nettamente l'interruzione operativa, la cui durata prevista è visualizzata nella console di Cyber Protect. L'informazione può essere visualizzata e utilizzata per pianificare le tempistiche e, se necessario, per avvisare i clienti del previsto e imminente periodo di inattività.

I processi di failback su un sistema fisico di destinazione e su una virtual machine di destinazione sono lievemente differenti. Per ulteriori informazioni sulle fasi del processo di failback, fare riferimento a "Failback in una virtual machine di destinazione" (pag. 808) e "Failback in un sistema fisico di destinazione" (pag. 813).

© Acronis International GmbH, 2003-2024

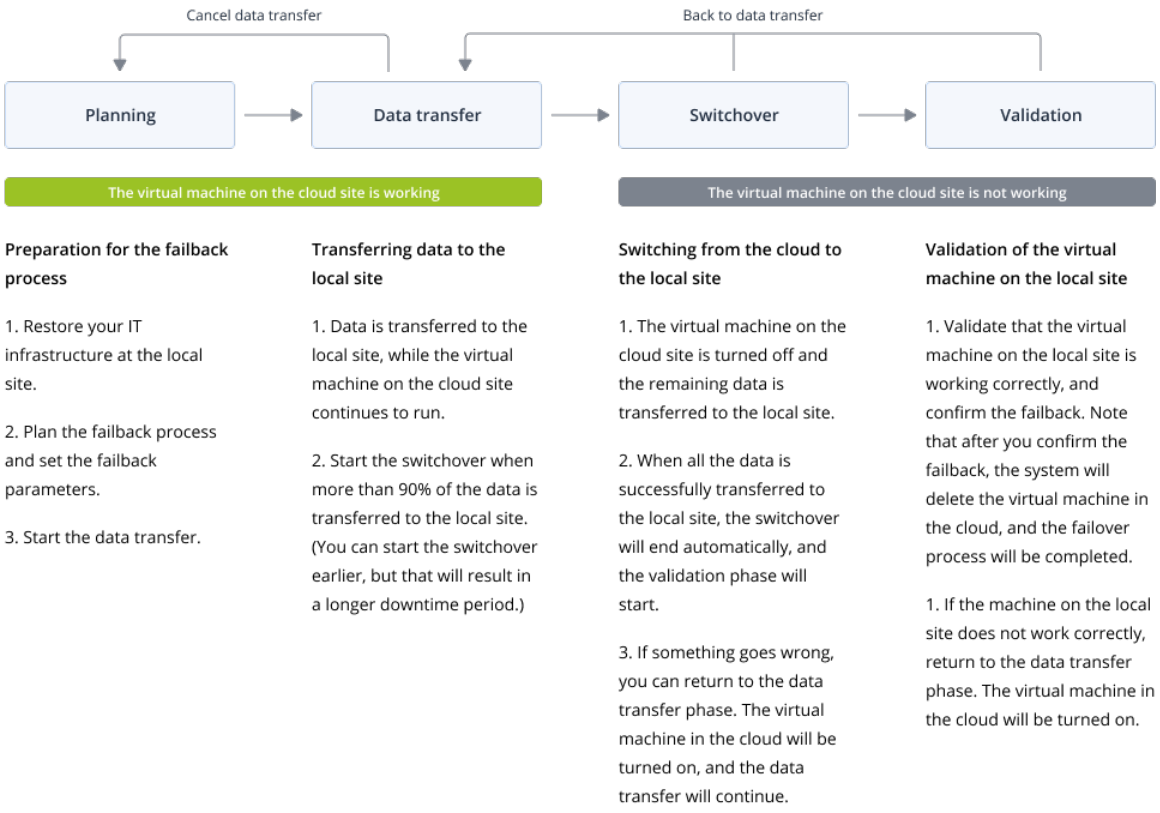
In alcuni casi specifici in cui non è possibile utilizzare la procedura di failback automatizzato, è possibile eseguire un failback manuale. Per ulteriori informazioni, consultare "Failback manuale" (pag. 817).

Nota
Le operazioni runbook supportano solo il failback in modalità manuale. Ciò significa che se si avvia il processo di failback eseguendo un runbook che include il passaggio **Esegui il failback del server**, la procedura richiederà un'interazione manuale: sarà necessario ripristinare manualmente il sistema, e confermare o annullare il processo di failback dalla scheda **Disaster Recovery** > **Server**.

Failback in una virtual machine di destinazione

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Il processo di failback in una virtual machine di destinazione è costituito da quattro fasi.



1. **Pianificazione**. Durante questa fase si esegue il ripristino dell'infrastruttura IT nel sito locale, ad esempio degli host e delle configurazioni di rete, si configurano i parametri di failback e si pianifica quando avviare il trasferimento dei dati.

© Acronis International GmbH, 2003-2024

Nota
Per ridurre al minimo il tempo totale del processo di failback, si consiglia di avviare la fase di trasferimento dei dati subito dopo aver configurato i server locali, e di proseguire quindi con la configurazione della rete e del resto dell'infrastruttura locale nel corso della fase di trasferimento dei dati.

2. **Trasferimento dei dati**. Durante questa fase i dati vengono trasferiti dal sito cloud al sito locale, mentre la virtual machine nel cloud resta in esecuzione. È possibile avviare la fase successiva (lo switchover) in qualsiasi momento durante la fase del trasferimento dei dati, ma occorre tenere presente quanto segue.

   Più tempo si rimane nella fase di trasferimento dei dati,

   - più a lungo la virtual machine nel cloud resta in esecuzione;
   - più dati verranno trasferiti nel sito locale;
   - più elevato sarà il costo che verrà addebitato (si consumano infatti più punti di calcolo);
   - minore il periodo di interruzione operativa che si sperimenta durante la fase di switchover.

   Per ridurre al minimo l'interruzione operativa, avviare la fase di switchover dopo aver trasferito oltre il 90% dei dati nel sito locale.

   Se è possibile tollerare un periodo di interruzione operativa più lungo e non si desidera utilizzare ulteriori punti di calcolo per l'esecuzione della virtual machine nel cloud, è possibile anticipare la fase di switchover.

   Se il processo di failback viene annullato durante la fase di trasferimento dei dati, i dati trasferiti non verranno eliminati dal sito locale. Per evitare potenziali problemi, cancellare manualmente i dati trasferiti prima di avviare un nuovo processo di failback. Il successivo processo di trasferimento dei dati si avvierà dall'inizio.
3. **Switchover**. Durante questa fase la virtual machine nel cloud viene disattivata e i dati rimanenti, incluso l'ultimo incremento di backup, vengono trasferiti nel sito locale. Se al server di ripristino non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover; ciò potrebbe rallentare il processo.

   Nella console di Cyber Protect è visibile il tempo stimato (periodo di interruzione operativa) prima del termine di questa fase. Quando tutti i dati sono stati trasferiti nel sito locale (non c'è alcuna perdita di dati e la virtual machine nel sito locale è una copia esatta della virtual machine nel cloud) la fase di switchover è considerata completa. La virtual machine nel sito locale viene ripristinata e la fase di convalida si avvia in automatico.
4. **Convalida**. Durante questa fase, la virtual machine nel sito locale è pronta e viene avviata automaticamente. È possibile verificare il corretto funzionamento della virtual machine e:
   - Se tutto funziona come previsto, confermare il failback. Dopo la conferma, la virtual machine nel cloud viene eliminata e il server di ripristino torna nello stato di **Standby**. Questa è l'ultima fase del processo di failback.
   - Se qualcosa non ha funzionato come previsto, è possibile annullare lo switchover e tornare alla fase di trasferimento dei dati.

© Acronis International GmbH, 2003-2024

Esecuzione del failback in una virtual machine

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile eseguire il failback in una virtual machine di destinazione nel sito locale.

Prerequisiti

- L'agente che verrà utilizzato per eseguire il failback è online e al momento non è impiegato in un'altra operazione di failback.
- La connessione Internet è stabile.
- Nel cloud è presente almeno un backup completo della virtual machine.

Per eseguire il failback in una virtual machine

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Server**.
2. Selezionare il server di ripristino che si trova nello stato di **Failover**.
3. Fare clic sulla scheda **Failback**.
4. Nella sezione **Parametri di failback**, selezionare **Macchina virtuale** come **Destinazione** e configurare gli altri parametri.
   Per impostazione predefinita, alcuni dei **Parametri di failback** vengono compilati automaticamente con i valori suggeriti, ma è possibile modificarli.
   La tabella seguente fornisce più informazioni sui **Parametri di failback**.

Parametro	Descrizione
Dimensioni backup	La quantità di dati che verranno trasferiti al sito locale durante il processo di failback. Dopo l'avvio del processo di failback in una virtual machine di destinazione, la **Dimensioni backup** aumenterà durante la fase di trasferimento dei dati, perché la virtual machine nel cloud resta in esecuzione e continua a generare nuovi dati. Per calcolare il periodo stimato di interruzione operativa durante il processo di failback in una virtual machine di destinazione, prendere il 10% del valore della **Dimensioni backup** (come già raccomandato, la fase di switchover deve essere avviata dopo che il 90% dei dati è stato trasferito al sito locale), e dividerlo per il valore della velocità di Internet. **Nota** Il valore della velocità di Internet diminuisce quando vengono eseguiti più processi di failback alla volta.
Destinazione	Il tipo di workload nel sito locale nel quale verrà ripristinato il server

© Acronis International GmbH, 2003-2024

Parametro	Descrizione
	cloud: **Macchina virtuale** o **Macchina fisica**.
Posizione del sistema di destinazione	Posizione del failback: un host VMware ESXi o un host Microsoft Hyper-V. È possibile scegliere tra tutti gli host che dispongono di un agente registrato nel servizio Cyber Protection.
Agente	L'agente che eseguirà l'operazione di failback. È possibile utilizzare un agente per eseguire un'operazione di failback a volta. L'agente selezionato non deve essere impiegato da un altro processo di failback, deve essere online, far parte di una versione che supporta la funzionalità di failback e disporre dei permessi di accesso al backup. È possibile installare più agenti sugli host VMware ESXi e avviare un processo di failback distinto utilizzando ognuno di essi. Questi processi di failback possono essere eseguiti in contemporanea.
Impostazioni del sistema di destinazione	Impostazioni della virtual machine: • **Processori virtuali**. Selezionare il numero di processori virtuali. • **Memoria**. Selezionare la quantità di memoria di cui disporrà la virtual machine. • **Unità**. Selezionare le unità per la memoria. • [Facoltativo] **Schede di rete**. Per aggiungere una scheda di rete, fare clic su **Aggiungi** e selezionare una rete nel campo **Rete**. Dopo aver completato la modifica, fare clic su **Fine**.
Percorso	(Per gli host Microsoft Hyper-V) La cartella nell'host in cui verrà archiviato il sistema. Verificare che lo spazio di memoria disponibile sull'host sia sufficiente per il sistema.
Datastore	(Per gli host VMware ESXi) Il datastore nell'host in cui verrà archiviato il sistema. Verificare che lo spazio di memoria disponibile sull'host sia sufficiente per il sistema.
Modalità di provisioning	Metodo di allocazione del disco virtuale. Per host Microsoft Hyper-V: • **Espansione dinamica** (valore predefinito). • **Dimensione fissa**. Per host Microsoft Hyper-V: • **Thin** (valore predefinito). • **Thick**.
Nome del sistema di	Nome del sistema di destinazione. Per impostazione predefinita, il nome del sistema di destinazione è lo stesso del nome del server di ripristino.

© Acronis International GmbH, 2003-2024

Parametro	Descrizione
destinazione	Il nome del sistema di destinazione deve essere univoco per la **Posizione del sistema di destinazione** selezionata.

5. Fare clic su **Avvia trasferimento dei dati**, e nella finestra di conferma fare clic di nuovo su **Avvia**.

Nota
Se nel cloud non esiste un backup della virtual machine, il sistema esegue automaticamente un backup prima della fase di trasferimento dei dati.

Viene avviata la fase di **Trasferimento dei dati**. La console visualizza le seguenti informazioni:

Campo	Descrizione
Avanzamento	Questo parametro mostra quanti dati sono stati già trasferiti nel sito locale, e la quantità totale di dati che devono essere ancora trasferiti. La quantità totale di dati include i dati dell'ultimo backup eseguito prima dell'avvio della fase di trasferimento dei dati, e i backup dei dati generati di recente (incrementi di backup), perché la virtual machine resta in esecuzione durante la fase di trasferimento dei dati. Per questa ragione, entrambi i valori del parametro **Avanzamento** aumentano nel tempo.
Stima del tempo di inattività	Questo parametro mostra per quanto tempo la virtual machine nel cloud non sarà disponibile se la fase di switchover viene avviata immediatamente. Il valore è calcolato in base ai valori del parametro **Avanzamento**, e diminuisce con il tempo.

6. Fare clic su **Switchover** e, nella finestra di conferma, fare clic di nuovo su **Switchover**.
Sia avvia la fase di switchover. La console visualizza le seguenti informazioni:

Campo	Descrizione
Avanzamento	Questo parametro mostra l'avanzamento del ripristino del sistema nel sito locale.
Tempo stimato al termine	Questo parametro mostra il tempo stimato per il completamento della fase di switchover, dopo la quale sarà possibile avviare il sistema nel sito locale.

Nota
Se alla virtual machine nel cloud non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover, e ciò potrebbe causare un'interruzione operativa più lunga.

7. Al completamento della fase di **switchover** la virtual machine nel sito locale viene avviata automaticamente. Verificare che funzioni come previsto.

© Acronis International GmbH, 2003-2024

8. Fare clic su **Conferma failback**, e nella finestra di conferma fare clic di nuovo su **Conferma** per finalizzare il processo.
   La virtual machine nel cloud viene eliminata e il server di ripristino torna nello stato di **Standby**.

   Nota
   L'operazione di applicazione di un piano di protezione al server ripristinato non fa parte del processo di failback. Una volta completato il processo di failback, applicare un piano di protezione al server ripristinato per assicurarsi che sia di nuovo protetto. È possibile applicare lo stesso piano di protezione che è stato applicato al server originario, oppure un nuovo piano di protezione per il quale sia abilitato il modulo **Disaster Recovery**.

Failback in un sistema fisico di destinazione

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Il processo di failback automatizzato in un sistema fisico di destinazione consiste delle fasi seguenti:

1. **Pianificazione**. Durante questa fase si esegue il ripristino dell'infrastruttura IT nel sito locale, ad esempio degli host e delle configurazioni di rete, si configurano i parametri di failback e si pianifica quando avviare il trasferimento dei dati.
2. **Trasferimento dei dati**. Durante questa fase i dati vengono trasferiti dal sito cloud al sito locale, mentre la virtual machine nel cloud resta in esecuzione. È possibile avviare la fase successiva (lo switchover) in qualsiasi momento durante la fase del trasferimento dei dati, ma occorre tenere presente quanto segue.
   Più tempo si rimane nella fase di trasferimento dei dati,
   - più a lungo la virtual machine nel cloud resta in esecuzione;
   - più dati verranno trasferiti nel sito locale;
   - più elevato sarà il costo che verrà addebitato (si consumano infatti più punti di calcolo);
   - minore il periodo di interruzione operativa che si sperimenta durante la fase di switchover.

   Per ridurre al minimo l'interruzione operativa, avviare la fase di switchover dopo aver trasferito oltre il 90% dei dati nel sito locale.
   Se è possibile tollerare un periodo di interruzione operativa più lungo e non si desidera utilizzare ulteriori punti di calcolo per l'esecuzione della virtual machine nel cloud, è possibile anticipare la fase di switchover.

   Nota
   Il processo di trasferimento dei dati si avvale di una tecnologia flashback. Tale tecnologia confronta i dati disponibili sul sistema di destinazione con quelli della virtual machine nel cloud. Se parte dei dati è già disponibile nel sistema di destinazione, tali dati non verranno trasferiti di nuovo. La tecnologia accelera quindi la fase di trasferimento dei dati.
   Per questo motivo si consiglia di ripristinare il server nel sistema originale nel sito locale.

© Acronis International GmbH, 2003-2024

3. **Switchover**. Durante questa fase la virtual machine nel cloud viene disattivata e i dati rimanenti, incluso l'ultimo incremento di backup, vengono trasferiti nel sito locale. Se al server di ripristino non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover; ciò potrebbe rallentare il processo.
4. **Convalida**. Durante questa fase, il sistema fisico nel sito locale è pronto ed è possibile riavviarlo utilizzando un supporto di avvio Linux. È possibile verificare il corretto funzionamento della virtual machine e:
   - Se tutto funziona come previsto, confermare il failback. Dopo la conferma, la virtual machine nel cloud viene eliminata e il server di ripristino torna nello stato di **Standby**. Questa è l'ultima fase del processo di failback.
   - Se qualcosa non ha funzionato come previsto, è possibile annullare il failover e tornare alla fase di pianificazione.

   Nota
   Una volta riavviato il supporto di avvio, non sarà possibile utilizzarlo di nuovo. Se, dopo la fase di convalida, il funzionamento è diverso dal previsto, è necessario registrare un nuovo supporto di avvio e avviare nuovamente il processo di failback.
   Poiché verrà utilizzata la tecnologia flashback, i dati che si trovano già sul sito locale non verranno trasferiti di nuovo, e il processo di failback sarà più rapido.

Esecuzione del failback in un sistema fisico

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile eseguire il failback automatizzato in un sistema fisico di destinazione nel sito locale.

Nota
Il processo di trasferimento dei dati si avvale di una tecnologia flashback. Tale tecnologia confronta i dati disponibili sul sistema di destinazione con quelli della virtual machine nel cloud. Se parte dei dati è già disponibile nel sistema di destinazione, tali dati non verranno trasferiti di nuovo. La tecnologia accelera quindi la fase di trasferimento dei dati.

Per questo motivo si consiglia di ripristinare il server nel sistema originale nel sito locale.

Prerequisiti

- L'agente che verrà utilizzato per eseguire il failback è online e al momento non è impiegato in un'altra operazione di failback.
- La connessione Internet è stabile.
- È disponibile un supporto di avvio registrato. Per ulteriori informazioni, consultare "Creazione di un supporto di avvio per recuperare i sistemi operativi" nel Manuale dell'utente di Cyber Protection.

© Acronis International GmbH, 2003-2024

- Il sistema fisico di destinazione è il sistema originale nel sito locale, o presenta lo stesso firmware del sistema originale.
- Nel cloud è presente almeno un backup completo della virtual machine.

Per eseguire il failback in un sistema fisico

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Server**.
2. Selezionare il server di ripristino che si trova nello stato di **Failover**.
3. Fare clic sulla scheda **Failback**.
4. Nel campo **Destinazione**, scegliere **Sistema fisico**.
5. Nel campo **Supporto di avvio di destinazione**, fare clic su **Specificare**, selezionare il supporto di avvio, quindi fare clic su **Fine**.

   Nota
   Si consiglia l'utilizzo di un supporto di avvio pronto all'uso, perché è già configurato. Per ulteriori informazioni, consultare "Creazione di un supporto di avvio per recuperare i sistemi operativi" nel Manuale dell'utente di Cyber Protection.

6. [Facoltativo] Per modificare il mapping al disco predefinito, nel campo **Mappatura disco** fare clic su **Specificare**, mappare i dischi del backup ai dischi del sistema di destinazione, quindi fare clic su **Fine**.
7. Fare clic su **Avvia trasferimento dei dati**, e nella finestra di conferma fare clic su **Avvia**.

   Nota
   Se nel cloud non esiste un backup della virtual machine, il sistema esegue automaticamente un backup prima della fase di trasferimento dei dati.

   Viene avviata la fase di trasferimento dei dati. La console visualizza le seguenti informazioni:

Campo	Descrizione
Avanzamento	Questo parametro mostra quanti dati sono stati già trasferiti nel sito locale, e la quantità totale di dati che devono essere ancora trasferiti. La quantità totale di dati include i dati dell'ultimo backup eseguito prima dell'avvio della fase di trasferimento dei dati, e i backup dei dati generati di recente (incrementi di backup), perché la virtual machine resta in esecuzione durante la fase di trasferimento dei dati. Per questa ragione, entrambi i valori del parametro **Avanzamento** aumentano nel tempo. Poiché durante il trasferimento dei dati il sistema utilizza una tecnologia flashback che evita il trasferimento dei dati che sono già disponibili nel sistema di destinazione, l'avanzamento potrebbe essere più veloce di quanto calcolato inizialmente dalla console.
Stima del tempo di	Questo parametro mostra per quanto tempo la virtual machine nel cloud non sarà disponibile se la fase di switchover viene avviata

© Acronis International GmbH, 2003-2024

Campo	Descrizione
inattività	immediatamente. Il valore è calcolato in base ai valori del parametro **Avanzamento**, e diminuisce con il tempo. Poiché durante il trasferimento dei dati il sistema utilizza una tecnologia flashback che evita il trasferimento dei dati che sono già disponibili nel sistema di destinazione, l'interruzione operativa potrebbe essere più breve rispetto al valore visualizzato inizialmente nella console.

8. Fare clic su **Switchover** e, nella finestra di conferma, fare clic di nuovo su **Switchover**.
   Sia avvia la fase di switchover. La console visualizza le seguenti informazioni:

Campo	Descrizione
Avanzamento	Questo parametro mostra l'avanzamento del ripristino del sistema nel sito locale.
Tempo stimato al termine	Questo parametro mostra il tempo stimato per il completamento della fase di switchover, dopo la quale sarà possibile avviare il sistema nel sito locale.

Nota
Se alla virtual machine nel cloud non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover, e ciò potrebbe causare un'interruzione operativa più lunga.

9. Al completamento della fase di **switchover**, riavviare il supporto di avvio e verificare che il sistema fisico nel sito locale funzioni come previsto.
   Per ulteriori informazioni, consultare la sezione relativa al ripristino di dischi con supporto di avvio nel Manuale dell'utente di Cyber Protection.
10. Fare clic su **Conferma failback**, e nella finestra di conferma fare clic di nuovo su **Conferma** per completare il processo.
    La virtual machine nel cloud viene eliminata e il server di ripristino torna nello stato di **Standby**.

Nota
L'operazione di applicazione di un piano di protezione al server ripristinato non fa parte del processo di failback. Una volta completato il processo di failback, applicare un piano di protezione al server ripristinato per assicurarsi che sia di nuovo protetto. È possibile applicare lo stesso piano di protezione che è stato applicato al server originario, oppure un nuovo piano di protezione per il quale sia abilitato il modulo **Disaster Recovery**.

© Acronis International GmbH, 2003-2024

Failback manuale

Nota
Si consiglia di utilizzare il processo di failback in modalità manuale solo se l'operazione è suggerita dal team di supporto.

È anche possibile avviare un processo di failback in modalità manuale. In questo caso, il trasferimento dei dati dal backup nel cloud al sito locale non viene eseguito automaticamente, ma deve essere avviato manualmente dopo aver spento la virtual machine nel cloud. Ciò rende il processo di failback in modalità manuale più lento e di conseguenza occorre prevedere un periodo di interruzione operativa più lungo.

Il processo di failback in modalità manuale consiste delle fasi seguenti:

1. **Pianificazione**. Durante questa fase si esegue il ripristino dell'infrastruttura IT nel sito locale, ad esempio degli host e delle configurazioni di rete, si configurano i parametri di failback e si pianifica quando avviare il trasferimento dei dati.
2. **Switchover**. Durante questa fase la virtual machine nel cloud viene disattivata e viene eseguito il backup dei dati generati più di recente. Se al server di ripristino non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover; ciò potrebbe rallentare il processo. Al termine del backup, il sistema viene ripristinato nel sito locale manualmente. È possibile ripristinare il disco utilizzando il supporto di avvio o l'intero sistema dallo storage di backup nel cloud.
3. **Convalida**. Durante questa fase viene verificato il corretto funzionamento del sistema fisico o della virtual machine nel sito locale, e viene confermato il failback. Dopo la conferma, la virtual machine nel sito cloud viene eliminata e il server di ripristino torna nello stato di **standby**.

Esecuzione di un failback manuale

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile eseguire il failback manuale in un sistema fisico o una virtual machine di destinazione nel sito locale.

Per eseguire un failback manuale

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Server**.
2. Selezionare il server di ripristino che si trova nello stato di **Failover**.
3. Fare clic sulla scheda **Failback**.
4. Nel campo **Destinazione**, scegliere **Sistema fisico**.
5. Fare clic sull'icona ingranaggio e quindi abilitare l'interruttore **Utilizzare la modalità manuale**.

© Acronis International GmbH, 2003-2024

6. [Facoltativo] Per calcolare il periodo stimato di inattività durante il processo di failback, dividere il valore della **dimensioni del backup** per il valore della velocità di Internet.

   Nota
   Il valore della velocità di Internet diminuisce quando vengono eseguiti più processi di failback alla volta.

7. Fare clic su **Switchover**, e nella finestra di conferma fare clic di nuovo su **Switchover**.
   La virtual machine nel sito cloud viene disattivata.

   Nota
   Se alla virtual machine nel cloud non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover, e ciò potrebbe causare un'interruzione operativa più lunga.

8. Ripristinare il server dal backup cloud al sistema fisico o alla virtual machine nel sito locale. Per ulteriori informazioni, consultare la sezione relativa al ripristino di un sistema nel Manuale dell'utente di Cyber Protection.
9. Accertarsi che il ripristino sia completato e che il sistema ripristinato funzioni correttamente, quindi fare clic su **Sistema ripristinato**.
10. Se tutto funziona come previsto, fare clic su **Conferma failback**, e nella finestra di conferma fare clic di nuovo su **Conferma**.
    Il server di ripristino e i punti di ripristino sono pronti per il successivo failover. Per creare nuovi punti di ripristino, applicare un piano di protezione al nuovo server locale.

    Nota
    L'operazione di applicazione di un piano di protezione al server ripristinato non fa parte del processo di failback. Una volta completato il processo di failback, applicare un piano di protezione al server ripristinato per assicurarsi che sia di nuovo protetto. È possibile applicare lo stesso piano di protezione che è stato applicato al server originario, oppure un nuovo piano di protezione per il quale sia abilitato il modulo **Disaster Recovery**.

Operare con backup crittografati

È possibile creare server di ripristino dai backup crittografati. Per praticità, configurare l'applicazione di una password automatica a un backup crittografato durante il failover su un server di ripristino.

Durante la creazione di un server di ripristino, è possibile specificare la password da utilizzare per le operazioni di disaster recovery automatico. Tali password vengono salvate nell'archivio delle credenziali, un archivio sicuro reperibile nella sezione **Impostazioni** > **Credenziali**.

Più backup possono condividere la stessa credenziale.

Per gestire le password salvate in Archivio credenziali

© Acronis International GmbH, 2003-2024

1. Passare a **Impostazioni** > **Credenziali**.
2. Per gestire una credenziale specifica, fare clic sull'icona nell'ultima colonna. È possibile visualizzare gli elementi collegati alla credenziale selezionata.
   - Per scollegare il backup dalla credenziale selezionata, fare clic sull'icona cestino accanto al backup. Sarà necessario specificare manualmente la password durante il failover nel server di ripristino.
   - Per modificare le credenziali, fare clic su **Modifica** e quindi specificare il nome e la password.
   - Per eliminare la credenziale, fare clic su **Elimina**. Tenere presente che sarà necessario specificare manualmente la password durante il failover nel server di ripristino.

Operazioni con virtual machine di Microsoft Azure

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

È possibile eseguire il failover di virtual machine di Microsoft Azure in Acronis Cyber Protect Cloud. Per ulteriori informazioni, consultare "Esecuzione di un failover" (pag. 804).

Dopo di ciò, sarà possibile eseguire il failback da Acronis Cyber Protect Cloud alle virtual machine di Azure. Il processo di failback è uguale al processo di failback in un sistema fisico. Per ulteriori informazioni, consultare "Prerequisiti" (pag. 814).

Nota
Per registrare una nuova virtual machine di Azure per il failback, utilizzare l'estensione Acronis Backup VM disponibile in Azure.

È inoltre possibile configurare una connessione VPN IPsec multisito tra Acronis Cyber Protect Cloud e il gateway VPN di Azure. Per ulteriori informazioni, consultare "Configurazione di una connessione VPN IPsec multisito" (pag. 772).

Configurazione dei server primari

In questa sezione viene descritto come trovare e gestire i server primari.

Creazione di un server primario

Prerequisiti

- È necessario configurare uno dei tipi di connessione al sito cloud.

Per creare un server primario

© Acronis International GmbH, 2003-2024

1. Passare alla scheda **Disaster Recovery** > **Server** > **Server primari**.
2. Fare clic su **Crea**.
3. Selezionare il modello per la nuova macchina virtuale.
4. Selezionare la versione della configurazione (numero di core virtuali e dimensione della RAM). La tabella seguente mostra la quantità massima totale di spazio su disco (GB) per ogni versione.

Tipo	vCPU	RAM (GB)	Quantità massima totale di spazio su disco (GB)
F1	1	2	500
F2	1	4	1000
F3	2	8	2000
F4	4	16	4000
F5	8	32	8000
F6	16	64	16000
F7	16	128	32000
F8	16	256	64000

Nota
Sono visibili i punti di calcolo per ogni opzione. Questo numero riflette il costo orario dell'esecuzione del server primario. Per ulteriori informazioni, consultare "Punti di calcolo" (pag. 753).

5. [Facoltativo] Modificare la dimensione del disco virtuale. Se è necessario più di un disco rigido, fare clic su **Aggiungi disco** e quindi specificare la dimensione del nuovo disco. Al momento non è possibile aggiungere più di 10 dischi a un server primario.
6. Specificare la rete cloud nella quale viene incluso il server primario.
7. Selezionare l'opzione **DHCP**.

Opzione DHCP	Descrizione
Fornito dal sito cloud	Impostazione predefinita. L'indirizzo IP del server verrà fornito da un server DHCP configurato automaticamente nel cloud.
Personalizzato	L'indirizzo IP del server verrà fornito dal server DHCP dell'utente nel cloud.

8. [Facoltativo] Specificare l'**indirizzo MAC**.
   L'indirizzo MAC è un identificatore univoco assegnato alla scheda di rete del server. Se si utilizza un DHCP personalizzato, è possibile configurarlo in modo che assegni sempre uno specifico indirizzo IP a uno specifico indirizzo MAC. Ciò garantisce che il server primario disponga sempre dello stesso indirizzo IP. È possibile eseguire applicazioni che hanno licenze che sono state registrate con l'indirizzo MAC.

© Acronis International GmbH, 2003-2024

9. Specificare l'indirizzo IP che avrà il server nella rete di produzione. Per impostazione predefinita, viene configurato il primo indirizzo IP libero della rete di produzione.

   Nota
   Se si utilizza un server DHCP, aggiungere questo indirizzo IP all'elenco di esclusione del server per evitare che l'indirizzo IP entri in conflitto.
   Se si utilizza un server DHCP personalizzato, è necessario specificare lo stesso indirizzo IP specificato in **Indirizzo IP in rete di produzione** nella configurazione del server DHCP. In caso contrario, il failover di prova non funzionerà correttamente e il server non sarà raggiungibile tramite un indirizzo IP pubblico.

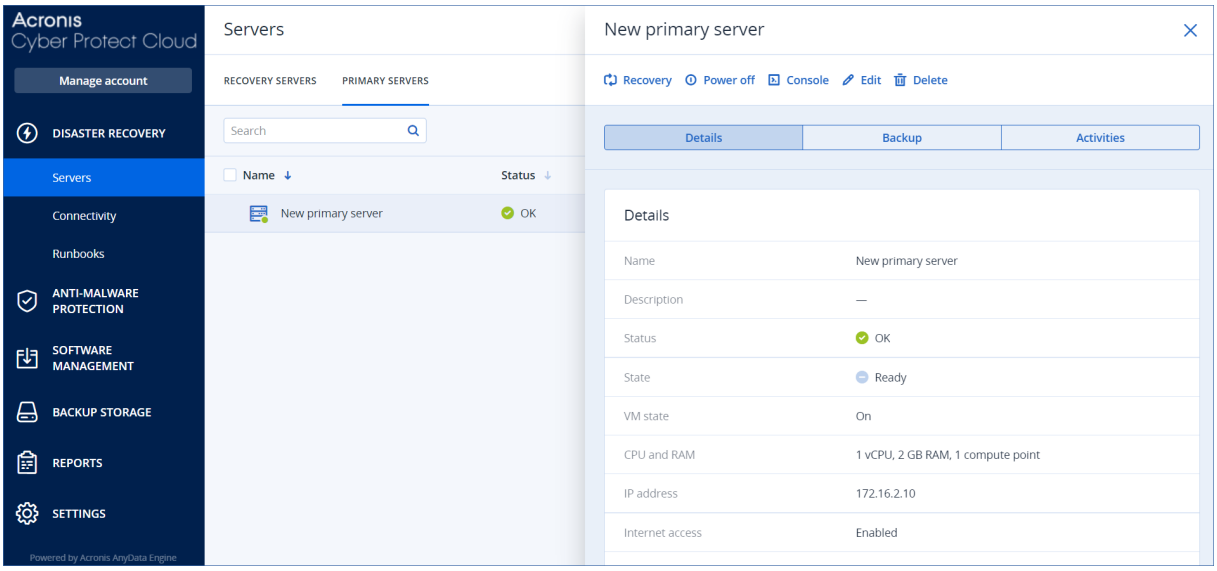
10. [Facoltativo] Selezionare la casella di controllo **Accesso Internet**.
    Viene così abilitato l'accesso a Internet per il server primario. Per impostazione predefinita, la porta TCP 25 è aperta per le connessioni in uscita verso gli indirizzi IP pubblici.
11. [Facoltativo] Selezionare la casella di controllo **Utilizza indirizzo IP pubblico**.
    Se dispone di un indirizzo IP pubblico, il server primario è disponibile anche da Internet. Se la casella di controllo non è selezionata, il server sarà disponibile solo nella rete di produzione.
    L'indirizzo IP pubblico verrà visualizzato dopo aver completato la configurazione. Per impostazione predefinita, la porta TCP 443 è aperta per le connessioni in entrata verso gli indirizzi IP pubblici.

    Nota
    Se si deseleziona la cartella di controllo **Utilizza indirizzo IP pubblico** o si elimina il server di ripristino, il relativo indirizzo IP pubblico non viene riservato.

12. [Facoltativo] Selezionare **Imposta soglia RPO**.
    La soglia RPO definisce l'intervallo di tempo massimo consentito tra l'ultimo punto di ripristino e l'ora corrente. È possibile impostare il valore tra 15–60 minuti, 1–24 ore, 1–14 giorni.
13. Definire il nome del server primario.
14. [Facoltativo] Specificare una descrizione per il server primario.
15. [Facoltativo] Fare clic sulla scheda **Regole del firewall cloud** per modificare le regole predefinite del firewall. Per ulteriori informazioni, consultare "Impostazione delle regole del firewall per server cloud" (pag. 824).
16. Fare clic su **Crea**.

Il server primario è ora disponibile nella rete di produzione. È possibile gestire il server utilizzando la relativa console, RDP, SSH o TeamViewer.

© Acronis International GmbH, 2003-2024



Operazioni con un server primario

Il server primario viene visualizzato nella scheda **Disaster Recovery** > **Server** > **Server primari** della console di Cyber Protect.

Per avviare o arrestare il server, fare clic su **Avvia** o **Arresta** nel riquadro del server primario.

Per modificare le impostazioni del server primario, arrestare il server e fare clic su **Modifica**.

Per applicare un piano di protezione al server primario, selezionarlo e fare clic su **Crea** nella scheda **Piano**. Verrà visualizzato un piano di protezione predefinito del quale è possibile modificare solo la pianificazione e le regole di conservazione. Per ulteriori informazioni, fare riferimento a "Backup dei server cloud".

Gestione dei server cloud

Per gestire i server cloud, passare a **Disaster Recovery** > **Server**. Sono disponibili due schede: **Server di ripristino** e **Server primari**. Per visualizzare tutte le colonne facoltative della tabella, fare clic sull'icona ingranaggio.

Selezionando ciascun server cloud saranno disponibili le seguenti informazioni.

Nome colonna	Descrizione
Nome	Il nome del server cloud definito dall'utente
Stato	Lo stato che riflette il problema più grave riscontrato in un server cloud (in base agli avvisi attivi)
Condizione	Una condizione di server cloud
Stato VM	Lo stato di alimentazione della macchina virtuale associata a un server cloud

© Acronis International GmbH, 2003-2024

Posizione attiva	La posizione in cui è ospitato il server cloud. Ad esempio, **Cloud**.
Soglia RPO	L'intervallo di tempo massimo consentito tra l'ultimo punto di ripristino idoneo per un failover e l'ora corrente. Il valore può essere impostato tra 15-60 minuti, 1-24 ore, 1-14 giorni.
Conformità RPO	La conformità RPO è il rapporto tra la soglia RPO effettiva e la soglia RPO definita. L'opzione Conformità RPO viene visualizzata se è stata definita la soglia RPO. Viene calcolata come indicato di seguito: **Conformità RPO = RPO effettiva/soglia RPO** dove **RPO effettiva = ora corrente – ora dell'ultimo punto di ripristino** **Stati di conformità RPO** In funzione del valore del rapporto tra la soglia RPO effettiva e la soglia RPO definita, vengono utilizzati gli stati seguenti: • **Conforme**. Conformità RPO < 1x. Un server rispetta la soglia RPO. • **Superato**. Conformità RPO <= 2x. Un server viola la soglia RPO. • **Gravemente superato**. Conformità RPO <= 4x. Un server viola la soglia RPO di un valore superiore al doppio consentito. • **Criticamente superato**. Conformità RPO > 4x. Un server viola la soglia RPO di un valore superiore al quadruplo consentito. • **In sospeso (nessun backup)**. Il server è protetto con il piano di protezione, tuttavia il backup creato non è stato ancora completato.
RPO effettivo	Tempo trascorso dalla creazione dell'ultimo punto di ripristino
Ultimo punto di ripristino	Data e ora in cui si è stato creato l'ultimo punto di ripristino

Regole del firewall per i server cloud

È possibile configurare le regole del firewall per controllare il traffico in entrata e in uscita dei server primario e di ripristino nel sito cloud.

È possibile configurare le regole in entrata dopo aver fornito un indirizzo IP pubblico al server cloud. Per impostazione predefinita, è consentita la porta TCP 443, mentre tutte le altre connessioni in entrata non vengono autorizzate. È possibile modificare le regole predefinite del firewall e aggiungere o rimuovere eccezioni in entrata. Se non è stato fornito un indirizzo IP pubblico, sarà possibile soltanto visualizzare le regole in entrata, ma non configurarle.

È possibile configurare le regole in uscita dopo aver fornito l'accesso a Internet per il server cloud. Per impostazione predefinita, è consentita la porta TCP 25, mentre tutte le altre connessioni in uscita sono autorizzate. È possibile modificare le regole predefinite del firewall e aggiungere o

© Acronis International GmbH, 2003-2024

rimuovere eccezioni in uscita. Se non è stato fornito un accesso a Internet, sarà possibile soltanto visualizzare le regole in uscita, ma non configurarle.

Nota
Per motivi di sicurezza, sono presenti regole del firewall predefinite che non è possibile modificare.

Per le connessioni in entrata e in uscita:

- Consenti ping: ICMP echo-request (type 8, code 0) and ICMP echo-reply (type 0, code 0)
- Consenti ICMP need-to-frag (type 3, code 4)
- Consenti TTL exceeded (type 11, code 0)

Solo per le connessioni in entrata:

- Parte non configurabile: Nega tutto

Solo per le connessioni in uscita:

- Parte non configurabile: Rifiuta tutto

Impostazione delle regole del firewall per server cloud

È possibile modificare le regole predefinite del firewall per i server primario e di ripristino nel cloud.

Per modificare le regole del firewall di un server nel sito cloud

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Server**.
2. Per modificare le regole del firewall di un server di ripristino, fare clic sulla scheda **Server di ripristino**. In alternativa, per modificare le regole del firewall di un server primario, fare clic sulla scheda **Server primari**.
3. Fare clic sul server, quindi scegliere **Modifica**.
4. Fare clic sulla scheda **Regole del firewall cloud**.
5. Per cambiare l'azione predefinita per le connessioni in entrata:

© Acronis International GmbH, 2003-2024

a. Nel campo a discesa **In entrata**, selezionare l'azione predefinita.

Azione	Descrizione
Nega tutto	Nega tutto il traffico in entrata. È possibile aggiungere eccezioni e consentire il traffico proveniente da indirizzi IP, protocolli e porte specifici.
Consenti tutto	Consente tutto il traffico TCP e UDP in entrata. È possibile aggiungere eccezioni e negare il traffico proveniente da indirizzi IP, protocolli e porte specifici.

Nota
La modifica dell'azione predefinita annulla e rimuove la configurazione delle regole in entrata esistenti.

b. [Facoltativo] Per salvare le eccezioni esistenti, nella finestra di conferma selezionare **Salvare le eccezioni compilate**.

c. Fare clic su **Conferma**.

6. Per aggiungere un'eccezione:

a. Fare clic su **Aggiungi eccezione**.

b. Specificare i parametri del firewall.

Parametro del firewall	Descrizione
Protocollo	Selezionare il protocollo di connessione. Sono supportate le seguenti opzioni: • **TCP** • **UDP** • **TCP+UDP**
Porta del server	Selezionare le porte alle quali applicare la regola. È possibile specificare quanto segue: • un numero di porta specifico (ad esempio `2298`) • un intervallo di numeri di porta (ad esempio `6000-6700`) • qualsiasi numero di porta. Utilizzare `*` per applicare la regola a qualsiasi numero di porta.
Indirizzo IP del client	Selezionare gli indirizzi IP ai quali applicare la regola. È possibile specificare quanto segue: • un indirizzo IP specifico (ad esempio `192.168.0.0`) • un intervallo di indirizzi IP mediante la notazione CIDR (ad esempio `192.168.0.0/24`) • qualsiasi indirizzo IP. Utilizzare `*` per applicare la regola a qualsiasi indirizzo IP.

© Acronis International GmbH, 2003-2024

7. Per rimuovere un'eccezione in entrata esistente, fare clic sull'icona del cestino accanto all'eccezione.
8. Per cambiare l'azione predefinita per le connessioni in uscita:
   a. Nel campo a discesa **In uscita**, selezionare l'azione predefinita.

Azione	Descrizione
Nega tutto	Nega tutto il traffico in uscita. È possibile aggiungere eccezioni e consentire il traffico verso indirizzi IP, protocolli e porte specifici.
Consenti tutto	Consente tutto il traffico in uscita. È possibile aggiungere eccezioni e negare il traffico proveniente da indirizzi IP, protocolli e porte specifici.

Nota
La modifica dell'azione predefinita annulla e rimuove la configurazione delle regole in uscita esistenti.

   b. [Facoltativo] Per salvare le eccezioni esistenti, nella finestra di conferma selezionare **Salvare le eccezioni compilate**.
   c. Fare clic su **Conferma**.
9. Per aggiungere un'eccezione:
   a. Fare clic su **Aggiungi eccezione**.
   b. Specificare i parametri del firewall.

Parametro del firewall	Descrizione
Protocollo	Selezionare il protocollo di connessione. Sono supportate le seguenti opzioni: • **TCP** • **UDP** • **TCP+UDP**
Porta del server	Selezionare le porte alle quali applicare la regola. È possibile specificare quanto segue: • un numero di porta specifico (ad esempio `2298`) • un intervallo di numeri di porta (ad esempio `6000-6700`) • qualsiasi numero di porta. Utilizzare `*` per applicare la regola a qualsiasi numero di porta.
Indirizzo IP del client	Selezionare gli indirizzi IP ai quali applicare la regola. È possibile specificare quanto segue: • un indirizzo IP specifico (ad esempio `192.168.0.0`) • un intervallo di indirizzi IP mediante la notazione CIDR (ad

© Acronis International GmbH, 2003-2024

Parametro del firewall	Descrizione
	esempio `192.168.0.0/24`) • qualsiasi indirizzo IP. Utilizzare * per applicare la regola a qualsiasi indirizzo IP.

10. Per rimuovere un'eccezione in uscita esistente, fare clic sull'icona del cestino accanto all'eccezione.
11. Fare clic su **Salva**.

Controllo delle attività del firewall cloud

Dopo un aggiornamento della configurazione delle regole del firewall di un server cloud, il registro dell'attività aggiornata è disponibile nella console di Cyber Protect. È possibile visualizzare il registro e verificare le seguenti informazioni:

- nome utente dell'utente che ha aggiornato la configurazione
- data e ora dell'aggiornamento
- impostazioni del firewall per le connessioni in entrata e in uscita
- azioni predefinite per le connessioni in entrata e in uscita
- protocolli, porte e indirizzi IP delle eccezioni per le connessioni in entrata e in uscita

Per visualizzare i dettagli delle modifiche alle configurazioni delle regole del firewall cloud

1. Nella console di Cyber Protect, fare clic su **Monitoraggio** > **Attività**.
2. Fare clic sull'attività corrispondente e quindi su **Tutte le proprietà**.
   La descrizione dell'attività dovrebbe essere **Aggiornamento configurazione del server cloud**.
3. Verificare le informazioni di interesse nel campo **Contesto**.

Backup dei server cloud

Il backup dei server primari e di ripristino viene eseguito in modalità agentless nel sito cloud. Questo tipo di backup presenta alcune limitazioni specifiche.

- L'unica posizione di backup possibile è l'archivio del cloud. Il backup dei server primari viene eseguito sullo storage di **backup dei server primari**.

  Nota
  Non sono supportate le posizioni di backup di Microsoft Azure.

© Acronis International GmbH, 2003-2024

- Non è possibile applicare un piano di backup a più server. Ogni server deve quindi disporre del proprio piano di backup, anche se tutti i piani di backup presentano le stesse impostazioni.
- A un server può essere applicato un solo piano di backup.
- Non è supportato il backup compatibile con le applicazioni.
- La crittografia non è disponibile.
- Non sono disponibili opzioni di backup.

Quando si elimina un server primario vengono eliminati anche i rispettivi backup.

Il backup di un server di ripristino viene eseguito solo in condizioni di failover. Tale backup prosegue la sequenza di backup del server originario. All'esecuzione del failback, il server originario potrà continuare questa sequenza di backup. Ne consegue che i backup del server di ripristino possano essere eliminati solo manualmente o come risultato dell'applicazione delle regole di conservazione. Quando viene eliminato un server di ripristino, i relativi backup vengono sempre conservati.

Nota
I piani di backup per i server cloud vengono eseguiti in base al fuso orario UTC.

Orchestrazione (runbook)

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

Un runbook è un insieme di istruzioni che descrive come allestire l'ambiente di produzione nel cloud. I runbook vengono creati nella console di Cyber Protect. Per accedere alla schermata **Runbooks**, selezionare **Disaster Recovery** > **Runbooks**.

Perché utilizzare i runbook?

Con i runbooks è possibile:

- Rendere automatico il failover di uno o più server
- Controllare automaticamente il risultato del failover eseguendo il ping dell'indirizzo IP del server e controllando la connessione alla porta specificata
- Impostando la sequenza di operazioni per i server che eseguono applicazioni distribuite
- Includere operazioni manuali nel flusso di lavoro
- Verificare l’integrità della soluzione di disaster recovery eseguendo i runbook in modalità di prova.

© Acronis International GmbH, 2003-2024

Creazione di runbook

Un runbook è costituito da passaggi che vengono eseguiti consecutivamente. Un passaggio è costituito da azioni il cui avvio è simultaneo.

È possibile attenersi alle istruzioni seguenti o guardare il tutorial video.

Per creare un runbook

1. Nella console di Cyber Protection, passare a **Disaster Recovery** > **Runbooks**.
2. Fare clic su **Crea runbook**.
3. Fare clic su **Aggiungi passaggio**.
4. Fare clic su **Aggiungi azione**, quindi selezionare l'azione da aggiungere al passaggio.

Azione	Descrizione
Esegui il failover del server	Esegue il failover di un server cloud. Per definire questa azione, è necessario selezionare un server cloud e configurare i parametri del runbook disponibili per questa azione. Per ulteriori informazioni su questi parametri, consultare "Parametri del runbook" (pag. 831). **Nota** Se il backup del server selezionato è stato crittografato utilizzando la crittografia come proprietà del sistema, l'azione **Esegui il failover del server** viene sospesa e modificata automaticamente in **Richiesta interazione**. Per procedere con l'esecuzione del runbook, fornire la password del backup crittografato.
Esegui il failback del server	Esegue il failback di un server cloud. Per definire questa azione, è necessario selezionare un server cloud e configurare i parametri del runbook disponibili per questa azione. Per ulteriori informazioni su queste impostazioni, consultare "Parametri del runbook" (pag. 831). **Nota** Le operazioni runbook supportano solo il failback in modalità manuale. Ciò significa che se si avvia il processo di failback eseguendo un runbook che include il passaggio **Esegui il failback del server**, la procedura richiederà un'interazione manuale: sarà necessario ripristinare manualmente il sistema, e confermare o annullare il processo di failback dalla scheda **Disaster Recovery** > **Server**.
Avvia server	Avvia un server cloud. Per definire questa azione, è necessario selezionare un server cloud e configurare i parametri del runbook disponibili per questa azione. Per ulteriori informazioni su queste impostazioni, consultare "Parametri del runbook" (pag. 831).

© Acronis International GmbH, 2003-2024

Azione	Descrizione
	Nota L'azione **Avvia server** non è applicabile alle operazioni di failover di prova nei runbook. Il tentativo di esecuzione di questa azione non riesce e restituisce il seguente messaggio di errore: Non riuscita: L'azione non è applicabile allo stato del server corrente.
Arresta server	Arresta un server cloud. Per definire questa azione, è necessario selezionare un server cloud e configurare i parametri del runbook disponibili per questa azione. Per ulteriori informazioni su queste impostazioni, consultare "Parametri del runbook" (pag. 831). **Nota** L'azione **Arresta server** non è applicabile alle operazioni di failover di prova nei runbook. Il tentativo di esecuzione di questa azione non riesce e restituisce il seguente messaggio di errore: Non riuscita: L'azione non è applicabile allo stato del server corrente.
Operazione manuale	Un'operazione manuale richiede un'interazione da parte di un utente. Per definire questa azione, è necessario inserire una descrizione. Quando una sequenza di runbook raggiunge un'operazione manuale, il runbook viene sospeso e non procede fino a quando un utente non esegue l'operazione manuale necessaria, ad esempio fare clic sul pulsante di conferma.
Esegui runbook	Esegue un altro runbook. Per definire questa azione, è necessario scegliere un runbook. Un runbook può includere solo un'esecuzione di un determinato runbook. Se, ad esempio, è stata aggiunta l'azione "Esegui Runbook A", è possibile aggiungere l'azione "Esegui Runbook B", ma non è possibile aggiungere un'altra azione "Esegui Runbook A".

5. Definire i parametri del runbook per l'azione. Per ulteriori informazioni su questi parametri, consultare "Parametri del runbook" (pag. 831).
6. [Facoltativo] Per aggiungere una descrizione del passaggio:
   a. Fare clic sull'icona dei puntini di sospensione, quindi su **Descrizione**.
   b. Inserire una descrizione del passaggio.
   c. Fare clic su **Fine**.
7. Ripetere i passaggi da 3 a 6 fino a quando non si ottiene la sequenza desiderata di passaggi e azioni.
8. [Facoltativo] Per modificare il nome predefinito del runbook:
   a. Fare clic sull'icona dei puntini di sospensione.
   b. Inserire il nome del runbook.

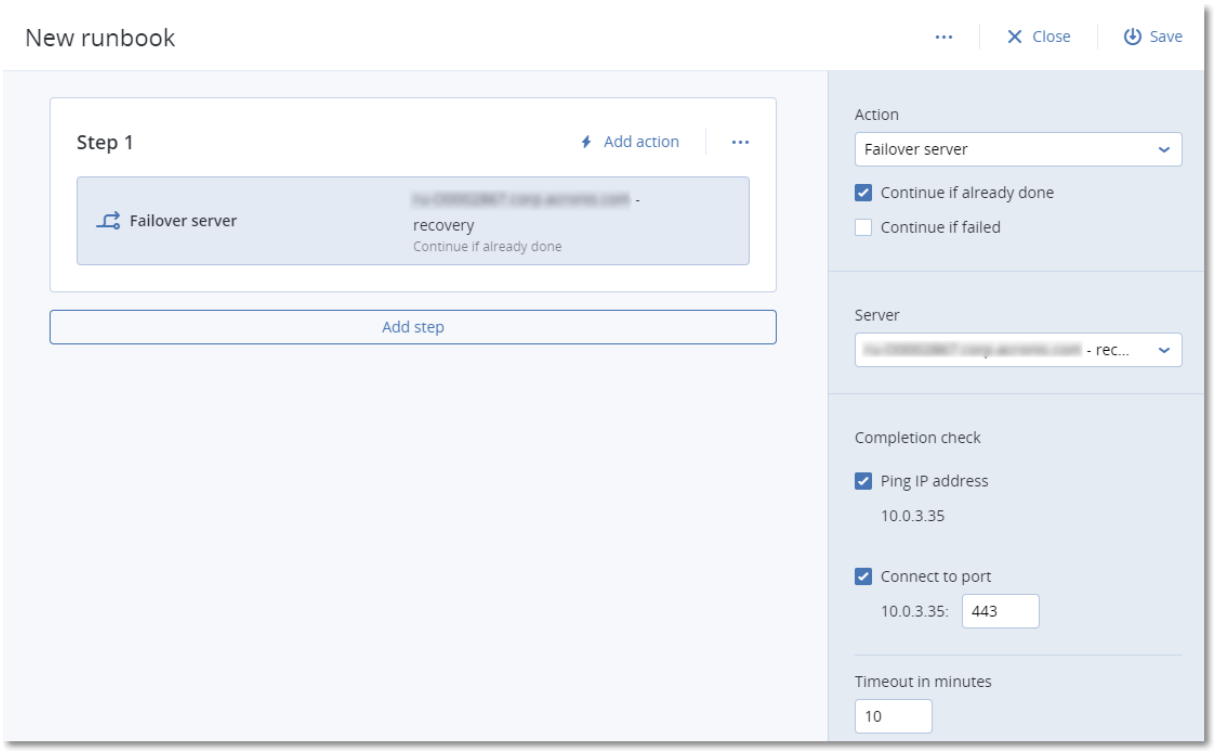
© Acronis International GmbH, 2003-2024

c. Inserire una descrizione del runbook.

d. Fare clic su **Fine**.

9. Fare clic su **Salva**.

10. Fare clic su **Chiudi**.



Parametri del runbook

I parametri del runbook sono impostazioni specifiche che devono essere configurate per definire un'azione del runbook. Esistono due categorie di parametri dei runbook: i parametri di azione e parametri di controllo della completezza.

I parametri di azione definiscono il comportamento del runbook in base allo stato iniziale o al risultato dell'azione.

I parametri di controllo della completezza verificano che il server sia disponibile e in grado di fornire i servizi necessari. Se un controllo di completezza non ha esito positivo, l'intera azione viene considerata non riuscita.

La tabella seguente descrive i parametri del runbook configurabili per ogni azione.

Parametro del runbook	Categoria	Disponibile per l'azione	Descrizione
Continuare se già completata	Parametro dell'azione	• **Esegui il failover del server**	Questo parametro definisce il comportamento del runbook quando l'azione richiesta è già stata completata

© Acronis International GmbH, 2003-2024

Parametro del runbook	Categoria	Disponibile per l'azione	Descrizione
		• **Avvia server** • **Arresta server** • **Esegui il failback del server**	(ad esempio, un failover è già stato eseguito o un server è già in esecuzione). Quando è attivo, il runbook invia un avviso e procede. Quando non è attivo, l'azione e il runbook non hanno esito positivo. Per impostazione predefinita, questo parametro è abilitato.
Continuare se non riuscita	Parametro dell'azione	• **Esegui il failover del server** • **Avvia server** • **Arresta server** • **Esegui il failback del server**	Questo parametro definisce il comportamento del runbook quando l'azione richiesta non riesce. Quando è attivo, il runbook invia un avviso e procede. Quando non è attivo, l'azione e il runbook non hanno esito positivo. Per impostazione predefinita, questo parametro è disabilitato.
Indirizzo IP del ping	Controllo del completamento	• **Avvia server**	Il software esegue il ping dell'indirizzo IP di produzione del server cloud fino a quando il server risponde o il timeout scade, a seconda della condizione che si verifica per prima.
Connetti alla porta (443 per impostazione predefinita)	Controllo del completamento	• **Esegui il failover del server** • **Avvia server**	Il software tenta di connettersi al server cloud usando l'indirizzo IP di produzione e la porta specificata, fino a quando la connessione viene stabilita o il timeout scade, a seconda della condizione che si verifica per prima. In questo modo è possibile controllare che l'applicazione in ascolto sulla porta specificata sia in esecuzione.
Timeout in minuti	Controllo del completamento	• **Esegui il failover del server** • **Avvia server**	Il timeout predefinito è di 10 minuti.

Operazioni con i runbook

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

© Acronis International GmbH, 2003-2024

Per accedere all'elenco delle operazioni, al passaggio del mouse sul runbook fare clic sull'icona con i puntini di sospensione. Se il runbook non è in esecuzione, sono disponibili le seguenti operazioni:

- **Esegui**
- **Modifica**
- **Clona**
- **Elimina**

Esecuzione di un runbook

Ogni volta che l'utente fa clic su **Esegui**, vengono richiesti i parametri di esecuzione. Tali parametri si applicano a tutte le operazioni di failover e failback incluse nel runbook. I runbook specificati nelle operazioni **Esegui runbook** ereditano tali parametri dal runbook principale.

- **Modalità di failover e failback**
  Selezionare se si desidera eseguire un failover di prova (impostazione predefinita) o un failover reale (produzione). La modalità di failback corrisponderà alla modalità di failover scelta.
- **Punto di ripristino di failover**
  Scegliere il punto di ripristino di failover più recente (impostazione predefinita) o selezionare un punto temporizzato passato. Nell'ultimo caso, per ogni server vengono selezionati i punti di ripristino più vicini precedenti alla data e all'ora specificate.

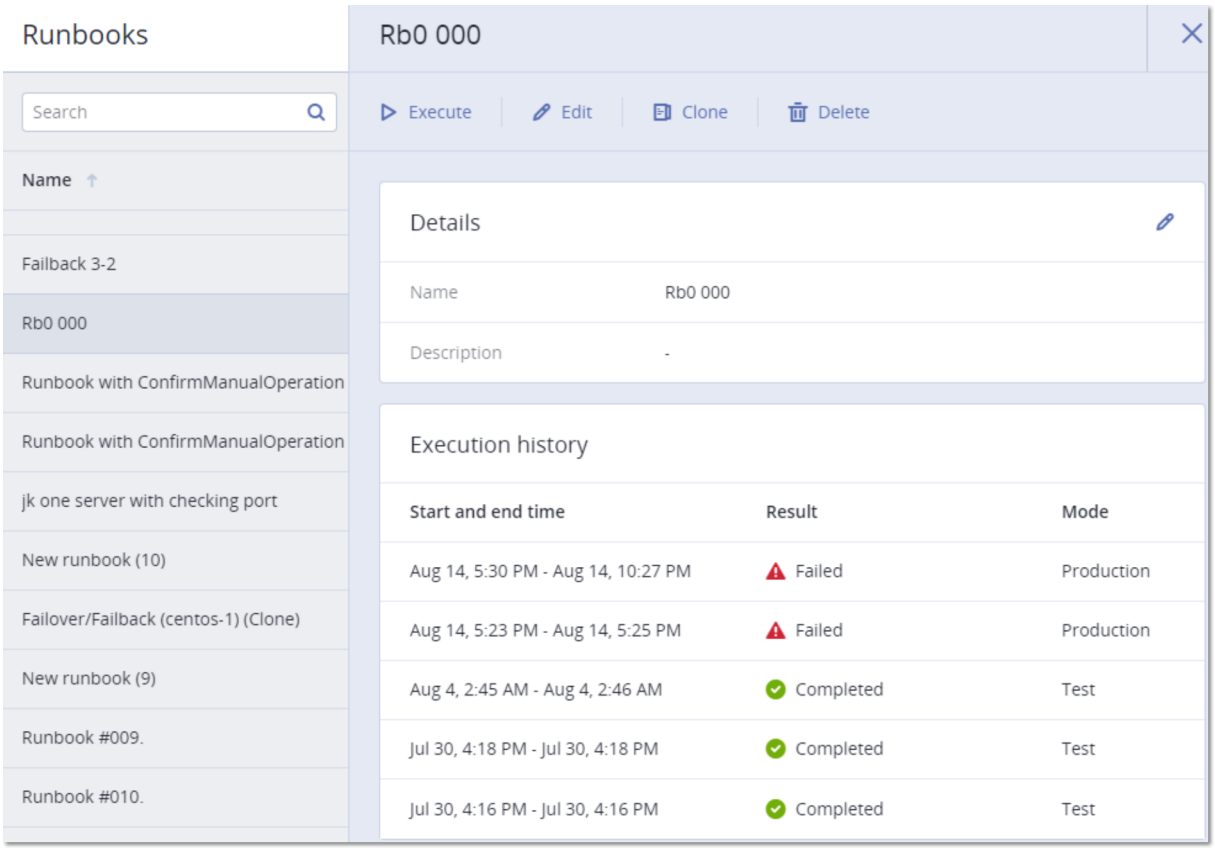
Arresto dell'esecuzione di un runbook

Durante l'esecuzione di un runbook è possibile selezionare l'opzione **Arresta** nell'elenco delle operazioni. Il software porterà a termine tutte le azioni già avviate ad eccezione di quelle che richiedono l'interazione dell'utente.

Visualizzazione della cronologia dell'esecuzione

Quando si seleziona un runbook nella scheda **Runbooks**, il software visualizza informazioni sul runbook e la cronologia di esecuzione. Fare clic sulla riga corrispondente a un'esecuzione specifica per visualizzare il log dell'esecuzione.

© Acronis International GmbH, 2003-2024



© Acronis International GmbH, 2003-2024

Configurazione della protezione antivirus e anti-malware

Nota
Nei sistemi Windows, la funzionalità di protezione anti-malware richiede l'installazione dell'Agente per la protezione anti-malware e la funzionalità di filtro degli URL richiede l'installazione dell'Agente per il filtro URL. Tali agenti vengono installati automaticamente per i workload protetti se i moduli **Protezione antivirus e anti-malware** e/o **Filtro URL** sono abilitati nei rispettivi piani di protezione.

La protezione anti-malware di Cyber Protection offre i seguenti vantaggi:

- Protezione superiore in ogni fase: proattiva, attiva e reattiva.
- Quattro diverse tecnologie anti-malware incluse, per fornire una protezione a più livelli d'eccellenza.
- Gestione di Microsoft Security Essentials e Microsoft Defender Antivirus.

  Nota
  La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Importante
È possibile rilevare il file di test EICAR solo se l'opzione **Advanced Antimalware** è abilitata nel piano di protezione. Tuttavia, il mancato rilevamento del file EICAR non incide sulle funzionalità anti-malware di Cyber Protection.

Piattaforme supportate

Le funzionalità Active Protection e Protezione antivirus e anti-malware sono supportate dalle piattaforme seguenti.

Sistema operativo	Versione/Distribuzione
Windows	Windows 7 Service Pack 1 e versioni successive Windows Server 2008 R2 Service Pack 1 e versioni successive

© Acronis International GmbH, 2003-2024

Sistema operativo	Versione/Distribuzione
	Nota Per Windows 7, è necessario installare i seguenti aggiornamenti Microsoft prima di installare l'agente di protezione. • Windows 7 Extended Security Updates (ESU) • KB4474419 • KB4490628 Per ulteriori informazioni sugli aggiornamenti richiesti, fare riferimento a questo articolo della Knowledge Base.
Linux	Red Hat Linux 7.x, 8.x, 9.x CloudLinux 6.10, 7.x, 8.x CentOS 6.5 e versioni 6.x successive, 7.x, 8.x Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 Debian 8.x, 9.x, 10,x, 11.x Oracle Linux 7.x, 8.x, 9.x SUSE Enterprise Linux 15.x openSUSE Leap 15.x
macOS	macOS 10.13.x e versioni successive

Funzionalità supportate per piattaforma

Nota
La protezione anti-malware per Linux e macOS è disponibile con il pacchetto Advanced Antimalware.

Caratteristiche	Windows	Linux	macOS
Protezione antivirus e anti-malware			
Funzionalità Active Protection completamente integrata	Sì	No	No
Protezione antimalware in tempo reale	Sì	Sì, con il pacchetto Advanced Antimalware	Sì, con il pacchetto Advanced Antimalware
Protezione antimalware Advanced in tempo reale con individuazione basata sulle firme in locale	Sì	Sì	Sì

© Acronis International GmbH, 2003-2024

Caratteristiche	Windows	Linux	macOS
Protezione antivirus e anti-malware			
Analisi statica per i file eseguibili con portabilità	Sì	No	Sì*
Scansione anti-malware su richiesta	Sì	Sì**	Sì
Protezione delle cartelle di rete	Sì	Sì	No
Protezione lato server	Sì	No	No
Scansione dei file archiviati	Sì	No	Sì
Scansione delle unità rimovibili	Sì	No	Sì
Scansione dei soli file nuovi e modificati	Sì	No	Sì
Esclusioni di cartelle/file	Sì	Sì	Sì***
Esclusioni di processi	Sì	No	Sì
Motore di analisi comportamentale	Sì	No	Sì
Prevenzione degli exploit	Sì	No	No
Quarantena	Sì	Sì	Sì
Pulizia automatica della cartella di quarantena	Sì	Sì	Sì
Filtro URL (http/https)	Sì	No	No
Elenco degli elementi consentiti aziendale	Sì	No	Sì
Gestione firewall****	Sì	No	No
Gestione di Microsoft Defender Antivirus*****	Sì	No	No
Gestione di Microsoft Security Essentials	Sì	No	No
Registrazione e gestione della protezione antivirus e anti-malware tramite il Centro sicurezza PC Windows	Sì	No	No
Per ulteriori informazioni sui sistemi operativi supportati e sulle rispettive versioni, consultare "Piattaforme supportate" (pag. 835).			

* L'analisi statica dei file eseguibili con portabilità è supportata solo per le scansioni pianificate su macOS.

** Le condizioni di avvio non sono supportate per la scansione su richiesta su Linux.

© Acronis International GmbH, 2003-2024

*** Le esclusioni di file/cartelle sono supportate solo nel caso in cui vengano specificati file e cartelle che non verranno scansionati dalla protezione in tempo reale o durante le scansioni pianificate su macOS.

**** La funzionalità di gestione del firewall è supportata in Windows 8 e versioni successive. Windows Server non è supportato.

***** La gestione di Windows Defender Antivirus è supportata in Windows 8.1 e versioni successive.

Caratteristiche	Windows	Linux	macOS
Active Protection			
Individuazione dell'iniezione di processi	Sì	No	No
Ripristino automatico dei file interessati dalla cache locale	Sì	Sì	Sì
Autodifesa dei file di backup Acronis	Sì	No	No
Autodifesa del software Acronis	Sì	No	Sì (Solo componenti di Active Protection e Anti-malware)
Gestione dei processi affidabili/bloccati	Sì	No	Sì
Esclusione di processi/cartelle	Sì	Sì	Sì
Individuazione del ransomware basata sul comportamento di un processo (basata su IA)	Sì	Sì	Sì
Individuazione dei processi di mining delle criptovalute basata sul comportamento di un processo	Sì	No	No
Protezione di unità esterne (HDD, unità flash, schede SD)	Sì	No	Sì
Protezione delle cartelle di rete	Sì	Sì	Sì
Protezione lato server	Sì	No	No
Protezione per Zoom, Cisco Webex, Citrix Workspace e Microsoft Teams	Sì	No	No
Per ulteriori informazioni sui sistemi operativi supportati e sulle rispettive versioni, consultare "Piattaforme supportate" (pag. 835).			

© Acronis International GmbH, 2003-2024

Protezione antivirus e anti-malware

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

Il modulo **Protezione antivirus e anti-malware** protegge i sistemi Windows, Linux e macOS da tutte le minacce malware più recenti. Consultare l'elenco completo delle funzioni anti-malware supportate in "Piattaforme supportate" (pag. 835).

Protezione antivirus e anti-malware è supportata e registrata in Windows Security Center.

Funzionalità anti-malware

- Individuazione del malware nei file in modalità di protezione in tempo reale e su richiesta
- Individuazione di comportamenti potenzialmente dannosi nei processi (per Windows)
- Blocco dell'accesso ai URL dannosi (per Windows)
- Posizionamento in quarantena dei file pericolosi
- Aggiunta di applicazioni aziendali attendibili alla lista di elementi consentiti

Tipi di scansione

È possibile configurare la protezione antivirus e anti-malware affinché sia eseguita costantemente in background o su richiesta.

Protezione in tempo reale

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

La protezione in tempo reale controlla tutti i file eseguiti o aperti nel sistema, per contrastare le minacce malware.

Per evitare possibili problemi di compatibilità e prestazioni, la protezione in tempo reale non può operare parallelamente ad altre soluzioni antivirus che utilizzano a loro volta le funzioni di protezione in tempo reale. Gli stati delle altre soluzioni antivirus installate vengono determinati tramite il Centro sicurezza PC Windows. Se il sistema Windows è già protetto da un'altra soluzione antivirus, la protezione in tempo reale viene disattivata in modo automatico.

Per attivare la protezione in tempo reale, disattivare o disinstallare l'altra soluzione antivirus. La protezione in tempo reale può sostituire automaticamente quella di Microsoft Defender.

© Acronis International GmbH, 2003-2024

Nota
Nei sistemi che eseguono Windows Server, Microsoft Defender non viene disattivato automaticamente quando è attivata la protezione in tempo reale. Per evitare potenziali problemi di compatibilità, è necessario che un amministratore disattivi manualmente Microsoft Defender.

È possibile selezionare una delle seguenti modalità di scansione:

- La scansione **Smart all'accesso** esegue il programma anti-malware in background e controlla in modo costante e attivo il sistema per individuare virus e altre minacce potenzialmente dannose, per tutto il tempo in cui il sistema è attivo. Il malware viene individuato in entrambi i casi, sia durante l'esecuzione del file sia durante le varie operazioni compiute sul file, come l'apertura per la lettura o la modifica.
- La scansione **Al momento dell'esecuzione** prevede solo l'analisi dei file eseguibili nel momento in cui vengono eseguiti, per garantire che siano puliti e che non possano danneggiare il sistema o i dati. La copia di un file infetto non viene individuata.

Scansione pianificata

La scansione anti-malware viene eseguita in base alla pianificazione.

È possibile selezionare una delle seguenti modalità di scansione.

- **Scansione rapida** - Controlla solo i file system del workload.
- **Scansione completa** - Controlla tutti i file nel workload.
- **Scansione personalizzata** - Controlla i file/le cartelle aggiunti dall'amministratore al piano di protezione.

Una volta completata la scansione anti-malware, è possibile visualizzare i dettagli relativi ai workload colpiti dalle minacce nel widget **Monitoraggio** > **Panoramica** > Recentemente interessato.

Impostazioni di Protezione antivirus e anti-malware

Questa sezione illustra le funzionalità che è possibile configurare nel modulo **Protezione antivirus e anti-malware** in un piano di protezione. Per ulteriori informazioni su come creare un piano di protezione, consultare "Creazione di un piano di protezione" (pag. 218).

Per il modulo Protezione antivirus e anti-malware di un piano di protezione è possibile configurare le funzionalità seguenti.

- "Active Protection" (pag. 841)
- "Advanced Antimalware" (pag. 842)
- "Protezione delle cartelle di rete" (pag. 842)
- "Protezione lato server" (pag. 843)
- "Auto-protezione" (pag. 844)

© Acronis International GmbH, 2003-2024

- "Individuazione dei processi di mining delle criptovalute" (pag. 845)
- "Quarantena" (pag. 845)
- "Motore comportamentale" (pag. 846)
- "Prevenzione degli exploit" (pag. 846)
- "Protezione in tempo reale" (pag. 848)
- "Pianifica scansione" (pag. 849)
- "Esclusioni dalla protezione" (pag. 853)

Nota
Non tutti i sistemi operativi supportano le funzionalità di Protezione antivirus e anti-malware. Per ulteriori informazioni sui sistemi operativi e sulle funzionalità supportate, consultare "Piattaforme supportate" (pag. 835). Alcune funzionalità richiedono una licenza specifica per essere disponibili nel piano di protezione.

Active Protection

Active Protection protegge il sistema dal software dannoso noto come ransomware, che crittografa i file e chiede un riscatto per la chiave di crittografia.

Impostazione predefinita: **Abilitata**.

Nota
Sul sistema protetto deve essere installato un agente di protezione. Per ulteriori informazioni sulle funzionalità e i sistemi operativi supportati consultare "Piattaforme supportate" (pag. 835).

Per configurare Active Protection

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Active Protection**.
3. Nella sezione **Azione al rilevamento**, selezionare una delle opzioni disponibili:

   Impostazione predefinita: **Ripristina utilizzando la cache**

   - **Solo notifica**: il software genera un avviso relativo al processo sospettato di attività ransomware.
   - **Arresta il processo**: il software genera un avviso e arresta il processo sospettato di attività ransomware.
   - **Ripristina utilizzando la cache**: il software genera un avviso, arresta il processo e ripristina le modifiche apportate al file utilizzando la cache del servizio.
4. Fare clic su **Fine** per applicare le opzioni selezionate al piano di protezione.

© Acronis International GmbH, 2003-2024

Advanced Antimalware

Questo motore si avvale di un database avanzato contenente le firme dei virus, per aumentare l'efficienza del rilevamento anti-malware nelle scansioni rapide e complete.

Importante
Questa funzionalità è disponibile solo se è abilitato il pacchetto di protezione Advanced Security. Per ulteriori informazioni, vedere https://www.acronis.com/it-it/products/cloud/cyber-protect/security/

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Per configurare Advanced Antimalware

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Nella sezione **Advanced Antimalware** utilizzare l'interruttore per abilitare il motore basato su firma locale.

Nota
Anche la protezione antivirus e anti-malware per macOS e Linux richiede il motore locale basato sulle firme. In Windows, la protezione antivirus e antimalware è disponibile con o senza questo motore.

Protezione delle cartelle di rete

La funzionalità **Protezione delle cartelle di rete** determina se Protezione antivirus e anti-malware protegge le cartelle di rete mappate come unità locali. La protezione viene applicata alle cartelle condivise tramite protocolli SMB o NFS.

Per configurare la protezione delle cartelle di rete

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Protezione delle cartelle di rete**.
3. Aggiungere i file nella posizione in cui eseguire il backup delle cartelle di rete.
   - Se, ad esempio, il workload è Windows, nel campo **Windows** aggiungere il percorso al file Windows in cui eseguire il backup delle cartelle di rete. Valore predefinito: C:\ProgramData\Acronis\Restored Network Files.
   - Se, ad esempio, il workload è macOS, nel campo **macOS** aggiungere il percorso al file macOS in cui eseguire il backup delle cartelle di rete. Valore predefinito: /Library/Application Support/Acronis/Restored Network Files/.

© Acronis International GmbH, 2003-2024

Nota
Inserire il percorso di una cartella locale. Le cartelle di rete, incluse quelle sulle unità mappate, non sono supportate come destinazioni di backup per le cartelle di rete.

4. Fare clic su **Fine** per applicare le opzioni selezionate al piano di protezione.

Protezione lato server

Questa funzionalità determina se Active Protection protegge le cartelle di rete condivise dall'utente dai collegamenti esterni in ingresso da altri server nella rete, che potrebbero determinare l'introduzione di minacce.

Impostazione predefinita: **Disattivata**.

Nota
La protezione lato server non è supportata in Linux.

Per impostare connessioni affidabili

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Protezione lato server**.
3. Utilizzare l'interruttore **Protezione lato server** per abilitare la funzionalità.
4. Selezionare la scheda **Attendibili**.
5. Nel campo **Connessioni affidabili**, fare clic su **Aggiungi** per specificare le connessioni a cui è consentita la modifica dei dati.
6. Nel campo **Nome computer/Account** digitare il nome del computer e l'account del sistema in cui è installato l'agente di protezione. Ad esempio, `MyComputer\TestUser`.
7. Nel campo **Nome host** digitare il nome host del sistema al quale è consentita la connessione al sistema che utilizza l'agente di protezione.
8. Fare clic sul segno di spunta a destra per salvare la definizione della connessione.
9. Fare clic su **Fine**.

Per impostare connessioni bloccate

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Protezione lato server**.
3. Utilizzare l'interruttore **Protezione lato server** per abilitare la funzionalità.
4. Selezionare la scheda **Bloccati**.
5. Nel campo **Connessioni bloccate**, fare clic su **Aggiungi** per specificare le connessioni a cui non è consentita la modifica dei dati.

© Acronis International GmbH, 2003-2024

6. Nel campo **Nome computer/Account** digitare il nome del computer e l'account del sistema in cui è installato l'agente di protezione. Ad esempio, `MyComputer\TestUser`.
7. Nel campo **Nome host** digitare il nome host del sistema al quale è consentita la connessione al sistema che utilizza l'agente di protezione.
8. Selezionare la casella di controllo a destra per salvare la definizione della connessione.
9. Fare clic su **Fine**.

Auto-protezione

L'auto-protezione impedisce modifiche non autorizzate ai processi del software, ai record del Registro di sistema, ai file eseguibili e di configurazione e ai backup posizionati nelle cartelle locali.

Gli amministratori possono abilitare l' **Auto-protezione** senza abilitare **Active Protection**.

Impostazione predefinita: **Attiva**.

Nota
L'auto-protezione non è supportata in Linux.

Per abilitare l'auto-protezione

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Auto-protezione**.
3. Utilizzare l'interruttore **Auto-protezione** per abilitare la funzionalità.

Per abilitare la protezione con password

1. Dopo aver abilitato la funzionalità **Auto-protezione**, è possibile abilitare la **Protezione con password** utilizzando il relativo interruttore.
2. Fare clic su **Genera nuova password** per ottenere una password per la modifica o l'eliminazione degli agenti locali.
3. Fare clic su **Copia**, quindi incollare la password in un luogo sicuro; viene richiesta per la modifica dell'elenco dei componenti a livello locale.

   Importante
   La password non sarà più disponibile dopo la chiusura della finestra. Per applicare questa password ai dispositivi, è necessario salvare le impostazioni del piano di protezione.

4. Fare clic su **Chiudi**.

Protezione con password impedisce a utenti o software non autorizzati di disinstallare l'Agente per Windows o di modificarne i componenti. Queste azioni diventano possibili solo con una password fornita da un amministratore.

Non è mai richiesta la password per le seguenti azioni:

© Acronis International GmbH, 2003-2024

- Aggiornare l'installazione eseguendo nuovamente il programma di installazione in locale
- Aggiornamento dell'installazione con la console di Cyber Protect
- Riparare l'installazione

Impostazione predefinita: **Disabilitato**

Per ulteriori informazioni su come abilitare **Protezione con password**, fare riferimento a Impedire la disinstallazione o la modifica non autorizzate degli agenti.

Individuazione dei processi di mining delle criptovalute

I malware di mining di criptovalute influiscono negativamente sulle prestazioni delle applicazioni utili, aumentano i costi dei consumi elettrici, possono causare arresti anomali del sistema e perfino guasti hardware dovuti all'eccessivo utilizzo. La funzionalità **Individuazione dei processi di mining delle criptovalute** protegge i dispositivi dai malware che eseguono il mining delle criptovalute, per impedire l'utilizzo non autorizzato delle risorse del computer.

Gli amministratori possono abilitare l'**Individuazione dei processi di mining delle criptovalute** senza abilitare **Active Protection**. Impostazione predefinita: **Abilitato**.

Nota
L'individuazione dei processi di mining delle criptovalute non è supportata in Linux.

Per configurare la protezione delle cartelle di rete

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Individuazione dei processi di mining delle criptovalute**.
3. Utilizzare l'interruttore **Individua i processi di mining delle criptovalute** per abilitare o disabilitare la funzionalità.
4. Specificare l'azione da compiere sui processi sospettati di attività di mining di criptovalute:

   Impostazione predefinita: **Arresta il processo**

   - **Solo notifica**: il software genera un avviso.
   - **Arresta il processo**: il software genera un avviso e arresta il processo.
5. Fare clic su **Fine** per applicare le opzioni selezionate al piano di protezione.

Quarantena

Quarantena è una cartella nella quale vengono isolati i file sospetti (probabilmente infetti) o potenzialmente pericolosi.

Per configurare la quarantena

© Acronis International GmbH, 2003-2024

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Quarantena**.
3. Nel campo **Rimuovi i file posti in quarantena dopo** è possibile specificare il periodo in giorni al termine del quale i file in quarantena verranno rimossi.
   Impostazione predefinita: **30 giorni**
4. Fare clic su **Fine**.

Per ulteriori informazioni su questa funzionalità, fare riferimento a Quarantena.

Motore comportamentale

La funzionalità **Motore comportamentale** protegge un sistema dal malware usando tecniche di euristica comportamentale per identificare i processi pericolosi.

Impostazione predefinita: **Abilitata**.

Nota
Il motore comportamentale non è supportato in Linux.

Per configurare la protezione delle cartelle di rete

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Motore comportamentale**.
3. Utilizzare l'interruttore **Motore comportamentale** per abilitare o disabilitare la funzionalità.
4. Nella sezione **Azione al rilevamento**, selezionare l'azione che il software dovrà eseguire quando viene individuata un'attività malware:
   Impostazione predefinita: **Quarantena**
   - **Solo notifica**: il software genera un avviso relativo al processo sospettato di attività malware.
   - **Arresta il processo**: il software genera un avviso e arresta il processo sospettato di attività malware.
   - **Quarantena**: il software genera un avviso, arresta il processo e sposta il file eseguibile nella cartella della quarantena.
5. Fare clic su **Fine** per applicare le opzioni selezionate al piano di protezione.

Prevenzione degli exploit

Importante
Questa funzionalità è disponibile solo se è abilitato il pacchetto di protezione Advanced Security. Per ulteriori informazioni, vedere https://www.acronis.com/it-it/products/cloud/cyber-protect/security/

© Acronis International GmbH, 2003-2024

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

La prevenzione degli exploit individua e previene i processi infetti che possono diffondersi e sfruttare le vulnerabilità software dei sistemi. Quando viene rilevato un exploit, il software può generare un avviso relativo al processo sospettato di attività di exploit e lo arresta.

La prevenzione degli exploit è disponibile solo con le versioni dell'agente 12.5.23130 (21.08, rilasciata ad agosto 2020) o successive.

Impostazione predefinita: **Abilitata** per i piani di protezione appena creati e **Disabilitata** per quelli esistenti, creati con versioni precedenti dell'agente.

Nota
La prevenzione degli exploit non è supportata in Linux.

È possibile selezionare le azioni che il programma dovrebbe compiere al rilevamento di un exploit, e quali metodi di prevenzione degli exploit vengono applicati dal programma.

Per configurare la prevenzione degli exploit

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Prevenzione degli exploit**.
3. Nella sezione **Azione al rilevamento**, selezionare una delle opzioni disponibili:

   Impostazione predefinita: **Arresta il processo**

   - **Solo notifica**
     Il software genera un avviso relativo al processo sospettato di attività di exploit.
   - **Arresta il processo**
     Il software genera un avviso e arresta il processo sospettato di attività di exploit.
4. Nella sezione **Tecniche di prevenzione degli exploit abilitate** selezionare tra le opzioni disponibili quelle da applicare:

   Impostazione predefinita: **Tutti i metodi sono abilitati**

   - **Protezione della memoria**
     Individua e previene modifiche sospette alle autorizzazioni di esecuzione nelle pagine della memoria. I processi dannosi applicano tali modifiche alle proprietà della pagina per abilitare l'esecuzione di codici della shell da aree di memoria non eseguibile, quali stack e heap.
   - **Protezione da attacchi ROP (Return-oriented programming)**
     Rileva e previene i tentativi di utilizzo della tecnica di exploit ROP.
   - **Protezione dall'escalation dei privilegi**
     Individua e previene i tentativi di innalzamento dei privilegi effettuati da codice o applicazioni non autorizzati. L'escalation dei privilegi viene utilizzata dai codici pericolosi per ottenere l'accesso completo al sistema attaccato, e per eseguire quindi attività critiche e inerenti a dati

© Acronis International GmbH, 2003-2024

sensibili. Al codice non autorizzato non è consentito l'accesso alle risorse di critiche del sistema o la modifica delle impostazioni di sistema.

- **Protezione dall'iniezione di codice**

  Individua e previene l'iniezione di codice dannoso nei processi remoti. L'iniezione di codice viene utilizzata per nascondere le finalità dannose di un'applicazione all'interno di processi puliti o non pericolosi, per eludere l'individuazione da parte di prodotti anti-malware.

5. Fare clic su **Fine** per applicare le opzioni selezionate al piano di protezione.

Nota
I processi elencati come attendibili nell'elenco delle esclusioni non saranno esaminati in cerca di exploit.

Autorizzazione alla modifica del backup da parte di processi specifici

L'opzione **Consenti a processi specifici di modificare i backup** è disponibile solo quando è abilitata l'impostazione **Auto-protezione**.

L'opzione viene applicata ai file che hanno estensione .tibx, .tib, .tia e si trovano nelle cartelle locali.

Questa impostazione consente di specificare i processi ai quali è consentito modificare i file di backup, anche se tali file sono protetti con l'Auto-protezione. La funzionalità è utile se, ad esempio, si eliminano o si spostano i file di backup in una posizione diversa utilizzando uno script.

Se l'impostazione è disabilitata, i file di backup possono essere modificati solo dai processi firmati dal fornitore del software di backup. Ciò consente al software di applicare delle regole di conservazione e di eliminare i backup quando un utente esegue questa richiesta dall'interfaccia web. Nessun altro processo, che sia sospetto o meno, può modificare i backup.

Se l'impostazione è abilitata, è possibile consentire ad altri processi di modificare i backup. Specificare il percorso completo del processo eseguibile, iniziando con la lettera di unità.

Impostazione predefinita: **Disabilitata**.

Protezione in tempo reale

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Protezione in tempo reale controlla in modo costante il sistema per individuare virus e altre minacce potenzialmente dannose, per tutto il tempo in cui il sistema è attivo, a meno che non venga sospeso dall'utente.

Impostazione predefinita: **Abilitata**.

© Acronis International GmbH, 2003-2024

Importante
Questa funzionalità è disponibile solo se è abilitato il pacchetto di protezione Advanced Security. Per ulteriori informazioni, vedere https://www.acronis.com/it-it/products/cloud/cyber-protect/security/

Per configurare la protezione in tempo reale

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Protezione in tempo reale**.
3. Nell'elenco a discesa **Azione al rilevamento**, selezionare una delle opzioni disponibili:

   Impostazione predefinita: **Quarantena**

   - **Solo notifica**

   Il software genera un avviso relativo al processo sospettato di attività di ransomware.

   - **Blocca e notifica**

   Il software blocca il processo e genera un avviso relativo al processo sospettato di attività malware.

   - **Quarantena**
4. Il software genera un avviso, arresta il processo e sposta il file eseguibile nella cartella della quarantena.
5. Nella sezione **Modalità di scansione**, selezionare l'azione che il software dovrà eseguire quando viene individuato un virus o un'altra minaccia potenzialmente dannosa:

   Impostazione predefinita: **Smart all'accesso**

   - **Smart all'accesso**: monitora tutte le attività di sistema e scansiona automaticamente i file quando vi si accede per attività di lettura o scrittura, o quando qualsiasi programma viene avviato.
   - **Al momento dell'esecuzione**: prevede solo l'analisi automatica dei file eseguibili che vengono avviati, per garantire che non presentino minacce e non danneggino il computer o i dati.
6. Fare clic su **Fine**.

Pianifica scansione

La scansione su richiesta controlla il sistema in uso alla ricerca di virus in base alla pianificazione specificata. La scansione completa verifica tutti i file presenti nel sistema, mentre la scansione rapida verifica solo i file system del sistema.

Per configurare l'opzione Pianifica scansione

Impostazioni predefinite:

© Acronis International GmbH, 2003-2024

- La scansione **Personalizzata** è disabilitata.
- Sono pianificate le scansioni **Rapida** e **Completa**.

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Pianifica scansione**.
3. Utilizzare l'interruttore per abilitare il tipo di scansione da applicare al sistema.

Tipi di scansione disponibili:

- **Completa**: rispetto alla scansione rapida, la scansione completa richiede molto tempo per essere completata, perché ogni file viene controllato.
- **Rapida**: la scansione rapida analizza solo le aree comuni del sistema nelle quali in genere si posiziona il malware.
- **Personalizzata**: controlla i file/le cartelle selezionate dall'amministratore del piano di Protezione.

> **Nota**
> È possibile pianificare tutte e tre le scansioni **Rapida**, **Completa** e **Personalizzata** in un unico piano di protezione.

Per configurare la scansione personalizzata

- Utilizzare l'interruttore **Scansione personalizzata** per abilitare o disabilitare questo tipo di scansione.
- Nell'elenco a discesa **Azione al rilevamento**, selezionare una delle opzioni disponibili:

Impostazione predefinita: **Quarantena**

Quarantena

Il software genera un avviso e sposta il file eseguibile nella cartella della quarantena.

Solo notifica

Il software genera un avviso relativo al processo sospettato di essere malware.

Campo	Descrizione
Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito	Questa impostazione determina quando l'attività viene eseguita. Sono disponibili i seguenti valori: • **Pianificazione oraria**: questo è il valore predefinito. L'attività viene eseguita all'orario specificato. • **Quando l'utente accede al sistema**: per impostazione predefinita, l'accesso di qualsiasi utente determina l'avvio dell'attività. È possibile modificare questa impostazione in modo che solo un account utente specifico possa determinare l'attivazione dell'attività. • **Quando l'utente si disconnette dal sistema**: per impostazione

© Acronis International GmbH, 2003-2024

Campo	Descrizione
	predefinita, la disconnessione di qualsiasi utente determina l'avvio dell'attività. È possibile modificare questa impostazione in modo che solo un account utente specifico possa determinare l'attivazione dell'attività. **Nota** L'attività non verrà eseguita allo spegnimento del sistema. Nella configurazione della pianificazione, l'arresto del sistema e la disconnessione vanno considerate come azioni differenti. • **All'avvio del sistema** – L'attività viene eseguita all'avvio del sistema operativo. • **All'arresto del sistema** – L'attività viene eseguita all'arresto del sistema operativo.
Tipo di pianificazione	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria**. Sono disponibili i seguenti valori: • **Ogni mese** – Specificare il mese e le settimane o i giorni del mese in cui verrà eseguita l'attività. • **Ogni giorno**: questo è il valore predefinito. Specificare i giorni della settimana in cui verrà eseguita l'attività. • **Ogni ora** – Specificare i giorni della settimana, il numero di ripetizioni e l'intervallo temporale in cui verrà eseguita l'attività.
Ora di avvio	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria** Specificare l'ora esatta di avvio dell'attività.
Esegui entro un intervallo di date	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria**. Impostare un intervallo di validità della pianificazione configurata.
Specificare l'account utente il cui accesso al sistema operativo avvierà l'esecuzione dell'attività	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Quando l'utente accede al sistema**. Sono disponibili i seguenti valori: • **Tutti gli utenti**: utilizzare questa opzione per far sì che l'accesso di qualsiasi utente determini l'avvio dell'attività. • **L'utente seguente**: utilizzare questa opzione per far sì che solo l'accesso di uno specifico account utente determini l'avvio dell'attività.

© Acronis International GmbH, 2003-2024

Campo	Descrizione
Specificare l'account utente la cui disconnessione dal sistema operativo avvierà l'esecuzione dell'attività	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Quando l'utente si disconnette dal sistema**. Sono disponibili i seguenti valori: • **Tutti gli utenti**: utilizzare questa opzione per far sì che la disconnessione di qualsiasi utente determini l'avvio dell'attività. • **L'utente seguente**: utilizzare questa opzione per far sì che solo la disconnessione di uno specifico account utente determini l'avvio dell'attività.
Condizioni di avvio	Definisce tutte le condizioni che devono essere soddisfatte simultaneamente per avviare l'attività. Le condizioni di avvio per le scansioni anti-malware sono simili alle condizioni di avvio del modulo **Backup** descritte in "Condizioni di avvio". È possibile definire le seguenti condizioni di avvio aggiuntive: • **Ripartisci orari di avvio dell'attività all'interno di una finestra dell'orario** – Questa opzione consente di definire l'intervallo di tempo durante il quale deve essere eseguita l'attività in modo da evitare colli di bottiglia sulla rete. È possibile specificare il ritardo in ore o minuti. Se, ad esempio, l'orario di avvio predefinito è alle 10:00 e il ritardo è di 60 minuti, l'attività verrà avviata tra le 10:00 e le 11:00. • **Se la macchina è spenta, esegui le attività mancanti all'avvio della macchina** • **Impedisci la modalità di sospensione o ibernazione durante l'esecuzione dell'attività** – Questa opzione è valida solo per i sistemi che eseguono Windows. • **Se le condizioni di avvio non sono soddisfatte, esegui comunque l'attività dopo** – Specificare il periodo successivamente al quale l'attività verrà comunque avviata, indipendentemente dalle altre condizioni di avvio. **Nota** In Linux le condizioni di avvio non sono supportate.

- Selezionare la casella di controllo **Scansiona solo i file nuovi e modificati** per analizzare soltanto i file nuovi e modificati.

Impostazione predefinita: **Abilitata**

- Due opzioni aggiuntive visualizzate solo per la **Scansione personalizzata** e per la **Scansione completa**:

1. **Scansiona file di archivio**

   Impostazione predefinita: **Abilitata**.

© Acronis International GmbH, 2003-2024

Profondità di ricorsione massima

Impostazione predefinita: **16**

Specifica quanti livelli di archivi incorporati possono essere scansionati. Ad esempio, Documento MIME > Archivio ZIP > Archivio Office > contenuto del documento.

Dimensione massima

Impostazione predefinita: **100**

La dimensione massima di un file di archivio da scansionare.

2. **Scansiona unità rimovibili**

Impostazione predefinita: **Disabilitato**

- **Unità di rete (remote) mappate**
- **Dispositivi di archiviazione USB** (come unità flash e unità esterne)
- **CD/DVD**

Nota
La scansione delle unità rimovibili non è supportata in Linux.

Esclusioni dalla protezione

Le esclusioni dalla protezione consentono di eliminare i falsi positivi quando un programma attendibile viene considerato un ransomware o un malware. È possibile definire gli elementi attendibili e bloccati aggiungendoli all'elenco delle esclusioni dalla protezione.

Nell'elenco degli elementi attendibili è possibile aggiungere file, processi e cartelle in modo che vengano considerati sicuri dal sistema, impedendo così che vengano rilevati in futuro.

Nell'elenco degli elementi bloccati è possibile aggiungere processi e hash. L'opzione garantisce che i processi indicati vengano bloccati e che il workload sia protetto.

Elemento escluso dalla protezione	Bloccato	Attendibile
Hash	Quando un hash viene aggiunto all'elenco degli elementi bloccati, il sistema arresta il processo in base all'hash fornito. Ad esempio, se si aggiunge l'hash MD5 938c2cc0dcc05f2b68c4287040cfcf71, il processo ad esso associato viene bloccato.	Quando un hash viene aggiunto all'elenco degli elementi attendibili, il sistema sarà in grado di determinare quali processi dovranno essere ignorati dal monitoraggio, in base all'hash fornito. Ad esempio, se si aggiunge l'hash MD5 938c2cc0dcc05f2b68c4287040cfcf71, il

© Acronis International GmbH, 2003-2024

Elemento escluso dalla protezione	Bloccato	Attendibile
		processo ad esso associato viene considerato attendibile ed escluso dal monitoraggio.
Processo	Quando un processo viene aggiunto all'elenco degli elementi bloccati, il sistema sarà in grado di determinare quali processi devono essere monitorati, e tali processi saranno sempre bloccati. Se, ad esempio, si aggiunge il percorso C:\Users\user1\application\nppInstaller.exe all'elenco degli elementi bloccati, questo specifico processo viene bloccato e quando si tenta di aprirlo non ne sarà consentito l'avvio.	Quando un processo viene aggiunto all'elenco degli elementi attendibili, il sistema sarà in grado di determinare che tali processi devono essere esclusi dal monitoraggio. **Nota** I processi firmati da Microsoft sono sempre considerati affidabili. Se, ad esempio, si aggiunge il percorso C:\Users\user1\application\nppInstaller.exe, questo specifico processo viene escluso dal monitoraggio, e l'antivirus non genera interferenze.
File/cartella		Quando un file o cartella viene aggiunto all'elenco degli elementi attendibili, il sistema sarà in grado di determinare che tali file o cartelle devono sempre essere considerate sicure, e che non devono essere scansionati o monitorati.

Per specificare gli elementi che vengono sempre considerati attendibili

1. Aprire il piano di protezione.
2. Espandere il modulo **Protezione antivirus e anti-malware**.
3. Selezionare l'opzione **Esclusioni**.
   Viene visualizzata la finestra **Esclusioni dalla protezione**.
4. Nella sezione **Elementi attendibili**, fare clic su **Aggiungi** per scegliere tra le opzioni disponibili.
   - Per rendere attendibili file, cartelle o processi, selezionare l'opzione **File/cartella/processo**.
     Viene visualizzata la finestra **Aggiungi file/cartella/processo**.
     - Nel campo **File/cartella/processo**, inserire il percorso di ogni processo, cartella o file su una nuova riga. Nella sezione **Descrizione**, inserire una breve descrizione che consenta di riconoscere la modifica nell'elenco degli elementi attendibili.
     - Selezionare la casella di controllo **Aggiungi come file/cartella** per rendere attendibile il file o la cartella.

© Acronis International GmbH, 2003-2024

Esempi di descrizione della cartella: D:\cartella\, /home/Cartella/cartella2, F:\

- Selezionare la casella di controllo **Aggiungi come processo** per rendere attendibile un processo. I processi selezionati verranno esclusi dal monitoraggio.

Nota
Specificare il percorso completo del processo eseguibile, iniziando con la lettera di unità. Ad esempio, `C:\Windows\Temp\er76s7sdkh.exe`.

Nota
Sono supportati i percorsi di rete locali, ad esempio: \\localhost\folderpath\file.exe

- Selezionare l'opzione **Hash** per aggiungere hash MD5 all'elenco degli elementi attendibili. Viene visualizzata la finestra **Aggiungi hash**.
  - Qui è possibile inserire, su righe separate, gli hash MD5 da includere come attendibili nell'elenco delle Esclusioni dalla protezione. In base a questi hash, Cyber Protection esclude i processi descritti dagli hash MD5 dal monitoraggio.

Impostazione predefinita: per impostazione predefinita non è definita alcuna esclusione.

Per specificare gli elementi che saranno sempre bloccati

1. Aprire il piano di protezione.
2. Espandere il modulo **Protezione antivirus e anti-malware**.
3. Selezionare l'opzione **Esclusioni dalla protezione**. Viene visualizzata la finestra **Esclusioni dalla protezione**.

   Nella sezione **Elementi bloccati**, fare clic su **Aggiungi** per scegliere tra le opzioni disponibili.
   - Per bloccare i processi, selezionare l'opzione **Processo**. Viene visualizzata la finestra **Aggiungi processo**.
     - Nel campo **Processo**, inserire il percorso di ogni processo su una nuova riga. Nel campo **Descrizione**, inserire una breve descrizione che renda possibile riconoscere la modifica nell'elenco degli elementi bloccati.

     Nota
     Fino a quando Active Protection è attivo nel computer, tali processi non potranno essere avviati.

   - Per bloccare gli hash, selezionare l'opzione **Hash**. Viene visualizzata la finestra **Aggiungi hash**.
     - Nel campo **Hash**, inserire l'hash di ogni processo su una nuova riga. Nel campo **Descrizione**, inserire una breve descrizione che renda possibile riconoscere la modifica nell'elenco degli elementi bloccati.

Impostazione predefinita: per impostazione predefinita non è definita alcuna esclusione.

© Acronis International GmbH, 2003-2024

Caratteri jolly

Per specificare le cartelle, è possibile utilizzare uno o più caratteri jolly * e ?. L'asterisco (*) sostituisce lo zero o altri caratteri. Il punto interrogativo (?) sostituisce un solo carattere. Non è possibile utilizzare le variabili di ambiente, ad esempio `%AppData%`.

È possibile utilizzare un carattere jolly (*) per aggiungere elementi agli elenchi di esclusione.

- I caratteri jolly possono essere inseriti nel mezzo o alla fine di una descrizione.

Esempi di caratteri jolly accettati nelle descrizioni:

C:*.pdf

D:\cartelle\file.*

C:\Users*\AppData\Roaming

- Non è possibile utilizzare i caratteri jolly all'inizio di una descrizione.

Esempi di caratteri jolly non accettati nelle descrizioni:

*.docx

*:\cartella\

Variabili

È inoltre possibile utilizzare le variabili per aggiungere elementi all'elenco delle Esclusioni dalla protezione, con le limitazioni seguenti:

- In Windows, sono supportate solo variabili SYSTEM. Non sono supportate le variabili utente, ad esempio %USERNAME%, %APPDATA%. Non sono supportate la variabili con {username}. Per ulteriori informazioni, vedere https://ss64.com/nt/syntax-variables.html.
- In macOS non sono supportate le variabili di ambiente.
- In Linux non sono supportate le variabili di ambiente.

Esempio di formati supportati:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Descrizione

Il campo **Descrizione** consente di aggiungere delle note alle esclusioni aggiunte all'elenco delle Esclusioni dalla protezione. Alcuni suggerimenti sul tipo di note da aggiungere:

- Motivi e finalità dell'esclusione.
- Nome corrente di un file di un'esclusione di hash.

© Acronis International GmbH, 2003-2024

- Indicatori data e ora.

Se sono stati aggiunti più elementi in un'unica voce, può essere presente un solo commento acquisito per i diversi elementi della voce.

Active Protection nell'edizione Cyber Backup Standard

Nelle edizioni Cyber Backup Standard, Active Protection è un modulo distinto del piano di protezione. Il modulo può essere configurato in modo separato e applicato a diversi dispositivi o gruppi di dispositivi.

Per tutte le altre edizioni del servizio Cyber Protection, Active Protection è parte del modulo **Protezione antivirus e anti-malware** del piano di protezione.

Impostazione predefinita: **Abilitata**.

Nota
Sul sistema protetto deve essere installato un agente di protezione. Per ulteriori informazioni sulle funzionalità e i sistemi operativi supportati consultare "Piattaforme supportate" (pag. 835).

Come funziona

Active Protection monitora i processi in esecuzione sul sistema protetto. Quando un processo di terze parti tenta di crittografare i file o di eseguire il mining di criptovalute, Active Protection genera un avviso ed esegue le azioni aggiuntive specificate nel piano di protezione.

Inoltre, impedisce modifiche non autorizzate ai processi del software, ai record di registro, ai file eseguibili e di configurazione e ai backup posizionati nelle cartelle locali.

Per individuare i processi dannosi, Active Protection utilizza euristiche comportamentali. Active Protection confronta la catena di azioni eseguita da un processo con le catene di eventi registrati nel database dei modelli di comportamento dannosi. Questo approccio consente ad Active Protection di individuare nuovi malware mediante il loro comportamento tipico.

Impostazioni di Active Protection in Cyber Backup Standard

Nell'edizione Cyber Backup Standard, è possibile configurare le seguenti funzionalità di Active Protection:

- Azione al rilevamento
- Auto-protezione
- Protezione delle cartelle di rete
- Protezione lato server
- Individuazione dei processi di mining delle criptovalute
- Esclusioni

© Acronis International GmbH, 2003-2024

Nota
Active Protection per Linux supporta le seguenti impostazioni: Azione al rilevamento, Protezione delle cartelle di rete ed Esclusioni. L'impostazione Protezione delle cartelle di rete è sempre attiva e non configurabile.

Azione al rilevamento

Nella sezione **Azione al rilevamento**, selezionare una delle opzioni disponibili:

- **Solo notifica**
  Il software genera un avviso relativo al processo sospettato di attività ransomware.
- **Arresta il processo**
  Il software genera un avviso relativo al processo sospettato di attività ransomware e lo arresta.
- **Ripristina utilizzando la cache**
  Il software genera un avviso, arresta il processo e ripristina le modifiche apportate al file utilizzando la cache di servizio.

Impostazione predefinita: **Ripristina utilizzando la cache**.

L'auto-protezione impedisce modifiche non autorizzate ai processi del software, ai record del Registro di sistema, ai file eseguibili e di configurazione e ai backup posizionati nelle cartelle locali.

Gli amministratori possono abilitare l' **Auto-protezione** senza abilitare **Active Protection**.

Impostazione predefinita: **Attiva**.

Nota
L'auto-protezione non è supportata in Linux.

Per abilitare l'auto-protezione

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Auto-protezione**.
3. Utilizzare l'interruttore **Auto-protezione** per abilitare la funzionalità.

Per abilitare la protezione con password

1. Dopo aver abilitato la funzionalità **Auto-protezione**, è possibile abilitare la **Protezione con password** utilizzando il relativo interruttore.
2. Fare clic su **Genera nuova password** per ottenere una password per la modifica o l'eliminazione degli agenti locali.
3. Fare clic su **Copia**, quindi incollare la password in un luogo sicuro; viene richiesta per la modifica dell'elenco dei componenti a livello locale.

© Acronis International GmbH, 2003-2024

Importante
La password non sarà più disponibile dopo la chiusura della finestra. Per applicare questa password ai dispositivi, è necessario salvare le impostazioni del piano di protezione.

4. Fare clic su **Chiudi**.

Protezione con password impedisce a utenti o software non autorizzati di disinstallare l'Agente per Windows o di modificarne i componenti. Queste azioni diventano possibili solo con una password fornita da un amministratore.

Non è mai richiesta la password per le seguenti azioni:

- Aggiornare l'installazione eseguendo nuovamente il programma di installazione in locale
- Aggiornamento dell'installazione con la console di Cyber Protect
- Riparare l'installazione

Impostazione predefinita: **Disabilitato**

Per ulteriori informazioni su come abilitare **Protezione con password**, fare riferimento a Impedire la disinstallazione o la modifica non autorizzate degli agenti.

Protezione delle cartelle di rete

L'impostazione **Proteggi le cartelle di rete mappate come unità locali** determina se il modulo Active Protection protegge le cartelle di rete mappate come unità locali dai processi dannosi locali.

L'impostazione si applica alle cartelle condivise tramite i protocolli SMB o NFS.

Se un file è posizionato in origine in un'unità mappata, non può essere salvato nella posizione originale quando viene estratto dalla cache dall'azione **Ripristina utilizzando la cache**. Viene invece salvato nella cartella specificata nelle impostazioni di questa impostazione. La cartella predefinita è `C:\ProgramData\Acronis\Restored Network Files` per Windows e `Library/Application Support/Acronis/Restored Network Files/` per macOS. Se la cartella non esiste, verrà creata. Se si desidera modificare questo percorso, specificare una cartella locale. Non sono supportate le cartelle di rete, incluse quelle sulle unità mappate.

Impostazione predefinita: **Attiva**.

Questa funzionalità determina se Active Protection protegge le cartelle di rete condivise dall'utente dai collegamenti esterni in ingresso da altri server nella rete, che potrebbero determinare l'introduzione di minacce.

Impostazione predefinita: **Disattivata**.

Nota
La protezione lato server non è supportata in Linux.

© Acronis International GmbH, 2003-2024

Per impostare connessioni affidabili

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Protezione lato server**.
3. Utilizzare l'interruttore **Protezione lato server** per abilitare la funzionalità.
4. Selezionare la scheda **Attendibili**.
5. Nel campo **Connessioni affidabili**, fare clic su **Aggiungi** per specificare le connessioni a cui è consentita la modifica dei dati.
6. Nel campo **Nome computer/Account** digitare il nome del computer e l'account del sistema in cui è installato l'agente di protezione. Ad esempio, `MyComputer\TestUser`.
7. Nel campo **Nome host** digitare il nome host del sistema al quale è consentita la connessione al sistema che utilizza l'agente di protezione.
8. Fare clic sul segno di spunta a destra per salvare la definizione della connessione.
9. Fare clic su **Fine**.

Per impostare connessioni bloccate

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Protezione lato server**.
3. Utilizzare l'interruttore **Protezione lato server** per abilitare la funzionalità.
4. Selezionare la scheda **Bloccati**.
5. Nel campo **Connessioni bloccate**, fare clic su **Aggiungi** per specificare le connessioni a cui non è consentita la modifica dei dati.
6. Nel campo **Nome computer/Account** digitare il nome del computer e l'account del sistema in cui è installato l'agente di protezione. Ad esempio, `MyComputer\TestUser`.
7. Nel campo **Nome host** digitare il nome host del sistema al quale è consentita la connessione al sistema che utilizza l'agente di protezione.
8. Selezionare la casella di controllo a destra per salvare la definizione della connessione.
9. Fare clic su **Fine**.

I malware di mining di criptovalute influiscono negativamente sulle prestazioni delle applicazioni utili, aumentano i costi dei consumi elettrici, possono causare arresti anomali del sistema e perfino guasti hardware dovuti all'eccessivo utilizzo. La funzionalità **Individuazione dei processi di mining delle criptovalute** protegge i dispositivi dai malware che eseguono il mining delle criptovalute, per impedire l'utilizzo non autorizzato delle risorse del computer.

Gli amministratori possono abilitare l'**Individuazione dei processi di mining delle criptovalute** senza abilitare **Active Protection**. Impostazione predefinita: **Abilitato**.

© Acronis International GmbH, 2003-2024

Nota
L'individuazione dei processi di mining delle criptovalute non è supportata in Linux.

Per configurare la protezione delle cartelle di rete

1. Nella finestra **Crea piano di protezione**, espandere il modulo **Protezione antivirus e anti-malware**.
2. Fare clic su **Individuazione dei processi di mining delle criptovalute**.
3. Utilizzare l'interruttore **Individua i processi di mining delle criptovalute** per abilitare o disabilitare la funzionalità.
4. Specificare l'azione da compiere sui processi sospettati di attività di mining di criptovalute:

   Impostazione predefinita: **Arresta il processo**

   - **Solo notifica**: il software genera un avviso.
   - **Arresta il processo**: il software genera un avviso e arresta il processo.
5. Fare clic su **Fine** per applicare le opzioni selezionate al piano di protezione.

Le esclusioni dalla protezione consentono di eliminare i falsi positivi quando un programma attendibile viene considerato un ransomware o un malware. È possibile definire gli elementi attendibili e bloccati aggiungendoli all'elenco delle esclusioni dalla protezione.

Nell'elenco degli elementi attendibili è possibile aggiungere file, processi e cartelle in modo che vengano considerati sicuri dal sistema, impedendo così che vengano rilevati in futuro.

Nell'elenco degli elementi bloccati è possibile aggiungere processi e hash. L'opzione garantisce che i processi indicati vengano bloccati e che il workload sia protetto.

Elemento escluso dalla protezione	Bloccato	Attendibile
Hash	Quando un hash viene aggiunto all'elenco degli elementi bloccati, il sistema arresta il processo in base all'hash fornito. Ad esempio, se si aggiunge l'hash MD5 938c2cc0dcc05f2b68c4287040cfcf71, il processo ad esso associato viene bloccato.	Quando un hash viene aggiunto all'elenco degli elementi attendibili, il sistema sarà in grado di determinare quali processi dovranno essere ignorati dal monitoraggio, in base all'hash fornito. Ad esempio, se si aggiunge l'hash MD5 938c2cc0dcc05f2b68c4287040cfcf71, il processo ad esso associato viene considerato attendibile ed escluso dal monitoraggio.
Processo	Quando un processo viene aggiunto	Quando un processo viene aggiunto

© Acronis International GmbH, 2003-2024

Elemento escluso dalla protezione	Bloccato	Attendibile
	all'elenco degli elementi bloccati, il sistema sarà in grado di determinare quali processi devono essere monitorati, e tali processi saranno sempre bloccati. Se, ad esempio, si aggiunge il percorso C:\Users\user1\application\nppInstaller.exe all'elenco degli elementi bloccati, questo specifico processo viene bloccato e quando si tenta di aprirlo non ne sarà consentito l'avvio.	all'elenco degli elementi attendibili, il sistema sarà in grado di determinare che tali processi devono essere esclusi dal monitoraggio. **Nota** I processi firmati da Microsoft sono sempre considerati affidabili. Se, ad esempio, si aggiunge il percorso C:\Users\user1\application\nppInstaller.exe, questo specifico processo viene escluso dal monitoraggio, e l'antivirus non genera interferenze.
File/cartella		Quando un file o cartella viene aggiunto all'elenco degli elementi attendibili, il sistema sarà in grado di determinare che tali file o cartelle devono sempre essere considerate sicure, e che non devono essere scansionati o monitorati.

Per specificare gli elementi che vengono sempre considerati attendibili

1. Aprire il piano di protezione.
2. Espandere il modulo **Protezione antivirus e anti-malware**.
3. Selezionare l'opzione **Esclusioni**.
   Viene visualizzata la finestra **Esclusioni dalla protezione**.
4. Nella sezione **Elementi attendibili**, fare clic su **Aggiungi** per scegliere tra le opzioni disponibili.
   - Per rendere attendibili file, cartelle o processi, selezionare l'opzione **File/cartella/processo**.
     Viene visualizzata la finestra **Aggiungi file/cartella/processo**.
     - Nel campo **File/cartella/processo**, inserire il percorso di ogni processo, cartella o file su una nuova riga. Nella sezione **Descrizione**, inserire una breve descrizione che consenta di riconoscere la modifica nell'elenco degli elementi attendibili.
     - Selezionare la casella di controllo **Aggiungi come file/cartella** per rendere attendibile il file o la cartella.
       Esempi di descrizione della cartella: D:\cartella\, /home/Cartella/cartella2, F:\
     - Selezionare la casella di controllo **Aggiungi come processo** per rendere attendibile un processo. I processi selezionati verranno esclusi dal monitoraggio.

© Acronis International GmbH, 2003-2024

Nota
Specificare il percorso completo del processo eseguibile, iniziando con la lettera di unità. Ad esempio, `C:\Windows\Temp\er76s7sdkh.exe`.

Nota
Sono supportati i percorsi di rete locali, ad esempio: \\localhost\folderpath\file.exe

- Selezionare l'opzione **Hash** per aggiungere hash MD5 all'elenco degli elementi attendibili. Viene visualizzata la finestra **Aggiungi hash**.
  - Qui è possibile inserire, su righe separate, gli hash MD5 da includere come attendibili nell'elenco delle Esclusioni dalla protezione. In base a questi hash, Cyber Protection esclude i processi descritti dagli hash MD5 dal monitoraggio.

Impostazione predefinita: per impostazione predefinita non è definita alcuna esclusione.

Per specificare gli elementi che saranno sempre bloccati

1. Aprire il piano di protezione.
2. Espandere il modulo **Protezione antivirus e anti-malware**.
3. Selezionare l'opzione **Esclusioni dalla protezione**. Viene visualizzata la finestra **Esclusioni dalla protezione**.

   Nella sezione **Elementi bloccati**, fare clic su **Aggiungi** per scegliere tra le opzioni disponibili.
   - Per bloccare i processi, selezionare l'opzione **Processo**. Viene visualizzata la finestra **Aggiungi processo**.
     - Nel campo **Processo**, inserire il percorso di ogni processo su una nuova riga. Nel campo **Descrizione**, inserire una breve descrizione che renda possibile riconoscere la modifica nell'elenco degli elementi bloccati.

     Nota
     Fino a quando Active Protection è attivo nel computer, tali processi non potranno essere avviati.

   - Per bloccare gli hash, selezionare l'opzione **Hash**. Viene visualizzata la finestra **Aggiungi hash**.
     - Nel campo **Hash**, inserire l'hash di ogni processo su una nuova riga. Nel campo **Descrizione**, inserire una breve descrizione che renda possibile riconoscere la modifica nell'elenco degli elementi bloccati.

Impostazione predefinita: per impostazione predefinita non è definita alcuna esclusione.

Caratteri jolly

Per specificare le cartelle, è possibile utilizzare uno o più caratteri jolly * e ?. L'asterisco (*) sostituisce lo zero o altri caratteri. Il punto interrogativo (?) sostituisce un solo carattere. Non è possibile utilizzare le variabili di ambiente, ad esempio `%AppData%`.

È possibile utilizzare un carattere jolly (*) per aggiungere elementi agli elenchi di esclusione.

© Acronis International GmbH, 2003-2024

- I caratteri jolly possono essere inseriti nel mezzo o alla fine di una descrizione.

Esempi di caratteri jolly accettati nelle descrizioni:

C:*.pdf

D:\cartelle\file.*

C:\Users*\AppData\Roaming

- Non è possibile utilizzare i caratteri jolly all'inizio di una descrizione.

Esempi di caratteri jolly non accettati nelle descrizioni:

*.docx

*:\cartella\

Variabili

È inoltre possibile utilizzare le variabili per aggiungere elementi all'elenco delle Esclusioni dalla protezione, con le limitazioni seguenti:

- In Windows, sono supportate solo variabili SYSTEM. Non sono supportate le variabili utente, ad esempio %USERNAME%, %APPDATA%. Non sono supportate la variabili con {username}. Per ulteriori informazioni, vedere https://ss64.com/nt/syntax-variables.html.
- In macOS non sono supportate le variabili di ambiente.
- In Linux non sono supportate le variabili di ambiente.

Esempio di formati supportati:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Descrizione

Il campo **Descrizione** consente di aggiungere delle note alle esclusioni aggiunte all'elenco delle Esclusioni dalla protezione. Alcuni suggerimenti sul tipo di note da aggiungere:

- Motivi e finalità dell'esclusione.
- Nome corrente di un file di un'esclusione di hash.
- Indicatori data e ora.

Se sono stati aggiunti più elementi in un'unica voce, può essere presente un solo commento acquisito per i diversi elementi della voce.

© Acronis International GmbH, 2003-2024

Filtro URL

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Il malware viene spesso diffuso tramite siti dannosi o infetti e impiega il metodo di infezione chiamato download inconsapevole.

La funzionalità Filtro URL consente di proteggere i sistemi dalle minacce come malware e phishing provenienti da Internet. Per proteggere l'organizzazione è possibile bloccare l'accesso degli utenti ai siti web con contenuti potenzialmente dannosi.

La funzionalità Filtro URL consente inoltre di controllare l'utilizzo del web in conformità alle normative esterne e alle policy aziendali interne. È possibile configurare l'accesso ai siti web a seconda della categoria di corrispondenza. Al momento, Filtro URL supporta 44 categorie di siti web e consente di gestire l'accesso a ognuna di loro.

Al momento, le connessioni HTTP/HTTPS sui sistemi Windows vengono controllate dall'agente di protezione.

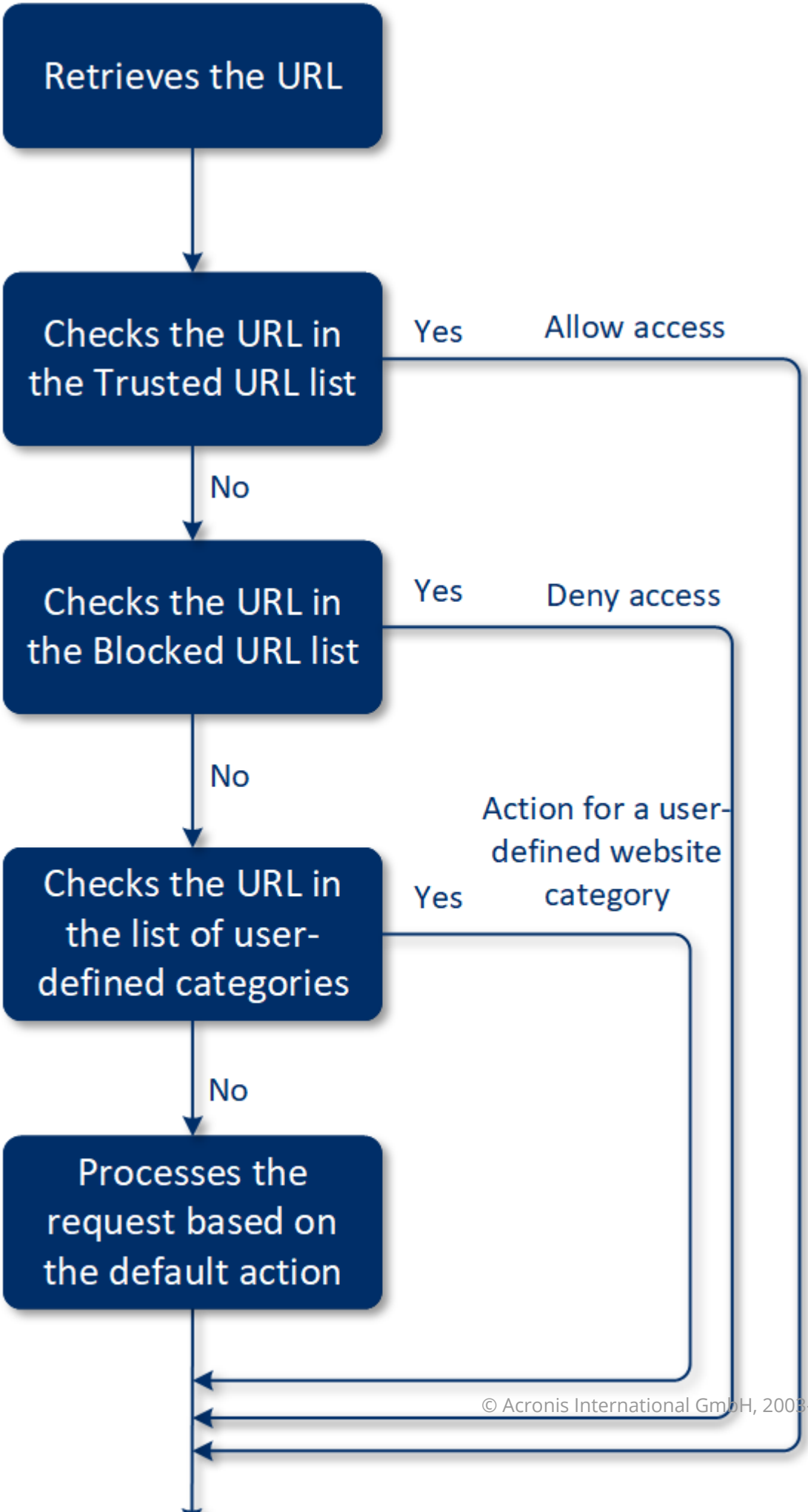
Per il funzionamento del filtro URL è richiesta una connessione Internet.

Nota
Per prevenire potenziali incompatibilità con l'agente di protezione versione 15.0.26692 (release C21.03 HF1) e versioni precedenti, la funzionalità di filtro URL verrà automaticamente disattivata se viene rilevata un'altra soluzione antivirus p se il servizio Centro Sicurezza PC Windows non è presente nel sistema.
Negli agenti di protezione successivi, i problemi di compatibilità sono stati risolti, e il filtro URL è sempre abilitato in base alla policy.

Come funziona

Un utente inserisce un collegamento URL in un browser. L'Intercettore acquisisce il collegamento e lo invia all'agente di protezione. L'agente acquisisce l'URL, lo analizza e quindi controlla il risultato. L'Intercettore reindirizza l'utente alla pagina con il messaggio con le azioni disponibili per passare manualmente alla pagina richiesta.

© Acronis International GmbH, 2003-2024



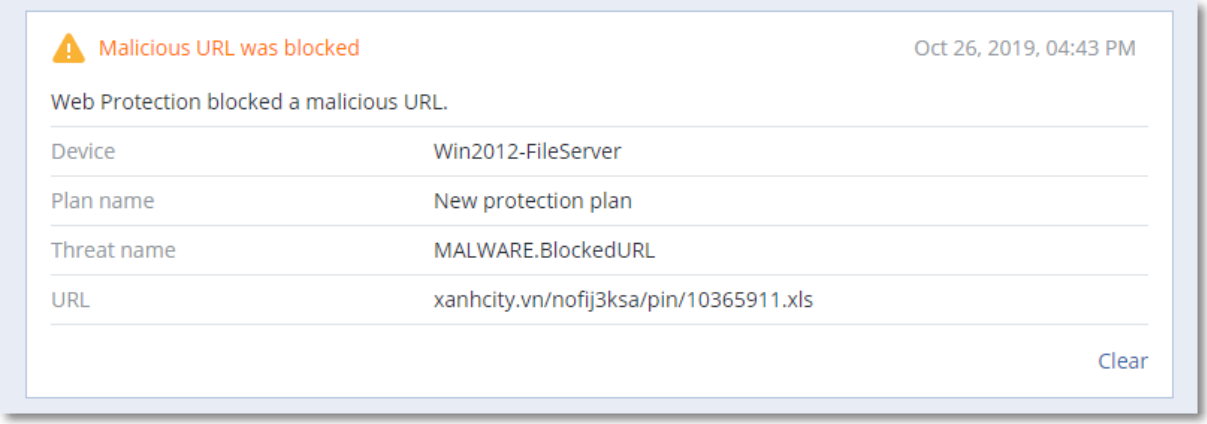
© Acronis International GmbH, 2003-2024

Flusso di lavoro di configurazione del filtro URL

In generale, il processo di configurazione del filtro URL consiste dei passaggi seguenti:

1. Creare un piano di protezione nel quale sia abilitato il modulo **Filtro URL**.
2. Specificare le impostazioni del filtro URL (vedere di seguito).
3. Assegnare il piano di protezione ai sistemi.

Per controllare quali URL sono stati bloccati, passare a **Monitoraggio** > **Avvisi**.



Impostazioni Filtro URL

Per il modulo Filtro URL è possibile specificare le impostazioni seguenti:

Accesso a siti web dannosi

Specificare le azioni da eseguire quando un utente apre un sito web dannoso:

- **Solo notifica**: il software genera un avviso relativo al processo sospettato di attività ransomware.
- **Blocca**: il sistema blocca l'accesso al sito web dannoso. L'utente non può accedere al sito web e viene generato un avviso di attenzione.
- **Chiedi sempre all'utente**: il sistema chiede all'utente se visitare comunque il sito web o se tornare indietro.

Categorie da filtrare

Sono disponibili 44 categorie di siti web per le quali è possibile configurare l'accesso:

- **Consenti** – consente l'accesso ai siti web correlati alla categoria selezionata.
- **Nega** – nega l'accesso ai siti web correlati alla categoria selezionata.

Per impostazione predefinita, sono consentite tutte le categorie.

Mostra tutte le notifiche per gli URL bloccati per categorie – se abilitata, l'utente riceve tutte le notifiche mostrate nella barra delle notifiche per gli URL bloccati in base alle categorie. Se un sito

© Acronis International GmbH, 2003-2024

web include diversi domini secondari, il sistema genera anche le notifiche relative a questi; di conseguenza il numero di notifiche potrebbe essere molto elevato.

Nella tabella seguente sono descritte le categorie:

	Categoria del sito web	Descrizione
1	**Pubblicità**	In questa categoria rientrano i domini il cui scopo principale è pubblicitario.
2	**Bacheca messaggi**	In questa categoria rientrano forum, bacheche di discussione e siti web di tipo domanda e risposta. Non include le sezioni specifiche dei siti aziendali in cui i clienti possono fare domande.
3	**Siti web personali**	In questa categoria rientrano i siti web personali e tutti i tipi di blog: individuali, di gruppi e anche aziendali. Un blog è una sorta di diario pubblicato sul web, costituito da una serie di articoli detti post, in genere visualizzati in ordine cronologico inverso in modo che il post più recente appaia per primo.
4	**Siti web aziendali/business**	Questa è una vasta categoria in cui rientrano siti web aziendali che in genere non appartengono a nessun altra categoria.
5	**Software per computer**	In questa categoria rientrano i siti web che offrono software per computer, in genere open source, freeware o shareware. Può includere anche alcuni negozi per la vendita di software online.
6	**Farmaci**	In questa categoria rientrano i siti web correlati a farmaci/alcolici/sigarette in cui si hanno discussioni sull'uso o sulla vendita (legale) di farmaci o accessori per il loro consumo, alcolici o prodotti a base di tabacco. Tenere presente che le droghe illegali sono incluse nella categoria Stupefacenti.
7	**Istruzione**	In questa categoria rientrano i siti web appartenenti a istituzioni educative ufficiali, inclusi quelli esterni al dominio .edu. Include anche siti web educativi, ad esempio quelli enciclopedici.
8	**Intrattenimento**	In questa categoria rientrano i siti web che forniscono informazioni relative ad attività artistiche e musei, nonché a siti web che recensiscono o classificano contenuti quali film, musica o arte.
9	**Condivisione file**	In questa categoria rientrano i siti web per la condivisione dei file nei quali un utente può caricare file e condividerli con altri utenti. Include anche i siti web di condivisione e keylogger per file torrent.
10	**Contabilità**	In questa categoria rientrano i siti web che appartengono alle istituzioni bancarie che offrono l'accesso online. Include anche alcune cooperative di credito e altre istituzioni finanziarie. Potrebbe non includere i siti di alcune banche locali.

© Acronis International GmbH, 2003-2024

11	**Scommesse**	In questa categoria rientrano i siti web dedicati alle scommesse e al gioco d'azzardo. Si tratta di siti di "casinò online" o "lotterie online", una tipologia di sito nella quale viene in genere richiesto un pagamento prima che l'utente possa puntare denaro su giochi come roulette, poker, blackjack o similari. Alcuni di questi siti sono legittimi, ovvero offrono una possibilità di vincita; altri sono invece fraudolenti, e non offrono alcuna possibilità di vincita. Nella categoria rientrano anche i siti web che forniscono suggerimenti e trucchi per fare soldi con le scommesse e il gioco d'azzardo online.
12	**Giochi**	In questa categoria rientrano i siti web che forniscono giochi online, in genere basati su applet Adobe Flash o Java. Il rilevamento non consente di stabilire se il gioco è gratuito o richiede un abbonamento. I siti di casinò, tuttavia, vengono rilevati nella categoria Scommesse. In questa categoria non rientrano: • Siti web ufficiali di aziende che sviluppano videogioco, a meno che non producano giochi online • Siti di forum di discussione in cui si parla di giochi • Siti web dai quali è possibile scaricare giochi non online (alcuni di questi sono inseriti nella categoria Illegale) • I giochi che richiedono a un utente di scaricare ed eseguire un file eseguibile, ad esempio World of Warcraft; questa tipologia può essere bloccata con sistemi diversi, ad esempio un firewall
13	**Istituzioni governative**	In questa categoria rientrano i siti web governativi, inclusi quelli degli enti pubblici, delle ambasciate e quelli ufficiali.
14	**Hacking**	In questa categoria rientrano i siti web che forniscono strumenti, articoli e piattaforme di discussione per hacker. Include anche i siti web che offrono sistemi per attaccare le piattaforme più diffuse e che facilitano la manomissione degli account Facebook o Gmail.
15	**Attività illegali**	Questa è una vasta categoria in cui rientrano siti web correlati alla diffusione di odio, violenza e razzismo. È ideata per bloccare le categorie di siti web seguenti: • Siti web appartenenti a organizzazioni terroristiche • Siti web con contenuti razzisti o xenofobi • Siti web con discussioni su sport aggressivi e/o di incentivazione alla violenza
16	**Salute e fitness**	In questa categoria rientrano i siti web associati agli istituti medici, alla prevenzione e al trattamento delle malattie, che offrono informazioni o prodotti su perdita di peso, diete, steroidi, anabolizzanti, prodotti a base di ormone della crescita, chirurgia plastica.
17	**Hobby**	In questa categoria rientrano i siti web che presentano risorse associate alle attività del tempo libero: collezioni, lavori artistici, e attività in

© Acronis International GmbH, 2003-2024

		bicicletta.
18	**Web hosting**	In questa categoria rientrano i siti web gratuiti e commerciali che offrono servizi con i quali utenti privati e organizzazioni possono creare e pubblicare pagine web.
19	**Download illegale**	In questa categoria rientrano i siti web associati alla pirateria software, inclusi: • Siti web con tracciatori peer-to-peer (BitTorrent, emule, DC++) e siti noti per offrire agli utenti contenuti protetti da copyright senza il consenso del proprietario dei diritti • Siti web e bacheche di discussione Warez (software commerciali pirata) • Siti web che forniscono agli utenti programmi con distribuzione illegale, generatori di codici e numeri di serie per facilitare l'impiego illegale del software Alcuni di questi siti possono essere individuati anche come siti di pornografia o di diffusione di alcolici/sigarette, poiché utilizzano pubblicità pornografica o di alcolici per trarre profitto.
20	**Messaggistica istantanea**	In questa categoria rientrano i siti web che offrono servizi di messaggistica e chat che consentono agli utenti di avviare chat in tempo reale. Vengono individuati anche i siti yahoo.com e gmail.com poiché entrambi integrano un servizio di messaggistica istantanea.
21	**Offerte di lavoro**	In questa categoria rientrano i siti web con bacheche di lavoro, offerte di lavoro qualificate, opportunità di carriera, nonché siti che raggruppano tali servizi. Non include le agenzie di collocamento o le pagine con le offerte di lavoro delle singole aziende.
22	**Contenuto per adulti**	In questa categoria rientrano i siti con contenuti etichettati dall'autore del sito come destinati a un pubblico adulto. Include una vasta gamma di siti web, da quelli che trattano del libro del Kama Sutra ai siti di educazione sessuale e pornografia hardcore.
23	**Stupefacenti**	In questa categoria rientrano i siti web che condividono informazioni sulle droghe illegali e per uso ricreativo. Include anche i siti web che trattano di coltivazione o creazione di droghe.
24	**Notizie**	In questa categoria rientrano i siti web che forniscono notiziari in forma di testo e video. La categoria punta a includere siti web di notizie internazionali e locali; tuttavia, la copertura potrebbe non includere siti web di notiziari locali.
25	**Appuntamenti online**	In questa categoria rientrano i siti web per gli appuntamenti online, gratuiti e a pagamento, in cui gli utenti possono cercare contatti utilizzando determinati criteri. In questi siti gli utenti possono pubblicare i propri profili per essere individuati da altri utenti. La categoria include siti di appuntamenti gratuiti e a pagamento.

© Acronis International GmbH, 2003-2024

		In questa categoria vengono inclusi anche siti di grande diffusione come Facebook, perché la maggior parte delle reti social più note può essere utilizzata con questa finalità. Si consiglia di utilizzare questa categoria insieme alla categoria Social network.
26	**Pagamenti online**	In questa categoria rientrano i siti web che offrono pagamenti online o trasferimenti di denaro. Include siti di pagamento di grande diffusione, come PayPal o Moneybookers. Nella categoria vengono individuate, in maniera euristica, le pagine web di siti legittimi che richiedono informazioni sulle carte di credito, consentendo così l'individuazione di negozi online nascosti, sconosciuti o illegali.
27	**Condivisione di foto**	In questa categoria rientrano i siti web per la condivisione di immagini, la cui principale finalità è il caricamento e la condivisione di immagini da parte degli utenti.
28	**Negozi online**	In questa categoria rientrano i negozi online più noti. Un sito web viene considerato negozio online se vende merci o servizi online.
29	**Pornografia**	In questa categoria rientrano i siti web che contengono materiale erotico e pornografico. Include siti web a pagamento e gratuiti. Vi rientrano i siti web che forniscono immagini, storie e video, e vengono individuati anche quelli che propongono contenuti pornografici in siti web a contenuto misto.
30	**Portali**	In questa categoria rientrano i siti web che aggregano informazioni da più fonti e da vari domini, e che spesso offrono funzionalità come motori di ricerca, e-mail, notizie e informazioni per l'intrattenimento.
31	**Radio**	In questa categoria rientrano i siti web che offrono servizi di streaming musicale, dalle stazioni radio online ai siti web che propongono contenuti audio on-demand, gratuiti o a pagamento.
32	**Religione**	In questa categoria rientrano i siti web che promuovono religioni o sette. Include anche i forum di discussione correlati a una o più religioni.
33	**Motori di ricerca**	In questa categoria rientrano i siti web dei motori di ricerca, come Google, Yahoo e Bing.
34	**Social network**	In questa categoria rientrano i siti web dei social network. Include Facebook.com, MySpace.com, Bebo.com e altri. I social network specializzati, come YouTube.com, sono elencati nella categoria Video/Foto.
35	**Sport**	In questa categoria rientrano i siti web che offrono informazioni, notizie e tutorial in ambito sportivo.
36	**Suicidio**	In questa categoria rientrano i siti web che promuovono, offrono o difendono il suicidio. Non include gli istituti clinici per la prevenzione del suicidio.
37	**Tabloid**	Questa categoria include principalmente i siti web che si occupano di

© Acronis International GmbH, 2003-2024

		pornografia soft e di gossip. Negli elenchi di individuazione di questa categoria possono essere incluse molte sottocategorie dei siti web di notiziari in stile tabloid. L'individuazione per questa categoria si basa anche sull'euristica.
38	**Perdita di tempo**	In questa categoria rientrano i siti web in cui le persone tendono a passare molto tempo. Può includere siti web di altre categorie come social network o intrattenimento.
39	**Viaggi**	In questa categoria rientrano i siti web che offrono offerte di viaggio, attrezzature da viaggio, recensioni o classifiche di destinazioni turistiche.
40	**Video**	In questa categoria rientrano i siti web che ospitano video o foto di diverso tipo, materiale caricato dagli utenti o fornito da diversi provider di contenuti. Include siti web come YouTube, Metacafe, Google Video, e siti web di immagini come Picasa o Flickr. Possono anche essere individuati video integrati in altri siti web o blog.
41	**Cartoni animati violenti**	In questa categoria rientrano i siti web che informano, condividono e offrono cartoni o manga con contenuto violento, che possono essere inadeguati per i minori in considerazione del contenuto violento, a sfondo sessuale o del linguaggio esplicito. Non include siti web che offrono cartoni animati tradizionali come “Tom and Jerry”.
42	**Armi**	In questa categoria rientrano i siti web che offrono armi per la vendita o lo scambio o trattano della loro produzione o utilizzo. Include anche risorse con contenuti dedicati alla caccia e all'uso di pistole ad aria compressa, nonché armi da corpo a corpo.
43	**E-mail**	In questa categoria rientrano i siti web che forniscono funzionalità di e-mail in forma di applicazione web.
44	**Proxy web**	In questa categoria rientrano i siti web che forniscono servizi di proxy web. Si tratta di siti web di tipo “browser dentro al browser” nei quali un utente apre una pagina web, immette l'indirizzo richiesto in un modulo e fa clic su “Invia”. Il sito proxy web scarica la pagina desiderata e la visualizza all'interno del browser dell'utente. Di seguito sono indicate le ragioni per l'identificazione (ed eventualmente il blocco) di questo tipo di sito: • Per la navigazione in modalità anonima. Poiché le richieste al server web di destinazione provengono dal server del proxy web, sarà visibile solo questo indirizzo IP e, nel caso in cui gli amministratori del server traccino l'utente, la traccia riporterà al proxy web, il quale può o meno memorizzare i log necessari per individuare l'utente originale. • Per lo spoofing delle posizioni. Gli indirizzi IP degli utenti sono spesso utilizzati per la profilazione del servizio in base alla posizione dell'origine (alcuni siti web di istituzioni nazionali possono essere

© Acronis International GmbH, 2003-2024

		disponibili solo da indirizzi IP locali), e l'utilizzo di questi servizi potrebbe aiutare l'utente a effettuare lo spoofing della posizione effettiva. • Per accedere a contenuti proibiti. Se viene utilizzato un semplice filtro URL, questo visualizzerà soltanto gli URL del proxy web e non i server effettivamente visitati dall'utente. • Per evitare il controllo aziendale. Alcune policy aziendali impongono il monitoraggio dell'utilizzo di Internet da parte dei dipendenti. Eseguendo l'accesso tramite un proxy web, un utente potrebbe sottrarsi al monitoraggio, che non fornirà le informazioni corrette. Poiché l'SDK analizza la pagina HTML (se fornita) e non soltanto gli URL, per alcune categorie l'SDK non sarà in grado di individuare il contenuto. Esistono tuttavia altre ragioni che non possono essere evitate semplicemente utilizzando l'SDK.

Esclusione di URL

Gli URL noti per essere sicuri possono essere aggiunti all'elenco dei domini attendibili. Gli URL che rappresentano una minaccia possono essere aggiunti all'elenco dei domini bloccati.

Per specificare gli URL che vengono sempre considerati attendibili o bloccati

1. Nel modulo Filtro URL di un piano di protezione, fare clic su **Esclusione di URL**.
   Viene visualizzata la finestra **Esclusione di URL**.
   Vengono visualizzate supportate le seguenti opzioni:

Elementi attendibili: fare clic su **Aggiungi** per scegliere tra le opzioni disponibili.

- **Dominio**: se si seleziona questa opzione viene visualizzata la finestra **Aggiungi dominio**.
  - Nel campo **Dominio**, inserire ogni dominio su una nuova riga. Nel campo **Descrizione**, inserire una breve descrizione che renda possibile riconoscere la modifica nell'elenco degli elementi attendibili.
- **Processo**: se si seleziona questa opzione viene visualizzata la finestra **Aggiungi processo**.
  - Nel campo **Processo**, inserire il percorso di ogni processo su una nuova riga. Nella sezione **Descrizione**, inserire una breve descrizione che consenta di riconoscere la modifica nell'elenco degli elementi attendibili.

Elementi bloccati: fare clic su **Aggiungi**. Viene visualizzata la finestra **Aggiungi dominio**.

Nel campo **Dominio**, inserire ogni dominio su una nuova riga. Nel campo **Descrizione**, inserire una breve descrizione che renda possibile riconoscere la modifica nell'elenco degli elementi bloccati.

Nota
Sono supportati i percorsi di rete locali, ad esempio: \\localhost\folderpath\file.exe.

© Acronis International GmbH, 2003-2024

Descrizione

Il campo **Descrizione** consente di aggiungere delle note alle esclusioni aggiunte all'elenco delle esclusioni dagli URL. Ecco alcuni suggerimenti sul tipo di note da aggiungere:

- Motivi e finalità dell'esclusione.
- Indicatori data e ora.

Se sono stati aggiunti più elementi in un'unica voce, può essere presente un solo commento acquisito per i diversi elementi della voce.

Microsoft Defender Antivirus e Microsoft Security Essentials

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Microsoft Defender Antivirus

Microsoft Defender Antivirus è un componente anti-malware integrato di Microsoft Windows, distribuito a partire da Windows 8.

Il modulo Microsoft Defender Antivirus (WDA) consente di configurare le policy per la sicurezza di Microsoft Defender Antivirus e di tracciarne lo stato tramite la console di Cyber Protect.

Il modulo è applicabile ai workload sui quali è installato Microsoft Defender Antivirus.

Microsoft Security Essentials

Microsoft Security Essentials è un componente anti-malware integrato di Microsoft Windows, distribuito nelle versioni di Windows precedenti a Windows 8.

Il modulo Microsoft Security Essentials consente di configurare le policy per la sicurezza di Microsoft Security Essentials e di tracciarne lo stato tramite la console di Cyber Protect.

Il modulo è applicabile ai workload sui quali è installato Microsoft Security Essentials.

Le impostazioni per Microsoft Security Essentials sono simili a quelle per Microsoft Defender Antivirus, ma non è possibile configurare la protezione in tempo reale, né definire le esclusioni tramite la console di Cyber Protect.

Pianifica scansione

Specificare la pianificazione per la scansione pianificata.

Modalità di scansione:

© Acronis International GmbH, 2003-2024

- **Completa** – un controllo completo di tutti i file e le cartelle aggiuntivo rispetto agli elementi scansionati con la scansione rapida. Per l'esecuzione, richiede un numero di risorse di sistema superiore a quello della scansione rapida.
- **Rapida** – un controllo rapido dei processi in memoria e delle cartelle in cui si trova in genere il malware. Per l'esecuzione, richiede un numero di risorse di sistema inferiore.

Definire il giorno della settimana e l'ora in cui verrà eseguita la scansione.

Scansione rapida quotidiana – indica l'ora della scansione rapida quotidiana.

A seconda delle proprie esigenze, è possibile impostare le seguenti opzioni:

Avvia la scansione pianificata quando la macchina è attiva ma non in uso

Verifica le più recenti definizioni di virus e spyware prima di eseguire una scansione pianificata

Limita l'utilizzo della CPU durante la scansione a

Per ulteriori informazioni sulle impostazioni di Microsoft Defender Antivirus, consultare https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings

Azioni predefinite

Definisce le azioni predefinite da eseguire sulle minacce rilevate con diversi livelli di gravità:

- **Pulisci** – pulisce il malware individuato in un workload.
- **Quarantena** – sposta il malware individuato nella cartella della quarantena, ma non lo elimina.
- **Rimuovi** – rimuove il malware individuato dal workload.
- **Consenti** – non rimuove né mette in quarantena il malware rilevato.
- **Definito dall'utente** – viene chiesto all'utente di indicare l'azione da eseguire sul malware individuato.
- **Nessuna azione** – non viene intrapresa alcuna azione.
- **Blocca** – blocca il malware individuato.

Per ulteriori informazioni sulle impostazioni delle azioni predefinite di Microsoft Defender Antivirus, consultare https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings

Protezione in tempo reale

Abilitare la **Protezione in tempo reale** per individuare e arrestare il malware impedendone l'installazione o l'esecuzione nei workload.

Scansiona tutti i download – se questa opzione è selezionata, viene effettuata la scansione su tutti i file e gli allegati scaricati.

© Acronis International GmbH, 2003-2024

Abilita il monitoraggio del comportamento – se l'opzione è selezionata, il monitoraggio del comportamento viene abilitato.

Scansiona file di rete – se l'opzione è selezionata, vengono scansionati i file di rete.

Consenti la scansione completa delle unità di rete mappate – se l'opzione è selezionata, le unità di rete mappate vengono completamente scansionate.

Consenti la scansione delle e-mail – se l'opzione è abilitata, il motore analizza caselle di posta e file di posta, in base al loro formato specifico, per analizzare il corpo e gli allegati delle e-mail.

Per ulteriori informazioni sulle impostazioni di protezione in tempo reale di Microsoft Defender Antivirus, consultare https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings

Avanzato

Specificare le impostazioni di scansione avanzate:

- **Scansiona file di archivio** – include i file di archivio, come quelli con estensione .zip o .rar, nella scansione.
- **Scansiona unità rimovibili** – scansiona le unità rimovibili durante le scansioni complete.
- **Crea punto di ripristino configurazione di sistema** – in alcuni casi, un file importante o una voce di registro potrebbero essere rimossi come "falsi positivi"; in questi casi, la presenza di un punto di ripristino può consentire il ripristino del sistema.
- **Rimuovi i file posti in quarantena dopo** – definisce il periodo al termine del quale i file in quarantena verranno rimossi.
- **Invia i file di esempio automaticamente quando è necessaria un'ulteriore analisi:**
  - **Chiedi sempre** – prima dell'invio del file viene sempre richiesta la conferma all'utente.
  - **Invia gli esempi sicuri automaticamente** – la maggior parte degli esempi vengono inviati automaticamente, ad eccezione dei file che possono contenere informazioni personali. Per questi file viene richiesta una conferma aggiuntiva.
  - **Invia tutti gli esempi automaticamente** – tutti gli esempi vengono inviati automaticamente.
- **Disabilita l'interfaccia utente di Windows Defender Antivirus** – se l'opzione è selezionata l'interfaccia utente di WDA non sarà disponibile all'utente. È possibile gestire i criteri di WDA tramite la console di Cyber Protect.
- **MAPS (Microsoft Active Protection Service)** – comunità online che aiuta a scegliere come reagire alle potenziali minacce.
  - **Non desidero aderire a MAPS** – nessuna informazione sul software individuato verrà inviata a Microsoft.
  - **Appartenenza di base** – informazioni di base sul software individuato verranno inviate a Microsoft.
  - **Appartenenza avanzata** – informazioni più dettagliate sul software individuato verranno inviate a Microsoft.

© Acronis International GmbH, 2003-2024

Per ulteriori informazioni, fare riferimento a https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/

Per ulteriori informazioni sulle impostazioni avanzate di Microsoft Defender Antivirus, consultare https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings

Esclusioni

È possibile specificare l'esclusione dalla scansione dei file e delle cartelle indicate di seguito:

- **Processi** – qualsiasi file letto o scritto dal processo stesso verrà escluso dalla scansione. È necessario definire il percorso completo al file eseguibile del processo.
- **File e cartelle** – i file e le cartelle specificate verranno escluse dalla scansione. È necessario definire il percorso completo al file o alla cartella, o indicare l'estensione del file.

Per ulteriori informazioni sulle impostazioni di esclusione di Microsoft Defender Antivirus, consultare https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings

Gestione firewall

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Gestione firewall consente di configurare facilmente le impostazioni del firewall per i workload protetti.

In Cyber Protect questa funzionalità è fornita tramite il componente integrato Microsoft Defender Firewall di Microsoft Windows. Microsoft Defender Firewall blocca il traffico di rete non autorizzato indirizzato verso o proveniente dai workload.

Gestione firewall è applicabile ai workload sui quali è installato Microsoft Defender Firewall.

Sistemi operativi Windows supportati

Per la gestione del firewall, sono supportati i seguenti sistemi operativi:

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server non è supportato.

© Acronis International GmbH, 2003-2024

Abilitazione e disabilitazione di Gestione firewall

È possibile abilitare la gestione del firewall durante la creazione di un piano di protezione. Un piano di protezione esistente può essere modificato per abilitare o disabilitare la gestione del firewall.

Per abilitare o disabilitare Gestione firewall

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Eseguire una delle seguenti operazioni per aprire il riquadro del piano di protezione:
   - Se si desidera creare un nuovo piano di protezione, selezionare un sistema da proteggere, fare clic su **Proteggi**, quindi su **Crea piano**.
   - Se si desidera modificare un piano di protezione esistente, selezionare un sistema protetto, fare clic su **Proteggi**, fare clic sui puntini di sospensione (...) accanto al nome del piano di protezione, quindi su **Modifica**.
3. Nel riquadro del piano di protezione, passare alla sezione **Gestione firewall** e attivare o disattivare l'opzione **Gestione firewall**.
4. Eseguire una delle seguenti operazioni per applicare le modifiche:
   - Se si sta creando un piano di protezione, fare clic su **Crea**.
   - Se si sta modificando un piano di protezione, fare clic su **Salva**.

Lo **Stato di Microsoft Defender Firewall** nella sezione **Gestione firewall** è visualizzato nel riquadro del piano di protezione come **On** o **Off**, a seconda che la Gestione firewall sia stata abilitata o disabilitata.

È inoltre possibile accedere al riquadro del piano di protezione dalla scheda Gestione. Questa funzionalità non è disponibile in tutte le edizioni del servizio Cyber Protection.

Quarantena

Quarantena è una cartella speciale isolata che si trova nel disco rigido del sistema, nella quale vengono collocati i file sospetti individuati da Protezione antivirus e anti-malware, per impedire un'ulteriore diffusione delle minacce.

La Quarantena consente di rivedere i file sospetti e potenzialmente dannosi presenti su tutti i sistemi, e di decidere se devono essere rimossi o ripristinati. I file in quarantena vengono automaticamente eliminati se il computer è rimosso dal sistema.

Come vengono spostati i file nella cartella Quarantena?

1. È possibile configurare il piano di protezione e definire le azioni predefinite per i file infetti, da spostare in Quarantena.
2. Durante la scansione pianificata o all'accesso, il sistema individua file dannosi e li sposta nella cartella sicura Quarantena.
3. Il sistema aggiorna l'elenco dei file in quarantena sul sistema.

© Acronis International GmbH, 2003-2024

4. Il file vengono automaticamente eliminati dalla cartella Quarantena al termine del periodo definito nell'impostazione **Rimuovi i file posti in quarantena dopo** del piano di protezione.

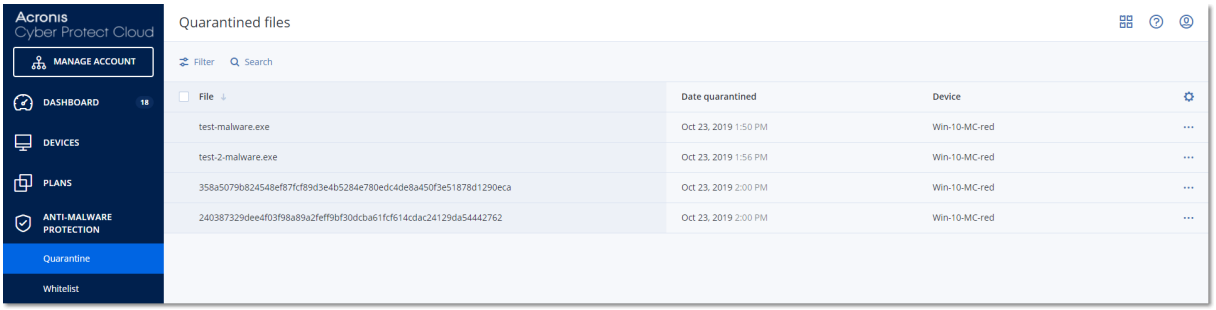
Gestione dei file in quarantena

Per gestire i file in quarantena, passare a **Protezione anti-malware** > **Quarantena**. Viene visualizzato un elenco dei file in quarantena presenti su tutti i sistemi.

Nome	Descrizione
File	Il nome del file.
Data di messa in quarantena	Data e ora in cui il file è stato messo in quarantena.
Dispositivo	Il dispositivo sul quale è stato trovato il file infetto.
Nome minaccia	Il nome della minaccia.
Piano di protezione	Il piano di protezione in base al quale il file sospetto è stato messo in quarantena.

Con i file in quarantena è possibile effettuare due azioni:

- **Elimina** – rimuove permanentemente i file in quarantena da tutti i sistemi. È possibile eliminare tutti i file con lo stesso hash del file. È possibile ripristinare tutti i file con lo stesso hash del file. Raggruppare i file in base all'hash, selezionare i file desiderati e quindi eliminarli.
- **Ripristino** – ripristina nella posizione originale un file in quarantena, senza modifiche. Se nella posizione originale è già presente un file con lo stesso nome, tale file verrà sovrascritto dal file ripristinato. Tenere presente che il file ripristinato viene aggiunto all'elenco degli elementi consentiti e ignorato durante le successive scansioni anti-malware.



Posizione della cartella Quarantena nei sistemi

La posizione predefinita per i file in quarantena è la seguente:

- Su sistemi Windows: `%programdata%\Acronis\NGMP\quarantine`
- Su sistemi Mac: `/Library/Application Support/Acronis/NGMP/quarantine`
- Su sistemi Linux: `/var/lib/Acronis/NGMP/quarantine`

L'archivio di quarantena è sotto la protezione autonoma del service provider.

© Acronis International GmbH, 2003-2024

Cartella personalizzata self-service su richiesta

È possibile selezionare le cartelle personalizzate nel workload e scansionarle direttamente dal menu contestuale.

Per accedere alla funzione di scansione con l'opzione Cyber Protect nel menu contestuale

Per i workload con un piano di protezione in cui sono abilitati antivirus e anti-malware, fare clic con il pulsante destro del mouse sul file o sulla cartella in cui eseguire la scansione.

Nota
Questa opzione è disponibile solo agli amministratori del workload.

Elenco degli elementi consentiti aziendale

Una soluzione antivirus potrebbe identificare come sospette applicazioni legittime e specifiche dell'azienda. Per prevenire il rilevamento di questi falsi positivi, le applicazioni attendibili vengono aggiunte manualmente all'elenco degli elementi consentiti, un'attività che richiede tempo.

Nota
L'elenco degli elementi consentiti aziendale non influisce sulle scansioni anti-malware dei backup.

Cyber Protection consente di automatizzare questo processo: i backup vengono scansionati dal modulo Protezione antivirus e anti-malware; i dati scansionati sono quindi analizzati e le applicazioni legittime spostate nell'elenco degli elementi consentiti; in questo modo si previene l'individuazione di falsi positivi. Inoltre, un elenco degli elementi consentiti a livello aziendale migliora le prestazioni di scansione anti-malware.

L'elenco degli elementi consentiti viene creato per ogni cliente, e si basa esclusivamente sui dati di tale cliente.

È possibile abilitarla e disabilitarla. Quando disabilitata, i file aggiunti vengono temporaneamente nascosti.

Nota
Le attività di configurazione e gestione dell'elenco degli elementi consentiti sono consentite soltanto agli account con il ruolo di amministrazione (ad esempio, amministratore di Cyber Protection; amministratore dell'azienda; amministratore del partner che agisce per conto di un amministratore dell'azienda; amministratore dell'unità). Questa funzionalità non è disponibile per gli account di amministrazione di sola lettura o per un account utente.

Aggiunta automatica all'elenco degli elementi consentiti

1. Eseguire la scansione in cloud dei backup su almeno due sistemi. A tale scopo, è possibile utilizzare i piani di scansione dei backup.

© Acronis International GmbH, 2003-2024

2. Abilitare l'opzione **Generazione automatica dell'elenco degli elementi consentiti** nelle impostazioni dell'elenco degli elementi consentiti.

Aggiunta manuale all'elenco degli elementi consentiti

Anche quando l'opzione **Generazione automatica dell'elenco degli elementi consentiti** è disabitata, è possibile aggiungere manualmente i file all'elenco degli elementi consentiti.

1. Nella console di Cyber Protect, passare a **Protezione anti-malware** > **Elenco degli elementi consentiti**.
2. Fare clic su **Aggiungi file**.
3. Specificare il percorso del file e fare clic su **Aggiungi**.

Aggiunta di file in quarantena all'elenco degli elementi consentiti

È possibile aggiungere all'elenco degli elementi consentiti i file in quarantena.

1. Nella console di Cyber Protect, passare a **Protezione anti-malware** > **Quarantena**.
2. Selezionare un file in quarantena e fare clic su **Aggiungi all'elenco degli elementi consentiti**.

Impostazioni dell'elenco degli elementi consentiti

Quando si abilita l'opzione **Generazione automatica dell'elenco degli elementi consentiti**, è necessario specificare uno dei livelli seguenti di protezione euristica:

- **Basso**
  Le applicazioni aziendali verranno aggiunte all'elenco degli elementi consentiti solo dopo una quantità significativa di tempo e di controlli. Le applicazioni di questo tipo sono più attendibili. Tuttavia, questo approccio aumenta la possibilità di individuazione di falsi positivi. I criteri per considerare un file pulito e attendibile sono elevati.
- **Predefinito**
  Le applicazioni aziendali verranno aggiunte all'elenco degli elementi consentiti in base al livello di protezione consigliato, per ridurre l'individuazione di possibili falsi positivi. I criteri per considerare un file pulito e attendibile sono medi.
- **Alto**
  Le applicazioni aziendali verranno aggiunte all'elenco degli elementi consentiti più rapidamente, per ridurre l'individuazione di possibili falsi positivi. Tuttavia, ciò non garantisce che il software non sia infetto; successivamente potrebbe essere riconosciuto come sospetto o come malware. I criteri per considerare un file pulito e attendibile sono alti.

Visualizzare informazioni sugli elementi dell'elenco degli elementi consentiti

È possibile fare clic su un elemento dell'elenco degli elementi consentiti per visualizzare ulteriori informazioni e per analizzarlo online.

© Acronis International GmbH, 2003-2024

Se non si è certi di un elemento che è stato aggiunto, è possibile verificarlo con lo strumento VirusTotal. Facendo clic su **Controlla su VirusTotal**, il sito analizza i file e gli URL sospetti, per individuare eventuali tipologie di malware utilizzando il file hash dell'elemento che è stato aggiunto. L'hash viene visualizzato nella stringa **Hash del file (MD5)**.

Il valore **Sistemi** rappresenta il numero di sistemi nei quali tale hash è stato individuato durante la scansione del backup. Questo valore viene compilato solo se l'elemento individuato proviene dalla Scansione del backup o dalla Quarantena. Il campo resta vuoto se il file è stato aggiunto manualmente all'elenco degli elementi consentiti.

Scansione anti-malware dei backup

Una scansione anti-malware dei backup consente di impedire il ripristino di file infetti, controllando che i backup non contengano potenziali malware. Le scansioni anti-malware vengono eseguite da un agente cloud residente nel data center Cyber Protection, senza utilizzare risorse di elaborazione locali.

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

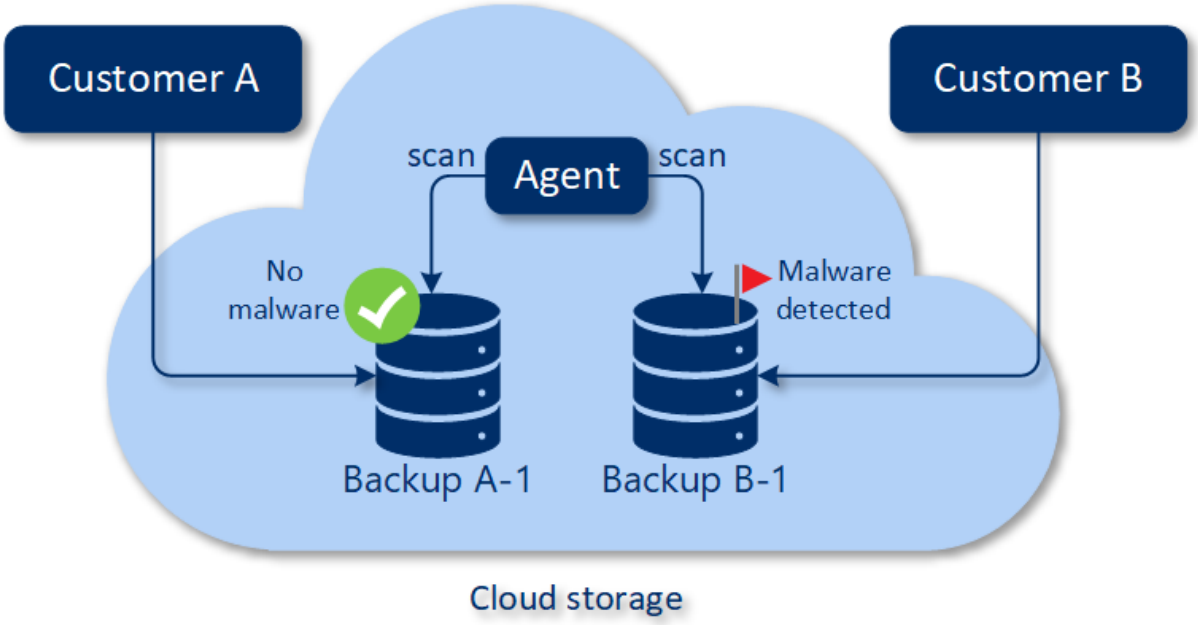
Per eseguire una scansione anti-malware, è necessario configurare un piano di scansione dei backup. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Piani di scansione del backup" (pag. 200).

Ogni piano di scansione dei backup crea un'attività di scansione per l'agente cloud e aggiunge questa attività a una coda; è presente una coda per ogni data center. Le attività di scansione vengono elaborate in base alla loro sequenza nella coda. Inoltre, la durata della scansione dipende dalla dimensione del backup. Per questa ragione c'è un ritardo tra la creazione di un piano di scansione del backup e il completamento della scansione.

I backup selezionati per la scansione possono trovarsi in uno degli stati seguenti:

- Non scansionato
- Nessun malware
- Malware rilevato

© Acronis International GmbH, 2003-2024



È possibile controllare i risultati della scansione nel widget **Informazioni sulla scansione del backup (minacce)**. Il widget si trova nella console di Cyber Protect, nella scheda **Monitoraggio** > **Panoramica**.

Limitazioni

- La funzionalità di scansione anti-malware è supportata solo per i backup dell'**Intera macchina** o di **Dischi/volumi** dei workload indicati di seguito.
  - Sistemi Windows nei quali è installato un agente di protezione.
  - Virtual machine Windows il cui backup viene eseguito a livello di hypervisor (backup agentless) da Agente per Hyper-V e Agente per VMware (Windows).

  La scansione anti-malware non è supportata per i backup creati da appliance virtuali, come l'Agente per VMware (appliance virtuale), l'Agente per Virtuozzo, l'Agente per Scale Computing HC3.
- Vengono scansionati solo i volumi con il file system NTFS e con partizionamento GPT e MBR.
- Come posizione di backup è supportato soltanto il cloud storage predefinito. Non sono invece supportati i cloud storage di proprietà del partner o gli storage locali.
- Quando si selezionano i backup da scansionare, è possibile selezionare set di backup che includono un backup con CDP (Protezione continua dei dati). Tuttavia, in questi set di backup verranno scansionati solo i backup senza CDP. Per ulteriori informazioni sui backup con CDP, fare riferimento a "Protezione continua dei dati (CDP)" (pag. 416).
- Quando si esegue il ripristino sicuro di un intero sistema, è possibile selezionare un set di backup che includa un backup CDP. Tuttavia, questa operazione di ripristino non utilizzerà i dati del backup CDP. Per i recuperare i dati CDP, eseguire un'operazione di ripristino di **File/cartelle**.

© Acronis International GmbH, 2003-2024

Lavorare con le funzionalità di protezione avanzata

Per impostazione predefinita, Cyber Protect include funzionalità che coprono la maggior parte delle minacce alla Cyber Security. Tali funzionalità possono essere utilizzate senza incorrere in tariffe aggiuntive. Inoltre, è possibile abilitare funzionalità avanzate che incrementano la protezione dei workload.

- Se è disponibile la funzionalità di protezione avanzata, questa verrà visualizzata nel piano di protezione e contrassegnata con l'icona Advanced .
- Se non è disponibile la funzionalità di protezione avanzata, contattare l'amministratore per abilitare il pacchetto di protezione Advanced richiesto.
- Se l'amministratore ha abilitato l'utente ad acquistare pacchetti di sicurezza extra, sarà possibile selezionarli per abilitare le funzionalità avanzate. Un messaggio indirizza l'utente a una schermata contenente le informazioni sulle tariffe aggiuntive applicate.

Nota
Se viene abilitata anche una sola funzionalità, è necessario acquistare il pacchetto di protezione Advanced corrispondente.

Nota
Se nel piano di protezione sono disabilitate tutte le funzionalità avanzate, viene disabilitato anche il pacchetto di protezione Advanced corrispondente.

Pacchetti di protezione avanzata	Funzionalità di protezione avanzata
Advanced Backup	Protegge costantemente i workload e garantisce che neanche le ultime modifiche apportate al lavoro vadano perse. Le funzionalità includono: • One-click Recovery • Protezione continua dei dati • Supporto per il backup di cluster Microsoft SQL Server e cluster di Microsoft Exchange - Gruppo di disponibilità Always On (AAG) e Gruppo di Disponibilità Database (DAG) • Supporto per il backup di database MariaDB, MySQL, Oracle DB e SAP HANA • Mappa della protezione dati e report di conformità • Elaborazione dei dati al di fuori dell'host • Frequenza di backup per workload Microsoft 365 e Google Workspace • Operazioni remoto con un supporto di avvio • Backup diretto al cloud storage pubblico di Microsoft Azure
Advanced	Protegge costantemente i workload da tutte le minacce malware. Le funzionalità

© Acronis International GmbH, 2003-2024

Security + EDR	includono: • Gestione dei problemi in una pagina centralizzata • Visualizzare ambito e impatto dei problemi • Consigli e raccomandazioni di correzione • Verificare gli attacchi resi pubblici ai workload utilizzando i Feed minacce • Archiviare gli eventi di sicurezza per 180 giorni • Protezione antivirus e anti-malware in tempo reale con individuazione basata sulle firme in locale (con protezione in tempo reale) • Prevenzione degli exploit • Filtro URL • Gestione firewall degli endpoint • Backup con dati forensi, scansione dei backup alla ricerca del malware, ripristino sicuro, elenco degli elementi consentiti aziendale • Piani di protezione smart (integrazione con gli avvisi dei CPOC) • Scansione centralizzata del backup alla ricerca del malware • Cancellazione remota • Microsoft Defender Antivirus • Microsoft Security Essentials
Advanced Management	Consente di applicare la patch alle vulnerabilità individuate nei workload protetti. Le funzionalità includono: • Gestione patch • Integrità del disco • Inventario software • Patch a prova di errore • Cyber Scripting • Assistenza remota • Trasferimento e condivisione di file • Selezionare una sessione a cui connettersi • Osservazione dei workload su più visualizzazioni • Modalità di connessione: controllo, solo visualizzazione e tenda • Connessione tramite applicazione Quick Assist • Protocolli di connessione remota: NEAR e Condivisione schermo di Apple • Sessione di registrazione per connessioni NEAR • Trasmissione screenshot • Report della cronologia della sessione • 24 monitor • Monitoraggio basato su soglia • Monitoraggio basato sulle anomalie
Advanced Data Loss Prevention	Previene la perdita di informazioni sensibili dai workload protetti. Le funzionalità includono:

© Acronis International GmbH, 2003-2024

	• Prevenzione sensibile al contesto della perdita di dati dai workload tramite dispositivi periferici e comunicazioni di rete • Rilevamento automatico integrato di Informazioni che consentono l'identificazione personale dell'utente (PII), Informazioni sanitarie protette (PHI) e Dati soggetti allo standard Payment Card Industry Data Security Standard, oltre a documenti della categoria “Contrassegnato come Riservato” • Creazione di policy automatiche per la prevenzione della perdita di dati con assistenza facoltativa all'utente finale • Applicazione adattativa della prevenzione della perdita di dati con adeguamento automatico delle policy basato sull'apprendimento • Registrazione centralizzata di audit, avvisi e notifiche agli utenti finali basata su cloud

Advanced Data Loss Prevention

Il modulo Advanced Data Loss Prevention analizza il contenuto e il contesto dei trasferimenti dei dati nei workload protetti e previene la perdita di dati sensibili attraverso dispositivi periferici o trasferimenti di rete interni o esterni all'azienda in base alla policy di flusso dei dati.

Le funzionalità di Advanced Data Loss Prevention possono essere incluse in qualsiasi piano di protezione di un tenant cliente, se per tale cliente sono abilitati il servizio di protezione e il pacchetto Advanced Data Loss Prevention.

Prima di iniziare a utilizzare il modulo Advanced Data Loss Prevention, accertarsi di aver letto e compreso i concetti di base e la logica di gestione della funzionalità descritti nella Guida ai concetti di base.

Può inoltre essere utile leggere il documento Specifiche tecniche.

Creazione della policy di flusso dei dati e delle regole della policy

Il principio su cui si basa la prevenzione della perdita di dati è che agli utenti di un sistema IT aziendale viene concesso di gestire i dati sensibili solo nella misura in cui è a loro necessario per eseguire le attività lavorative. Qualsiasi altro trasferimento di dati sensibili irrilevante dal punto di vista dei processi aziendali dovrebbe essere bloccato. È pertanto cruciale riuscire a distinguere tra flussi e trasferimenti dei dati correlati alle attività aziendali oppure non autorizzati.

La policy di flusso dei dati contiene regole che specificano quali flussi sono consentiti e quali proibiti, consentendo così di prevenire trasferimenti non autorizzati di informazioni sensibili quando il modulo Data Loss Prevention è abilitato in un piano di protezione ed eseguito in modalità di applicazione.

Ogni categoria di riservatezza della policy contiene una regola predefinita, contrassegnata con un (*) e una o più regole esplicite (non predefinite) che definiscono i flussi dei dati per utenti o gruppi specifici. Nella Guida ai concetti di base sono reperibili più informazioni sui tipi di regole delle policy.

In genere, la policy di flusso dei dati viene creata automaticamente mentre Advanced Data Loss Prevention è in esecuzione in modalità di osservazione. Il tempo necessario per creare una policy di

© Acronis International GmbH, 2003-2024

flusso dei dati rappresentativa è di circa un mese, ma questo intervallo può differire in funzione dei processi aziendali dell'organizzazione. La policy di flusso dei dati può inoltre essere creata, configurata e modificata manualmente da un amministratore dell'azienda o dell'unità.

Per avviare la creazione automatica di una policy di flusso dei dati

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Gestione** > **Piani di protezione**.
3. Fare clic su **Crea piano**.
4. Espandere la sezione **Prevenzione della perdita di dati** e fare clic sulla riga **Modalità**.
5. Nella finestra di dialogo Modalità, selezionare **Modalità di osservazione** e selezionare come elaborare i trasferimenti dei dati:

Opzione	Descrizione
Consenti tutto	Tutti i trasferimenti di dati sensibili dai workload degli utenti vengono considerati necessari per i processi aziendali e sicuri. Viene creata una nuova regola ogni volta che viene individuato un flusso dei dati che non corrisponde a una regola già definita nella policy.
Giustifica tutto	Tutti i trasferimenti dei dati sensibili dai workload degli utenti vengono considerati necessari per i processi aziendali, ma a rischio. Pertanto, per ogni trasferimento dei dati sensibili intercettato verso qualsiasi destinatario o destinazione, interna ed esterna all'organizzazione, che non corrisponde a una regola di flusso dei dati precedentemente creata, l'utente deve inserire una giustificazione aziendale temporanea. Una volta inviata la giustificazione, nella policy di flusso dei dati verrà creata una nuova regola per il flusso dei dati.
Mista	La logica Consenti tutto viene applicata a tutti i flussi dei dati sensibili interni, mentre la logica Giustifica tutto viene applicata a tutti i flussi dei dati esterni. **Nota** Per ulteriori informazioni sui dati interni ed esterni vedere Rilevamento automatico della destinazione

6. Salvare il piano di protezione e applicarlo ai workload dai quali acquisire i dati per creare la policy.

Nota
Durante la modalità di osservazione non si avrà alcuna prevenzione della perdita di dati.

Per configurare manualmente la policy di flusso dei dati

1. Nella console di Cyber Protect, passare a **Protezione** > **Policy di flusso dei dati**.
2. Fare clic su **Nuova regola di flusso dei dati**.
   Il riquadro Nuova regola di flusso dei dati viene visualizzato a destra.

© Acronis International GmbH, 2003-2024

3. Selezionare una categoria di riservatezza, aggiungere un mittente e un destinatario e definire l'autorizzazione per il trasferimento dei dati della categoria, del mittente e del destinatario selezionati.

Opzione	Descrizione
Consenti	Consenti a questo mittente di trasferire i dati di questa categoria di riservatezza a questo destinatario.
Eccezione	Consenti a questo mittente di trasferire i dati di questa categoria di riservatezza a questo destinatario, ma consenti al mittente di aggiungere un'eccezione alla regola per un trasferimento specifico. Quando questo mittente tenta di trasferire i dati di questa categoria di riservatezza a questo destinatario, blocca il trasferimento e chiede al mittente di aggiungere un'eccezione per consentire questo trasferimento. Una volta inviata l'eccezione, il trasferimento dei dati viene consentito. **Importante** Tutti i trasferimenti successivi tra questo mittente e questo destinatario, per questa categoria di riservatezza, verranno consentiti per i cinque minuti successivi all'invio dell'eccezione.
Nega	Non consentire a questo mittente di trasferire i dati di questa categoria di riservatezza a questo destinatario, e non consentire al mittente di richiedere un'eccezione alla regola.

4. (Facoltativo) Selezionare un'azione da eseguire quando viene attivata la regola.

Azione	Descrizione
Scrivi nel registro	Archivia un record evento nel registro di audit degli eventi quando viene attivata la regola. È consigliabile selezionare questa azione per le regole con l'autorizzazione **Eccezione**.
Genera un avviso	Genera un avviso nella scheda Cyber Protect **Avvisi** quando viene attivata la regola. Se per l'amministratore sono abilitate le notifiche, viene inoltre inviata una notifica e-mail.
Notifica all'utente finale quando viene negato un trasferimento dei dati	Quando viene attivata la regola, l'utente riceve una notifica in tempo reale con un avviso a schermo.

5. Fare clic su **Salva**.
6. Ripetere i passaggi da 2 a 5 per creare più regole per categorie di riservatezza e opzioni differenti, e verificare che le regole risultanti corrispondano alle opzioni selezionate.

Struttura della policy di flusso dei dati

© Acronis International GmbH, 2003-2024

Nella vista **Policy di flusso dei dati**, le regole della policy sono raggruppate in base alla categoria di dati sensibili che controllano. L'identificatore della categoria di riservatezza è visualizzato sopra al gruppo di regole della policy.

- Sensibili
  - Informazioni sanitarie protette (PHI)
  - Informazioni che consentono l'identificazione personale dell'utente (PII)
  - Dati soggetti allo standard Payment Card Industry Data Security Standard (PCI DSS)
  - Contrassegnato come Riservato
- Non sensibili

Per ulteriori informazioni sui concetti e sulle funzionalità della policy di flusso dei dati, vedere la Guida ai concetti di base.

Struttura della regola

Ogni regola della policy è formata dai seguenti elementi.

- **Categoria di riservatezza**
  - **Informazioni sanitarie protette (PHI)**
  - **Informazioni che consentono l'identificazione personale dell'utente (PII)**
  - **Dati soggetti allo standard Payment Card Industry Data Security Standard (PCI DSS)**
  - **Contrassegnato come Riservato**

    Vedere "Definizioni di dati sensibili" (pag. 900)
- **Mittente** - specifica chi ha iniziato il trasferimento dei dati controllato da questa regola. Può trattarsi di un singolo utente, di un elenco di utenti o di un gruppo di utenti.
  - **Qualsiasi utente interno** - un gruppo di utenti che include tutti gli utenti interni dell'organizzazione.
  - **Contatto/Dall'organizzazione** - un account Windows dell'organizzazione, riconosciuto da Advanced Data Loss Prevention, nonché tutti gli altri account (inclusi quelli utilizzati dalle applicazioni di comunicazione di terze parti) che uno specifico account Windows ha utilizzato in precedenza.
  - **Contatto/Identità personalizzata** - identificatore di un utente interno specificato in uno dei seguenti formati: e-mail, ID Skype, identificatore ICQ, identificatore IRC, e-mail Jabber, e-mail agente Mail.ru, numero telefonico Viber, e-mail Zoom.
    Per specificare un gruppo di contatti è possibile utilizzare i seguenti caratteri jolly:
    - ***** - qualsiasi numero di simboli
    - **?** - qualsiasi simbolo singolo
- **Destinatario** - specifica la destinazione del trasferimento dei dati controllato da questa regola. Può trattarsi di un singolo utente, di un elenco di utenti o di un gruppo di utenti, oppure degli altri tipi di destinazione specificati di seguito.

© Acronis International GmbH, 2003-2024

- **Qualsiasi** - uno qualsiasi dei tipi di destinatario supportati da Advanced DLP.
- **Contatto/Qualsiasi contatto** - qualsiasi contatto interno o esterno.
- **Contatto/Qualsiasi contatto interno** - qualsiasi contatto di un utente interno (vedere "Rilevamento automatico della destinazione" (pag. 900)).
- **Contatto/Qualsiasi contatto esterno** - qualsiasi contatto di una persona o di un'entità esterna.
- **Contatto/Dall'organizzazione** - la stessa entità descritta nel campo Mittente.
- **Contatto/Identità personalizzata** - la stessa entità descritta nel campo Mittente.
- **Servizi di condivisione file** - identificatore di un servizio di condivisione file controllato.
- **Social network** - identificatore di un social network controllato.
- **Host/Qualsiasi host** - qualsiasi computer riconosciuto da Advanced DLP come interno o esterno.
- **Host/Qualsiasi host interno** - qualsiasi computer riconosciuto da Advanced DLP come interno.
- **Host/Qualsiasi host esterno** - qualsiasi computer riconosciuto da Advanced DLP come esterno.
- **Host/Host specifico** - identificatore di computer specificato come nome host (ad esempioFQDN) o indirizzo IP (IPv4 o IPv6).
- **Dispositivo/Qualsiasi dispositivo** - qualsiasi dispositivo periferico connesso al workload.
- **Dispositivo/Storage esterno** - unità mappata di storage rimovibile o unità mappata reindirizzata connessa al workload.
- **Dispositivo/Rimovibile crittografato** - un dispositivo di storage rimovibile crittografato con BitLocker To Go.
- **Dispositivo/Appunti reindirizzati** - appunti reindirizzati connessi al workload.
- **Stampanti** - qualsiasi stampante locale o di rete connessa al workload.

- **Autorizzazione** - controllo preventivo applicato a un trasferimento dei dati controllato da questa regola. È descritto in maggior dettaglio nell'argomento Autorizzazioni nelle regole della policy di flusso dei dati.
- **Azione** - azione non preventiva eseguita quando questa regola viene attivata. Per impostazione predefinita questo campo è impostato su "Nessuna azione". Le opzioni sono:
  - **Scrivi nel registro** - archivia un record evento nel registro di audit degli eventi quando viene attivata la regola.
  - **Notifica all'utente finale quando viene negato un trasferimento dei dati** - invia all'utente una notifica di avviso a schermo in tempo reale quando viene attivata la regola.
  - **Genera un avviso** - avvisa l'amministratore quando viene attivata la regola.

© Acronis International GmbH, 2003-2024

Attenzione!
Quando è selezionata l'opzione **Nessuna azione** e la regola viene attivata:

- nessun record evento viene aggiunto al registro di audit;
- nessun avviso viene inviato all'amministratore;
- nessuna notifica a schermo viene mostrata all'utente finale.

Cosa attiva una regola di policy?

Un trasferimento dei dati corrisponde a una regola della policy di flusso dei dati se tutte le condizioni seguenti sono vere:

- Tutti i mittenti di questo trasferimento dei dati sono elencati o appartengono a un gruppo di utenti specificato nel campo **Mittente** della regola.
- Tutti i destinatari di questo trasferimento dei dati sono elencati o appartengono a un gruppo di utenti specificato nel campo **Destinatario** della regola.
- I dati in corso di trasferimento corrispondono alla **Categoria di riservatezza** della regola.

Adeguamento delle autorizzazioni nelle regole della policy di flusso dei dati

Advanced Data Loss Prevention supporta tre tipi di autorizzazioni delle regole della policy di flusso dei dati. Le autorizzazioni vengono configurate singolarmente per ogni regola della policy.

Consenti (permissiva)	Sono consentiti i trasferimenti dei dati che corrispondono alla combinazione di categoria di riservatezza, mittente e destinatario definita nella regola.
Eccezione (proibitiva)	Non sono consentiti i trasferimenti dei dati che corrispondono alla combinazione di categoria di riservatezza, mittente e destinatario definita nella regola, ma il mittente può inviare un'eccezione alla regola per consentire un trasferimento specifico. **Importante** Tutti i trasferimenti successivi tra questo mittente e questo destinatario, per questa categoria di riservatezza, verranno consentiti per i cinque minuti successivi all'invio dell'eccezione.
Nega (proibitiva)	Non sono consentiti i trasferimenti dei dati che corrispondono alla combinazione di categoria di riservatezza, mittente e destinatario definita nella regola, e il mittente non ha l'opzione di inviare un'eccezione.

In aggiunta, è possibile assegnare un contrassegno di priorità alle autorizzazioni **Consenti** e **Eccezione**, per aumentare la flessibilità di gestione della policy. Con questa impostazione è possibile ignorare le autorizzazioni impostate per gruppi specifici in altre regole del flusso dei dati della policy. È possibile utilizzare l'impostazione per applicare una regola di flusso dei dati di un gruppo solo ad alcuni dei suoi membri. Per ottenere questo risultato, è necessario creare una regola di flusso dei dati per gli specifici utenti che si desidera escludere dalle regole del gruppo, e quindi

© Acronis International GmbH, 2003-2024

rendere prioritarie le loro autorizzazioni rispetto alle restrizioni del flusso dei dati configurate nelle regole del gruppo a cui appartengono gli utenti specificati. Per informazioni sulle priorità delle autorizzazioni nelle combinazioni di regole, vedere "Combinare le regole della policy di flusso dei dati" (pag. 892).

Importante
Prima di trasferire una policy aziendale o di unità dalla modalità di osservazione a quella di applicazione, è fondamentale modificare le regole predefinite per ogni categoria di dati sensibili impostandole dalla condizione permissiva alla condizione proibitiva. Le regole predefinite sono contrassegnate con un asterisco (*) nella vista **Policy di flusso dei dati**. Nella Guida ai concetti di base sono reperibili più informazioni sui tipi di regole delle policy.

Per modificare le autorizzazioni nelle regole della policy

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Protezione** > **Policy di flusso dei dati**.
3. Selezionare la regola della policy da modificare e fare clic su **Modifica** in alto nell'elenco delle regole.
   Viene visualizzata la finestra **Modifica regola di flusso dei dati**.
4. Nella sezione **Autorizzazione**, selezionare **Consenti**, **Eccezione** o **Nega**.
5. (Facoltativo) Per dare priorità all'autorizzazione **Consenti** o **Eccezione** di questa regola rispetto alle autorizzazioni in altre regole, selezionare la casella di controllo **Definisci priorità**.
   Non utilizzare questa casella di controllo per dare priorità a una regola di flusso dei dati rispetto alla regola predefinita Qualsiasi > Altro, perché per impostazione predefinita nella policy avrà sempre la priorità inferiore.
   Per informazioni sulle priorità delle autorizzazioni nelle combinazioni di regole, vedere "Combinare le regole della policy di flusso dei dati" (pag. 892).
6. (Facoltativo) Selezionare un'azione da eseguire quando viene attivata la regola.
7. Salvare le modifiche alla regola della policy.

Combinare le regole della policy di flusso dei dati

Quando un trasferimento dei dati soddisfa più di una regola, le autorizzazioni e le azioni configurate per tutte le regole vengono combinate e applicate come indicato di seguito.

Autorizzazioni

Se un trasferimento dei dati soddisfa più di una regola e se queste regole hanno autorizzazioni differenti per la stessa categoria di dati, la regola superiore è quella con le autorizzazioni di priorità più elevate, in base al seguente elenco di priorità delle autorizzazioni (in ordine decrescente):

1. Eccezione con il flag **Con priorità**
2. Consenti con il flag **Con priorità**
3. Nega

© Acronis International GmbH, 2003-2024

4. Eccezione
5. Consenti

Se un trasferimento dei dati soddisfa più di una regola e se queste regole hanno autorizzazioni differenti per diverse categorie di dati, come regola superiore viene applicata la logica seguente:

1. L'autorizzazione della regola più restrittiva viene definita per ognuna delle categorie di riservatezza a cui corrisponde il trasferimento dei dati.
2. Viene applicata la più restrittiva delle autorizzazioni della regola indicata al punto 1.

Esempio

Un trasferimento di file soddisfa tre regole in categorie di riservatezza differenti, come indicato di seguito:

Categoria di riservatezza	Autorizzazione
PII	Consenti - Con priorità
PHI	Eccezione - Con priorità
PCI	Nega

L'autorizzazione applicata è Nega.

Azioni

Se un trasferimento dei dati soddisfa più di una regola e per queste regole sono configurate opzioni diverse nel campo **Azione**, vengono eseguite tutte le azioni configurate in tutte le regole attivate.

Revisione e gestione delle policy

Prima che la policy di flusso dei dati di base creata automaticamente venga applicata, deve essere rivista, convalidata e approvata dal cliente, perché è il cliente che conosce con esattezza tutte le specifiche e le esigenze dei propri processi aziendali e che può valutare se sono state interpretate in modo omogeneo nella policy di base. Inoltre, il cliente può identificare le imprecisioni, la cui correzione spetta all'amministratore del partner.

Durante la revisione della policy, l'amministratore del partner presenta la policy di base al cliente, che rivede ogni flusso dei dati nella policy e ne convalida la coerenza rispetto ai propri processi aziendali. La convalida non richiede competenze tecniche, poiché la rappresentazione delle regole della policy nella console di Cyber Protect è estremamente intuitiva: ogni regola designa il mittente e il destinatario di un flusso di dati sensibili.

Seguendo le istruzioni del cliente, l'amministratore del partner adatta manualmente la policy di base modificando, eliminando e creando regole per la policy di flusso dei dati. Dopo l'approvazione del cliente, la policy rivista viene applicata sui workload protetti trasferendo il piano di protezione applicato a tali workload alla modalità di applicazione.

© Acronis International GmbH, 2003-2024

Prima di applicare una policy rivista, è importante modificare l'autorizzazione **Consenti** in tutte le regole della policy predefinita create automaticamente per le categorie di dati sensibili sull'impostazione **Nega** o **Eccezione**. L'autorizzazione **Nega** non può essere sostituita dagli utenti, mentre l'autorizzazione **Eccezione** blocca un trasferimento che corrisponde alla regola ma consente agli utenti di ignorare il blocco in una situazione di emergenza, inviando un'eccezione correlata all'attività aziendale.

Rinnovo della policy di flusso dei dati

In caso di modifica sostanziale del processo aziendale dell'azienda o di sue unità, è necessario rinnovare le policy di DLP in modo omogeneo alle modifiche apportate ai flussi dei dati sensibili dei processi aziendali aggiornati. Il rinnovo di una policy è necessario anche se il ruolo professionale di un dipendente cambia; in questo caso è necessario rinnovare anche la parte di policy dell'unità utilizzata per proteggere il workload del dipendente.

Il flusso di lavoro di gestione della policy di Advanced DLP consente agli amministratori di automatizzare i rinnovi delle policy per un'intera azienda, un'unità, un utente, o una parte di utenti di un'unità.

Rinnovare la policy per un'azienda o un'unità

È possibile utilizzare tutte le opzioni della modalità di osservazione per rinnovare la policy dell'azienda, dell'unità o di una parte di una policy dell'unità per uno o più utenti dell'unità stessa.

Per rinnovare la policy per un'azienda o un'unità

Il processo di rinnovo è costituito dai passaggi seguenti, che devono essere effettuati dall'amministratore di un'azienda o da un partner che gestisce i workload dell'azienda.

1. Eliminare tutte le regole non predefinite nella policy applicata.
2. Per avviare il rinnovo, trasferire il piano di protezione in cui la funzionalità Advanced DLP è applicata all'azienda o all'unità a una delle opzioni della modalità di osservazione, in base a quella ottimale per questa specifica azienda o unità, e quindi applicare il piano a tutti i workload dell'azienda o dell'unità.
3. Al termine del periodo di rinnovo, rivedere la nuova policy aziendale o di unità con il cliente, modificarla se necessario, e ottenere l'approvazione del cliente.
4. Attivare il piano di protezione applicato ai workload dell'azienda o dell'unità all'opzione della modalità di applicazione adeguata che il cliente considera come ottimale per prevenire la perdita dei dati dai workload dell'unità.

Rinnovare la policy per uno o più utenti dell'azienda o dell'unità

Le policy a livello di utente possono essere rinnovate utilizzando qualsiasi opzione della modalità di osservazione, e anche la modalità di applicazione adattiva.

© Acronis International GmbH, 2003-2024

Utilizzo della modalità di osservazione per il rinnovo di una policy utente

L'utilizzo della modalità di osservazione per il rinnovo di una policy per un utente o per una parte di utenti dell'azienda (o dell'unità) prevede le specifiche seguenti: la policy di flusso dei dati applicata all'intera azienda (o unità) non si applica ai trasferimenti dei dati dell'utente durante il periodo di rinnovo. Di conseguenza, durante il periodo di rinnovo potrebbero essere create nuove regole individuali per l'utente che contrastano o corrispondono a regole del gruppo già esistenti nella policy applicata per l'azienda (o unità). Una volta completato il rinnovo e applicata la policy ai trasferimenti dei dati dell'utente, l'applicazione o meno di queste nuove regole individuali create per l'utente dipende dalle loro priorità rispetto alle altre regole della policy a cui corrispondono questi trasferimenti dei dati.

Per rinnovare la policy per un utente tramite la modalità di osservazione

Il processo di rinnovo è costituito dai passaggi seguenti, che devono essere effettuati dall'amministratore di un'azienda o da un partner che gestisce i workload dell'azienda.

1. Eliminare tutte le regole non predefinite nella policy applicata per l'azienda (o l'unità) che hanno l'utente come unico mittente.
2. Rimuovere l'utente dagli elenchi dei mittenti di tutte le regole di flussi dei dati non predefinite nella policy applicata.
3. Creare un nuovo piano di protezione con Advanced DLP in modalità di osservazione e applicarlo al workload dell'utente per avviare il periodo di rinnovo (osservazione).
   La durata del periodo di rinnovo dipende dal tempo necessario all'utente per eseguire tutte o almeno il 90-95% delle proprie attività di lavoro standard che implicano il trasferimento di dati sensibili dai propri workload.
4. Al termine del periodo di rinnovo, rivedere le nuove regole relative a questo utente che sono state aggiunte alla policy applicata, modificarle se necessario, e ottenere l'approvazione del cliente.
5. Trasferire il piano di protezione applicato ai workload dell'utente alla modalità **Applicazione rigida** o **Applicazione adattiva**, a seconda di quale opzione il cliente considera come ottimale per prevenire la perdita dei dati dai workload dell'utente.
   In alternativa, è possibile riapplicare al workload dell'utente il piano di protezione applicato all'azienda (o unità).

Utilizzo della modalità di Applicazione adattiva per il rinnovo di una policy utente

Il rinnovo della policy per un singolo utente o per una parte di tutti gli utenti dell'azienda (o unità) può essere eseguito mediante la modalità di Applicazione adattiva di un piano di protezione con Advanced DLP applicato al workload dell'utente.

© Acronis International GmbH, 2003-2024

Nota
Questo metodo di rinnovo della policy prevede le specifiche seguenti: le regole della policy applicate all'azienda (unità) per i gruppi di mittenti con l'appartenenza dell'utente (ad esempio, qualsiasi utente interno) sono applicate anche ai trasferimenti dei dati da questo utente durante il rinnovo. Di conseguenza, il rinnovo non crea nuove regole individuali per l'utente che contrastano o corrispondono alle regole delle policy già esistenti per i gruppi di mittenti. Quale tra questi due metodi sia più efficace per i rinnovi delle policy utente per un particolare cliente dipende dagli specifici requisiti di sicurezza IT

Per rinnovare la policy per un utente tramite la modalità di applicazione adattiva

Il processo di rinnovo è costituito dai passaggi seguenti, che devono essere effettuati dall'amministratore di un'azienda o da un partner che gestisce i workload dell'azienda.

1. Eliminare tutte le regole non predefinite nella policy applicata per l'azienda (unità) che hanno l'utente come unico mittente.
2. Rimuovere l'utente dagli elenchi dei mittenti di tutte le regole di flussi dei dati non predefinite nella policy applicata.
3. Per tutte le regole predefinite nella policy applicata per l'azienda (o unità), impostare l'autorizzazione su **Eccezione** e selezionare l'azione **Scrivi nel registro** nel campo **Azione**.
4. Se il piano di protezione attualmente applicato al workload dell'utente è impostato sulla modalità **Applicazione rigida**, creare un nuovo piano di protezione con Advanced DLP e applicarlo al workload dell'utente in modalità di **Applicazione adattiva** per avviare il periodo di rinnovo.
   La durata del periodo di rinnovo dipende dal tempo necessario all'utente per eseguire tutte o almeno il 90-95% delle proprie attività di lavoro standard che implicano il trasferimento di dati sensibili dai propri workload.
5. Al termine del periodo di rinnovo, rivedere le nuove regole relative a questo utente che sono state aggiunte alla policy applicata, modificarle se necessario, e ottenere l'approvazione del cliente.
6. Trasferire il piano di protezione applicato al workload dell'utente alla modalità **Applicazione rigida** o lasciarlo in modalità **Applicazione adattiva**, a seconda di quale opzione il cliente consideri ottimale per prevenire la perdita dei dati dai workload dell'utente.
   In alternativa, è possibile riapplicare al workload dell'utente il piano di protezione applicato all'azienda (o unità).

Abilitazione di Advanced Data Loss Prevention nei piani di protezione

Le funzionalità di Advanced Data Loss Prevention possono essere incluse in qualsiasi piano di protezione di un tenant cliente, se per tale cliente sono abilitati il servizio di protezione e il pacchetto Advanced Data Loss Prevention.

© Acronis International GmbH, 2003-2024

Advanced DLP è il modulo avanzato del gruppo di funzionalità di prevenzione della perdita di dati. Le funzionalità di Advanced DLP e Controllo dispositivo possono essere utilizzati indipendentemente o insieme (in un piano di protezione singolo o in due piani che proteggono lo stesso workload). Se utilizzati insieme, le loro capacità funzionali sono coordinate come segue.

- Controllo dispositivo smette di controllare l'accesso degli utenti ai canali locali nei quali Advanced DLP ispeziona il contenuto dei dati trasferiti. Tuttavia, Controllo dispositivo mantiene il controllo sui seguenti tipi di dispositivo, se configurati per l'accesso di sola lettura o per l'accesso negato:
  - Rimovibile
  - Rimovibile crittografato
  - Unità mappata

  Ad esempio, se Controllo dispositivo e Advanced DLP sono entrambi abilitati in un singolo piano di protezione o in due piani che proteggono lo stesso workload, e se l'accesso di sola lettura è configurato per i dispositivi USB in Controllo dispositivo, l'accesso di sola lettura viene applicato a tutti i dispositivi USB ad eccezione di quelli nell'elenco degli elementi consentiti, indipendentemente dalle impostazioni di accesso del modulo Advanced DLP. Se l'impostazione predefinita Abilita accesso è configurata in Controllo dispositivo, viene applicata l'impostazione di accesso in Advanced DLP.
- L'accesso utente ai seguenti canali e periferiche locali nell'elenco degli elementi consentiti è applicato da Controllo dispositivo:
  - Unità ottiche
  - Unità floppy
  - Dispositivi mobile connessi tramite MTP
  - Schede Bluetooth
  - Appunti di Windows
  - Acquisizioni di screenshot
  - Dispositivi USB e tipi di dispositivo (ad eccezione dello storage rimovibile e crittografato)

Per creare un piano di protezione con Advanced DLP

1. Passare a **Gestione** > **Piani di protezione**.
2. Fare clic su **Crea piano**.
3. Espandere la sezione **Prevenzione della perdita di dati** e fare clic sulla riga **Modalità**.
   Viene visualizzata la finestra di dialogo **Modalità**.
   - Per avviare la creazione o il rinnovo di una policy di flusso dei dati, selezionare **Modalità di osservazione** e quindi selezionare come elaborare i trasferimenti dei dati:

Opzione	Descrizione
Consenti tutto	Tutti i trasferimenti di dati sensibili dai workload degli utenti vengono considerati necessari per i processi aziendali e sicuri. Viene creata una nuova regola ogni volta che viene individuato un flusso dei dati che non corrisponde a una regola già definita

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
	nella policy.
Giustifica tutto	Tutti i trasferimenti dei dati sensibili dai workload degli utenti vengono considerati necessari per i processi aziendali, ma a rischio. Pertanto, per ogni trasferimento dei dati sensibili intercettato verso qualsiasi destinatario o destinazione, interna ed esterna all'organizzazione, che non corrisponde a una regola di flusso dei dati precedentemente creata, l'utente deve inserire una giustificazione aziendale temporanea. Una volta inviata la giustificazione, nella policy di flusso dei dati verrà creata una nuova regola per il flusso dei dati.
Mista	La logica Consenti tutto viene applicata a tutti i trasferimenti dei dati sensibili interni, mentre la logica Giustifica tutto viene applicata a tutti i trasferimenti dei dati sensibili esterni. Per una definizione di destinazioni interne, vedere "Rilevamento automatico della destinazione" (pag. 900)

Attenzione!

- Selezionare **Modalità di osservazione** solo se non è già stata creata una policy di flusso dei dati o se si sta rinnovando la policy. Prima di avviare il rinnovo della policy, vedere "Rinnovo della policy di flusso dei dati" (pag. 894).
- In modalità di osservazione non si avrà alcuna prevenzione della perdita di dati. Vedere Modalità di osservazione nella Guida ai concetti di base.

- Per applicare la policy di flusso dei dati esistente, selezionare **Modalità di applicazione**, e quindi selezionare la rigidità con cui applicare le regole della policy:

Opzione	Descrizione
Applicazione rigida	La policy di flusso dei dati viene applicata così come è non sarà ampliata con nuove regole permissive quando vengono rilevati flussi di dati sensibili mai osservati prima. Vedere Applicazione rigida nella Guida ai concetti di base.
Applicazione adattiva (Applicazione con apprendimento)	La policy applicata continua l'adattamento automatico alle operazioni aziendali che non sono state eseguite durante il periodo di osservazione, o alle modifiche apportate ai processi aziendali. Questa modalità consente l'espansione della policy di flusso dei dati applicata in base ai nuovi flussi dei dati appresi con l'individuazione nei workload. Vedere Applicazione adattiva nella Guida ai concetti di base.

Importante

Prima di trasferire una policy aziendale o di unità dalla modalità di osservazione a quella di applicazione, è fondamentale modificare le regole predefinite per ogni categoria di dati sensibili impostandole dalla condizione permissiva alla condizione proibitiva. Le regole predefinite sono contrassegnate con un asterisco (*) nella vista **Policy di flusso dei dati**. Nella Guida ai concetti di base sono reperibili più informazioni sui tipi di regole delle policy.

© Acronis International GmbH, 2003-2024

4. Fare clic su **Fine** per chiudere la finestra di dialogo Modalità.
5. (Facoltativo) Per configurare il riconoscimento ottico dei caratteri, gli elenchi degli elementi consentiti e altre opzioni di protezione, fare clic su **Impostazioni avanzate**.
   Per informazioni sulle opzioni disponibili, vedere "Impostazioni avanzate" (pag. 899).
6. Salvare il piano di protezione e applicarlo ai workload da proteggere.

Impostazioni avanzate

È possibile utilizzare le impostazioni avanzate nei piani di protezione con Advanced Data Loss Prevention per migliorare la qualità dell'ispezione del contenuto dei dati nei canali controllati dalla funzionalità. È anche possibile escludere da qualsiasi controllo preventivo i trasferimenti dei dati verso i tipi di dispositivi periferici inclusi nell'elenco degli elementi consentiti, le categorie di comunicazione di rete, gli host di destinazione e i trasferimenti dei dati avviati da applicazioni incluse nell'elenco degli elementi consentiti. Sono configurabili le impostazioni avanzate indicate di seguito:

- **Riconoscimento ottico dei caratteri**
  Questa impostazione attiva o disattiva il riconoscimento ottico dei caratteri (Optical Character Recognition, OCR) per estrarre parti di testo in 31 lingue da sottoporre a successiva ispezione, dai file di grafica e immagini in documenti, messaggi, scansioni, screenshot e altri oggetti.
- **Trasferimento di dati protetti da password**
  Non è possibile ispezionare i contenuti di archivi e documenti protetti da password. Con questa impostazione, Advanced DLP consente all'amministratore di selezionare se i trasferimenti in uscita dei dati protetti da password possono essere consentiti o devono essere bloccati.
- **Prevenzione del trasferimento dei dati per errore**
  A volte durante l'attività dell'agente DLP l'analisi del contenuto in corso di invio potrebbe non riuscire, o potrebbe verificarsi un altro errore di controllo. Se questa opzione è abilitata, il trasferimento verrà bloccato. Se questa opzione è disabilitata, il trasferimento verrà consentito malgrado l'errore.
- **Elenco degli elementi consentiti per tipi di dispositivo e comunicazioni di rete**
  Sono consentiti i trasferimenti dei dati verso i tipi di dispositivi periferici e le comunicazioni di rete specificati in questo elenco, indipendentemente dalla sensibilità dei dati e dalla policy di flusso dei dati applicata.

  Attenzione!
  Questa opzione è utilizzata nel caso in cui si verificano problemi con un tipo di dispositivo o protocollo specifico. Non abilitarla se non su consiglio di un tecnico del supporto.

- **Elenco degli elementi consentiti per host remoti**
  Sono consentiti i trasferimenti dei dati verso gli host specificati in questo elenco, indipendentemente dalla sensibilità dei dati e dalla policy di flusso dei dati applicata.
- **Elenco degli elementi consentiti per applicazioni**
  Sono consentiti i trasferimenti dei dati eseguiti dalle applicazioni specificate in questo elenco, indipendentemente dalla sensibilità dei dati e dalla policy di flusso dei dati applicata.

© Acronis International GmbH, 2003-2024

L'indicatore **Livello di sicurezza** delle impostazioni avanzate visualizzato in **Crea piano di protezione** e nella vista "Dettagli" di un piano di protezione segnala il livello in base alla logica seguente:

- **Di base** indica che nessuna impostazione avanzata è attivata.
- **Moderato** indica che una o più impostazioni sono attivate, ma che non è attivata la combinazione di **OCR**, **Trasferimento di dati protetti da password** e **Prevenzione del trasferimento dei dati per errore**.
- **Rigido** indica che la combinazione di **OCR**, **Trasferimento di dati protetti da password** e **Prevenzione del trasferimento dei dati per errore** è attivata.

Rilevamento automatico della destinazione

Nella modalità di Osservazione mista, Advanced Data Loss Prevention applica regole diverse a seconda del fatto che la destinazione del trasferimento dei dati rilevato sia interna o esterna. La logica per determinare una destinazione come interna è descritta di seguito. Tutte le altre destinazioni sono considerate esterne.

Per ogni trasferimento dei dati intercettato, Advanced Data Loss Prevention rileva automaticamente se il server HTTP, FTP o SMB di destinazione è interno inviando una richiesta DNS e confrontando i nomi FQDN del sistema nel quale viene eseguito l'agente di prevenzione della perdita di dati e del server remoto. Se la richiesta DNS ha esito negativo, Advanced DLP controlla se il workload protetto e il server remoto sono sulla stessa rete. I server che hanno lo stesso nome di dominio o che si trovano nella stessa rete secondaria del sistema in cui viene eseguito l'agente DLP sono considerati interni.

Per le comunicazioni e-mail, Advanced DLP considera come trasferimenti interni tutte le e-mail inviate da un indirizzo e-mail aziendale tramite il server di posta aziendale se il destinatario dell'e-mail si trova nello stesso dominio del mittente dell'e-mail e se il nome del server di posta del destinatario è lo stesso.

Le e-mail non aziendali sono considerate comunicazioni esterne, a meno che non sia noto l'account del destinatario. Gli indirizzi e-mail noti vengono aggiornati quando Data Loss Prevention monitora l'attività dell'utente nella rete e aggiorna il database sul backend con i dati degli indirizzi e-mail associati all'utente.

Le comunicazioni tramite sistemi di messaggistica sono considerate comunicazioni esterne, a meno che non sia noto l'account del destinatario. Gli account noti vengono aggiornati quando Data Loss Prevention monitora l'attività dell'utente nella rete e aggiorna il database sul backend con i dati degli account associati all'utente.

Definizioni di dati sensibili

Questo argomento descrive la logica di identificazione dei dati sensibili durante l'analisi del contenuto.

© Acronis International GmbH, 2003-2024

Per ridurre il numero di falsi positivi, le corrispondenze identiche sono conteggiate come una sola corrispondenza per tutti i gruppi delle espressioni logiche descritte.

Importante
Le espressioni logiche utilizzate per l'identificazione dei contenuti sono fornite solo a scopo informativo e non descrivono completamente la soluzione.

Informazioni sanitarie protette (PHI)

Lingue supportate

- Inglese (Stati Uniti), Inglese (Regno Unito), Inglese internazionale
- Finlandese
- Italiano
- Francese
- Polacco
- Russo
- Ungherese
- Norvegese
- Spagnolo

Dati considerati Informazioni sanitarie protette (PHI)

I seguenti dati sono considerati informazioni sanitarie protette.

- Nomi e cognomi
- Indirizzo (via, città, isolato, provincia, codice postale, e loro equivalenti)
- Numeri di telefono
- Indirizzi e-mail
- Numeri della previdenza sociale
- Numeri di beneficiari di piani sanitari
- Numeri di conto bancario
- URL
- Numeri di indirizzi IP
- Codici ICD-10-CM
- ICD-10-PCS-and-GEMs
- HIPAA
- Altri codici sanitari
- Numeri della carta di credito

© Acronis International GmbH, 2003-2024

Espressioni logiche utilizzate per l'individuazione di contenuti

L'espressione logica è formata dalle stringhe seguenti unite dall'operatore logico OR. L'operatore OR è utilizzato per unire diversi gruppi di dati dell'elenco precedente se l'operatore AND non è esplicitato specificamente. I numeri tra parentesi rappresentano il numero di istanze rilevate che restituiscono un risultato di rilevamento positivo.

- **Numeri della previdenza sociale** (5)
- (Nomi e cognomi (3) OR Indirizzo (3) OR Numeri di telefono (3) OR Indirizzo e-mail (3) OR Numeri di conto bancario (3) OR Numeri di carta di credito (3)) AND (Numeri della previdenza sociale (3) OR Numeri di beneficiari di piani sanitari (3) * OR Codici ICD-10-CM (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR * Altri codici sanitari (3))

Informazioni che consentono l'identificazione personale dell'utente (PII)

Lingue supportate

- Inglese (Stati Uniti), Inglese (Regno Unito), Inglese internazionale
- Bulgaro
- Cinese
- Ceco
- Danese
- Olandese
- Finlandese
- Francese
- Tedesco
- Ungherese
- Indonesiano
- Italiano
- Coreano
- Malay
- Norvegese
- Polacco
- Portoghese (Brasile)
- Portoghese (Portogallo)
- Rumeno
- Russo
- Serbo

© Acronis International GmbH, 2003-2024

- Singapore
- Spagnolo
- Svedese
- Taiwan
- Turco
- Tailandese
- Giapponese

Dati considerati Informazioni che consentono l'identificazione personale dell'utente (PII)

- Nomi e cognomi
- Indirizzo (via, città, provincia, codice postale)
- Numeri di conto bancario
- Numeri di identificazione personale e fiscale
- Numeri di passaporto
- Numeri della previdenza sociale
- Numeri di telefono
- Numeri di targa
- Numeri della patente di guida
- Numeri di identificazione e numeri di serie
- Indirizzi IP
- Indirizzi e-mail
- Numeri della carta di credito

Espressioni logiche utilizzate per l'individuazione di contenuti

Espressione logica per tutte le lingue supportate ad eccezione del giapponese

L'espressione logica è formata dalle stringhe seguenti unite dall'operatore logico OR oppure AND. I numeri tra parentesi rappresentano il numero di istanze rilevate che restituiscono un risultato di rilevamento positivo.

- Numeri di identificazione personale e fiscale (5)
- Nomi e cognomi (3) AND **(**Numero della carta di credito (3) OR Numero della previdenza sociale (3) OR Numero di conto bancario (3) OR Numeri di identificazione personale e fiscale (3) OR Numeri della patente di guida (3) OR Numeri di passaporto (3) OR Numeri della previdenza sociale (3) OR Indirizzi IP (3) OR Numeri di targa (3) OR Numeri di identificazione e numeri di serie**)**

© Acronis International GmbH, 2003-2024

- Numeri di telefono (3) AND **(**Numero della carta di credito (3) OR Numero della previdenza sociale (3) OR Numero di conto bancario (3) OR Indirizzo (3) OR Numeri di identificazione personale e fiscale (3) OR Numeri della patente di guida (3) OR Numeri di passaporto (3) OR Numeri della previdenza sociale (3) OR Numeri di targa (3) OR Numeri di identificazione e numeri di serie (3)**)**
- **(**Nomi e cognomi (30) OR Indirizzo (30)**)** AND **(**Indirizzi e-mail (30) OR Numeri di telefono (30) OR Indirizzi IP (30)**)**
- Indirizzi e-mail (3) AND **(**Numero della carta di credito (3) OR Numero della previdenza sociale (3) OR Numero di conto bancario (3) OR Numeri di identificazione personale e fiscale (3) OR Numeri della patente di guida (3) OR Numeri di passaporto (3) OR Numeri della previdenza sociale (3) OR Numeri di targa (3) OR Numeri di identificazione e numeri di serie (3)**)**
- Indirizzo e-mail (30) AND **(**Indirizzo (30) OR Numeri di telefono (30)**)**
- Nomi e cognomi (30) AND Indirizzo (30)
- Numeri di telefono (30) AND Indirizzo (30)
- Nomi e cognomi (3) AND Numeri di conto bancario (3)
- Numeri di telefono (3) AND **(**Numero della carta di credito (3) OR Numero di conto bancario (3) OR Numeri della previdenza sociale (3) OR Numeri di identificazione personale e fiscale (3) OR Numeri della patente di guida (3) OR Numeri di passaporto (3)**)**

Espressioni logiche per il giapponese

Nota
Il rilevatore di contenuti conteggia solo le corrispondenze univoche.

L'espressione logica è formata dalle stringhe seguenti unite dall'operatore logico OR. L'operatore OR viene utilizzato per unire gruppi differenti se l'operatore logico AND non è specificamente esplicitato.

- Numeri della previdenza sociale (5)
- Nomi e cognomi (3) AND **(**Numero della carta di credito (3) OR Numero del conto bancario (3) OR Numeri della patente di guida (3) OR Numeri di passaporto (3) OR Numeri della previdenza sociale (3)**)**
- Nomi e cognomi (30) AND **(**Indirizzi e-mail (30) OR Numeri di telefono (30) OR Indirizzi IP (30) OR Indirizzo (30)**)**
- Indirizzo (3) AND **(**Numero della carta di credito (3) OR Numero del conto bancario (3) OR Numeri della patente di guida (3) OR Numeri di passaporto (3) OR Numeri della previdenza sociale (3)**)**
- Indirizzo e-mail (3) AND **(**Numero della carta di credito (3) OR Numero del conto bancario (3) OR Numeri della previdenza sociale (3) OR Numeri della patente di guida (3)**)**
- Indirizzo (5) AND **(**Indirizzo e-mail (5) OR Nomi e cognomi (5) OR Numeri di telefono (5) OR Indirizzi IP (5)**)**
- Nomi e cognomi (3) AND Numeri di conto bancario (3)
- Numeri di telefono (3) AND **(**Numero della carta di credito (3) OR Numero del conto bancario (3) OR Indirizzo (3) OR Numeri della previdenza sociale (3) OR Numeri della patente di guida (3)**)**

© Acronis International GmbH, 2003-2024

Dati soggetti allo standard Payment Card Industry Data Security Standard (PCI DSS)

Lingue supportate

Questo gruppo di dati riservati è indipendente dalla lingua. I dati PCI DSS sono in inglese in tutti i paesi.

Dati considerati PCI DSS

- Dati del titolare della carta
  - Numero di account principale (PAN)
  - Nome del titolare della carta
  - Data di scadenza
  - Codice del servizio
- Dati sensibili di autenticazione
  - Traccia dati completa (dati della banda magnetica o equivalenti su chip)
  - CAV2/CVC2/CVV2/CID
  - PIN/Blocchi PIN

Espressioni logiche utilizzate per l'individuazione di contenuti

L'espressione logica è formata dalle stringhe seguenti unite dall'operatore logico OR. I numeri tra parentesi rappresentano il numero di istanze rilevate che restituiscono un risultato di rilevamento positivo.

- Numero della carta di credito (5)
- Numero della carta di credito (3) AND (Nome americano (Ex) (3) OR Nome americano (3) OR Parole chiave PCI DSS (3) OR Data (mese/anno) (3))
- Dump della carta di credito (5)

Contrassegnato come Riservato

I dati contrassegnati come riservati vengono identificati tramite gruppi di parole chiave.

La condizione di corrispondenza è ponderata e ogni parola ha peso == 1. Il rilevamento del contenuto viene considerato positivo quando la corrispondenza ha peso > 3.

Lingue supportate

- Inglese
- Bulgaro
- Cinese semplificato

© Acronis International GmbH, 2003-2024

- Cinese tradizionale
- Ceco
- Danese
- Olandese
- Finlandese
- Francese
- Tedesco
- Ungherese
- Indonesiano
- Italiano
- Giapponese
- Coreano
- Malay
- Norvegese
- Polacco
- Portoghese - Brasile
- Portoghese - Portogallo
- Russo
- Serbo
- Spagnolo
- Svedese
- Turco

Gruppi di parole chiave

Il gruppo di parole chiave per ogni lingua contiene gli equivalenti specifici per il paese delle parole chiave seguenti, utilizzate per la lingua inglese (senza distinzione tra maiuscole e minuscole).

- riservato
- divulgazione interna
- divulgazione non consentita
- non divulgare
- non per il pubblico
- divulgazione all'esterno non consentita
- solo per uso interno
- documentazione altamente qualificata

© Acronis International GmbH, 2003-2024

- privato
- informazioni privilegiate
- solo per uso interno
- solo per uso ufficiale

Eventi di prevenzione della perdita di dati

La funzionalità Advanced Data Loss Prevention genera gli eventi nella vista Eventi DLP come indicato di seguito.

- In modalità di osservazione, gli eventi vengono generati per tutti i trasferimenti dei dati giustificati.
- In modalità di applicazione, gli eventi vengono generati in base all'azione **Scrivi nel registro** configurata per ogni regola della policy attivata.

Per visualizzare gli eventi per una regola della policy di flusso dei dati

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Protezione** > **Policy di flusso dei dati**.
3. Individuare la regola per la quale visualizzare gli eventi e fare clic sull'icona a tre punti alla fine della riga della regola.
4. Selezionare **Visualizza eventi**.

Per visualizzare i dettagli su un evento nella vista Eventi DLP

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Protezione** > **Eventi DLP**.
3. Fare clic su un evento nell'elenco per visualizzare più informazioni.
   Il riquadro dei dettagli dell'evento si espande a destra.
4. Scorrere verso l'alto e verso il basso il riquadro dei dettagli dell'evento per visualizzare le informazioni disponibili.
   Le informazioni visualizzate nel riquadro dipendono dal tipo di regola e dalle impostazioni della regola che hanno attivato l'evento.

Per filtrare gli eventi nell'elenco degli eventi DLP

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Protezione** > **Eventi DLP**.
3. In alto a sinistra, fare clic su **Filtro**.
4. Selezionare la categoria di riservatezza, il workload, il tipo di azione, l'utente e il canale dai menu a discesa.

© Acronis International GmbH, 2003-2024

I menu consentono di selezionare più di una voce. La funzionalità di filtro applica l'operatore logico OR tra voci dello stesso menu, mentre l'operatore logico AND viene utilizzato tra voci di menu differenti.

Se, ad esempio, si selezionano le categorie di riservatezza **PHI** e **PII**, verranno restituiti tutti gli eventi che contengono PHI o PII o entrambi. Se si seleziona la categoria di riservatezza **PHI** e l'azione **Accesso in scrittura**, i risultati filtrati mostreranno soltanto gli eventi che corrispondono a entrambe le categorie.

5. Fare clic su **Applica**.
6. Per visualizzare di nuovo tutti gli eventi fare clic su **Filtro**, quindi su **Ripristina allo stato predefinito** e infine su **Applica**.

Per cercare gli eventi nell'elenco degli eventi DLP

1. Ripetere i passaggi 1-2 della precedente procedura.
2. Nell'elenco a discesa a destra della voce Filtro, selezionare la categoria nella quale effettuare la ricerca: **Mittente**, **Destinazione**, **Processo**, **Oggetto del messaggio** o **Motivo**.
3. Nella casella di testo inserire la frase da cercare e confermare premendo il tasto Invio. Nell'elenco vengono visualizzati soltanto gli eventi che corrispondono alla frase inserita.
4. Per ripristinare l'elenco degli eventi, fare clic sul segno **X** nella casella del testo di ricerca e premere Invio.

Per visualizzare l'elenco degli eventi relativi a regole specifiche nella policy di flusso dei dati

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Protezione** > **Policy di flusso dei dati**.
3. Selezionare la casella di controllo accanto al nome della regola della policy cui si è interessati. Se è necessario selezionare più policy.
4. Fare clic su **Visualizza eventi**.
   La vista passa a **Protezione** > **Eventi DLP** e gli eventi correlati alle regole della policy selezionata vengono visualizzati nell'elenco.

Widget di Advanced Data Loss Prevention nella dashboard Panoramica

La dashboard **Panoramica** fornisce una serie di widget personalizzabili che offrono un'anteprima delle operazioni relative al servizio Cyber Protection, inclusa Advanced Data loss Prevention. I seguenti widget di Advanced Data Loss Prevention si trovano nella dashboard **Panoramica** in **Monitoraggio**.

- **Trasferimenti dei dati sensibili** - Mostra il numero totale di operazioni di trasferimento dei dati sensibili verso destinatari esterni e interni. Il grafico è suddiviso per tipo di autorizzazione: consentito, giustificato o bloccato. È possibile personalizzare questo widget selezionando l'intervallo di tempo desiderato (1 giorno, 7 giorni, 30 giorni, questo mese).

© Acronis International GmbH, 2003-2024

- **Categorie di dati sensibili in uscita** - Mostra il numero totale di operazioni di trasferimento dei dati sensibili verso destinatari esterni. Il grafico è suddiviso per categorie di dati sensibili: Informazioni sanitarie protette (PHI), Informazioni che consentono l'identificazione personale dell'utente (PII), PCI DSS e Contrassegnato come Riservato (Riservato).
- **Principali mittenti di dati sensibili in uscita** - Mostra il numero totale dei trasferimenti dei dati sensibili dall'organizzazione a destinatari esterni e un elenco dei 5 utenti con il maggior numero di trasferimenti (oltre al conteggio di tali trasferimenti). Questa statistica include i trasferimenti consentiti e giustificati. È possibile personalizzare questo widget selezionando l'intervallo di tempo desiderato (1 giorno, 7 giorni, 30 giorni, questo mese).
- **Principali mittenti di trasferimenti dei dati sensibili bloccati** - Mostra il numero totale dei trasferimenti dei dati sensibili bloccati e un elenco dei 5 utenti con il maggior numero di trasferimenti tentati (oltre al conteggio di tali trasferimenti). È possibile personalizzare questo widget selezionando l'intervallo di tempo desiderato (1 giorno, 7 giorni, 30 giorni, questo mese).
- **Eventi DLP recenti** - Mostra i dettagli dei recenti eventi di prevenzione della perdita di dati per l'intervallo di tempo selezionato. È possibile personalizzare il widget utilizzando le opzioni seguenti:
  - **Intervallo (data di pubblicazione)** (1 giorno, 7 giorni, 30 giorni, questo mese).
  - Nome del **workload**
  - **Stato dell'operazione** (consentita, giustificata o bloccata)
  - **Riservatezza** (PHI, PII, Riservato, PCI DSS)
  - **Tipo di destinazione** (esterna, interna)
  - **Raggruppamento** (workload, utente, canale, tipo di destinazione)

I widget vengono aggiornati ogni cinque minuti. I widget presentano elementi cliccabili che consentono di indagare e risolvere i problemi. È possibile scaricare lo stato corrente del pannello di controllo in formato .pdf e/o .xlsx, oppure inviarlo tramite e-mail.

Categorie di riservatezza personalizzate

Le categorie personalizzate inerenti i dati sensibili possono aiutare un'organizzazione a proteggere la proprietà intellettuale e dati riservati specifici della stessa, ampliando il catalogo integrato di Advanced DLP di definizioni di contenuti correlati alle normative in materia di conformità.

Per creare una categoria di riservatezza personalizzata

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Protezione** > **Prevenzione della perdita di dati** > **Classificatori dati**.
3. Selezionare **Categoria di riservatezza**.
4. Viene visualizzato un elenco di dati potenzialmente sensibili, sia integrati (ad esempio Informazioni sanitarie protette o Informazioni che consentono l'identificazione personale dell'utente) e di dati personalizzati.
5. Fare clic su **Crea categoria di riservatezza** nell'angolo in alto a destra della finestra.

© Acronis International GmbH, 2003-2024

6. Inserire il nome della categoria nella finestra successiva.
7. Per impostazione predefinita, le nuove categorie di riservatezza personalizzate sono sempre disabilitate. È possibile abilitarle dopo aver configurato tutti i rispettivi parametri.
8. Dopo aver creato una nuova categoria di riservatezza, è necessario impostare i rispettivi rilevatori di contenuti. Fare clic su una freccia per espandere i contenuti della nuova categoria di riservatezza e selezionare **Aggiungi rilevatore di contenuti**.
9. Nella finestra successiva è possibile utilizzare uno qualsiasi dei rilevatori di contenuto esistenti (facendo clic sul segno di spunta accanto al nome e quindi su **Aggiungi** nell'angolo in basso a destra) oppure definirne uno nuovo.
10. Invece di creare da zero una nuova categoria di riservatezza, è possibile riutilizzarne una esistente (sia integrata sia personalizzata) clonandola e adeguandone i parametri.
    - Per clonare una categoria di riservatezza esistente, fare clic sul segno di spunta accanto al nome e quindi selezionare **Clona** dal menu a discesa Azione (indicato dai puntini di sospensione) nell'angolo in alto a sinistra. È possibile selezionare più elementi alla volta per clonare più di una categoria di riservatezza.
    - Nella finestra successiva è possibile selezionare quali parametri della categoria esistente mantenere, facendo clic sul segno di spunta accanto a ciascun parametro.

Nota
La copia delle categorie di riservatezza integrate all'interno di un tenant consente di creare una nuova categoria che presenta gli stessi rilevatori, che diventeranno personalizzati una volta copiati

Per creare un nuovo rilevatore di contenuti

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Protezione** > **Prevenzione della perdita di dati** > **Classificatori dati**.
3. Selezionare **Rilevatori di contenuti**.
4. Viene visualizzato un elenco di rilevatori di contenuti, sia integrati che personalizzati.
5. Fare clic su **Crea rilevatore di contenuti** nell'angolo in alto a destra della finestra.
6. Viene visualizzato un menu a discesa nel quale è possibile selezionare il tipo di rilevatore da creare; in questa fase è disponibile solo il rilevatore di contenuti **Tipo di file**; altri rilevatori verranno aggiunti nei futuri aggiornamenti.
7. Nella finestra successiva è possibile configurare il rilevatore di contenuti.

Tipo di rilevatore di contenuti	Descrizione
Rilevatore di contenuti: tipi di file	a. Sono presenti due elenchi: **Tipi di file supportati** e **Tipi di file selezionati**. Facendo clic sull'icona "+" a destra del tipo di file supportato, tale file viene aggiunto all'elenco Tipi di file selezionati. È anche possibile selezionare più tipi di file supportati facendo clic sui segni di spunta accanto ai rispettivi nomi e

© Acronis International GmbH, 2003-2024

Tipo di rilevatore di contenuti	Descrizione
	utilizzando il pulsante **Aggiungi selezionati** nell'angolo in alto a destra. b. Per rimuovere un tipo di file dall'elenco Tipi di file selezionati, fare clic sull'icona del cestino a destra del rispettivo nome. È possibile rimuovere più tipi di file in una sola volta utilizzando i segni di spunta e il pulsante **Rimuovi selezionati**.
Rilevatore di contenuti: parole chiave	a. Quando si crea un nuovo rilevatore di contenuti per parole chiave, sarà necessario importare le parole chiave da un file. Una volta completata correttamente l'importazione, è possibile unire le nuove parole chiave con l'elenco di quelle esistenti, o sostituire quelle esistenti con parole chiave importate. b. È anche possibile indicare se il rilevatore di contenuti deve individuare la corrispondenza con tutte le parole chiave dell'elenco, con qualsiasi parola chiave dell'elenco o con un numero personalizzato di parole chiave.

8. Invece di creare da zero un nuovo rilevatore di contenuti, è possibile riutilizzarne uno esistente (sia integrato sia personalizzato) clonandolo e adeguandone i parametri.
   - Per clonare un rilevatore di contenuti esistente, fare clic sul segno di spunta accanto al nome e quindi selezionare **Clona** dal menu a discesa Azione (indicato dai puntini di sospensione) nell'angolo in alto a sinistra. È possibile selezionare più elementi alla volta per clonare più di un rilevatore di contenuti.

Nota
Dopo essere stato copiato, un rilevatore integrato diventa personalizzato.

Mappa dell'organizzazione

Nota
Questa funzionalità è accessibile solo agli utenti con il ruolo di Amministratore società.

La mappa dell'organizzazione è un database che contiene i dati degli utenti e di tutti i relativi account utilizzati per il trasferimento dei dati tramite messaggistica istantanea, e-mail o qualsiasi altro sistema, che sono stati intercettati da Advanced DLP.

La mappa dell'organizzazione permette di creare e gestire i gruppi di utenti in Advanced DLP e di gestire gli utenti e gli account associati agli utenti in Advanced DLP. I gruppi di utenti possono quindi essere utilizzati per la gestione delle policy DLP basata su gruppi.

Per individuare la mappa dell'organizzazione

- Nella console di Cyber Protect Cloud, passare a **Protezione** > **Prevenzione della perdita di dati** > **Mappa dell'organizzazione**.

© Acronis International GmbH, 2003-2024

Come funziona?

Nota
La mappa dell'organizzazione viene compilata mentre il modulo Advanced DLP è in modalità Osservazione.

Per ogni trasferimento dei dati intercettato dall'agente DLP, gli attributi seguenti vengono raccolti nel back end.

Attributo	Descrizione	Etichetta nell'interfaccia utente
Unità organizzativa	Gruppo creato manualmente. L'Unità organizzativa può contenere una o più Unità organizzative nidificate.	Nome del gruppo, come definito
ID di sicurezza	Identificatore di sicurezza univoco.	Sulla pagina dei dettagli dell'utente > **SID**
	Un nome visualizzato intuitivo derivato dai nomi account per l'utente. Questo nome non è sempre disponibile nella mappa dell'organizzazione.	**Nome**
PC\NomeUtente	Nome dell'utente dell'endpoint (workload). Un nome utente può essere assegnato a una sola Unità organizzativa.	**Nome utente**
Dispositivo (Workload)	Nome dell'endpoint (workload).	**Workload**
Account	Account utilizzati da un utente per la comunicazione tramite messaggistica istantanea ed e-mail, intercettati dall'agente DLP. Ad esempio, se l'agente rileva che il nome utente 'PC\John' usa john@gmail.com per inviare un'e-mail, questo account viene collegato al nome utente PC\John.	**Account**

Nella mappa dell'organizzazione è possibile visualizzare e cercare account, utenti e gruppi e creare, modificare ed eliminare gruppi.

Per cercare account specifici

Nell'ambito dell'indagine su un problema, gli amministratori potrebbero dover trovare il proprietario di un account specifico coinvolto in una possibile violazione dei dati.

1. Nella console di Cyber Protect Cloud, passare a **Protezione** > **Prevenzione della perdita di dati** > **Mappa dell'organizzazione**.
2. Nella casella di testo **Cerca** sopra l'elenco degli utenti, digitare o incollare l'account.
   L'elenco viene filtrato durante la digitazione.

© Acronis International GmbH, 2003-2024

Per cercare un nome utente specifico

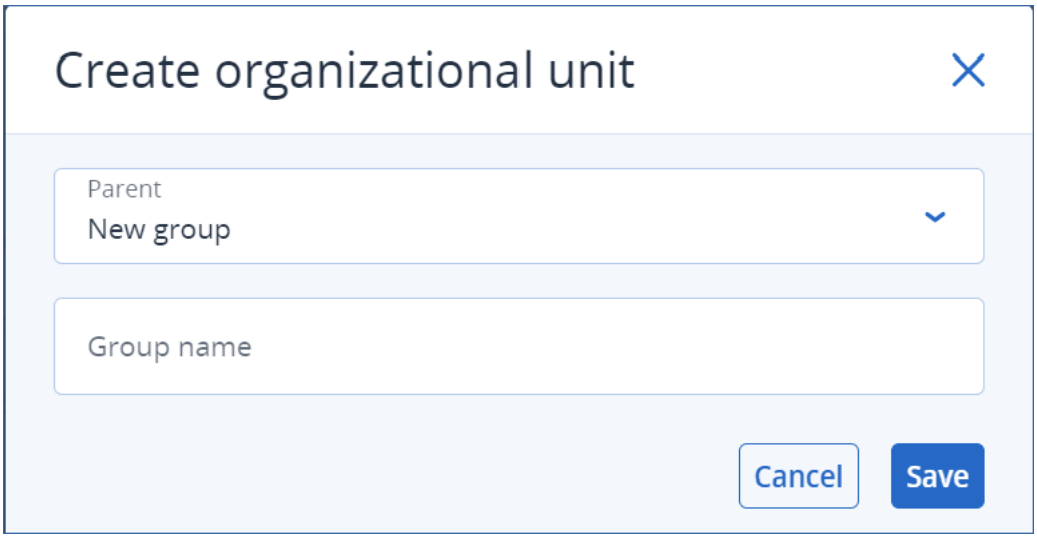
1. Nella console di Cyber Protect Cloud, passare a **Protezione** > **Prevenzione della perdita di dati** > **Mappa dell'organizzazione**.
2. Per eseguire una ricerca in un gruppo specifico, fare clic sul nome del gruppo nell'elenco.
3. Nella casella di testo **Cerca** sopra l'elenco degli utenti, digitare o incollare un nome utente. L'elenco viene filtrato durante la digitazione.

Per visualizzare gli account utilizzati da uno specifico nome utente

1. Individuare l'utente nell'elenco degli utenti.
2. Fare clic sui tre punti alla fine della riga dell'utente e selezionare **Visualizza**.
3. Nella finestra dei dettagli dell'utente, individuare la sezione **Account associati**.
4. È possibile aggiungere commenti nella casella di testo Descrizione.

Per creare un gruppo di utenti

1. Nella console di Cyber Protect Cloud, passare a **Protezione** > **Prevenzione della perdita di dati** > **Mappa dell'organizzazione**.
2. Nella sezione in basso a sinistra nell'elenco dei gruppi, fare clic su **Crea gruppo**. Viene visualizzata la finestra di dialogo Crea unità organizzativa.



3. Dal menu a discesa Padre, selezionare il contesto del nuovo gruppo.

Nota
Non sarà possibile modificare il padre in un secondo momento. Il gruppo resterà nidificato in questo contesto.

4. Inserire un nome per il gruppo e fare clic su **Salva**.

Per aggiungere un utente a un gruppo

1. Nella console di Cyber Protect Cloud, passare a **Protezione** > **Prevenzione della perdita di dati** > **Mappa dell'organizzazione**.

© Acronis International GmbH, 2003-2024

2. Nell'elenco degli utenti, individuare l'utente da aggiungere e selezionare la casella di controllo all'inizio della riga dell'utente.
   Sopra all'elenco degli utenti vengono visualizzati i pulsanti **Sposta selezionato** ed **Elimina selezionato**.

3. Fare clic su **Sposta selezionato**.
   Viene visualizzata la finestra di dialogo Sposta utente.
4. Selezionare un nuovo padre per l'utente selezionato e fare clic su **Salva**.

Nota
Un utente può far parte di un solo gruppo.

Per eliminare un account associato a un utente

1. Individuare l'utente nell'elenco degli utenti.
2. Fare clic sui tre punti alla fine della riga dell'utente e selezionare **Visualizza**.
3. Nella finestra dei dettagli dell'utente, individuare la sezione **Account associati**.
4. Trovare l'account da eliminare e fare clic sui tre punti accanto ad esso.
5. Dal menu a discesa, selezionare **Elimina**.

Per rinominare un gruppo di utenti

1. Nella console di Cyber Protect Cloud, passare a **Protezione** > **Prevenzione della perdita di dati** > **Mappa dell'organizzazione**.
2. Fare clic sui tre punti accanto al nome del gruppo e quindi su **Rinomina**.

Per eliminare un gruppo di utenti

1. Nella console di Cyber Protect Cloud, passare a **Protezione** > **Prevenzione della perdita di dati** > **Mappa dell'organizzazione**.
2. Fare clic sui tre punti accanto al nome del gruppo e quindi su **Elimina**.
   Tutti gli utenti del gruppo vengono spostati all'entità padre.

Problemi noti e limitazioni

- [DEVLOCK-4028] Non c'è controllo per le chat di gruppo nell'agente desktop di Zoom.
- [DEVLOCK-4016] Nome descrittivo e ID del mittente non acquisiti per GMX Web Mail e Web.de Mail in caso di creazione di una bozza.
- [DEVLOCK-4447] Non è presente alcuna finestra di dialogo Giustificazione per naver.com WebMail in caso di creazione di una bozza.
- [DEVLOCK-1033] DeviceLockDriver: potenziale controllo degli errori DRIVER_POWER_STATE_FAILURE causato da un deadlock durante l'elaborazione di IRP_MN_QUERY_DEVICE_RELATIONS.

© Acronis International GmbH, 2003-2024

Endpoint Detection and Response (EDR)

Nota
Questa funzionalità fa parte del pacchetto di protezione Advanced Security + EDR, che a sua volta è parte del servizio Cyber Protection. Tenere presente che l'aggiunta della funzionalità EDR a un piano di protezione può essere soggetta a costi aggiuntivi.

EDR rileva le attività sospette nel workload, inclusi gli attacchi passati inosservati. La funzionalità genera quindi i problemi, che forniscono una panoramica passo per passo di ogni attacco e aiutano a comprendere come si è verificato l'evento e come impedire che accada di nuovo. Grazie alla possibilità di interpretare in modo semplice ogni fase dell'attacco, il tempo dedicato all'indagine può ridursi a pochi minuti.

Perché Endpoint Detection and Response (EDR) è una soluzione necessaria

Nell'odierno panorama di minacce informatiche e attacchi dannosi in continua evoluzione, la prevenzione non garantisce più una protezione davvero totale. Alcuni attacchi riusciranno comunque a superare i livelli di difesa preventivi e a penetrare nella rete. Le soluzioni convenzionali non riescono a registrare questi eventi, lasciando ai criminali la piena libertà di permanere nell'ambiente per giorni, settimane o mesi.

Le soluzioni EDR esistenti sono un valido aiuto nel prevenire queste "infiltrazioni silenti" perché in breve tempo individuano e rimuovono gli attaccanti. Richiedono tuttavia un elevato livello di esperienza in sicurezza o la presenza di analisti dei centri operativi SOC; l'analisi dei problemi riscontrati può richiedere tempi molto lunghi.

La funzionalità Acronis Advanced Security + EDR supera queste limitazioni perché rileva gli attacchi passati inosservati e consente di comprendere come si è verificato l'evento e come impedire che accada di nuovo. Contribuisce inoltre a ridurre il tempo dedicato alle indagini sugli attacchi.

Di seguito i motivi che rendono indispensabile la funzionalità EDR:

- **Visibilità completa**. Comprendere cosa è successo e come, anche in merito agli attacchi passati inosservati. La funzionalità tiene traccia dell'evoluzione di ogni attacco, passo per passo, dal punto iniziale di accesso alla visualizzazione dei dati oggetto dell'attacco e/o esfiltrati, consentendo di comprendere velocemente l'ambito e l'impatto del problema. Per ulteriori informazioni, consultare "Come indagare sui problemi rilevati nella sequenza di attacco" (pag. 929).
- **Riduzione dei tempi di indagine**. EDR è in grado di ridurre i tempi di indagine sui problemi da ore a minuti. La funzionalità illustra in dettaglio ogni fase dell'attacco con un linguaggio chiaro e di facile comprensione, contribuendo a ridurre la necessità di esperti costosi o di personale aggiuntivo. Per ulteriori informazioni, consultare "Eseguire l'indagine sul problema" (pag. 928).

© Acronis International GmbH, 2003-2024

- **Controllo delle minacce note presenti nei workload**. È possibile avviare ricerche automatiche nei workload, per individuare la presenza di malware, vulnerabilità e altri tipi di eventi globali che possono interessare la protezione dati. Questi pericoli vengono denominati indicatori di compromissione, e si basano su dati relativi alle minacce emessi dai centri operativi di Cyber Protection (CPOC). Per ulteriori informazioni, consultare "Controllare la presenza di indicatori di compromissione di attacchi pubblicamente noti nei workload" (pag. 940).
- **Reazione più rapida ai problemi**. L'accesso a tutte le attività successive alla violazione e la suddivisione di ogni passaggio della sequenza di attacco consente di intraprendere numerose azioni di correzione su ogni punto attaccato. È possibile svolgere indagini avvalendosi del controllo remoto e dei backup forensi (questa funzionalità non è disponibile nella versione Accesso in anteprima), mettere in quarantena i workload e arrestare i processi malware. Infine, è possibile ripristinare l'operatività aziendale con Cyber Disaster Recovery Cloud Per ulteriori informazioni, consultare "Correzione dei problemi" (pag. 944).
- **Creazione di report attendibili sul profilo di sicurezza**. Abilitando la funzionalità EDR, si eliminano molte delle insicurezze e dei timori causati dal potenziale impatto che gli attacchi informatici possono avere sull'azienda. Le informazioni correlate al problema vengono archiviate per 180 giorni, consentendone l'utilizzo per le finalità di audit.

Caratteristiche

Endpoint Detection and Response (EDR) include le funzionalità seguenti:

- Ricezione di notifiche di avviso in caso di violazione
- Gestione dei problemi nella pagina Problemi
- Visualizzazione intuitiva della sequenza di attacco
- Consigli e raccomandazioni di correzione
- Verifica degli attacchi resi pubblici ai workload utilizzando i feed sulle minacce
- Dashboard con panoramica rapida
- Archiviazione degli eventi di sicurezza per 180 giorni

Ricezione di notifiche di avviso in caso di violazione

EDR fornisce notifiche di avviso ogni volta che registra un problema. Tali avvisi vengono evidenziati nel menu principale della console di Cyber Protect. È possibile indagare su un avviso facendo clic sul pulsante **Indagine sul problema**, che reindirizza l'utente alla schermata di indagine, anche detta sequenza della catena di attacco.

Per ulteriori informazioni, consultare "Analisi riepilogativa dei problemi" (pag. 920).

Gestione dei problemi nella pagina Problemi

EDR consente di gestire tutti i problemi registrati nella pagina Problemi, a cui è possibile accedere dal menu Protezione nella console di Cyber Protect. La pagina Problemi, a cui possono essere applicati i filtri necessari, consente di comprendere in modo semplificato e rapido lo stato attuale

© Acronis International GmbH, 2003-2024

del problema, con informazioni sulla gravità, sui workload interessati e sul livello di positività. Inoltre, è possibile aprire direttamente la sequenza di attacco e visualizzare le varie fasi dell'attacco nodo per nodo.

Per ulteriori informazioni sulla pagina Problemi, consultare "Analisi riepilogativa dei problemi" (pag. 920).

Visualizzazione intuitiva della sequenza di attacco

EDR fornisce una rappresentazione visiva di un attacco in un formato chiaro e facilmente leggibile. In questo modo, anche il personale non esperto in sicurezza può comprendere gli obiettivi e la gravità di qualsiasi attacco. Non è quindi necessario disporre dei servizi di un centro operativo di sicurezza (SOC) né di assumere esperti in sicurezza, perché EDR indica in dettaglio come si è verificato un attacco e offre anche informazioni su:

- In che modo l'attaccante si è infiltrato
- In che modo l'attaccante ha nascosto le proprie tracce
- Che danni ha causato
- In che modo l'attacco si è diffuso

Per ulteriori informazioni, consultare "Come indagare sui problemi rilevati nella sequenza di attacco" (pag. 929).

Consigli e raccomandazioni di correzione

EDR offre modalità chiare e facili per adottare i consigli dati per risolvere gli attacchi a un workload. Per risolvere rapidamente un attacco, fare clic sul pulsante **Correggi intero problema** per visualizzare e seguire i passaggi consigliati per ridurre al minimo le conseguenze dell'evento. I passaggi consentono di riprendere rapidamente il controllo e riavviare le operazioni in caso di attacco. Se, tuttavia, si desidera mettere in atto azioni di correzione più dettagliate, è possibile aprire ciascun nodo e applicare l'azione più adatta a ognuno.

Per ulteriori informazioni, consultare "Correzione dei problemi" (pag. 944).

Verifica degli attacchi resi pubblici ai workload utilizzando i feed sulle minacce

EDR prevede la capacità di esaminare gli attacchi noti esistenti nel feed sulle minacce a fronte dei workload. I feed sulle minacce vengono generati automaticamente in base ai dati sulle minacce ricevuti dai centri operativi di Cyber Protection (CPOC); EDR consente di verificare se una minaccia sta interessando il workload e di intraprendere quindi le azioni necessarie per neutralizzarla.

Per ulteriori informazioni, consultare "Controllare la presenza di indicatori di compromissione di attacchi pubblicamente noti nei workload" (pag. 940).

Dashboard con panoramica rapida

EDR offre una vasta gamma di statistiche, reperibili nella dashboard della console di Cyber Protect. Tali statistiche mostrano, tra gli altri dati:

© Acronis International GmbH, 2003-2024

- Lo stato attuale della minaccia, incluso il numero di problemi sui quali è necessario indagare.
- L'evoluzione degli attacchi in base alla loro gravità, e la presenza di possibili campagne di attacco.
- Il tasso di efficienza nella chiusura dei problemi.
- Le tattiche più utilizzate per attaccare i clienti.
- Lo stato della rete del workload, ovvero se il workload è isolato o connesso.

Archiviazione degli eventi di sicurezza per 180 giorni

EDR raccoglie gli eventi inerenti ai workload e alle applicazioni e li archivia per 180 giorni. Gli eventi con data precedente al periodo di 180 giorni vengono eliminati (l'eliminazione dell'evento si basa sull'età e non sullo spazio di storage). Tenere presente che se anche EDR viene disattivato, tutti gli eventi precedentemente raccolti relativi a un workload vengono conservati, e restano disponibili per eventuali indagini sul problema.

Requisiti software

Endpoint Detection and Response (EDR) supporta i sistemi operativi seguenti:

- Microsoft Windows 7 Service Pack 1 e versioni successive
- Microsoft Windows Server 2008 R2 e versioni successive

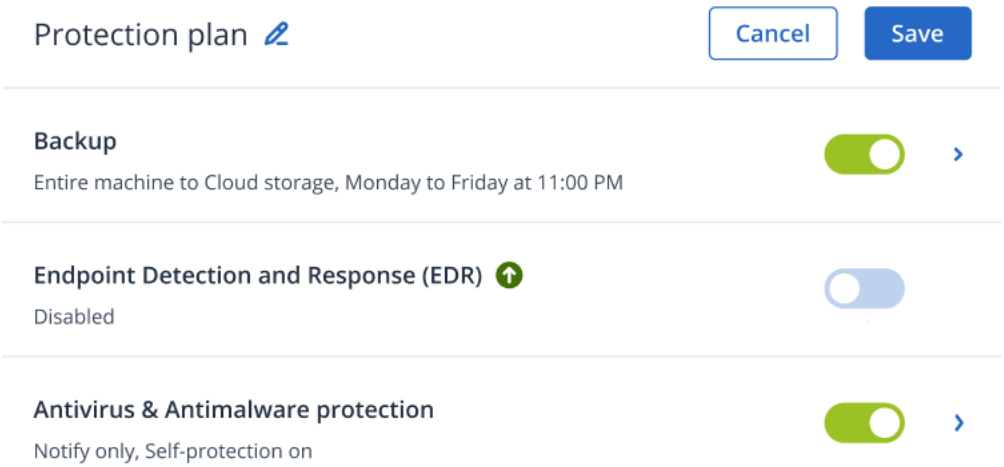
Abilitare la funzionalità Endpoint Detection and Response (EDR)

È possibile abilitare EDR in qualsiasi piano di protezione.

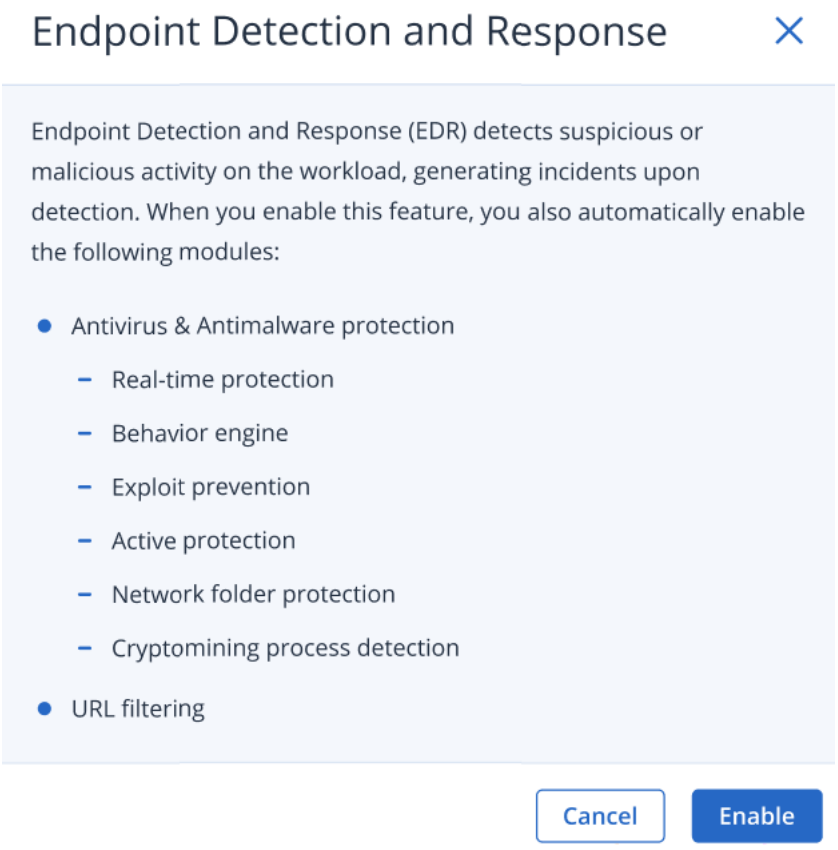
Per abilitare EDR

1. Nella console di Cyber Protect, passare a **Gestione > Piani di protezione**.
2. Selezionare il piano di protezione pertinente dall'elenco visualizzato e, nella barra laterale destra, fare clic su **Modifica**.
   In alternativa, è possibile creare un nuovo piano di protezione e procedere al passaggio successivo. Per ulteriori informazioni sul funzionamento dei piani di protezione, consultare "Piani e moduli di protezione" (pag. 217).
3. Nella barra laterale del piano di protezione, abilitare il modulo **Endpoint Detection and Response (EDR)** facendo clic sull'opzione accanto al nome del modulo.

© Acronis International GmbH, 2003-2024



4. Nella finestra di dialogo visualizzata, fare clic su **Abilita**. Tenere presente che quando EDR è abilitato, sono abilitati anche gli altri moduli di protezione indicati nella finestra di dialogo visualizzata.



Nota
Se uno qualsiasi dei moduli **Active Protection**, **Motore comportamentale**, **Prevenzione degli exploit** o **Filtro URL** sono impostati su **Off**, anche **Endpoint Detection and Response (EDR)** sarà impostata su **Off**.

© Acronis International GmbH, 2003-2024

5. Come mostrato di seguito, l'icona del pacchetto **Advanced Security + EDR** viene aggiunta all'elenco dei pacchetti di protezione per l'implementazione del piano di protezione, in base ai pacchetti aggiuntivi selezionati.

Come utilizzare la funzionalità Endpoint Detection and Response (EDR)

La funzionalità EDR permette di rilevare gli attacchi passati inosservati e aiuta a comprendere come si è verificato l'evento e come impedire che accada di nuovo. Grazie alla possibilità di interpretare in modo semplice ogni fase dell'attacco, il tempo dedicato all'indagine può ridursi a pochi minuti.

La tabella seguente illustra un flusso di lavoro generico di EDR. In primo luogo, ogni nuovo problema viene esaminato e prioritizzato, quindi si procede con l'indagine sulla sequenza di attacco per poi concludere con l'applicazione delle azioni di correzione più adeguate.

Passaggio	Come utilizzare EDR
PASSAGGIO 1: Analisi riepilogativa dei problemi	Nell'elenco dei problemi generato da EDR: • Comprendere il profilo di sicurezza di un'organizzazione, in base al numero di problemi sui quali indagare. • Comprendere quali sono i problemi più critici, per dare priorità alle indagini su questi in base al livello di gravità riscontrato. • Comprendere quali sono i problemi nuovi o quelli che esistono da tempo.
PASSAGGIO 2: Indagine sul problema	Nella sequenza dell'attacco informatico generata da EDR: • Comprendere gli obiettivi degli attaccanti e visualizzare le tecniche di attacco utilizzate. • Verificare la probabilità che un problema sia un autentico attacco dannoso. • Verificare se un feed sulle minacce ha o meno impatto sul workload. • Visualizzare quali azioni di risposta sono state già applicate a un problema.
PASSAGGIO 3: Correzione dei problemi	Nelle sezioni di correzione di EDR pertinenti: • Correggere in modo facile e semplice un intero problema applicando azioni di risposta globali. • Correggere singoli punti di attacco nell'ambito di un problema. • Applicare azioni per impedire all'attacco in corso o agli attacchi futuri di diffondersi o colpire workload che non sono ancora stati presi di mira dall'attaccante.

Analisi riepilogativa dei problemi

Endpoint Detection and Response (EDR) fornisce un elenco di problemi che segnala sia i rilevamenti preventivi (o il malware) sia quelli sospetti individuati in un workload. Tale elenco offre una rapida

© Acronis International GmbH, 2003-2024

panoramica degli attacchi o delle minacce che interessano i workload, incluse quelle che devono essere mitigate.

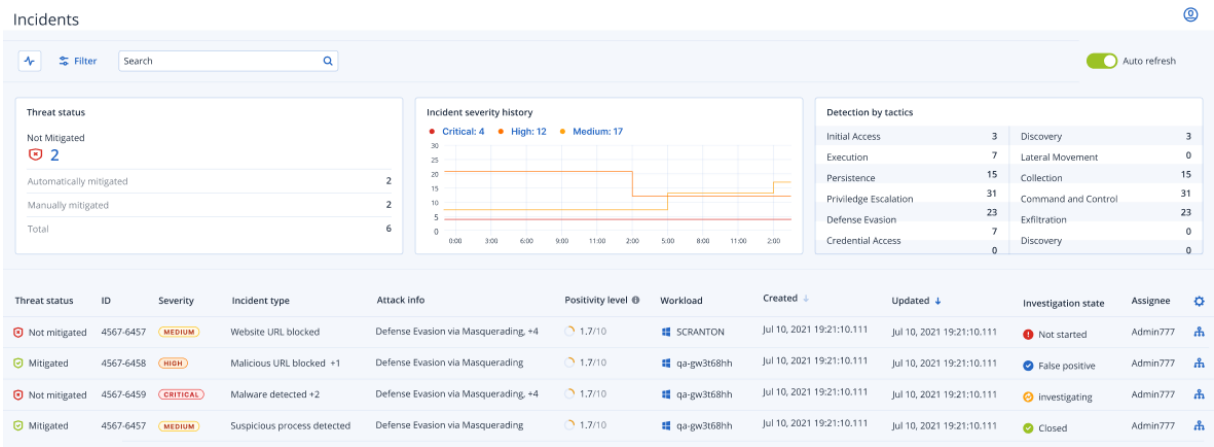
Dall'elenco dei problemi è possibile determinare rapidamente:

- Il profilo di sicurezza di un'organizzazione, in base al numero di problemi sui quali indagare.
- Quali sono i problemi critici, per dare priorità alle indagini su questi in base al livello di gravità riscontrato.
- Quali sono i problemi nuovi o quelli che esistono da tempo.

Nota
Quando si effettua l'accesso come amministratore del partner, è possibile visualizzare tutti i problemi EDR rilevati in un'unica schermata, che unisce quanto accaduto a tutti i clienti, senza dove visualizzare singolarmente i problemi di ciascun cliente. Viene visualizzata la colonna aggiuntiva **Clienti**, che include il nome del cliente a cui appartiene ciascun problema. Inoltre, i widget mostrati nel dashboard **Panoramica** mostrano i dati delle metriche aggregati di tutti i clienti.

Come indicato di seguito, è possibile accedere all'elenco dei problemi dal menu **Protezione** nella console di Cyber Protect. Per altre informazioni su come rivedere i problemi presenti nell'elenco, vedere "Visualizzazione dei problemi attualmente non risolti" (pag. 924). Per saperne di più su come viene creato un problema, vedere In cosa consiste esattamente un problema?.

Nota
Se la funzionalità Managed Detection and Response (MDR) è abilitata per i workload, viene visualizzata la colonna aggiuntiva **Ticket MDR**, nella quale è visualizzato il numero di ticket fornito dal vendor di servizi MDR.



Nota
La console di Cyber Protect deve essere aperta per poter ricevere le notifiche dei problemi.

© Acronis International GmbH, 2003-2024

In cosa consiste esattamente un problema?

Possiamo immaginare i problemi, o incidenti di sicurezza, come dei *container* per almeno un punto di prevenzione o rilevamento sospetto (o una loro combinazione), e includono tutti gli eventi e i rilevamenti correlati di un singolo attacco. Questi problemi di sicurezza possono includere anche eventi benigni aggiuntivi che offrono un ulteriore contesto su quanto accaduto.

In questo modo l'utente può visualizzare gli elementi dell'attacco unificati in un singolo problema, e comprendere i passaggi logici eseguiti dall'attaccante. L'elenco inoltre riduce il tempo dedicato alle indagini sull'attacco.

Quando EDR è abilitato nel piano di protezione, i problemi di sicurezza vengono creati se:

- **Un livello di protezione arresta qualcosa.** Questi problemi vengono chiusi automaticamente dal sistema in base alle impostazioni del piano di protezione. È tuttavia possibile indagare su quanto esattamente compiuto dal malware prima del suo arresto. Ad esempio, il ransomware viene arrestato quando inizia a crittografare i file, ma prima di ciò avrebbe potuto rubare delle credenziali o installare un servizio.
- **EDR rileva un'attività sospetta.** Si tratta di rilevamenti che devono essere indagati e corretti. Esaminando la sequenza dell'attacco informatico, che è stata migliorata dal punto di vista grafico, è più facile applicare le azioni di correzione pertinenti (per altre informazioni, consultare "Come indagare sui problemi rilevati nella sequenza di attacco" (pag. 929)).

Assegnare la priorità ai problemi che richiedono un intervento immediato

In qualsiasi momento, è possibile accedere all'elenco dei problemi della console di Cyber Protect dal menu **Protezione** della console di Cyber Protect. Tale elenco offre una rapida panoramica degli attacchi o delle minacce, consentendo di dare priorità ai problemi più urgenti.

Importante
Per garantire che i workload siano costantemente protetti, è bene analizzare e dare priorità *sempre* ai problemi in corso o non ancora corretti.

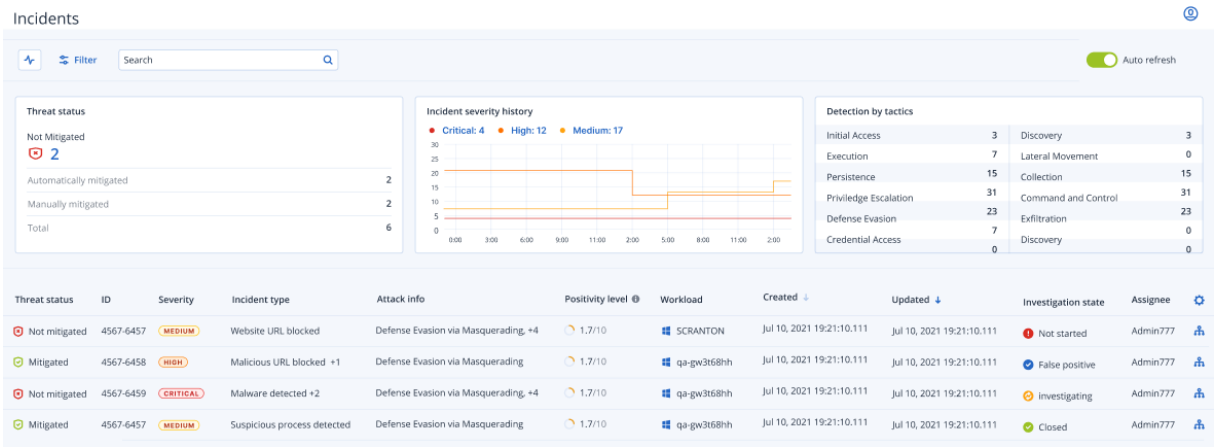
Come capire quali problemi di sicurezza richiedono un intervento immediato

L'elenco consente di analizzare e dare priorità ai problemi elencati che richiedono attenzione. È possibile:

- Visualizzare i problemi attualmente non risolti. Per capire rapidamente dall'elenco dei problemi se sono presenti attacchi in corso. Qualunque problema non risolto, come indicato nella colonna **Stato minaccia**, richiede attenzione immediata (per impostazione predefinita, all'elenco dei problemi è applicato un filtro che visualizza i problemi di questa categoria).
- Comprendere ambito e impatto dei problemi. Il filtro applicato agli attacchi appena sferrati o in corso deve facilitare la comprensione della gravità dei problemi filtrati e dell'impatto che possono avere sulla continuità operativa.

© Acronis International GmbH, 2003-2024

Una volta ottenuto un elenco perfezionato dei problemi più importanti, è possibile analizzare i relativi dettagli per comprendere meglio il problema specifico e le tecniche utilizzate dagli attaccanti per ottenere i propri obiettivi. Per ulteriori informazioni, consultare "Analisi dei dettagli del problema" (pag. 926).



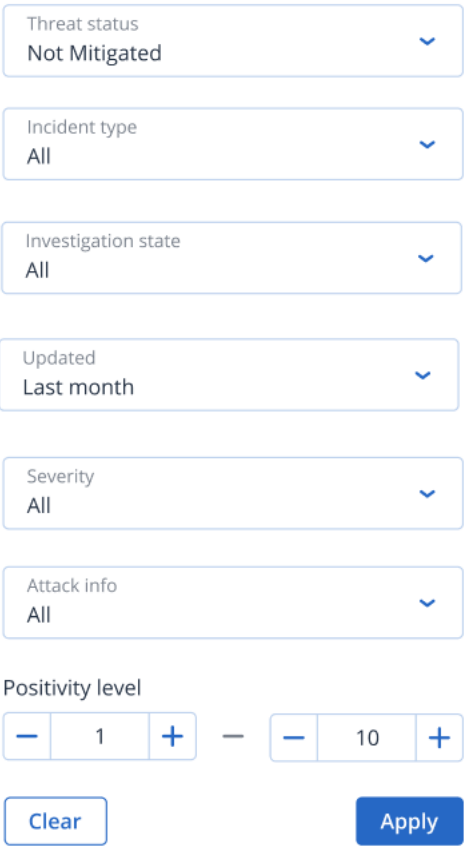
Nota

Per impostazione predefinita, l'elenco dei problemi è ordinato in base alla colonna **Aggiornato**, che mostra la data e l'ora dell'ultimo aggiornamento del problema con i nuovi rilevamenti registrati. Tenere presente che un problema esistente può essere aggiornato in qualsiasi momento, anche se è stato precedentemente chiuso. È anche possibile filtrare l'elenco in modo da visualizzare solo i nuovi attacchi aperti o solo quelli in corso, secondo necessità, come descritto nella procedura seguente.

Per filtrare l'elenco dei problemi

1. Nella parte superiore dell'elenco dei problemi, fare clic su **Filtro** per applicare un filtro all'elenco dei problemi visualizzato. Se, ad esempio, si selezionano le data di inizio e fine nel campo **Creazione**, l'elenco dei problemi e i widget mostrano i problemi pertinenti insorti durante l'intervallo di tempo specificato.

© Acronis International GmbH, 2003-2024



2. Al termine, fare clic su **Applica**.

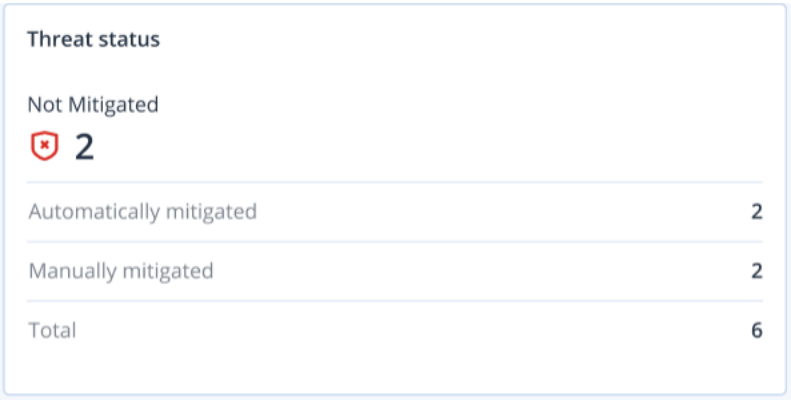
Visualizzazione dei problemi attualmente non risolti

È possibile visualizzare lo stato della minaccia corrente per i problemi nella colonna **Stato minaccia**, che mostra se il problema è **Mitigato** o **Non mitigato**. Lo stato della minaccia viene definito automaticamente da EDR; è necessario indagare al più presto su qualsiasi problema non mitigato.

È quindi possibile ridefinire ulteriormente l'elenco dei problemi visualizzati applicando altri filtri. Ad esempio, per filtrare l'elenco in base allo stato della minaccia *e* a un livello di gravità specifico, impostare le opzioni di filtro pertinenti. Dopo aver filtrato i problemi ritenuti più interessanti, è possibile passare alla fase di indagine, come descritto in "Eseguire l'indagine sul problema" (pag. 928).

È inoltre possibile utilizzare il widget **Stato minaccia**, come indicato di seguito, per una rapida panoramica sullo stato corrente delle minacce. Tenere presente che i dati visualizzati in questo widget rispecchiano i filtri applicati; vedere "Per filtrare l'elenco dei problemi" (pag. 923).

© Acronis International GmbH, 2003-2024



Comprensione dell'ambito e dell'impatto dei problemi

Per comprendere rapidamente ambito e impatto dei problemi, è possibile consultare le colonne **Gravità**, **Informazioni sull'attacco** e **Livello di positività**. Come indicato sopra, dopo aver determinato quali problemi sono attualmente in corso, è possibile filtrare queste colonne aggiuntive per:

- Rivedere i problemi più critici nella colonna **Gravità**. Un problema può riportare un livello di gravità **Critico**, **Alto** o **Medio**.
  - **Critico**: sussiste un rischio grave che un'attività digitale dannosa possa compromettere gli host critici dell'ambiente.
  - **Alto**: sussiste un rischio elevato che un'attività digitale dannosa possa danneggiare gravemente l'ambiente.
  - **Medio**: sussiste un aumentato rischio di attività digitale dannosa.

  Nota
  Nel determinare la gravità, l'algoritmo EDR tiene conto del tipo di workload e dell'ambito di ogni fase dell'attacco. Ad esempio, un problema che include fasi correlate al furto delle credenziali viene classificato come **Critico**.

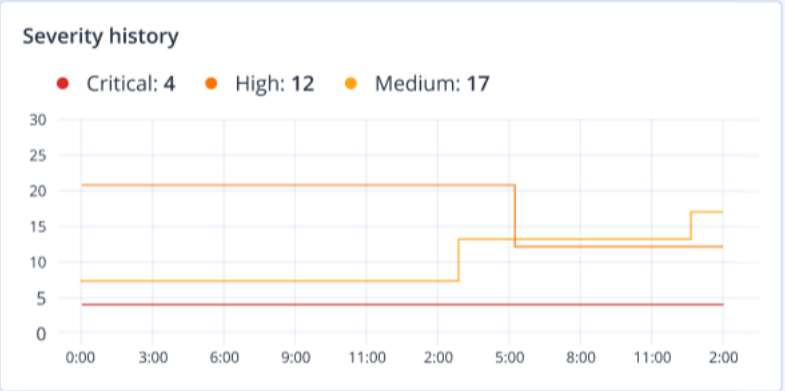
- Comprendere le ragioni della creazione del problema nella colonna **Tipo di problema**. Può trattarsi di uno o più tra i tipi di problema seguenti:
  - **Rilevamento di ransomware**
  - **È stato individuato del malware**
  - **Rilevamento di processo sospetto**
  - **Rilevamento di processo dannoso**
  - **Blocco di URL sospetto**
  - **Blocco di URL dannoso**
- Determinare quali tecniche di attacco sono state utilizzate nella colonna **Informazioni sull'attacco**, e comprendere se gli attacchi presentano un tema o uno schema comune.

© Acronis International GmbH, 2003-2024

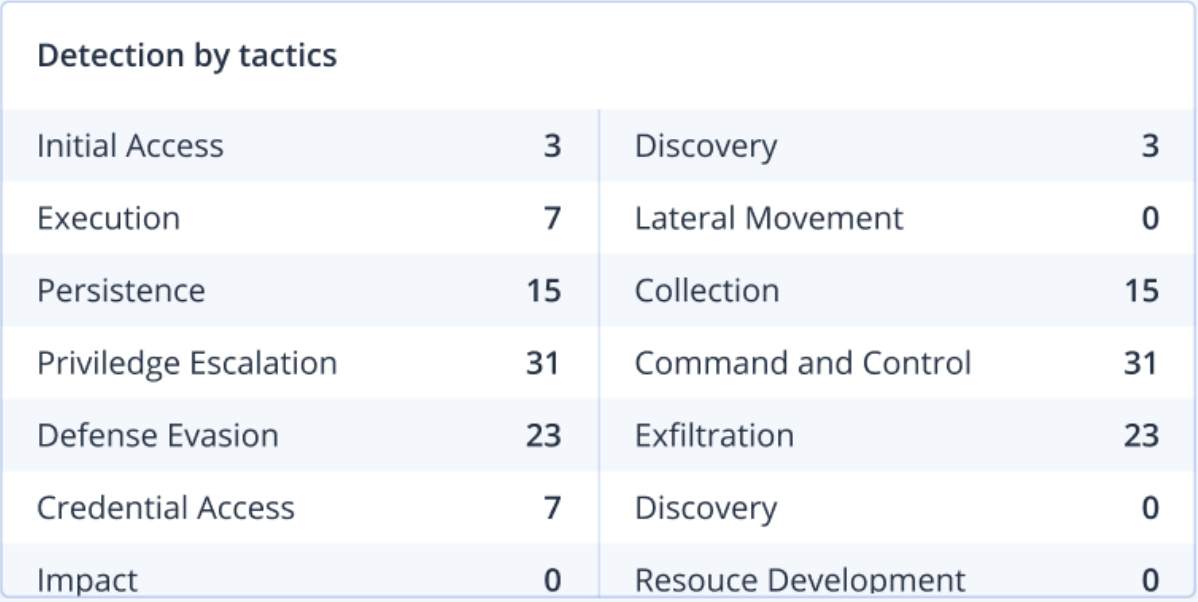
- Confermare la probabilità che un problema sia un autentico attacco dannoso; la colonna **Livello di positività** prevede un punteggio compreso tra 1 e 10 (più alto è il punteggio, maggiore la probabilità che l'attacco sia un autentico attacco dannoso).

Dopo aver individuato i problemi che richiedono un intervento immediato, è possibile passare alla fase di indagine, come descritto in "Eseguire l'indagine sul problema" (pag. 928).

È inoltre possibile utilizzare i widget **Cronologia gravità** e **Rilevamento per tattica** per una rapida panoramica sulla gravità e sulle tecniche dell'attacco.



Il widget **Rilevamento per tattica** visualizza le diverse tecniche di attacco utilizzate, con valori verdi o rossi che indicano l'aumento o la diminuzione rispetto al precedente intervallo di tempo specificato. Questo widget offre una visualizzazione aggregata di tutti gli obiettivi nei problemi filtrati, fornendo una rapida panoramica dell'impatto degli stessi sui clienti.



Analisi dei dettagli del problema

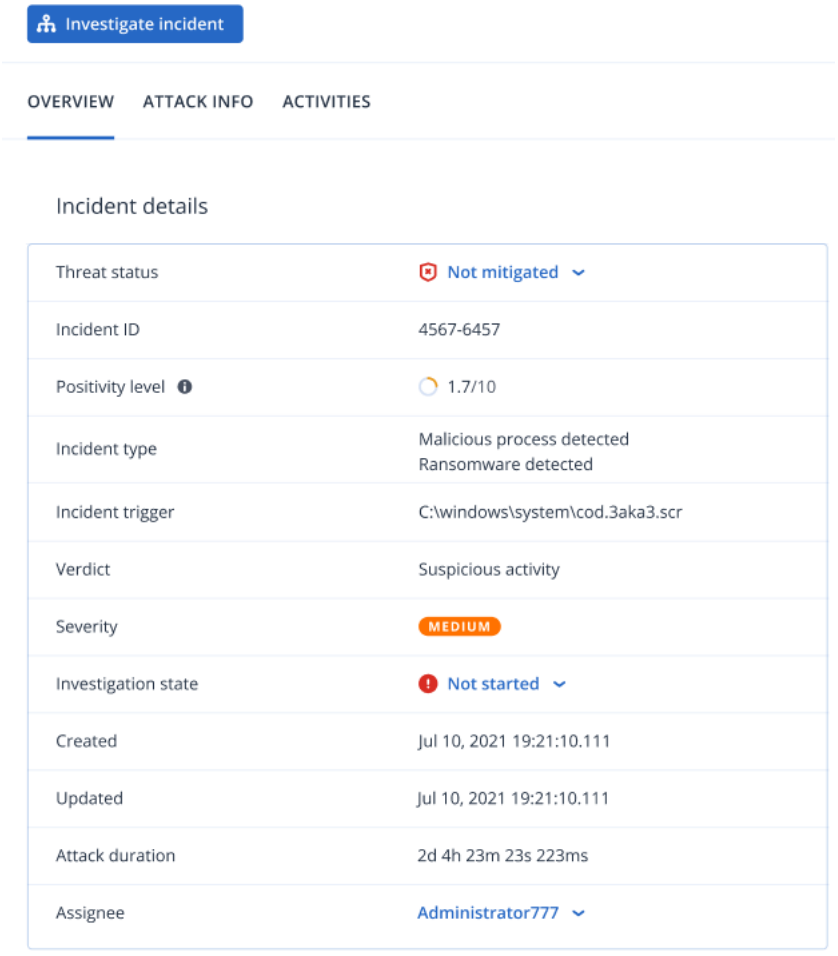
Durante la fase di riepilogo del problema, l'utente può analizzare i dettagli di ogni problema nell'elenco dei problemi di Endpoint Detection and Response (EDR). Queste informazioni consentono di esaminare in dettaglio l'intero problema per comprendere come e quando si è

© Acronis International GmbH, 2003-2024

verificato. È anche possibile assegnare un problema a utenti specifici che svolgeranno le attività di indagine, e impostare lo stato dell'indagine.

Per analizzare i dettagli del problema

1. Nella console di Cyber Protect, passare a **Protezione > Problemi**. Viene visualizzato l'elenco dei problemi.
2. Fare clic sul problema da analizzare. Vengono visualizzati i dettagli del problema selezionato.
3. Nella scheda **Panoramica** visualizzata, è possibile rivedere le informazioni sul problema e sul workload, incluso lo stato e la gravità della minaccia corrente. È anche possibile definire lo **Stato indagine** (selezionando uno degli stati tra **Indagine in corso**, **Non avviata** (stato predefinito), **Falso positivo** o **Chiusa**) e selezionare un utente al quale assegnare il problema (nell'elenco a discesa **Assegnatario** selezionare l'utente pertinente).



4. Fare clic sulla scheda **Informazioni sull'attacco** per visualizzare i dettagli dell'attacco e le tecniche utilizzate. Il link accanto a ogni tecnica di attacco dell'elenco consente di esaminare ulteriori informazioni sulla tecnica, indirizzando l'utente al sito MITRE.org.
5. Fare clic sulla scheda **Attività** per rivedere le azioni intraprese per mitigare un problema durante la sequenza di attacco. Per ulteriori informazioni, consultare "Come indagare sui problemi rilevati nella sequenza di attacco" (pag. 929).

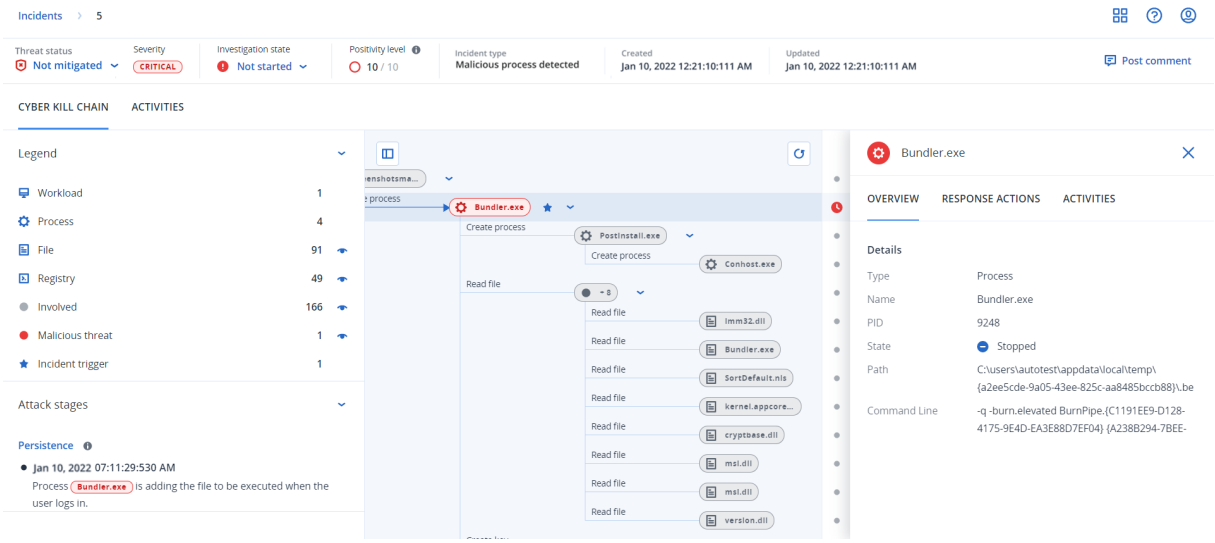
© Acronis International GmbH, 2003-2024

Se, ad esempio, è stata applicata una patch a un workload, vengono visualizzate informazioni su chi ha avviato la patch, il tempo che ha richiesto l'attività e qualsiasi eventuale errore che si è verificato durante la sua implementazione.

6. Fare clic su **Indagine sul problema** per accedere alla sequenza dell'attacco, dalla quale è possibile approfondire ogni singolo nodo del problema. Per ulteriori informazioni, consultare "Come indagare sui problemi rilevati nella sequenza di attacco" (pag. 929).

Eseguire l'indagine sul problema

Endpoint Detection and Response (EDR) consente di eseguire un'indagine su un intero problema, incluse tutte le fasi e gli oggetti (processi, voci dei registri, attività pianificate e domini) su cui ha impatto un attacco. Questi oggetti sono rappresentati dai nodi di una sequenza di attacco che è facile da comprendere, come mostrato di seguito. La sequenza è utile per avere una chiara e rapida comprensione degli eventi e di quando si sono verificati.



Ogni singola fase di un attacco è visualizzata nella sequenza dell'attacco informatico, che offre un'interpretazione dettagliata delle ragioni e delle modalità con cui si è verificato un attacco. La sequenza di attacco si avvale di frasi e grafici di facile comprensione, che consentono di approfondire ogni passaggio dell'attacco, il che si traduce in una riduzione del tempo necessario a compiere indagini sul problema.

Dall'evoluzione dell'attacco associata al framework MITRE è possibile comprendere rapidamente l'ambito e l'impatto di un problema. Ciò consente di esaminare quanto avvenuto in ogni fase dell'attacco, incluso:

- Il punto di accesso iniziale
- In che modo l'attacco è stato sferrato
- Eventuale escalation dei privilegi
- Prevenzione delle tecniche di rilevamento
- Movimenti laterali su altri workload

© Acronis International GmbH, 2003-2024

- Furto delle credenziali
- Tentativi di esfiltrazione

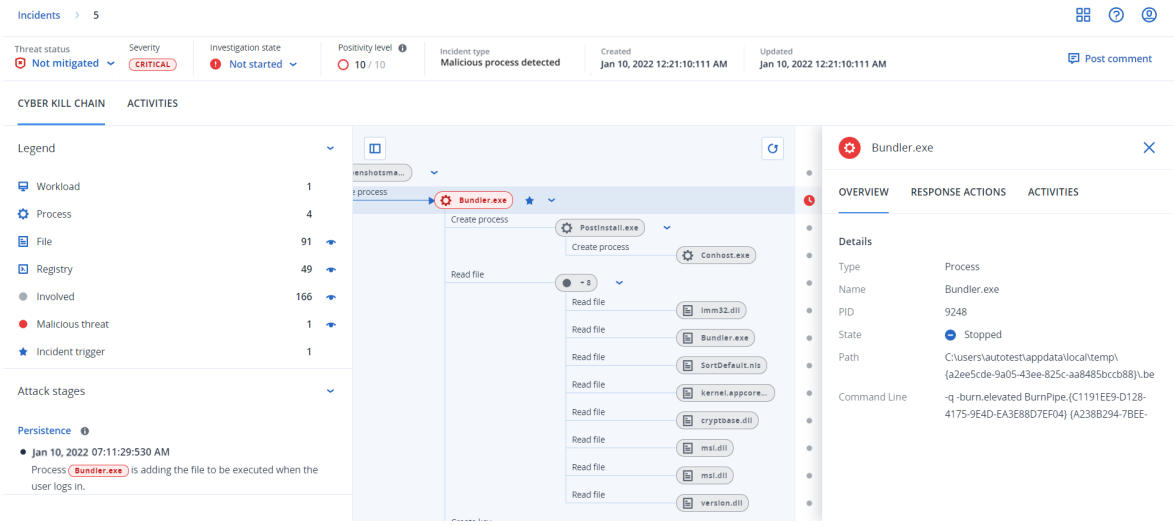
Nota
Ogni oggetto interessato dall'attacco, che si tratti di un processo, di un registro, di un'attività pianificata o di un dominio, è rappresentato da un nodo nella sequenza di attacco.

Come indagare sui problemi rilevati nella sequenza di attacco

È possibile indagare su ogni singola fase di un attacco nella sequenza dell'attacco informatico. Seguendo le frasi e i grafici di facile comprensione visualizzati nella sequenza di attacco, è possibile approfondire ogni passaggio dell'attacco, il che si traduce in una riduzione del tempo necessario a compiere indagini sul problema.

Per avviare un'indagine nella sequenza di attacco

1. Nella console di Cyber Protect, passare a **Protezione > Problemi**.
2. Nell'elenco dei problemi visualizzato, fare clic su nella colonna più a destra del problema per il quale avviare l'indagine. Viene visualizzata la sequenza dell'attacco informatico del problema selezionato.



3. Visualizza un riepilogo del problema nella relativa barra di stato, nella parte superiore della pagina. La barra di stato della minacce include le informazioni seguenti:
   - Stato corrente della minaccia. Lo stato della minaccia viene definito automaticamente dal sistema. È necessario indagare al più presto possibile su qualsiasi problema con lo stato **Non mitigato**.

© Acronis International GmbH, 2003-2024

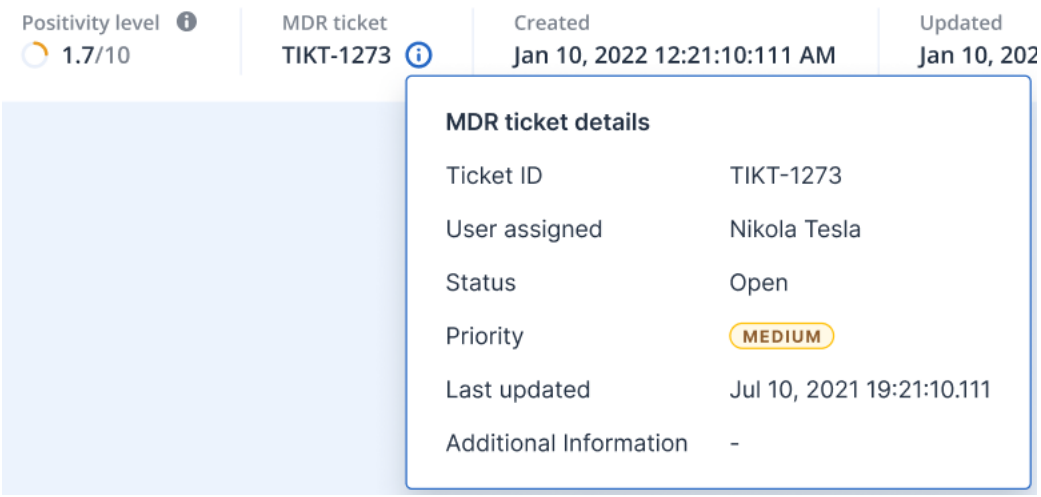
Importante
Un problema viene impostato su **Mitigato** quando è stato completato correttamente il ripristino dal backup o quando tutti i rilevamenti sono stati corretti tramite un'azione di arresto di un processo, quarantena o rollback.

Un problema viene impostato su **Non mitigato** quando il ripristino dal backup non è stato completato correttamente o quando non è stato possibile correggere anche un solo rilevamento tramite un'azione di arresto di un processo, quarantena o rollback.

È possibile anche impostare manualmente lo stato della minaccia su **Mitigato** o **Non mitigato**. Quando si seleziona uno dei due stati, viene chiesto di inserire un commento. Tale commento viene salvato come parte dell'attività di indagine e potrà essere visualizzato nella scheda **Attività**. EDR può riportare lo stato della minaccia su **Mitigato** o su **Non mitigato** se vengono individuati nuovi rilevamenti relativi al problema o se le azioni di risposta eseguite vengono completate in modo corretto.

- Gravità del problema: **Critico**, **Alto** o **Medio**. Per ulteriori informazioni, consultare "Analisi riepilogativa dei problemi" (pag. 920).
- Stato corrente dell'indagine. Uno degli stati tra **Indagine in corso**, **Non avviata** (stato predefinito), **Falso positivo** o **Chiusa**. È necessario modificare lo stato quando si avvia l'indagine sul problema, in modo che i colleghi siano a conoscenza delle eventuali modifiche apportate.
- Livello di positività. Indica la probabilità che un problema sia un autentico attacco dannoso; prevede un punteggio compreso tra 1 e 10. Per ulteriori informazioni, consultare "Analisi riepilogativa dei problemi" (pag. 920).
- Tipo di problema: uno o più tra **Rilevamento di ransomware**, **Rilevamento di malware**, **Rilevamento di processo sospetto**, **Rilevamento di processo dannoso**, **Blocco di URL sospetto** e **Blocco di URL dannoso**.
- Se la funzionalità Managed Detection and Response (MDR) è abilitata per il workload, viene visualizzata la colonna aggiuntiva **Ticket MDR**, nella quale sono visualizzate le informazioni sul ticket MDR creato per il problema e l'analista per l'analisi MDR assegnato al problema.

© Acronis International GmbH, 2003-2024



- Data di creazione e aggiornamento del problema. Data e ora di rilevamento del problema, o ultimo aggiornamento con i nuovi rilevamenti registrati all'interno del problema.

4. Fare clic sulla scheda **Legenda** per visualizzare i vari nodi che costituiscono il grafico della sequenza di attacco, quindi definire i nodi da visualizzare. Per ulteriori informazioni, consultare "Comprendere e personalizzare la visualizzazione della sequenza dell'attacco informatico" (pag. 931).
5. Indagare e correggere il problema completando i passaggi seguenti. L'esempio riporta il flusso di lavoro tipico per l'indagine e la correzione di un problema, ma può variare in funzione dei diversi problemi e delle singole esigenze.
   a. Indagare su ogni fase dell'attacco nella scheda **Fasi di attacco**. Per ulteriori informazioni, consultare "Come orientarsi nelle fasi di attacco" (pag. 934).
   b. Fare clic su **Correggi intero problema** per applicare le azioni di correzione. Per ulteriori informazioni, consultare "Correggere un intero problema" (pag. 944).

      È anche possibile indagare su singoli nodi nella sequenza di attacco, come descritto in "Azioni di risposta per singoli nodi della sequenza di attacco informatico" (pag. 949).
   c. Rivedere le azioni intraprese per mitigare il problema nella scheda **Attività**. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Comprendere e personalizzare la visualizzazione della sequenza dell'attacco informatico

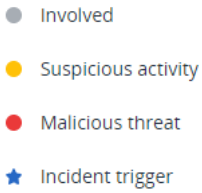
Per esaminare i nodi interessati dalla sequenza di attacco, accedere alla legenda. La legenda visualizza tutti i nodi coinvolti in un problema, consentendo di capire come siano stati interessati dall'azione dell'attaccante. È anche possibile definire i nodi da nascondere o da mostrare nella sequenza dell'attacco informatico.

Per accedere alla legenda

1. Fare clic sull'icona a freccia alla destra della sezione Legenda.
   La sezione si amplia come mostrato di seguito.

© Acronis International GmbH, 2003-2024

2. Nella legenda sono utilizzati quattro colori principali, che consentono di comprendere rapidamente ciò che è accaduto in ogni nodo della sequenza di attacco, come mostrato di seguito. Questi nodi con classificazione basata su colori sono inclusi anche nelle fasi di attacco, come descritto in "Come orientarsi nelle fasi di attacco" (pag. 934).



Per nascondere o visualizzare i nodi nella sequenza di attacco

1. Nella sezione estesa della Legenda verificare che sia visualizzata accanto ai nodi da mostrare nella sequenza dell'attacco informatico. Se l'icona visualizzata è , fare clic sull'icona affinché cambi in .
2. Per nascondere un nodo nella sequenza di attacco, fare clic su . L'icona diventa e il nodo non viene visualizzato nella sequenza di attacco.

Indagare sulle fasi di attacco di un problema

Le fasi di attacco di un problema forniscono interpretazioni di facile comprensione di ogni evento di sicurezza.

Ogni fase riepiloga esattamente ciò che è successo e quali sono gli oggetti presi di mira, definiti *nodi* nella sequenza di attacco. Se, ad esempio, un file scaricato si spaccia per qualcos'altro, la fase di

© Acronis International GmbH, 2003-2024

attacco lo segnala e include il link al nodo pertinente nella sequenza di attacco, che potrà quindi essere ulteriormente esaminato, e alla relativa tecnica MITRE ATT&CK.

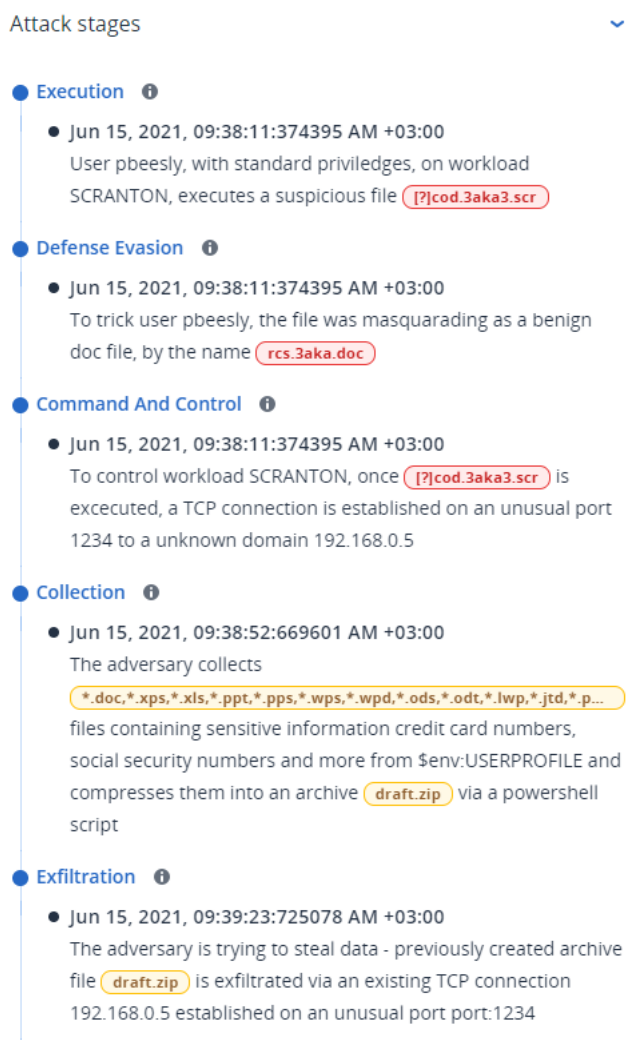
Ogni fase dell'attacco fornisce le informazioni necessarie per risolvere tre questioni cruciali:

- Qual era l'obiettivo dell'attaccante?
- In che modo l'attaccante ha ottenuto questo obiettivo?
- Quali nodi sono stati colpiti dall'attacco?

Un elemento di fondamentale importanza è che l'interpretazione fornita consente di ridurre il tempo dedicato all'indagine sul problema, perché non è più necessario esaminare ogni evento di sicurezza partendo da una sequenza temporale o da un nodo grafico per poi comprendere l'attacco.

Le fasi di attacco includono anche informazioni sui file compromessi che contengono informazioni sensibili, come numero di carte di credito e codici della previdenza sociale, come mostra la fase **Raccolta** dell'esempio seguente.

Per ulteriori informazioni, consultare "Quali informazioni sono incluse in una fase di attacco?" (pag. 934).



© Acronis International GmbH, 2003-2024

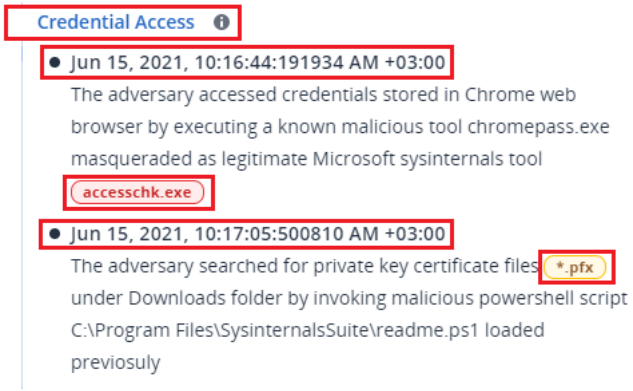
Come orientarsi nelle fasi di attacco

Le fasi di attacco sono elencate in ordine cronologico. Scorrere per visualizzare l'elenco completo delle fasi di attacco del problema.

Per indagare ulteriormente su una fase di attacco specifica, fare clic su qualsiasi punto della fase nella rappresentazione grafica della sequenza di attacco e individuare il nodo che interessa. Per ulteriori informazioni su come orientarsi nel grafico della sequenza di attacco e nei nodi specifici, consultare "Indagare su singoli nodi nella sequenza di attacco" (pag. 936).

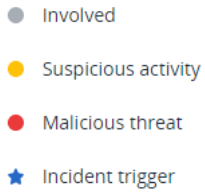
Quali informazioni sono incluse in una fase di attacco?

Ogni fase fornisce un'interpretazione della sequenza di attacco con un linguaggio chiaro e di facile comprensione. Questa interpretazione è composta da numerosi elementi, mostrati e descritti nella tabella seguente.



Elemento della fase di attacco	Descrizione
Intestazione	Descrive i tentativi effettuati dagli attaccanti e i loro obiettivi (nell'esempio l'**Accesso alle credenziali**), con un link a una tecnica nota del framework MITRE ATT&CK. Fare clic sul link per ulteriori informazioni sul sito web di MITRE ATT&CK. **Nota** Se la fase di attacco non corrisponde a una tecnica MITRE ATT&CK nota, nell'intestazione non sarà presente alcun link. L'informazione è importante per le tecniche generiche, ad esempio i file rilevati in una cartella casuale.
Indicatore data e ora	L'orario in cui si è verificata la fase di attacco.
Tecnica	Il modo in cui gli attaccanti hanno raggiunto tecnicamente i propri obiettivi e quali oggetti

© Acronis International GmbH, 2003-2024

Elemento della fase di attacco	Descrizione
	(voci del Registro di sistema, file o attività pianificate) sono stati interessati dall'attacco. Il testo descrittivo della tecnica di attacco include i link, con classificazione basata su colori, a ogni nodo interessato della sequenza di attacco, come mostrato nell'esempio precedente. Tali link consentono di passare rapidamente al nodo interessato e indagare con precisione su quanto accaduto. I colori utilizzati in una fase di attacco indicano quanto segue:  Osservando la precedente legenda, possiamo vedere che la fase di attacco di esempio Accesso alle credenziali presenta un link a un nodo malware accesschk.exe e un nodo file sospetto *.pfx (fare clic sui link per passare al nodo corrispondente della sequenza di attacco). Per ulteriori informazioni su come orientarsi tra i nodi e sulle azioni disponibili, consultare "Indagare su singoli nodi nella sequenza di attacco" (pag. 936). Si noti che le fasi di attacco includono anche link ai nodi file con informazioni sui file compromessi che contengono dati sensibili, come informazioni sanitarie protette, numeri di carte di credito e codici della previdenza sociale.

Nota

Ogni fase di attacco costituisce un singolo evento di rilevamento. Il contenuto elencato in ogni fase (intestazione, indicatore data e ora, tecnica) viene generato in base a parametri specifici nell'evento di rilevamento, a loro volta basati sui modelli delle fasi di attacco archiviati da Endpoint Detection and Response (EDR).

© Acronis International GmbH, 2003-2024

Indagare su singoli nodi nella sequenza di attacco

Oltre a rivedere le fasi dell'attacco, è anche possibile esaminare ogni singolo nodo della sequenza di attacco. Ciò consente di approfondire in dettaglio nodi specifici della sequenza di attacco, indagando e correggendo ogni nodo come necessario.

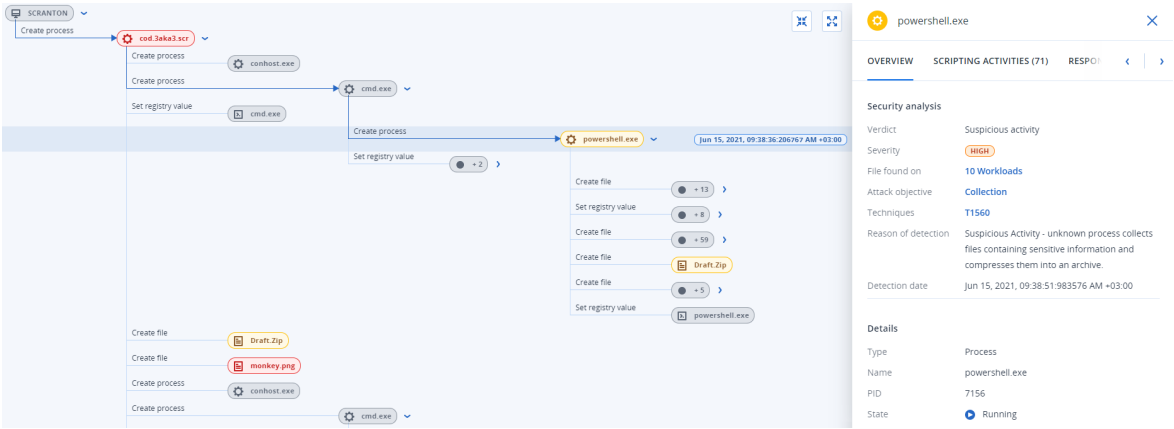
Ad esempio, è possibile determinare la probabilità che un problema sia un attacco dannoso vero e proprio. A seconda degli esiti dell'indagine, al nodo possono essere applicate diverse azioni di risposta, ad esempio isolare un workload o mettere in quarantena un file sospetto.

Per indagare su singoli nodi nella sequenza di attacco

1. Nella console di Cyber Protect, passare a **Protezione > Problemi**.
2. Nell'elenco dei problemi visualizzato, fare clic su nella colonna più a destra del problema per il quale avviare l'indagine. Viene visualizzata la sequenza dell'attacco informatico del problema selezionato.
3. Passare al nodo pertinente e fare clic per visualizzare la barra laterale del nodo.

   Nota
   Fare clic su nodo per espanderlo e visualizzare i nodi associati.

   Nell'esempio seguente, facendo clic sul nodo **powershell.exe** viene visualizzata la barra laterale relativa al nodo. È anche possibile fare clic sull'icona a freccia accanto al nodo per visualizzare i nodi associati, inclusi file e valori del Registro di sistema, che possono essere influenzati dal nodo **powershell.exe**. Per approfondire ulteriormente l'indagine, fare clic sui nodi associati.



4. Indagare sulle informazioni incluse nelle schede della barra laterale:
   - **Panoramica**: Include due sezioni principali che forniscono un riepilogo sulla sicurezza del nodo oggetto dell'attacco.
     - **Analisi di sicurezza**: Fornisce un'analisi del nodo oggetto dell'attacco, inclusa l'analisi del verdetto di EDR sulla minaccia (ad esempio Attività sospetta), l'obiettivo dell'attacco secondo le tecniche di attacco MITRE (fare clic sul link per aprire il sito web MITRE), la ragione del rilevamento, e il numero di workload potenzialmente interessati dall'attacco (fare clic sul link con il **numero di workload** per visualizzare i workload interessati).

© Acronis International GmbH, 2003-2024

Nota
Il link con il **numero di workload** indica che gli oggetti dannosi o sospetti specifici sono stati *individuati* anche in altri workload. Non significa che c'è un attacco in corso su questi altri workload, ma che questi presentano un indicatore di compromissione. L'attacco può essere già avvenuto (e aver creato un altro problema), oppure l'attaccante si sta preparando a colpire questi altri workload utilizzando la propria serie di strumenti di attacco.

  - **Dettagli**: Mostra informazioni sul nodo, ad esempio il tipo, il nome, lo stato attuale, il percorso e qualsiasi hash file e firma digitale, come i numeri di serie di certificati e MD5.
- **Attività di scripting**: Include informazioni su qualsiasi script invocato o caricato durante l'attacco. Fare clic su per copiare lo script negli appunti per un'eventuale indagine successiva.

Nota
La scheda **Attività di scripting** viene visualizzata solo per i nodi dei processi che eseguono comandi o script (ad esempio cmd o i comandi PowerShell).

- **Azioni di risposta**: Include un numero di sezioni che forniscono azioni aggiuntive di indagine, correzione e prevenzione, in base al tipo di nodo.
  Per i nodi workload, ad esempio, è possibile definire una serie di risposte tra cui il backup forense e il ripristino da backup. In alternativa, in presenza di nodi dannosi o sospetti è possibile arrestare o mettere in quarantena il nodo, eseguire il rollback delle modifiche apportate dall'attacco e aggiungere i nodi all'elenco degli elementi consentiti o all'elenco degli elementi bloccati di un piano di protezione.
  Per ulteriori informazioni su come applicare le azioni di risposta a nodi specifici, consultare "Azioni di risposta per singoli nodi della sequenza di attacco informatico" (pag. 949).
- **Attività**: Visualizza le azioni applicate al problema in ordine cronologico. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Comprendere le azioni intraprese per mitigare un problema

Dopo aver riesaminato un problema e indagato su come si è svolto l'attacco, in genere vengono applicate le azioni di risposta. Dopo aver applicato le azioni di risposta, queste possono essere visualizzate in diverse posizioni, per ottenere un quadro più chiaro dei passaggi intrapresi per mitigare il problema.

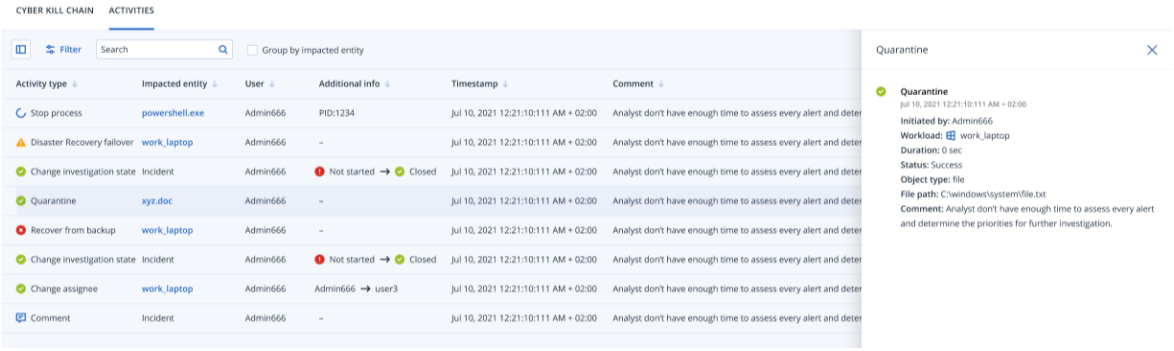
Nota
Ai problemi generati dai livelli di prevenzione si applicano automaticamente le azioni configurate nel piano di protezione. Per i punti di rilevamento, è necessario definire le azioni di risposta più adeguate a correggere ogni scenario di attacco.

© Acronis International GmbH, 2003-2024

Per comprendere le azioni di risposta intraprese, è possibile visualizzare tutte le azioni di risposta applicate a un intero problema, oppure visualizzare le azioni applicate a un nodo specifico nella sequenza dell'attacco informatico.

Per visualizzare tutte le azioni di risposta applicate a un problema

1. Nella console di Cyber Protect, passare a **Protezione > Problemi**.
2. Nell'elenco dei problemi visualizzato, fare clic su nella colonna più a destra del problema per il quale avviare l'indagine. Viene visualizzata la sequenza dell'attacco informatico del problema selezionato.
3. Fare clic sulla scheda **Attività**.
   Viene visualizzato l'elenco delle azioni di risposta già applicate al problema.



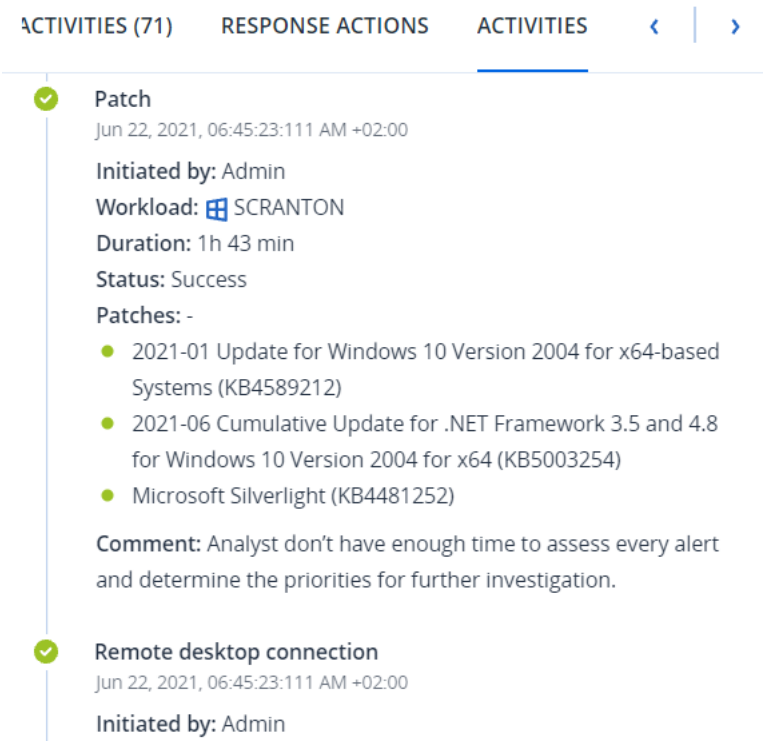
4. Sull'elenco visualizzato è possibile eseguire numerose azioni:
   - Fare clic su una riga di un tipo di attività per visualizzare più informazioni sull'attività selezionata. Le informazioni vengono mostrate nella barra laterale, come descritto nel Passaggio 3, e includono informazioni su chi ha avviato l'azione, lo stato, il percorso del file e qualsiasi commento aggiunto dall'iniziatore.
   - Utilizzare la casella **Cerca** per individuare un'azione specifica.
   - Fare clic su **Filtra** per applicare i filtri all'elenco.
   - Selezionare la casella di controllo **Raggruppa per entità interessata** per raggruppare le azioni pertinenti in base all'entità di appartenenza.
   - Fare clic su per mostrare/nascondere l'elenco delle azioni completate.
     Verificare che sia visualizzata accanto alle azioni da mostrare. Per nascondere un'azione dall'elenco delle azioni visualizzate, fare di nuovo clic per modificare l'immagine in .

© Acronis International GmbH, 2003-2024

Per visualizzare le azioni di risposta applicate a un nodo specifico

© Acronis International GmbH, 2003-2024

1. Nella sequenza di attacco, fare clic su un nodo per visualizzare la relativa barra laterale.
2. Fare clic sulla scheda **Attività**.



3. Per comprendere in modo più completo quali azioni sono state applicate e perché, è necessario sfogliare le azioni di risposta applicate al nodo. Ad esempio, per le azioni di connessione desktop remoto è possibile visualizzare chi ha avviato l'azione e quando, la durata dell'azione e lo stato complessivo (se è stata completata correttamente, se non è riuscita o se è stata completata con errori).

Controllare la presenza di indicatori di compromissione di attacchi pubblicamente noti nei workload

Endpoint Detection and Response (EDR) prevede la capacità di esaminare gli attacchi noti esistenti nel feed sulle minacce a fronte dei workload. I feed sulle minacce vengono generati automaticamente in base ai dati sulle minacce ricevuti dai centri operativi di Cyber Protection (CPOC); EDR consente di verificare se una minaccia sta interessando il workload e di prendere quindi le azioni necessarie per neutralizzarla.

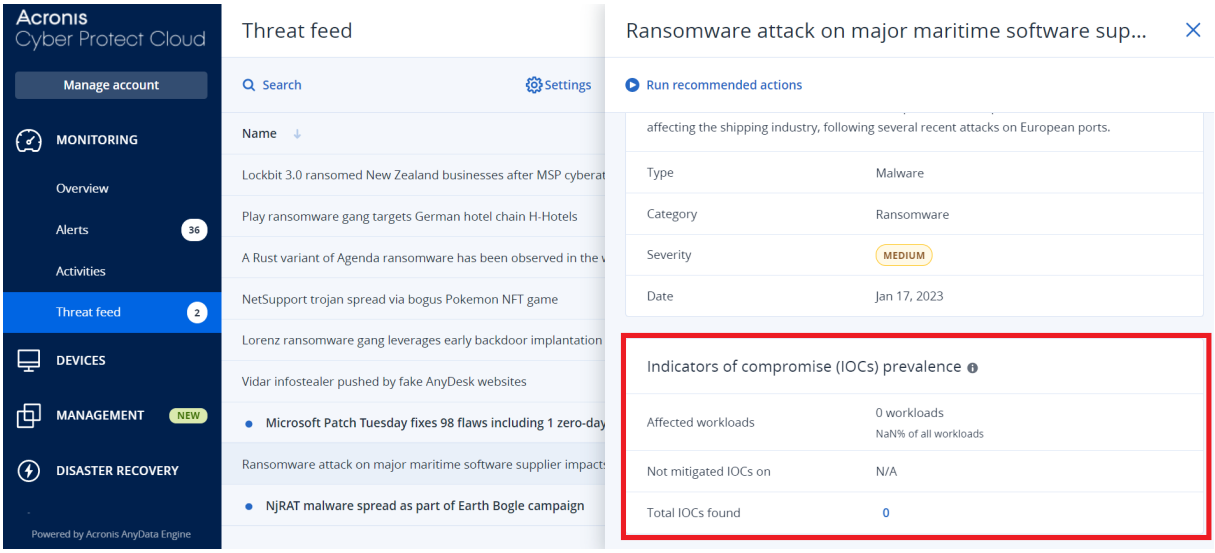
È possibile accedere al feed sulle minacce dal menu **Monitoraggio** nella console di Cyber Protect. Per ulteriori informazioni, consultare "Feed minacce" (pag. 309).

Per rivedere i dettagli di minacce specifiche e confermare che hanno colpito i workload in esame, fare clic su un feed sulle minacce. È possibile visualizzare il numero di indicatori di compromissione rilevati e i workload interessati, e sfogliare in dettaglio i workload che contengono indicatori non mitigati.

© Acronis International GmbH, 2003-2024

Nota

Se EDR non è abilitato per il piano di protezione, la funzionalità aggiuntiva mostrata di seguito non viene visualizzata.



Definire le impostazioni del feed sulle minacce

È possibile definire una serie di impostazioni del feed sulle minacce per individuare e mitigare automaticamente qualsiasi minaccia nota.

Per definire le impostazioni del feed sulle minacce

1. Nella console di Cyber Protect, passare a **Monitoraggio > Feed minacce**.
2. Nella pagina Feed minacce visualizzata, fare clic su **Impostazioni**.

© Acronis International GmbH, 2003-2024

3. Nella finestra di dialogo visualizzata, selezionare una tra le opzioni seguenti:

Opzione	Descrizione
Cerca indicatori di compromissione	Fare clic sull'opzione per abilitare la ricerca automatica degli indicatori di compromissione nei workload. Quando l'opzione è abilitata, vengono visualizzate anche le opzioni **Azione al rilevamento** e **Genera un avviso**.
Azione al rilevamento	Dall'elenco a discesa, selezionare l'azione da intraprendere sui file interessati quando nel workload viene individuata una minaccia: • **Nessuna azione** • **Quarantena** • **Elimina** • **Isola workload**
Genera un avviso	Selezionare la casella di controllo per generare un avviso se in un workload viene rilevato un indicatore di compromissione. L'avviso verrà visualizzato nella pagina Avvisi.

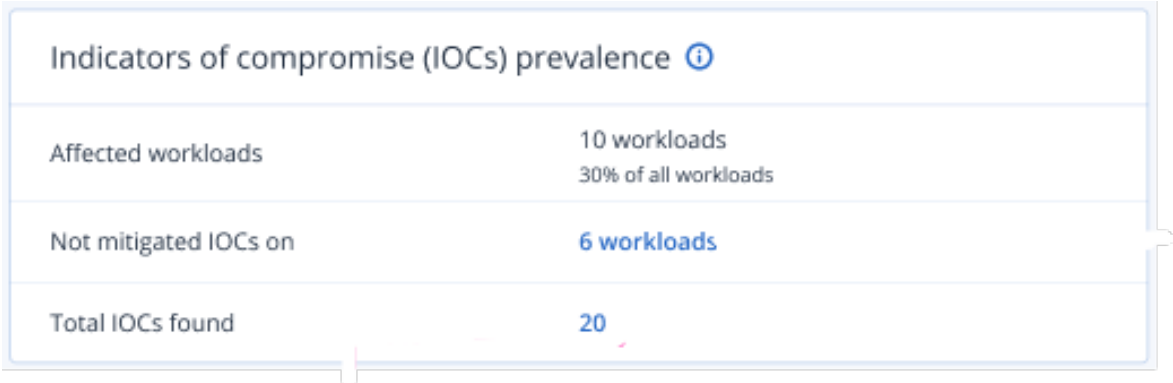
4. Fare clic su **Applica**.

Rivedere e mitigare gli indicatori di compromissione sui workload interessati

Se Endpoint Detection and Response (EDR) è abilitato in un piano di protezione, è possibile visualizzare qualsiasi minaccia nota che interessi i workload inclusi nel piano. La soluzione consente anche di mitigare qualsiasi indicatore di compromissione rimanente che non sia stato corretto automaticamente. Per informazioni su come mitigare gli indicatori di compromissione in modo automatico, consultare "Definire le impostazioni del feed sulle minacce" (pag. 941).

Per rivedere e mitigare i workload interessati

1. Nella console di Cyber Protect, passare a **Monitoraggio > Feed minacce**.
2. Fare clic su una minaccia per visualizzare tutte le informazioni disponibili.
3. Nella sezione **Prevalenza di indicatori di compromissione** fare clic sul link con il ***numero*** **di workload** per visualizzare i workload con indicatori di compromissione non mitigati.



© Acronis International GmbH, 2003-2024

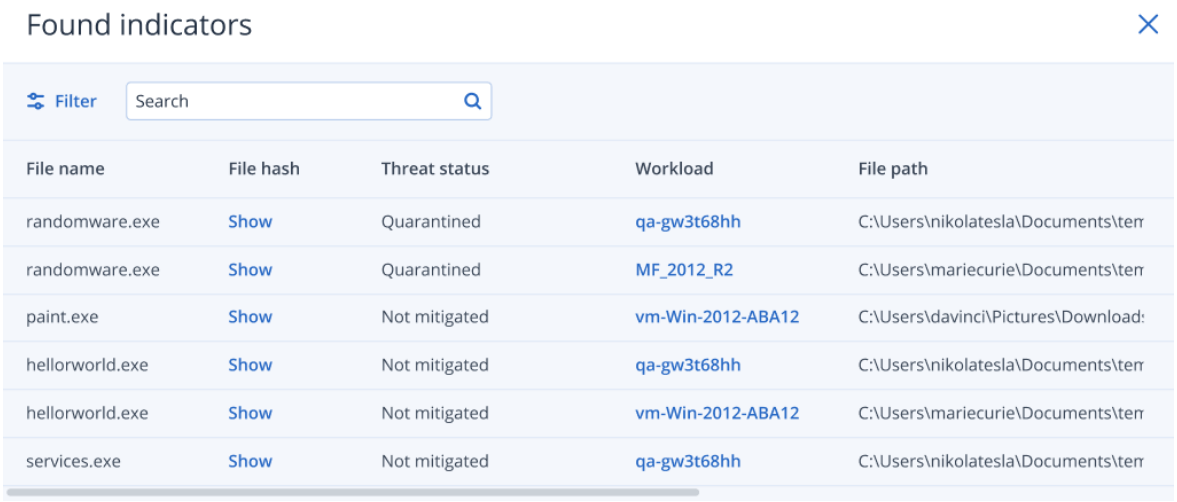
4. Nella pagina Workload visualizzata, fare clic sul workload pertinente per rivederne le informazioni. Nel workload è possibile eseguire funzionalità specifiche, incluso definire URL aggiuntivi per filtrare (consultare "Filtro URL" (pag. 865)) e bloccare processi dannosi (fare riferimento alla sezione Esclusioni in "Impostazioni di Protezione antivirus e anti-malware" (pag. 840)).
   Se, ad esempio, il feed sulle minacce indica che un workload è interessato da un indicatore di compromissione, innanzitutto individuare e analizzare l'indicatore come descritto in "Rivedere e analizzare gli indicatori di compromissione individuati" (pag. 943). Passare quindi al piano di protezione del workload e definire le funzionalità di protezione aggiuntive, ad esempio bloccare gli hash file o i processi dannosi.

Rivedere e analizzare gli indicatori di compromissione individuati

Oltre a rivedere qualsiasi workload colpito da minacce note, è anche possibile rivedere e analizzare indicatori di compromissione specifici. Ciò consente di esaminare i singoli workload interessati da un indicatore di compromissione e quindi correggerlo.

Per rivedere e analizzare gli indicatori di compromissione

1. Nella console di Cyber Protect, passare a **Monitoraggio > Feed minacce**.
2. Fare clic su una minaccia per visualizzare tutte le informazioni disponibili.
3. Nella sezione **Prevalenza di indicatori di compromissione**, fare clic su **Indicatori di compromissione totali individuati**.
   Viene visualizzata la pagina Indicatori rilevati.



4. [Facoltativo] Utilizzare l'opzione **Filtro** per filtrare l'elenco degli Indicatori di compromissione in base al proprio stato. È inoltre possibile utilizzare l'opzione **Cerca** per cercare indicatori di compromissione specifici.
5. Per visualizzare il workload interessato da un indicatore di compromissione, fare clic sul link nella colonna **Workload**. Sul workload è possibile eseguire numerose azioni, ad esempio gestire l'applicazione delle patch o modificare un piano di protezione.

© Acronis International GmbH, 2003-2024

6. [Facoltativo] nella colonna **Hash del file**, fare clic su **Mostra** per visualizzare gli hash file individuati per uno specifico indicatore di compromissione. Nella finestra di dialogo visualizzata, fare clic su per copiare l'hash file dell'indicatore di compromissione in un editor di testo.

Correzione dei problemi

Endpoint Detection and Response (EDR) consente di correggere interi problemi o i singoli punti di attacco che li costituiscono.

Correggendo un intero problema, è possibile scegliere le correzioni da eseguire globalmente sul problema. Se occorre gestire il problema con un maggiore livello di dettaglio, è possibile intervenire sui singoli punti di attacco, secondo necessità. Ad esempio, può essere utile isolare la rete di un workload per arrestare attività di movimento laterale o di comando e controllo; ciò garantisce la funzionalità di tutte le tecnologie di Acronis Cyber Protect e la possibilità di avviare l'indagine, anche se il workload resta isolato.

EDR garantisce una correzione efficace tramite:

- Mitigazione, per garantire che la minaccia venga arrestata.
- Ripristino, per garantire che i servizi tornino immediatamente operativi.
- Prevenzione, per garantire che non sia più possibile utilizzare le tecniche utilizzate in attacchi futuri.

Correggere un intero problema

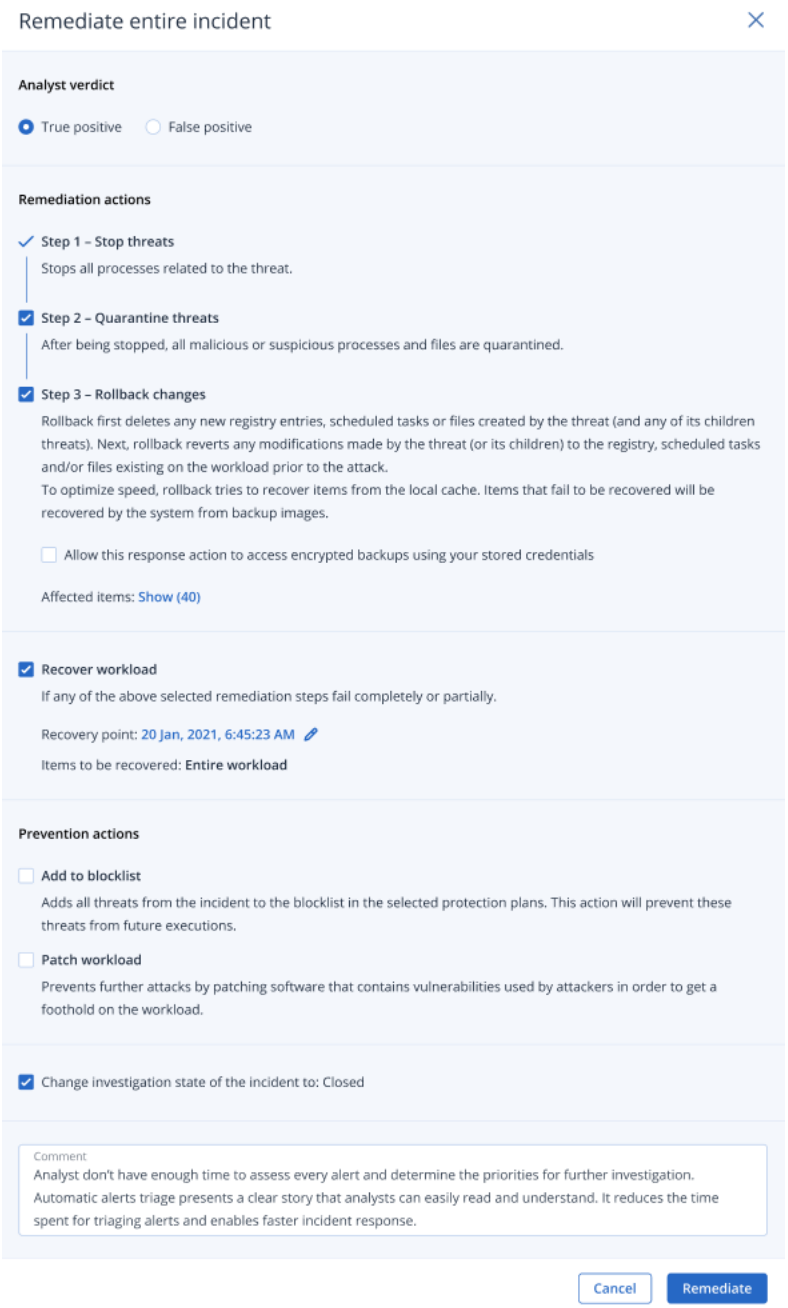
Correggendo un intero problema, è possibile scegliere in modo facile e rapido le correzioni da eseguire globalmente sul problema. EDR guida l'utente passo per passo durante il processo di correzione.

Se occorre gestire il problema con un maggiore livello di dettaglio, vedere "Azioni di risposta per singoli nodi della sequenza di attacco informatico" (pag. 949).

Per correggere un intero problema

1. Nella console di Cyber Protect, passare a **Protezione > Problemi**.
2. Nell'elenco dei problemi visualizzato, fare clic su nella colonna più a destra del problema per il quale avviare l'indagine. Viene visualizzata la sequenza dell'attacco informatico del problema selezionato.
3. Fare clic su **Correggi intero problema**. Viene visualizzata la finestra di dialogo Correggi intero problema.

© Acronis International GmbH, 2003-2024



4. Nella sezione **Risultato dell'analisi**, in base all'indagine sul problema corrente, selezionare una delle seguenti opzioni:
   - **Vero positivo**: Selezionare questa casella di controllo se si è certi che l'attacco sia un attacco legittimo. Al termine della selezione, aggiungere le azioni di correzione e prevenzione come descritto nei passaggi seguenti.
   - **Falso positivo**: Selezionare questa casella di controllo se si è certi che l'attacco non sia un attacco autentico. In questo modo, sarà possibile indicare come impedire che l'evento si verifichi di nuovo, ad esempio aggiungendo il problema a un elenco degli elementi consentiti di un piano di protezione.

© Acronis International GmbH, 2003-2024

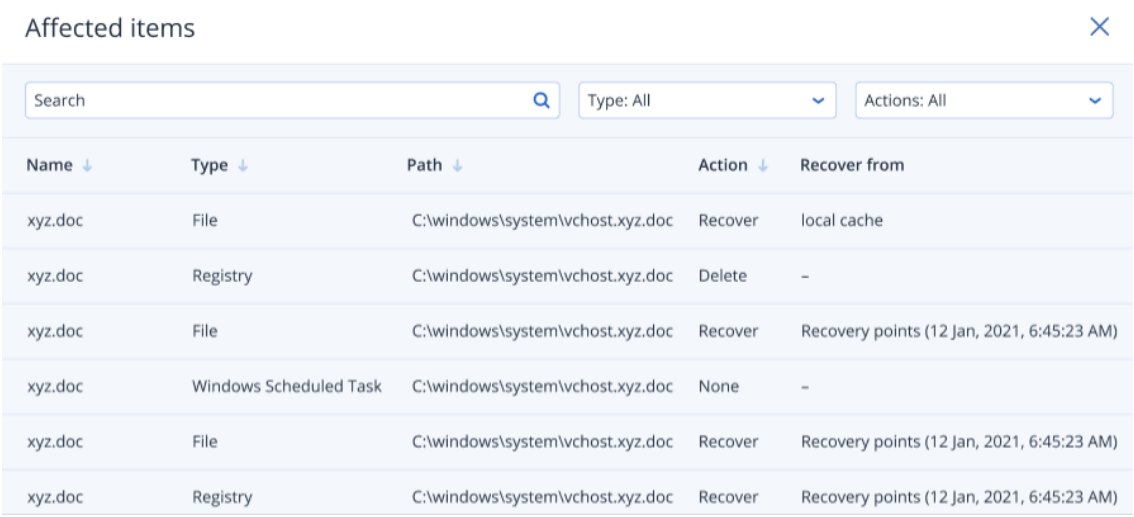
Nota
Dopo aver selezionato **Falso positivo**, è possibile definire soltanto azioni preventive. Per ulteriori informazioni, consultare "Correggere un problema falso positivo" (pag. 948).

5. Nella sezione **Azioni di correzione**, eseguire i passaggi correttivi indicati di seguito. Tenere presente che devono essere eseguiti in ordine sequenziale, ovvero non è possibile selezionare il Passaggio 2 prima che il Passaggio 1 sia completato.
   a. **Passaggio 1 - Arresta minacce**: Selezionare questa casella di controllo per arrestare tutti i processi correlati alla minaccia.
   b. **Passaggio 2 - Minacce in quarantena**: Una volta arrestata la minaccia, selezionare la casella di controllo per mettere in quarantena tutti i processi e i file ritenuti dannosi e sospetti.
   c. **Passaggio 3 – Rollback modifiche**: Dopo aver messo le minacce in quarantena, selezionare la casella di controllo per eliminare qualsiasi nuova voce del Registro di sistema, eventuali attività pianificate o file creati dalla minaccia (e da qualsiasi minaccia figlio correlata). Successivamente, il rollback ripristina qualsiasi modifica apportata dalla minaccia (o dai suoi figli) al Registro di sistema, alle attività pianificate e/o ai file esistenti nel workload prima dell'attacco. Per ottimizzare la velocità, il processo di rollback tenta di recuperare gli elementi dalla cache locale. Gli elementi impossibili da recuperare verranno ripristinati dal sistema a partire dalle immagini di backup.

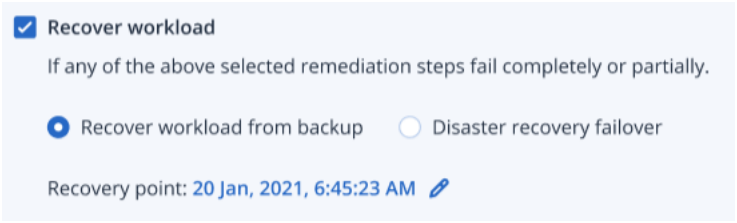
   Nota
   Il processo di rollback esegue il recupero solo dagli elementi presenti nella cache locale. Il rollback dagli archivi di backup sarà disponibile nelle release future.

   Selezionare la casella di controllo **Consenti a questa azione di risposta di accedere ai backup crittografati utilizzando le credenziali archiviate** se l'accesso ai backup di interesse è crittografato. EDR accede alle credenziali utente archiviate per decrittografare gli archivi criptati e cercare i file pertinenti.
   È anche possibile fare clic su **Elementi interessati** per visualizzare tutti gli elementi (file, Registro di sistema o attività pianificate) interessati dal rollback, le azioni applicate (**Elimina**, **Ripristina** o **Nessuna**), e se gli elementi vengono ripristinati dalla cache locale o dalle immagini di backup.

© Acronis International GmbH, 2003-2024



d. **Ripristina workload**: Selezionare questa casella di controllo per ripristinare un workload nel caso in cui uno dei passaggi di correzione selezionati in precedenza non riesca parzialmente o completamente.



Selezionare una delle seguenti opzioni di ripristino:

- **Ripristino del workload dal backup**: Consente di ripristinare un workload da uno specifico punto di ripristino. Fare clic sull'icona di modifica del punto di ripristino per eseguire una selezione da un elenco di backup di ripristino.
- **Failover di disaster recovery**: Consente di avviare un disaster recovery, se la funzionalità è abilitata nel piano di protezione. Questa opzione è consigliata per i workload critici, come i server AD o i server di database. Per ulteriori informazioni, consultare "Implementazione del disaster recovery" (pag. 749).

6. Nella sezione **Azioni di prevenzione**, selezionare i passaggi di correzione pertinenti:
   - **Aggiungi alla lista degli elementi bloccati**: Selezionare la casella di controllo e, nell'elenco del piano di protezione visualizzato, selezionare i piani di protezione pertinenti. Questa azione di prevenzione garantisce che venga bloccata l'esecuzione di tutti i rilevamenti del problema per i piani di protezione selezionati.
   - **Applica patch al workload**: Selezionare la casella di controllo per applicare la patch a qualsiasi software vulnerabile e per impedire agli attaccanti di riuscire ad accedere al workload. È quindi possibile selezionare l'azione pertinente da eseguire una volta completata l'applicazione della patch (**Non riavviare**, **Riavvia** o **Riavvia solo se necessario**), a seconda che l'utente sia connesso o meno.
     È inoltre possibile selezionare la casella di controllo **Non riavviare mentre il backup è in corso** per accertarsi che il workload non venga riavviato se è in corso un backup.

© Acronis International GmbH, 2003-2024

7. Selezionare la casella di controllo **Modifica lo stato dell'indagine sul problema in: Chiuso**. Se non selezionata, lo stato dell'indagine permane nello stato precedente.
8. Fare clic su **Correggi**. Le azioni correttive selezionate vengono eseguite passo dopo passo, e l'avanzamento di ogni passo viene visualizzato nella finestra di dialogo Correggi intero problema. Sul pulsante verrà visualizzata l'opzione **Passa alle attività**. Fare clic su **Passa alle attività** per rivedere le azioni di risposta applicate al problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Correggere un problema falso positivo

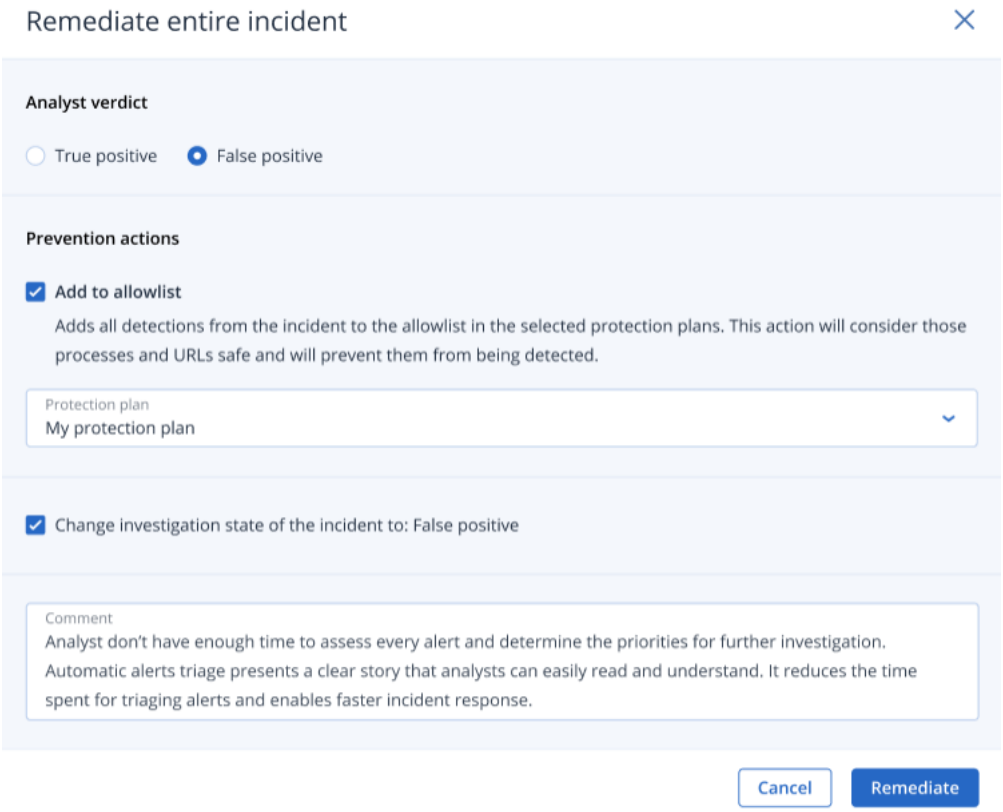
Se si è certi che un attacco non è autenticamente tale (se, in altre parole, si tratta di un falso positivo), è possibile definire come evitare che il problema si verifichi di nuovo. Ad esempio, è possibile aggiungere il problema a un elenco degli elementi consentiti del piano di protezione.

Per correggere un problema falso positivo

1. Nella sequenza dell'attacco informatico del problema selezionato, fare clic su **Correggi intero problema**. Viene visualizzata la finestra di dialogo Correggi intero problema.

© Acronis International GmbH, 2003-2024

2. Nella sezione **Risultato dell'analisi**, selezionare **Falso positivo**.



3. Nella sezione **Azioni di prevenzione**, selezionare la casella di controllo **Aggiungi all'elenco degli elementi consentiti**. Nell'elenco del piano di protezione visualizzato, selezionare i piani di protezione pertinenti.
   Questa azione di prevenzione evita che venga rilevato il problema per i piani di protezione selezionati.
4. Selezionare la casella di controllo **Modifica lo stato dell'indagine sul problema in: Falso positivo**.
5. Fare clic su **Correggi**.
   Sul pulsante verrà visualizzata l'opzione **Passa alle attività**. Fare clic su **Passa alle attività** per rivedere tutte le azioni di risposta applicate al problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Azioni di risposta per singoli nodi della sequenza di attacco informatico

Se occorre gestire il problema con un maggiore livello di dettaglio, è possibile applicare varie azioni di risposta sui singoli punti della sequenza di attacco. Queste azioni di risposta consentono di correggere con semplicità e facilità qualsiasi nodo.

Nota
Per applicare le azioni di risposta globali all'intero problema, vedere "Correggere un intero problema" (pag. 944).

© Acronis International GmbH, 2003-2024

Le azioni di risposta si suddividono nelle seguenti categorie, sebbene non tutti i nodi includano tutte le categorie seguenti:

- **Correggi**: Le azioni di questa categoria consentono di applicare una risposta immediata all'attacco e prevedono la gestione dell'isolamento della rete per un workload e l'eliminazione della quarantena per file, processi e valori del registro di sistema.
- **Indaga**: Le azioni di questa categoria (applicabile solo ai workload) consentono di eseguire un backup forense o una connessione desktop remoto, per eseguire indagini più approfondite.
- **Indaga**: Le azioni di questa categoria (applicabile solo ai workload) consentono di eseguire una connessione desktop remoto, per eseguire indagini più approfondite.
- **Ripristino**: Le azioni di questa categoria (applicabile solo ai workload) consentono di rispondere a un attacco massiccio avviando un ripristino da un backup o un failover di disaster recovery.
- **Previeni**: Le azioni di questa categoria consentono di prevenire minacce future o falsi positivi aggiungendole all'elenco degli elementi consentiti o all'elenco degli elementi bloccati di un piano di protezione.

Nota
Se un problema è chiuso, non è possibile applicare un'azione di risposta a un nodo. È possibile tuttavia riaprire un problema chiuso modificando lo stato dell'indagine su **Indagine in corso**. Una volta riaperto il problema, sarà possibile applicare le azioni di risposta.

La tabella seguente descrive ogni tipo di nodo nella sequenza di attacco, le categorie applicabili a ciascun nodo e le azioni di risposta disponibili.

Nodo	Categoria	Azioni di risposta
Workload	Correggi	• Gestisci isolamento della rete • Riavvia workload
	Indaga	• Backup con dati forensi • Connessione al desktop remoto
	Indaga	• Connessione al desktop remoto
	Ripristino	• Ripristino da backup • Failover di disaster

© Acronis International GmbH, 2003-2024

Nodo	Categoria	Azioni di risposta
		recovery
	Previeni	• Patch
Processo	Correggi	• Arresta processo • Quarantena
	Previeni	• Aggiungi all'elenco degli elementi consentiti • Aggiungi alla lista degli elementi bloccati
File	Correggi	• Elimina • Quarantena
	Previeni	• Aggiungi all'elenco degli elementi consentiti • Aggiungi alla lista degli elementi bloccati
Registro	Correggi	• Elimina
Network	Previeni	• Aggiungi all'elenco degli elementi consentiti • Aggiungi alla lista degli elementi bloccati

Definire le azioni di risposta per un workload interessato

Come parte della risposta a un attacco, è possibile applicare le azioni seguenti ai workload interessati:

© Acronis International GmbH, 2003-2024

- **Gestisci isolamento della rete**: Consente di gestire l'isolamento della rete di un workload per arrestare attività di movimento laterale o di comando e controllo. Per ulteriori informazioni, consultare "Gestire l'isolamento della rete di un workload" (pag. 952).
- **Patch**: Consente di applicare una patch a un workload per prevenire che le vulnerabilità vengano sfruttate per potenziali attacchi futuri. Per ulteriori informazioni, consultare "Applicare una patch a un workload" (pag. 956).
- **Riavvia workload**: Consente di riavviare immediatamente un workload o di riavviarlo in base a un periodo di timeout predefinito. Per ulteriori informazioni, consultare "Riavvia un workload" (pag. 957).
- **Backup con dati forensi**: Consente di eseguire un backup forense su richiesta per finalità di audit o per indagini approfondite. Per ulteriori informazioni, consultare "Eseguire un backup forense su richiesta su un workload" (pag. 959).
- **Connessione al desktop remoto**: Consente di accedere da remoto al workload su cui sono in corso le indagini. Per ulteriori informazioni, consultare "Connessione remota a un workload" (pag. 960).
- **Ripristina da backup**: Consente di ripristinare dal backup l'intero sistema oppure specifici file e cartelle. Per ulteriori informazioni, consultare "Ripristino da backup" (pag. 960).
- **Failover di disaster recovery**: Consente di eseguire "Implementazione del disaster recovery" (pag. 749). Si noti che il workload deve disporre di un abbonamento ad Advanced Disaster Recovery. Per ulteriori informazioni, consultare "Failover di disaster recovery" (pag. 961).

Gestire l'isolamento della rete di un workload

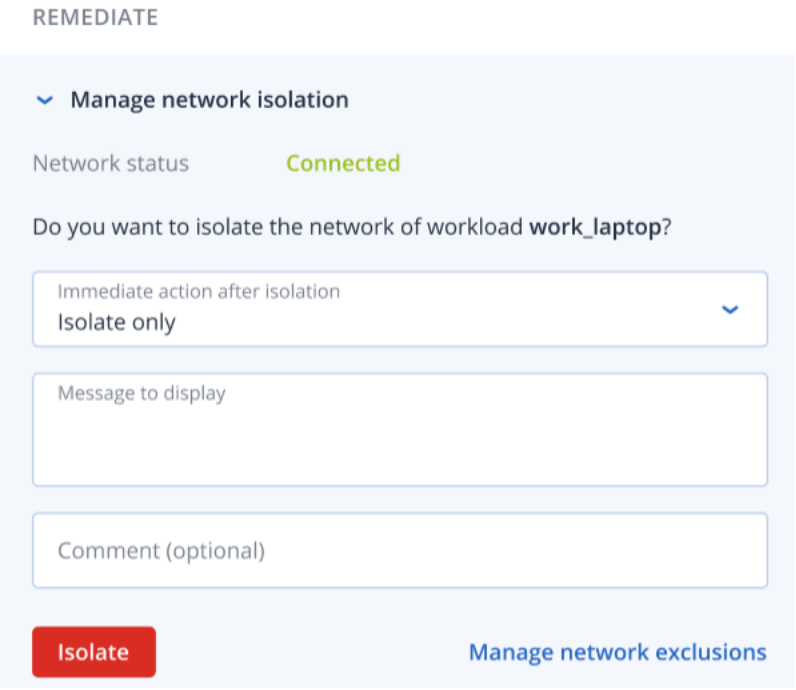
EDR consente di gestire l'isolamento della rete di un workload per arrestare attività di movimento laterale o di comando e controllo. È possibile scegliere tra numerose opzioni di isolamento, in base alle proprie esigenze. Tenere presente che tutte le tecnologie di Acronis Cyber Protect sono in funzione anche se un workload è isolato, garantendo in ogni caso il completamento dell'indagine.

Per isolare un workload dalla rete

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del workload da correggere.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.

© Acronis International GmbH, 2003-2024

3. Nella sezione **Correggi**, fare clic su **Gestisci isolamento della rete**.



Nota
Il valore **Stato della rete** indica se il workload è attualmente connesso o meno. Se il valore visualizzato è **Isolato**, è possibile riconnettere il workload isolato alla rete, come descritto nella procedura seguente. È possibile isolare il workload anche se è offline; non appena torna online viene automaticamente impostato sullo stato **Isolato**.

4. Nell'elenco a discesa **Azione immediata dopo l'isolamento**, selezionare un'opzione tra:
   - **Isola solo**
   - **Isola ed esegui il backup del workload**
   - **Isola ed esegui il backup con dati forensi del workload**
   - **Isola e disattiva il workload**

   Per ulteriori informazioni su come definire la posizione di backup del workload e le opzioni di crittografia, consultare "Gestione del backup e del ripristino di workload e file" (pag. 404).
5. [Facoltativo] Nel campo **Messaggio da visualizzare**, aggiungere un messaggio da visualizzare agli utenti finali che accedono al workload isolato. È ad esempio possibile informare gli utenti che il workload è isolato al momento e che l'accesso dalla rete da e verso il workload non è al momento disponibile. Tenere presente che questo messaggio viene visualizzato anche come notifica in Tray monitor, e resta visualizzato fino a quando gli utenti non chiudono il messaggio.
6. [Facoltativo] Nel campo **Commento**, aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.

© Acronis International GmbH, 2003-2024

7. Fare clic su **Gestisci esclusioni di rete** per aggiungere porte, URL, nomi host e indirizzi IP che potranno accedere al workload durante l'isolamento. Per ulteriori informazioni, consultare la sezione Gestione delle esclusioni di rete.
8. Fare clic su **Isola**.
   Il workload è isolato. Questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

   Nota
   Il workload viene mostrato come **Isolato** anche nel menu **Workload** nella console di Cyber Protect. È possibile isolare singoli o più workload nel menu **Workload > Workload con agenti**; selezionare i workload necessari e nella barra laterale destra selezionare **Gestisci isolamento della rete**. Nella finestra visualizzata, è possibile gestire le esclusioni dalla rete e fare clic su **Isola** o su **Isola tutti** per isolare i workload selezionati.

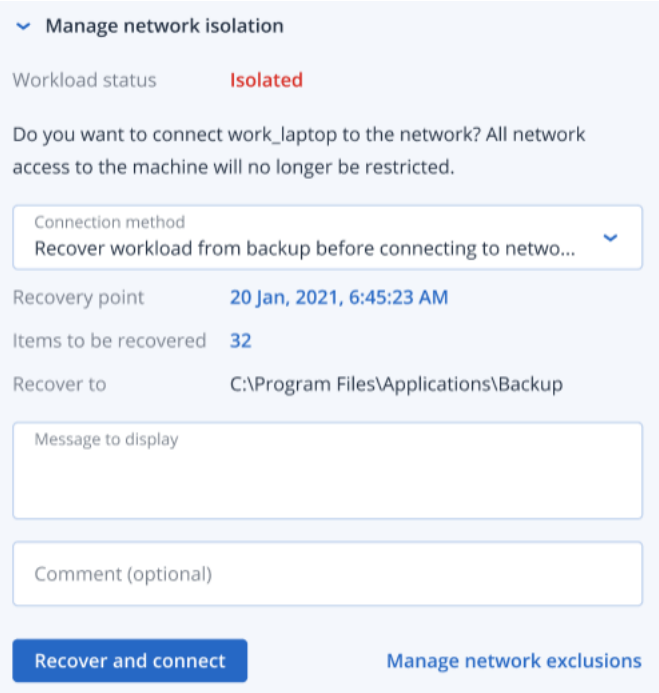
Per riconnettere un workload isolato alla rete

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del workload a cui riconnettersi.

   Nota
   Se il workload isolato è attualmente offline è possibile comunque riconnetterlo alla rete; non appena torna online viene automaticamente impostato sullo stato **Connesso**.

2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Correggi**, fare clic su **Gestisci isolamento della rete**.
4. Selezionare una delle seguenti opzioni:
   - **Connetti immediatamente alla rete**: Il workload viene riconnesso alla rete.
   - **Ripristina il workload dal backup prima di connetterlo alla rete**: Selezionare un punto di ripristino dal quale ripristinare il workload.
     a. Nel campo **Punto di ripristino**, fare clic su **Seleziona**.
     b. Nella barra laterale visualizzata, selezionare il punto di ripristino pertinente.
     c. Fare clic su **Ripristina > Intero workload** per ripristinare tutti i file e le cartelle nel workload.
        Oppure
        Fare clic su **Ripristina > File/cartelle** per ripristinare file e cartelle specifici nel workload. Il sistema chiede di selezionare i file o le cartelle pertinenti. Completata la selezione, è possibile visualizzare l'elenco degli elementi selezionati facendo clic sul valore pertinente nel campo **Elementi da ripristinare**.

© Acronis International GmbH, 2003-2024



Nota
Se il punto di ripristino selezionato è crittografato, il sistema chiede di inserire la password.

5. [Facoltativo] Selezionare la casella di controllo **Riavvia il workload automaticamente, se necessario**. Questa opzione è pertinente solo se al passaggio 4 è stato selezionato **Ripristina > Intero workload**.
6. [Facoltativo] Nel campo **Messaggio da visualizzare**, aggiungere un messaggio da visualizzare agli utenti finali che accedono al workload connesso. È ad esempio possibile informare gli utenti che il backup è stato ripristinato nel workload e che l'accesso dalla rete da e verso il workload è di nuovo disponibile.
7. [Facoltativo] Nel campo **Commento**, aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
8. Fare clic su **Connettere** se al Passaggio 4 è stata selezionata l'opzione **Connetti immediatamente alla rete**.
   Oppure
   Fare clic su **Ripristina e connetti** se nel Passaggio 4 è stata selezionata l'opzione **Ripristina il workload dal backup prima di connetterlo alla rete**.
   Il workload viene riconnesso alla rete ed è possibile accedere al workload dalla rete senza alcuna limitazione.

© Acronis International GmbH, 2003-2024

Nota
È anche possibile connettere singoli o più workload isolati nel menu **Workload > Workload con agenti** nella console di Cyber Protect; selezionare i workload necessari e nella barra laterale destra selezionare **Gestisci isolamento della rete**. Nella finestra di dialogo selezionata, fare clic su **Connettere** oppure su **Connetti tutto** per riconnettere i workload selezionati alla rete.

Per gestire le esclusioni di rete

Nota
Anche se tutte le tecnologie di Acronis Cyber Protect sono in funzione quando il workload è in isolamento, possono presentarsi scenari in cui è necessario stabilire ulteriori connessioni di rete (ad esempio, può essere necessario caricare un file dal workload a una directory condivisa). In questi casi è possibile aggiungere un'esclusione di rete, ma occorre accertarsi che ogni minaccia venga rimossa prima di aggiungere l'esclusione.

1. Nella sezione **Correggi** della scheda **Azioni di risposta**, fare clic su **Gestisci esclusioni di rete**.
2. Nella barra laterale Esclusioni di rete, aggiungere le esclusioni pertinenti. Per ognuna delle opzioni disponibili (porte, indirizzi URL, nome host, indirizzo IP), procedere come segue:
   a. Fare clic su **Aggiungi** e quindi inserire le porte, gli indirizzi URL, i nomi host o gli indirizzi IP pertinenti.
   b. Nell'elenco a discesa **Direzione del traffico**, selezionare un'opzione tra **Connessioni in entrata e in uscita**, **Solo connessioni in entrata** oppure **Solo connessioni in uscita**.
   c. Fare clic su **Aggiungi**.
3. Fare clic su **Salva**.

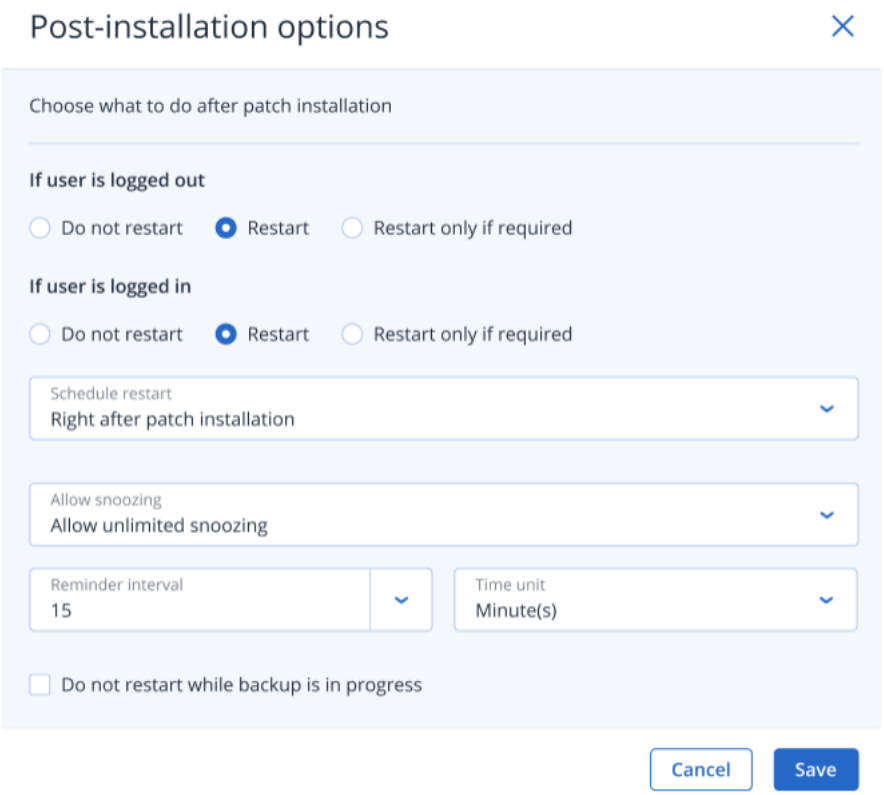
Applicare una patch a un workload

EDR rileva automaticamente la necessità di applicare una patch a un workload, permettendo di installarla per prevenire che le vulnerabilità vengano sfruttate per potenziali attacchi futuri. Questa funzionalità è disponibile solo se al workload del Partner è associato un abbonamento Advanced Management.

Per applicare una patch a un workload

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del workload a cui applicare la patch.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Correggi**, fare clic su **Patch**.
4. Nel campo **Patch da installare**, fare clic su **Seleziona**. Nella finestra di dialogo visualizzata, selezionare le patch rilevanti e quindi fare clic su **Seleziona**.
5. Nel campo **Opzioni post-installazione** fare clic sul link visualizzato. Viene visualizzata la finestra di dialogo Opzioni post-installazione.

© Acronis International GmbH, 2003-2024



6. Selezionare l'azione da eseguire dopo aver installato la patch:
   - **Se l'utente è disconnesso**: Selezionare un'opzione tra **Non riavviare**, **Riavvia** o **Riavvia solo se richiesto**.
   - **Se l'utente è connesso**: Selezionare un'opzione tra **Non riavviare**, **Riavvia** o **Riavvia solo se richiesto**.
     Se si seleziona **Riavvia**, è possibile definire anche le attività seguenti:
     - Pianificare il riavvio.
     - Consentire il posticipo e definire gli intervalli tra i posticipi.
7. [Facoltativo] Selezionare la casella di controllo **Non riavviare mentre il backup è in corso** per accertarsi che il workload non venga riavviato se è in corso un backup.
8. Fare clic su **Salva**.
9. Nella scheda **Azioni di risposta**, fare clic su **Patch**.
   La patch selezionata viene eseguita. Questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

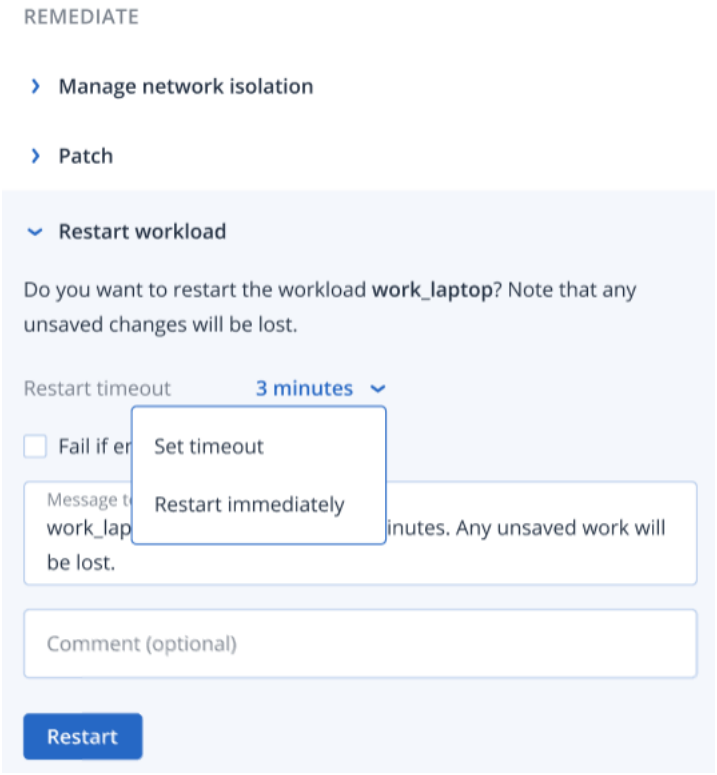
Riavvia un workload

Come parte della risposta correttiva a un attacco, EDR consente di riavviare immediatamente un workload o di riavviarlo in base a un periodo di timeout predefinito.

Per riavviare un workload

© Acronis International GmbH, 2003-2024

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del workload per il quale impostare un riavvio pianificato.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Correggi**, fare clic su **Riavvia workload**.



4. Fare clic sul campo **Riavvia timeout**, fare clic sul link visualizzato e selezionare una delle seguenti opzioni:
   - **Imposta timeout**: Nella finestra di dialogo Riavvia timeout, impostare il periodo di riavvio del workload, quindi fare clic su **Salva**.
   - **Riavvia immediatamente**: Selezionare questa opzione per riavviare il workload immediatamente.
5. [Facoltativo] Selezionare la casella di controllo **Non riesce se l'utente finale è connesso** per accertarsi che il workload non venga riavviato se l'utente è connesso.
6. Nel campo **Messaggio da visualizzare**, aggiungere un messaggio da visualizzare agli utenti che accedono al workload isolato.
7. [Facoltativo] Nel campo **Commento**, aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
8. Fare clic su **Riavvia**.
   Il workload è impostato per essere riavviato in base alla pianificazione stabilita. Questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

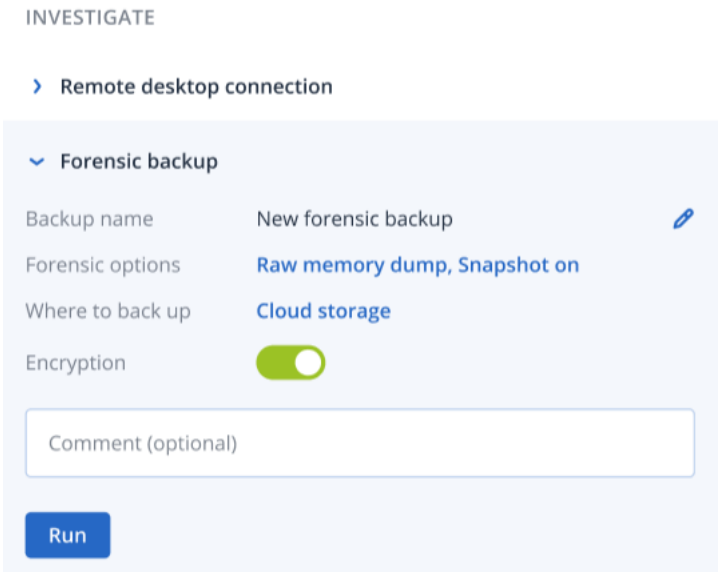
© Acronis International GmbH, 2003-2024

Eseguire un backup forense su richiesta su un workload

Come parte delle indagini relative a un attacco, EDR consente di eseguire un backup forense su richiesta per finalità di audit o per indagini approfondite. Questa funzionalità è disponibile solo se al workload del Partner è associato un abbonamento Advanced Backup.

Per eseguire un backup forense

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del workload per il quale eseguire un backup forense.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Indaga**, fare clic su **Backup con dati forensi**.



4. [Facoltativo] Nel campo **Nome backup**, fare clic sull'icona di modifica per modificare il nome del backup.
5. Nel campo **Opzioni forensi**, fare clic sul link visualizzato. Nella finestra di dialogo Opzioni forensi, selezionare una delle seguenti opzioni:
   - **Raccogli dump della memoria raw**
   - **Raccogli dump della memoria kernel**

   È anche possibile selezionare la casella di controllo **Snapshot dei processi in esecuzione** per aggiungere informazioni sui processi in esecuzione al momento dell'avvio del backup. Queste informazioni sono archiviate in un'immagine di backup.

   Fare clic su **Salva** per chiudere la finestra di dialogo Opzioni forensi.
6. Nel campo **Dove eseguire il backup**, fare clic sul link visualizzato per definire una posizione per il backup.
7. [Facoltativo] Fare clic sull'opzione **Crittografia** per abilitare la crittografia. Nella finestra di dialogo visualizzata, modificare la password per il backup crittografato e selezionare l'algoritmo di crittografia pertinente.

© Acronis International GmbH, 2003-2024

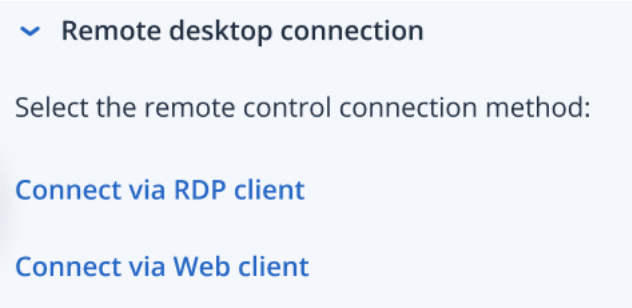
8. [Facoltativo] Nel campo **Commento**, aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
9. Fare clic su **Esegui**.
   Il backup forense viene avviato. Questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Connessione remota a un workload

Come parte dell'attività di ricerca dopo un attacco, EDR consente di accedere da remoto al workload su cui sono in corso le indagini.

Per connettersi da remoto a un workload

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del workload a cui connettersi da remoto.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Indaga**, fare clic su **Connessione desktop remoto**.



4. Selezionare uno dei seguenti metodi di connessione remota:
   - **Connessione tramite client RDP**: Questo metodo richiede di scaricare e installare il client di Connessione desktop remoto. A questo punto sarà possibile connettersi da remoto a un workload dalla console di Cyber Protect.
   - **Connessione tramite client web**: Questo metodo non richiede l'installazione di un client RDP nel workload. L'utente verrà reindirizzato alla schermata di accesso, dove dovrà inserire le proprie credenziali per accedere al sistema remoto.

   Una volta avviata la connessione remota, questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

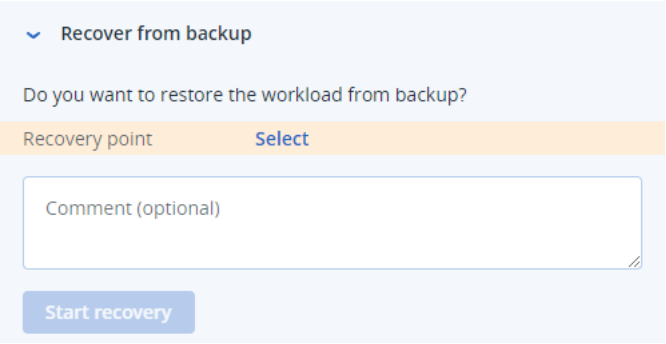
Ripristino da backup

Come parte dell'attività di ripristino dopo un attacco, EDR consente di ripristinare dal backup l'intero sistema oppure specifici file e cartelle.

Per ripristinare il workload dal backup

© Acronis International GmbH, 2003-2024

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del workload da ripristinare.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Ripristino**, fare clic su **Ripristina da backup**.



4. Nel campo **Punto di ripristino**, fare clic su **Seleziona** e quindi procedere come segue:
   a. Nella barra laterale visualizzata, selezionare il punto di ripristino pertinente.
   b. Fare clic su **Ripristina > Intero workload** per ripristinare tutti i file e le cartelle nel workload.
   Oppure
   Fare clic su **Ripristina > File/cartelle** per ripristinare file e cartelle specifici nel workload. Il sistema chiede di selezionare i file o le cartelle pertinenti. Completata la selezione, è possibile visualizzare gli elementi selezionati per il ripristino facendo clic sul valore pertinente nel campo **Elementi da ripristinare**.

   Nota
   Se il punto di ripristino selezionato è crittografato, il sistema chiede di inserire la password.

5. [Facoltativo] Selezionare la casella di controllo **Riavvia il workload automaticamente**. Questa opzione è pertinente solo se al passaggio 4 è stato selezionato **Ripristina > Intero workload**.
6. [Facoltativo] Nel campo **Commento**, aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
7. Fare clic su **Avvia ripristino**.
   Il processo di ripristino del workload si avvia. L'avanzamento dell'operazione può essere visualizzato nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

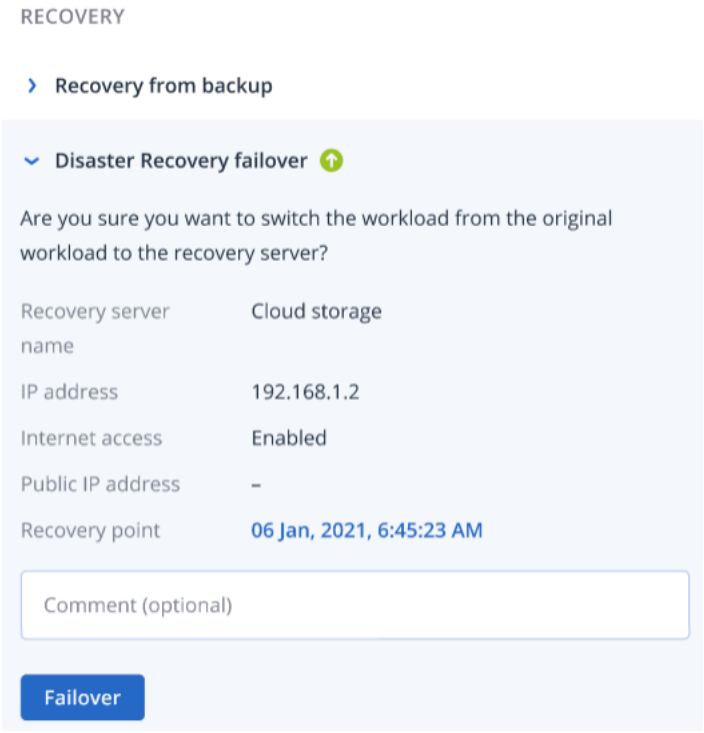
Failover di disaster recovery

Come parte dell'attività di ripristino dopo un attacco, EDR consente di eseguire "Implementazione del disaster recovery" (pag. 749) per trasferire il workload al server di ripristino. Si noti che il workload deve disporre di un abbonamento ad Advanced Disaster Recovery.

Per eseguire un failover di disaster recovery

© Acronis International GmbH, 2003-2024

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del workload da ripristinare.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Ripristino**, fare clic su **Failover di disaster recovery**.



4. Nel campo **Punto di ripristino**, procedere come segue:
   a. Fare clic sulla data del punto di ripristino corrente per selezionare un punto di ripristino.
   b. Nella barra laterale visualizzata, selezionare il punto di ripristino pertinente.

   Nota
   Se si dispone di un abbonamento Advanced Disaster Recovery, è possibile selezionare il server di ripristino pertinente (VM offline) creato in Disaster Recovery. Se non si dispone di un abbonamento, il sistema chiede di configurare il Disaster Recovery.

5. [Facoltativo] Nel campo **Commento**, aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
6. Fare clic su **Failover**.
   Il workload viene trasferito al server di ripristino. Questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Definire le azioni di risposta per un processo sospetto

Come parte della risposta di correzione a un attacco, è possibile applicare le azioni seguenti ai processi sospetti:

© Acronis International GmbH, 2003-2024

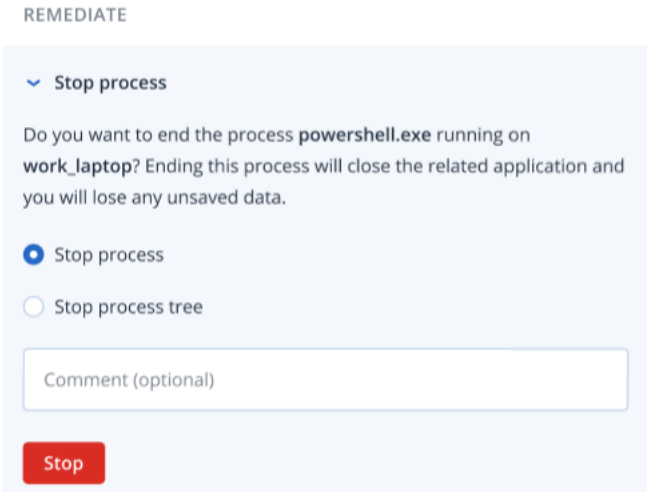
- Arrestare un processo (vedere di seguito)
- Mettere in quarantena un processo (vedere di seguito)
- Eseguire il rollback delle modifiche apportate da un processo (vedere di seguito)
- Aggiungere il processo a un elenco degli elementi consentiti o a un elenco degli elementi bloccati del piano di protezione (vedere "Aggiungere o rimuovere un processo, un file o una rete nell'elenco degli elementi consentiti o nell'elenco degli elementi bloccati del piano di protezione" (pag. 968))

Per arrestare un processo sospetto

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del processo da correggere.

   Nota
   I processi critici di Windows o i processi non in esecuzione non possono essere arrestati e vengono disabilitati nella sequenza dell'attacco informatico.

2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Correggi**, fare clic su **Arresta processo**.



4. Selezionare una delle seguenti opzioni:
   - **Arresta processo** (arresta il processo specifico)
   - **Arresta struttura processo** (arresta il processo specifico e tutti i processi figlio)
5. [Facoltativo] Aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
6. Fare clic su **Arresta**. Il processo viene arrestato.

   Nota
   L'applicazione correlata viene chiusa e tutti i dati non salvati andranno perduti.

© Acronis International GmbH, 2003-2024

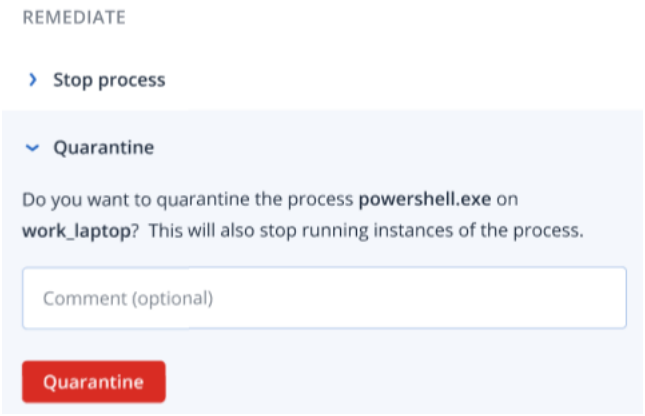
Questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Per mettere in quarantena un processo sospetto

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del processo da mettere in quarantena.

   Nota
   I processi critici di Windows non possono essere messi in quarantena e vengono disabilitati nella sequenza dell'attacco informatico.

2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Correggi**, fare clic su **Quarantena**.



4. [Facoltativo] Aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
5. Fare clic su **Quarantena**. Il processo viene arrestato e messo in quarantena.

   Nota
   Il processo viene aggiunto e gestito nella sezione della quarantena disponibile in Protezione anti-malware.

   Questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

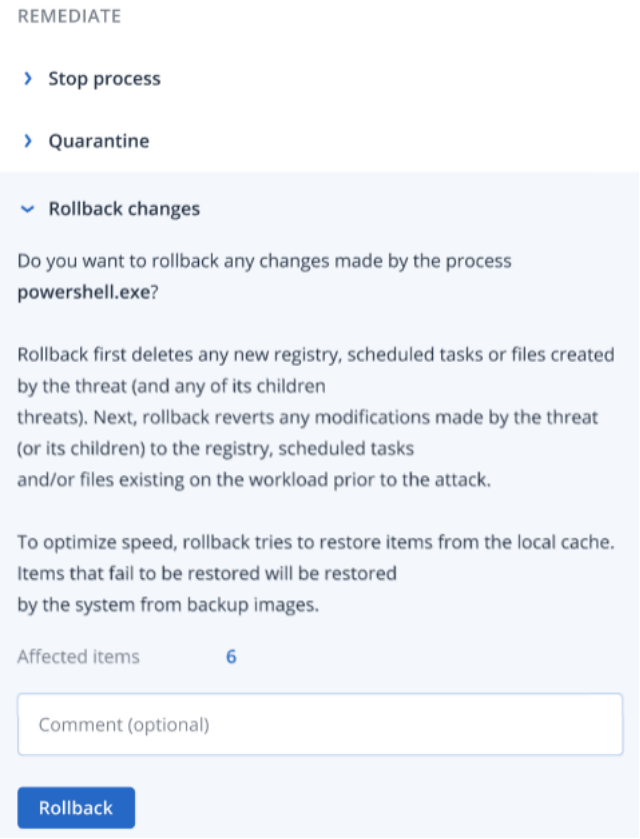
Per eseguire il rollback delle modifiche

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del processo per il quale eseguire il rollback delle modifiche.

© Acronis International GmbH, 2003-2024

Nota
Questa azione è disponibile solo per i nodi di rilevamento (mostrati come nodi rossi o gialli).

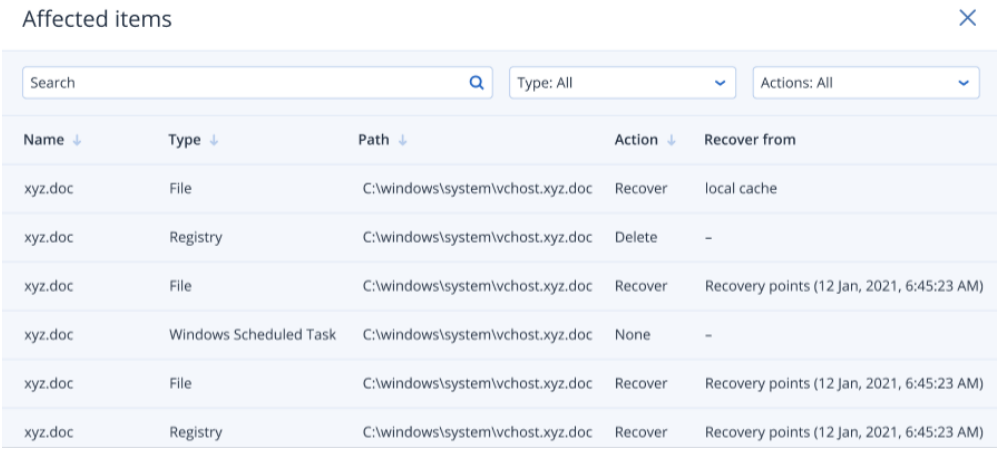
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Correggi**, fare clic su **Rollback modifiche**.



Nota
Il processo di rollback esegue il recupero solo dagli elementi presenti nella cache locale. Il rollback dagli archivi di backup sarà disponibile nelle release future.

4. Per visualizzare gli elementi interessati dal rollback delle modifiche, fare clic sul link **Elementi interessati**. La finestra di dialogo visualizzata mostra tutti gli elementi (file, Registro di sistema, attività pianificate) che verranno ripristinati dal rollback e con quale azione (**Elimina**, **Ripristina** oppure **Nessuna**). Inoltre, è possibile visualizzare se gli elementi ripristinati vengono recuperati dalla cache locale o dai punti di ripristino del backup.

© Acronis International GmbH, 2003-2024



5. [Facoltativo] Aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
6. Fare clic su **Rollback**. La funzionalità di rollback ripristina qualsiasi modifica al Registro di sistema, a file o attività pianificate apportata dal processo, applicando i passaggi seguenti:
   a. Viene eliminata qualsiasi nuova voce (Registro di sistema, attività pianificate o file) creata dalla minaccia e da qualsiasi minaccia figlio correlata.
   b. Viene ripristinata qualsiasi modifica apportata dalla minaccia (o dai suoi figli) al Registro di sistema, alle attività pianificate e/o a file esistenti nel workload prima dell'attacco.
   c. Il rollback tenta di recuperare gli elementi dalla cache locale. Gli elementi che non possono essere recuperati vengono automaticamente ripristinati da EDR da immagini di backup pulite.

   L'azione di rollback può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Definire le azioni di risposta per un file sospetto

Come parte della risposta di correzione a un attacco, è possibile applicare le azioni seguenti ai file sospetti:

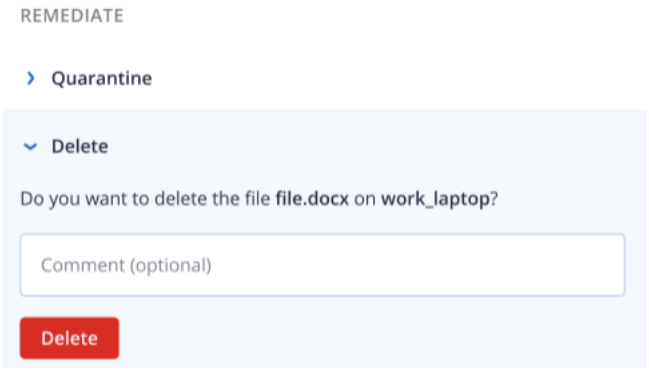
- Eliminare un file (vedere di seguito)
- Mettere in quarantena un file (vedere di seguito)
- Aggiungere il file a un elenco degli elementi consentiti o a un elenco degli elementi bloccati del piano di protezione (vedere "Aggiungere o rimuovere un processo, un file o una rete nell'elenco degli elementi consentiti o nell'elenco degli elementi bloccati del piano di protezione" (pag. 968))

Per eliminare un file sospetto

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del file da correggere.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.

© Acronis International GmbH, 2003-2024

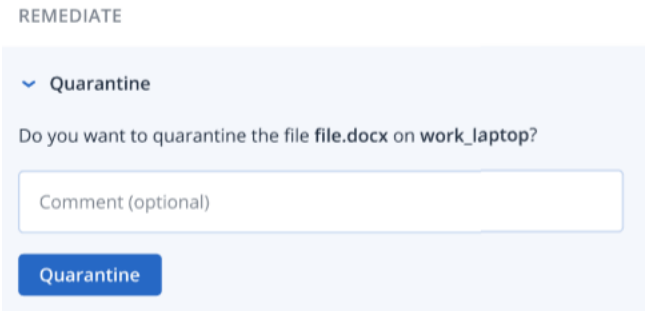
3. Nella sezione **Correggi**, fare clic su **Elimina**.



4. [Facoltativo] Aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
5. Fare clic su **Elimina**.
   Il file viene eliminato. Questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Per mettere in quarantena un file sospetto

1. Nella sequenza dell'attacco informatico, fare clic sul nodo del file da correggere.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Correggi**, fare clic su **Quarantena**.



4. [Facoltativo] Aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
5. Fare clic su **Quarantena**.
   Il file viene messo in quarantena. Questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

© Acronis International GmbH, 2003-2024

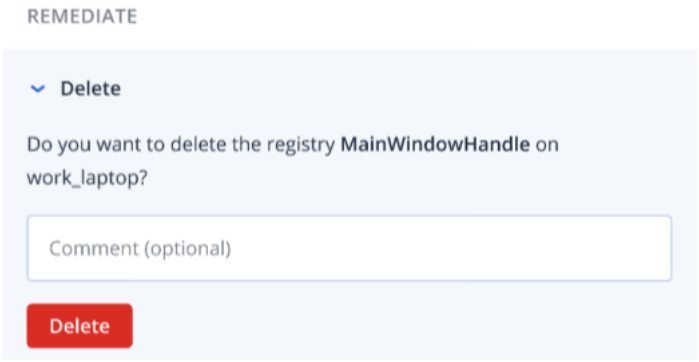
Definire le azioni di risposta per una voce del Registro di sistema sospetta

Come parte della risposta di correzione a un attacco, è possibile eliminare le voci del Registro di sistema sospette.

Questa opzione è disponibile per i nodi della sequenza dell'attacco relativi al Registro di sistema.

Per eliminare una voce del Registro di sistema sospetta

1. Nella sequenza dell'attacco informatico, fare clic sul nodo da correggere.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Correggi**, fare clic su **Elimina**.



4. [Facoltativo] Aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
5. Fare clic su **Elimina**.
   La voce del Registro di sistema viene eliminata. Questa azione può essere visualizzata nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Aggiungere o rimuovere un processo, un file o una rete nell'elenco degli elementi consentiti o nell'elenco degli elementi bloccati del piano di protezione

Come parte della risposta preventiva a un attacco, è possibile aggiungere un nodo allìelenco degli elementi consentiti o all'elenco degli elementi bloccati del piano di protezione.

Aggiungere un nodo a un elenco degli elementi consentiti se si considera il nodo sicuro e si vuole evitare che venga rilevato in futuro. Aggiungere un nodo a un elenco degli elementi bloccati per evitare che il nodo venga eseguito in futuro.

È inoltre possibile rimuovere un nodo dall'elenco degli elementi consentiti o dall'elenco degli elementi bloccati per consentire o impedire qualsiasi accesso futuro al nodo.

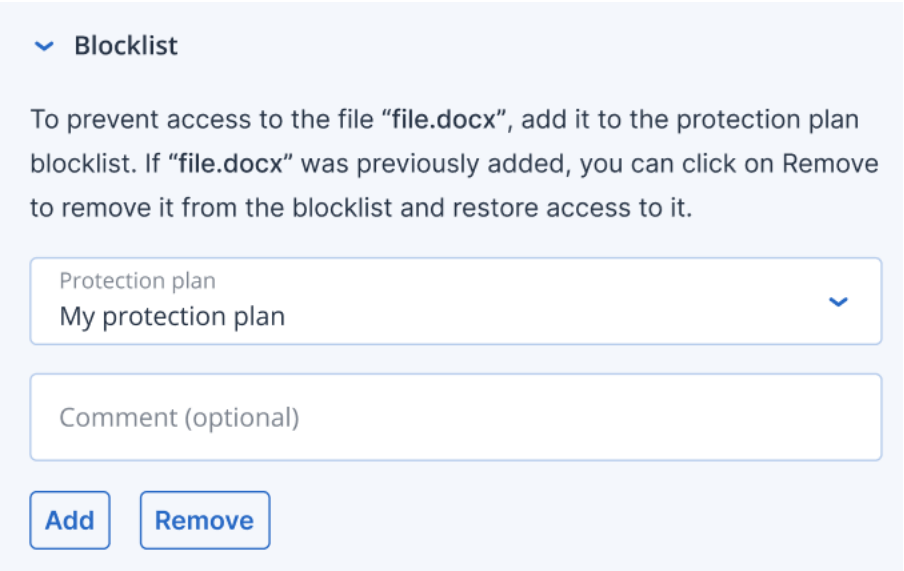
Questa opzione è disponibile per i seguenti nodi della sequenza dell'attacco informatico:

© Acronis International GmbH, 2003-2024

- Processo
- File
- Network

Per aggiungere o rimuovere un processo, un file o una rete nell'elenco degli elementi bloccati del piano di protezione

1. Nella sequenza dell'attacco informatico, fare clic sul processo, sul file o sul nodo di rete da correggere.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Previeni**, fare clic sull'icona freccia accanto a **elenco degli elementi bloccati**.

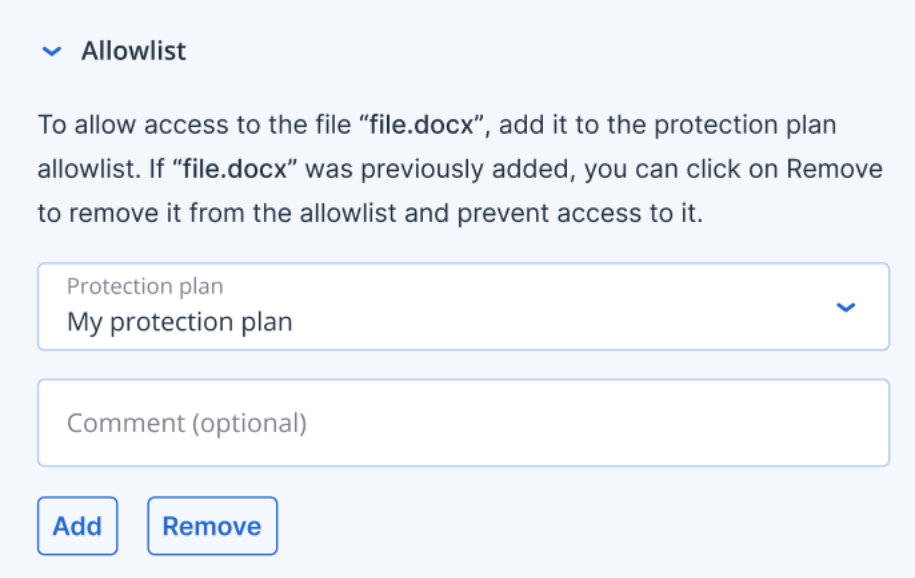


4. Selezionare il piano o i piani pertinenti a cui applicare l'azione selezionata.
5. [Facoltativo] Aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
6. Fare clic su **Aggiungi**.
   L'azione viene implementata e in futuro l'avvio del processo, del file o della rete verrà impedito.
   In alternativa, se il processo, il file o la rete erano stati precedentemente aggiunti all'elenco degli elementi bloccati e ora è necessario rimuoverli, fare clic su **Rimuovi**. In questo modo, l'accesso futuro al nodo verrà consentito.
   L'azione di aggiunta o rimozione può essere visualizzata anche nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Per aggiungere o rimuovere un processo, un file o una rete nell'elenco degli elementi consentiti del piano di protezione

© Acronis International GmbH, 2003-2024

1. Nella sequenza dell'attacco informatico, fare clic sul processo, sul file o sul nodo di rete da correggere.
2. Nella barra laterale visualizzata, fare clic sulla scheda **Azioni di risposta**.
3. Nella sezione **Previeni**, fare clic sull'icona freccia accanto a **Elenco degli elementi consentiti**.



4. Selezionare il piano o i piani pertinenti a cui applicare l'azione selezionata.
5. [Facoltativo] Aggiungere un commento. Questo commento è visibile nella scheda **Attività** (per un singolo nodo o per l'intero problema) e può essere di aiuto per ricordare perché una determinata azione è stata intrapresa se, in un secondo momento, è necessario rivedere il problema.
6. Fare clic su **Aggiungi**.
   L'azione viene implementata e in futuro l'avvio del processo, del file o della rete verrà impedito.
   In alternativa, se il processo, il file o la rete erano stati precedentemente aggiunti all'elenco degli elementi consentiti e ora è necessario rimuoverli, fare clic su **Rimuovi**. In questo modo, l'accesso futuro al nodo verrà impedito.
   L'azione di aggiunta o rimozione può essere visualizzata anche nelle schede **Attività** sia del singolo nodo che dell'intero problema. Per ulteriori informazioni, consultare "Comprendere le azioni intraprese per mitigare un problema" (pag. 937).

Abilitazione della modalità di monitoraggio per Endpoint Detection and Response (EDR)

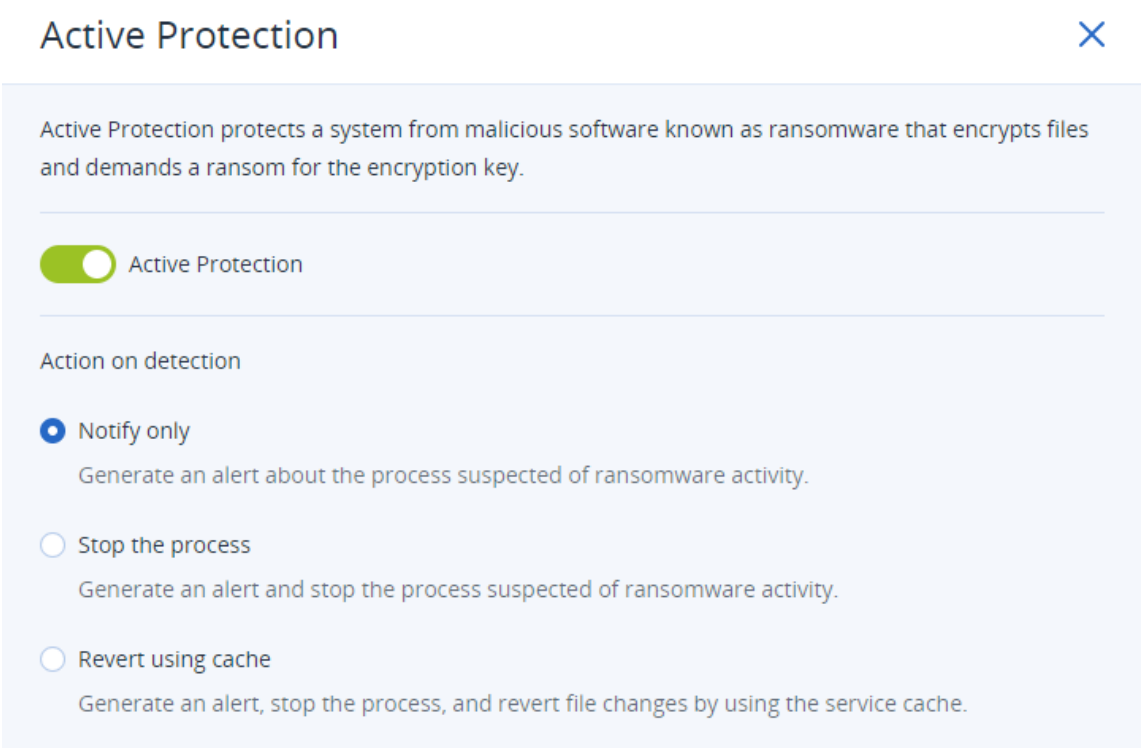
La modalità di monitoraggio in Cyber Protection consente di utilizzare EDR in un ambiente di produzione. In questo modo è possibile controllare la presenza di falsi positivi e di applicare le esclusioni necessarie prima di installare EDR su larga scala.

Nella modalità di monitoraggio, nessun elemento viene bloccato o fermato; vengono creati i problemi di sicurezza ma non vengono avviate azioni di risposta.

Per abilitare la modalità di monitoraggio per EDR

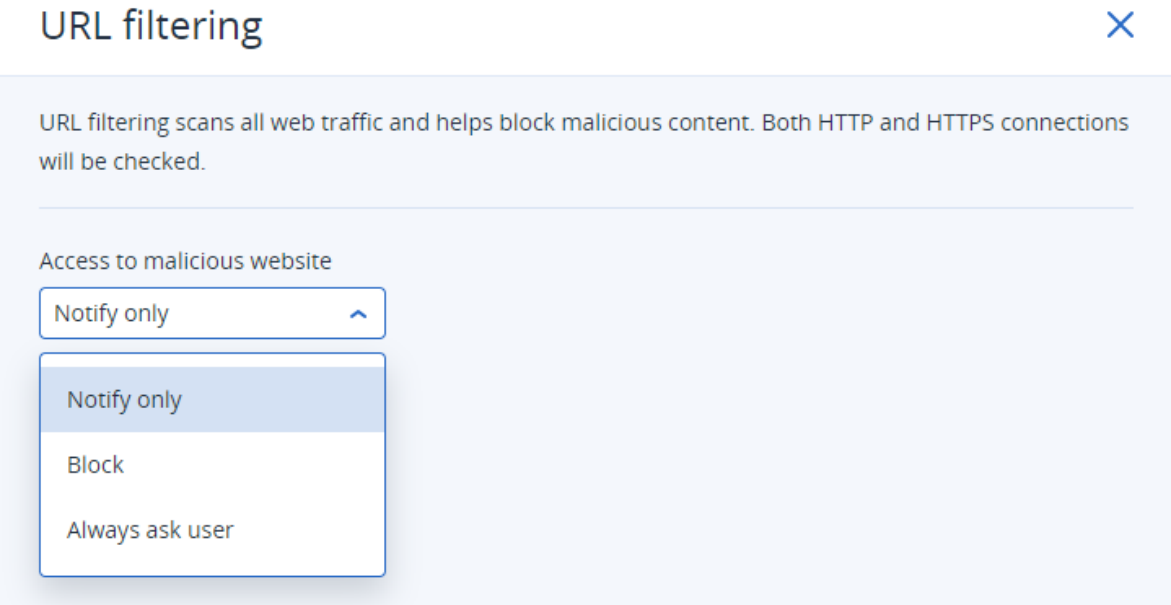
© Acronis International GmbH, 2003-2024

1. Nel piano di protezione pertinente, verificare che EDR sia abilitato. Per ulteriori informazioni, consultare "Abilitare la funzionalità Endpoint Detection and Response (EDR)" (pag. 918).
2. Espandere il modulo **Protezione antivirus e anti-malware** e definire quanto segue:
   - Fare clic su **Active Protection** e nella sezione **Azione al rilevamento** selezionare **Solo notifica**, quindi fare clic su **Fine**. Per ulteriori informazioni, consultare "Active Protection" (pag. 841).



   - Fare clic su **Motore comportamentale** e nella sezione **Azione al rilevamento** selezionare **Solo notifica**, quindi fare clic su **Fine**. Per ulteriori informazioni, consultare "Motore comportamentale" (pag. 846).
   - Fare clic su **Prevenzione degli exploit** e nella sezione **Azione al rilevamento** selezionare **Solo notifica**, quindi fare clic su **Fine**. Per ulteriori informazioni, consultare "Prevenzione degli exploit" (pag. 846).
   - Fare clic su **Protezione in tempo reale** e nella sezione **Azione al rilevamento** selezionare **Solo notifica**, quindi fare clic su **Fine**. Per ulteriori informazioni, consultare "Protezione in tempo reale" (pag. 848).
   - Fare clic su **Pianifica scansione** e nella sezione **Azione al rilevamento** selezionare **Solo notifica**, quindi fare clic su **Fine**. Per ulteriori informazioni, consultare "Pianifica scansione" (pag. 849).
3. Espandere il modulo **Filtro URL** e nell'elenco a discesa **Accesso ai siti web dannosi** selezionare **Solo notifica**, quindi fare clic su **Fine**. Per ulteriori informazioni, consultare "Filtro URL" (pag. 865).

© Acronis International GmbH, 2003-2024



Come verificare il corretto funzionamento della funzionalità Endpoint Detection and Response (EDR)

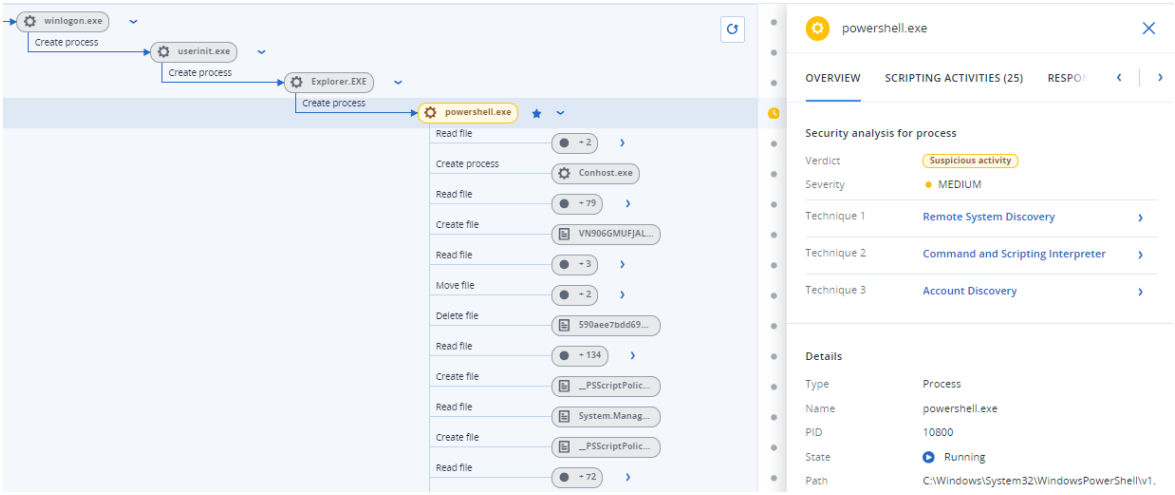
Per accertarsi che la funzionalità EDR sia stata correttamente installata e funzioni come previsto, è possibile eseguire alcuni comandi che attivano i rilevamenti EDR.

Nota
Dopo aver distribuito EDR, non appena si verifica un'attività sospetta il problema viene immediatamente visualizzato. I passaggi seguenti consentono di accertarsi che EDR sia in funzione nel caso in cui per diversi giorni non venga segnalato alcun nuovo problema.

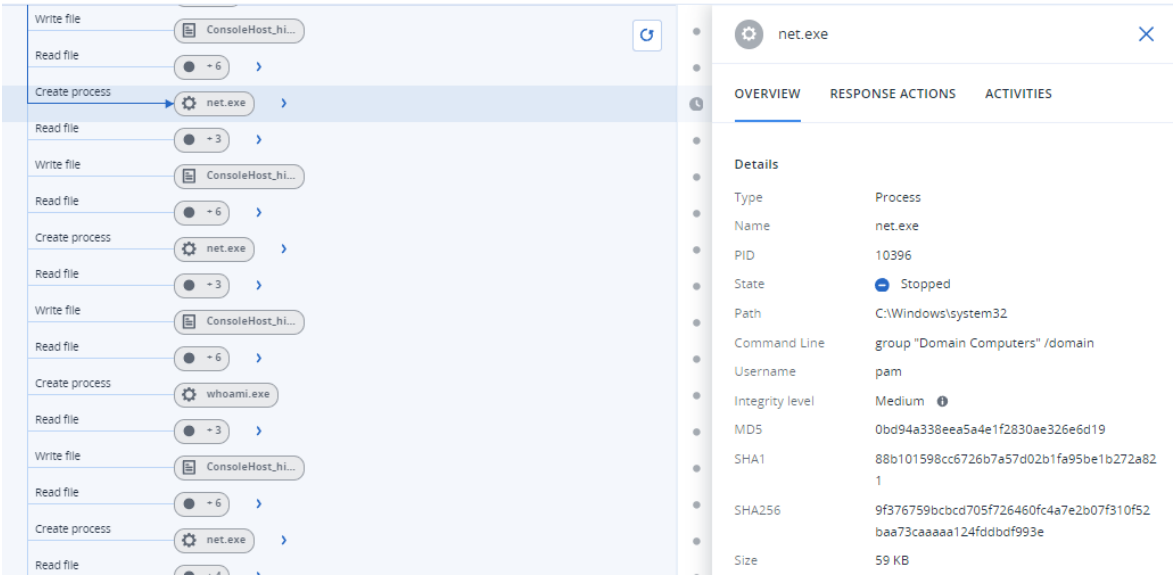
Per verificare che la funzionalità EDR sia correttamente installata e funzioni come previsto

1. Accedere all'account utente Active Directory nel dominio congiunto pertinente.
2. In Windows PowerShell, eseguire i due seguenti comandi:
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. Nella console di Cyber Protect, passare a **Protezione > Problemi** per visualizzare il problema generato.
   È inoltre possibile fare clic sul problema con livello di gravità **Medio** generato per visualizzarlo nella sequenza dell'attacco EDR e confermare i comandi PowerShell eseguiti al passaggio precedente, come mostrato nell'esempio seguente.

© Acronis International GmbH, 2003-2024



4. In Windows PowerShell, eseguire i seguenti comandi:
   - `c:\>whoami`
   - `c:\>net localgroup`
   - `c:\>net localgroup administrators`
   - `c:\>powershell -command start-process cmd -verb runas`
   - `c:\WINDOWS\system32>net user administrator /active:yes`
   - `c:\>powershell -command Get-Hotfix`
5. Nella sequenza dell'attacco EDR, fare clic sui nodi eseguibili (ad esempio **net.exe** o **whoami.exe**) per visualizzare i comandi PowerShell esatti eseguiti nella riga di comando. Tali comandi sono mostrati nella sezione **Dettagli** della scheda **Panoramica** nell'esempio seguente.



6. Dopo aver confermato l'attivazione di un problema EDR, impostare manualmente l'opzione **Stato minaccia** del problema su **Mitigato** e l'opzione **Stato indagine** su **Chiuso**. Per ulteriori informazioni, consultare "Come indagare sui problemi rilevati nella sequenza di attacco" (pag. 929). È anche possibile inserire un commento per segnalare che si tratta di un incidente di prova.

© Acronis International GmbH, 2003-2024

Valutazione delle vulnerabilità e gestione delle patch

Vulnerability assessment è il processo che consente di identificare, quantificare e assegnare la priorità alle vulnerabilità individuate nel sistema. Nel modulo Vulnerability Assessment è possibile scansionare i sistemi alla ricerca delle vulnerabilità e controllare che i sistemi operativi e le applicazioni installate siano aggiornati e funzionino in modo corretto.

La Valutazione delle vulnerabilità è supportata sui sistemi con i seguenti sistemi operativi:

- Windows. Per ulteriori informazioni, consultare "Prodotti Microsoft e prodotti di terze parti supportati" (pag. 975).
- macOS. Per ulteriori informazioni, consultare "Prodotti Apple e prodotti di terze parti supportati" (pag. 976).
- Sistemi Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Per ulteriori informazioni, consultare "Prodotti Linux supportati" (pag. 977).

Utilizzare la funzionalità di **Gestione patch** per gestire patch e aggiornamenti delle applicazioni e dei sistemi operativi installati nei sistemi e per mantenere i sistemi aggiornati. Nel modulo Gestione patch è possibile approvare in modo automatico o manuale l'installazione degli aggiornamenti sui sistemi.

Gestione patch è supportata sui sistemi con i seguenti sistemi operativi Windows. Per ulteriori informazioni, consultare "Prodotti Microsoft e prodotti di terze parti supportati" (pag. 975).

Valutazione delle vulnerabilità

Il processo di Valutazione delle vulnerabilità consiste dei passaggi seguenti:

1. Creare un piano di protezione nel quale sia abilitato il modulo di valutazione delle vulnerabilità, specificare le impostazioni di valutazione delle vulnerabilità e assegnare il piano ai sistemi.
2. Il sistema, in base alla pianificazione o su richiesta, invia il comando per l'esecuzione della scansione di valutazione delle vulnerabilità agli agenti di protezione installati nei sistemi.
3. Gli agenti ricevono il comando, avviano la scansione dei sistemi alla ricerca delle vulnerabilità e generano l'attività di scansione.
4. Dopo aver completato la scansione di valutazione delle vulnerabilità, gli agenti generano i risultati e li inviano al servizio di monitoraggio.
5. Il servizio di monitoraggio elabora i dati provenienti dagli agenti e mostra i risultati nei widget di valutazione della vulnerabilità, insieme all'elenco delle vulnerabilità individuate.
6. Quando si riceve l'elenco delle vulnerabilità individuate, è possibile elaborarlo e decidere se risolvere i problemi rilevati.

I risultati della scansione di valutazione delle vulnerabilità vengono visualizzati nel widget **Monitoraggio** > **Panoramica** > **Vulnerabilità/Vulnerabilità esistenti**.

© Acronis International GmbH, 2003-2024

Prodotti Microsoft e prodotti di terze parti supportati

Il vulnerability assessment e la gestione delle patch sono supportati nei seguenti prodotti Microsoft e prodotti di terze parti per sistemi operativi Windows:

Prodotti Microsoft supportati

Sistema operativo Windows

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Sistema operativo Windows Server

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office e componenti correlati

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Componenti correlati al sistema operativo Windows

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studio e Applications
- Componenti del sistema operativo

Applicazioni server

© Acronis International GmbH, 2003-2024

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019

Prodotti di terze parti supportati per i sistemi operativi Windows

L'aumentata diffusione del telelavoro nel mondo ha reso strategici strumenti di collaborazione e comunicazione e client VPN; è fondamentale che questi siano sempre aggiornati e monitorati per individuarne eventuali vulnerabilità. Il servizio Cyber Protection supporta le funzioni di valutazione delle vulnerabilità e gestione delle patch per queste applicazioni.

Strumenti di collaborazione e comunicazione, client VPN

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

Per ulteriori informazioni sui prodotti di terze parti supportati per i sistemi operativi Windows, fare riferimento a List of third-party products supported by Patch Management (62853) (in inglese).

Prodotti Apple e prodotti di terze parti supportati

La valutazione delle vulnerabilità è supportata nei seguenti prodotti Apple e prodotti di terze parti per macOS:

Prodotti Apple supportati

macOS

- macOS 10.13.x e versioni successive

© Acronis International GmbH, 2003-2024

applicazioni integrate macOS

- Safari, iTunes e altri.

Prodotti di terze parti supportati per macOS

- Microsoft Office (Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC Media Player

Prodotti Linux supportati

La valutazione delle vulnerabilità è supportata nelle seguenti distribuzioni e versioni Linux:

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

Impostazioni di Valutazione delle vulnerabilità

Per ulteriori informazioni su come creare un piano di protezione con il modulo Valutazione delle vulnerabilità, fare riferimento a "Creazione di un piano di protezione". La scansione delle vulnerabilità può essere eseguita in base a una pianificazione o su richiesta (utilizzando l'azione **Esegui ora** in un piano di protezione).

È possibile specificare le impostazioni seguenti per il modulo Valutazione delle vulnerabilità.

Elementi da scansionare

Definire gli elementi da scansionare alla ricerca di vulnerabilità.

- Sistemi Windows:
  - **Prodotti Microsoft**
  - **Prodotti di terze parti per Windows** (per ulteriori informazioni sui prodotti di terze parti supportati per i sistemi operativi Windows, fare riferimento a List of third-party products supported by Patch Management (62853) (in inglese))
- Sistemi MacOS:

© Acronis International GmbH, 2003-2024

- **Prodotti Apple**
- **Prodotti di terze parti per macOS**

- Sistemi Linux:
  - **Scansiona pacchetti Linux**

Pianificazione

Definire la pianificazione in base alla quale la scansione di valutazione delle vulnerabilità verrà eseguita nei sistemi selezionati:

Campo	Descrizione
Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito	Questa impostazione determina quando l'attività viene eseguita. Sono disponibili i seguenti valori: • **Pianificazione oraria**: questo è il valore predefinito. L'attività viene eseguita all'orario specificato. • **Quando l'utente accede al sistema**: per impostazione predefinita, l'accesso di qualsiasi utente determina l'avvio dell'attività. È possibile modificare questa impostazione in modo che solo un account utente specifico possa determinare l'attivazione dell'attività. • **Quando l'utente si disconnette dal sistema**: per impostazione predefinita, la disconnessione di qualsiasi utente determina l'avvio dell'attività. È possibile modificare questa impostazione in modo che solo un account utente specifico possa determinare l'attivazione dell'attività. **Nota** L'attività non verrà eseguita allo spegnimento del sistema. Nella configurazione della pianificazione, l'arresto del sistema e la disconnessione vanno considerate come azioni differenti. • **All'avvio del sistema** – L'attività viene eseguita all'avvio del sistema operativo. • **All'arresto del sistema** – L'attività viene eseguita all'arresto del sistema operativo.
Tipo di pianificazione	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria**. Sono disponibili i seguenti valori: • **Ogni mese** – Specificare il mese e le settimane o i giorni del mese in cui verrà eseguita l'attività. • **Ogni giorno**: questo è il valore predefinito. Specificare i giorni della settimana in cui verrà eseguita l'attività. • **Ogni ora** – Specificare i giorni della settimana, il numero di ripetizioni

© Acronis International GmbH, 2003-2024

Campo	Descrizione
	e l'intervallo temporale in cui verrà eseguita l'attività.
Ora di avvio	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria** Specificare l'ora esatta di avvio dell'attività.
Esegui entro un intervallo di date	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria**. Impostare un intervallo di validità della pianificazione configurata.
Specificare l'account utente il cui accesso al sistema operativo avvierà l'esecuzione dell'attività	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Quando l'utente accede al sistema**. Sono disponibili i seguenti valori: • **Tutti gli utenti**: utilizzare questa opzione per far sì che l'accesso di qualsiasi utente determini l'avvio dell'attività. • **L'utente seguente**: utilizzare questa opzione per far sì che solo l'accesso di uno specifico account utente determini l'avvio dell'attività.
Specificare l'account utente la cui disconnessione dal sistema operativo avvierà l'esecuzione dell'attività	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Quando l'utente si disconnette dal sistema**. Sono disponibili i seguenti valori: • **Tutti gli utenti**: utilizzare questa opzione per far sì che la disconnessione di qualsiasi utente determini l'avvio dell'attività. • **L'utente seguente**: utilizzare questa opzione per far sì che solo la disconnessione di uno specifico account utente determini l'avvio dell'attività.
Condizioni di avvio	Definisce tutte le condizioni che devono essere soddisfatte simultaneamente per avviare l'attività. Le condizioni di avvio per le scansioni anti-malware sono simili alle condizioni di avvio del modulo **Backup** descritte in "Condizioni di avvio". È possibile definire le seguenti condizioni di avvio aggiuntive: • **Ripartisci orari di avvio dell'attività all'interno di una finestra dell'orario** – Questa opzione consente di definire l'intervallo di tempo durante il quale deve essere eseguita l'attività in modo da evitare colli di bottiglia sulla rete. È possibile specificare il ritardo in ore o minuti. Se, ad esempio, l'orario di avvio predefinito è alle 10:00 e il ritardo è di 60 minuti, l'attività verrà avviata tra le 10:00 e le 11:00.

© Acronis International GmbH, 2003-2024

Campo	Descrizione
	• **Se la macchina è spenta, esegui le attività mancanti all'avvio della macchina** • **Impedisci la modalità di sospensione o ibernazione durante l'esecuzione dell'attività** – Questa opzione è valida solo per i sistemi che eseguono Windows. • **Se le condizioni di avvio non sono soddisfatte, esegui comunque l'attività dopo** – Specificare il periodo successivamente al quale l'attività verrà comunque avviata, indipendentemente dalle altre condizioni di avvio. **Nota** In Linux le condizioni di avvio non sono supportate.

Valutazione delle vulnerabilità per sistemi Windows

È possibile scansionare sistemi Windows e prodotti di terze parti alla ricerca di vulnerabilità.

Per configurare la valutazione della vulnerabilità per sistemi Windows

1. Nella console di Cyber Protect, creare un piano di protezione con il modulo **Vulnerability assessment** abilitato.
2. Specificare le impostazioni di valutazione delle vulnerabilità:
   - **Elementi da scansionare** – selezionare **Prodotti Microsoft**, **Prodotti di terze parti per Windows** o entrambi.
   - **Pianificazione** – definisce la pianificazione dell'esecuzione della valutazione delle vulnerabilità.

   Per ulteriori informazioni sulle opzioni di **Pianificazione**, fare riferimento a "Impostazioni di Valutazione delle vulnerabilità" (pag. 977).
3. Assegnare il piano ai sistemi Windows.

Dopo una scansione di valutazione delle vulnerabilità, è possibile visualizzare un elenco delle vulnerabilità individuate. Queste informazioni possono essere analizzate per decidere quali problemi rilevati devono essere risolti.

Per controllare i risultati della scansione di valutazione delle vulnerabilità, vedere i widget **Monitoraggio** > **Panoramica** > **Vulnerabilità/Vulnerabilità esistenti**.

Valutazione delle vulnerabilità per sistemi Linux

È possibile analizzare i sistemi Linux per individuare vulnerabilità a livello di applicazione e di kernel.

Per configurare la valutazione delle vulnerabilità per i sistemi Linux

1. Nella console di Cyber Protect, creare un piano di protezione con il modulo **Vulnerability assessment** abilitato.

© Acronis International GmbH, 2003-2024

2. Specificare le impostazioni di valutazione delle vulnerabilità:
   - **Elementi da scansionare** – selezionare **Scansiona pacchetti Linux**.
   - **Pianificazione** – definisce la pianificazione dell'esecuzione della valutazione delle vulnerabilità.

   Per ulteriori informazioni sulle opzioni di **Pianificazione**, fare riferimento a "Impostazioni di Valutazione delle vulnerabilità" (pag. 977).
3. Assegnare il piano ai sistemi Linux.

Dopo una scansione di valutazione delle vulnerabilità, è possibile visualizzare un elenco delle vulnerabilità individuate. Queste informazioni possono essere analizzate per decidere quali problemi rilevati devono essere risolti.

Per controllare i risultati della scansione di valutazione delle vulnerabilità, vedere i widget **Monitoraggio** > **Panoramica** > **Vulnerabilità/Vulnerabilità esistenti**.

Valutazione della vulnerabilità per dispositivi macOS

È possibile scansionare i dispositivi macOS alla ricerca di vulnerabilità a livello di sistema e di applicazione.

Per configurare la valutazione della vulnerabilità per dispositivi macOS

1. Nella console di Cyber Protect, creare un piano di protezione con il modulo **Vulnerability assessment** abilitato.
2. Specificare le impostazioni di valutazione delle vulnerabilità:
   - **Elementi da scansionare** – selezionare **Prodotti Apple**, **Prodotti di terze parti per macOS** o entrambi.
   - **Pianificazione** – definisce la pianificazione dell'esecuzione della valutazione delle vulnerabilità.

   Per ulteriori informazioni sulle opzioni di **Pianificazione**, fare riferimento a "Impostazioni di Valutazione delle vulnerabilità" (pag. 977).
3. Assegnare il piano ai dispositivi macOS.

Dopo una scansione di valutazione delle vulnerabilità, è possibile visualizzare un elenco delle vulnerabilità individuate. Queste informazioni possono essere analizzate per decidere quali problemi rilevati devono essere risolti.

Per controllare i risultati della scansione di valutazione delle vulnerabilità, vedere i widget **Monitoraggio** > **Panoramica** > **Vulnerabilità/Vulnerabilità esistenti**.

Gestione delle vulnerabilità individuate

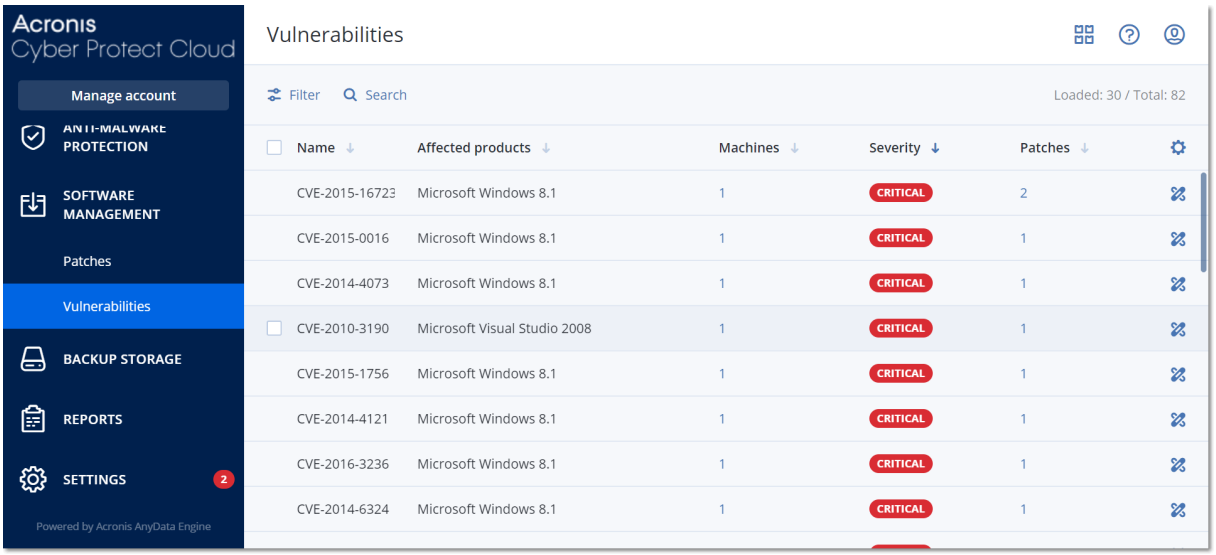
Se la valutazione delle vulnerabilità è stata eseguita almeno una volta e se sono state individuate alcune vulnerabilità, queste verranno visualizzate in **Gestione software** > **Vulnerabilità**. L'elenco delle vulnerabilità mostra sia le vulnerabilità per le quali sono presenti patch da installare, sia quelle

© Acronis International GmbH, 2003-2024

per le quali non sono state suggerite patch. È possibile applicare il filtro per visualizzare solo le vulnerabilità con patch.

Nome	Descrizione
Nome	Il nome della vulnerabilità.
Prodotti interessati	Prodotti software per i quali sono state individuate vulnerabilità.
Sistemi	Il numero di sistemi interessati.
Gravità	La gravità delle vulnerabilità individuate. Conformemente al sistema CVSS (Common Vulnerability Scoring System), la vulnerabilità individuata può presentare uno dei seguenti livelli di gravità: • **Critico**: 9 - 10 CVSS • **Alto**: 7 - 9 CVSS • **Medio**: 3 - 7 CVSS • **Basso**: 0 - 3 CVSS • **Nessuno**
Patch	Il numero di patch appropriate.
Pubblicata	Data e ora di pubblicazione della vulnerabilità in CVE (Common Vulnerabilities and Exposures).
Individuata	La prima data in cui una vulnerabilità esistente è stata individuata nei sistemi.

È possibile reperire la descrizione della vulnerabilità individuata facendo clic sul nome nell'elenco.



Per avviare il processo di correzione della vulnerabilità

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Gestione software** > **Vulnerabilità**.
2. Selezionare la vulnerabilità nell'elenco e fare clic su **Installa patch**. Viene visualizzata la procedura di correzione guidata delle vulnerabilità.
3. Selezionare le patch da installare nei sistemi selezionati, quindi fare clic su **Avanti**.
4. Selezionare i sistemi sui quali installare le patch.
5. Selezionare le opzioni di riavvio.
   a. Selezionare se il sistema deve essere riavviato al termine dell'installazione delle patch.

Opzione	Descrizione
No	I sistemi non vengono riavviati automaticamente al termine dell'installazione delle patch.
Se richiesto	I sistemi vengono riavviati solo se è necessario per l'applicazione delle patch.
Sì	I sistemi vengono riavviati automaticamente al termine dell'installazione delle patch. È anche possibile specificare un ritardo di riavvio.

   b. [Facoltativo] Per ritardare il riavvio di un sistema mentre è in corso il suo backup, selezionare l'opzione **Non riavviare fino al completamento del backup**.
6. Fare clic su **Installa patch**.

Le patch selezionate vengono installate nei sistemi selezionati.

Gestione patch

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Per ulteriori informazioni sui prodotti di terze parti supportati per i sistemi operativi Windows, fare riferimento a List of third-party products supported by Patch Management (62853) (in inglese).

Utilizzare la funzionalità gestione patch per:

- installare aggiornamenti a livello di sistema operativo e di applicazione
- approvare le patch in modo manuale o automatico
- installare le patch su richiesta e in base a una pianificazione
- definire con precisione quali patch installare in base a diversi criteri: gravità, categoria e stato di approvazione
- eseguire backup precedenti all'aggiornamento per impedire aggiornamenti non funzionanti
- definire l'azione di riavvio dopo l'installazione della patch

© Acronis International GmbH, 2003-2024

Nota
Per operare con gli aggiornamenti di Windows, la funzionalità di gestione delle patch richiede l'abilitazione degli aggiornamenti di Windows sul workload.

Cyber Protection introduce la tecnologia peer-to-peer per ridurre il traffico sulla larghezza di banda della rete. È possibile scegliere uno o più agenti dedicati che eseguono il download degli aggiornamenti da Internet e li distribuiscono agli altri agenti nella rete. Tutti gli agenti condivideranno gli aggiornamenti con gli altri, come agenti peer-to-peer.

Flusso di lavoro di gestione delle patch

Il flusso di lavoro di gestione delle patch è costituito dai passaggi di configurazione e applicazione di un piano di protezione, esecuzione di una scansione di vulnerability assessment, configurazione delle impostazioni delle patch, approvazione delle patch e infine installazione delle patch approvate. Di seguito sono elencati gli esatti passaggi del flusso di lavoro.

1. Configurare un piano di protezione per il quale sono abilitati i moduli **Vulnerability assessment** e **Gestione patch**.
2. Configurare le impostazioni di vulnerability assessment. Per ulteriori informazioni su queste impostazioni, consultare "Impostazioni di Valutazione delle vulnerabilità" (pag. 977).
3. Configurare le impostazioni di gestione delle patch. Per ulteriori informazioni su queste impostazioni, consultare "Impostazioni di gestione delle patch nel piano di protezione" (pag. 985)
4. Applicare il piano di protezione a uno o più sistemi.
5. Attendere il completamento della scansione di vulnerability assessment. La scansione si avvia automaticamente in base alla pianificazione configurata nel piano di protezione. In alternativa, è possibile avviare manualmente la scansione su richiesta facendo clic sull'icona **Esegui ora** nel modulo **Vulnerability assessment** del piano di protezione.
6. Approvare le patch. È possibile definire le impostazioni per l'approvazione automatica delle patch, che includono anche l'installazione automatica delle patch sui sistemi di test. Per ulteriori informazioni, consultare "Approvazione automatica della patch" (pag. 992). In alternativa, è possibile approvare manualmente le patch impostando il relativo stato di approvazione su **Approvato**. Per ulteriori informazioni, consultare "Approvazione manuale delle patch" (pag. 997).
7. Installare le patch. Le patch approvate possono essere installate automaticamente in base alla pianificazione configurata nel piano di protezione. In alternativa, è possibile installare manualmente le patch su richiesta. Per ulteriori informazioni, consultare "Installazione delle patch su richiesta" (pag. 997).

I risultati dell'installazione della patch vengono visualizzati nel widget **Monitoraggio**> **Panoramica** > **Cronologia di installazione patch**.

© Acronis International GmbH, 2003-2024

Impostazioni di gestione delle patch nel piano di protezione

Nel modulo **Gestione patch** del piano di protezione è possibile configurare le impostazioni di gestione delle patch seguenti:

- Quali aggiornamenti installare per i prodotti Microsoft e di terze parti per il sistema operativo Windows.
- Quando eseguire l'installazione automatica delle patch.
- Se eseguire un backup prima dell'aggiornamento.

Per ulteriori informazioni sulla creazione di un piano di protezione e sull'abilitazione del modulo **Gestione patch**, consultare "Creazione di un piano di protezione" (pag. 218).

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

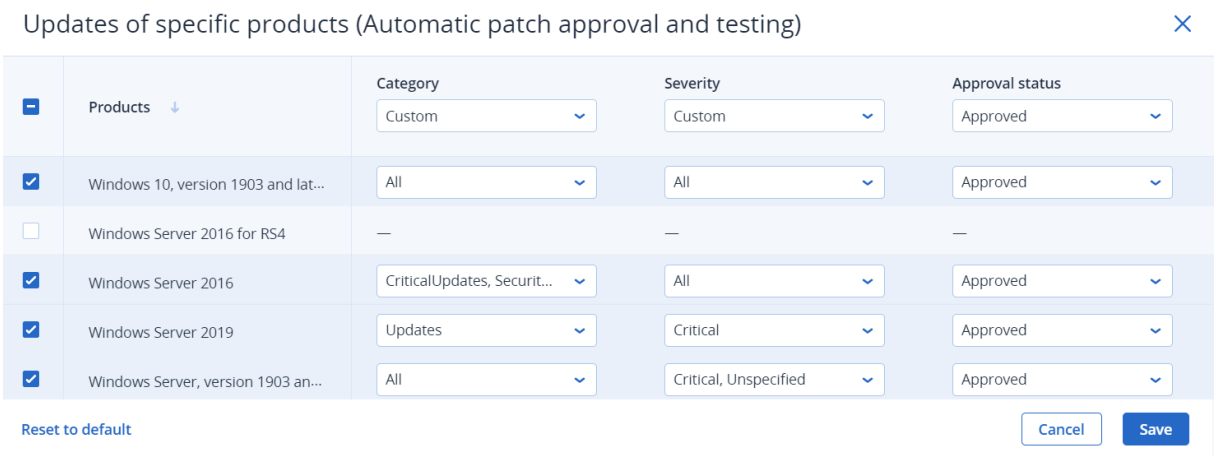
Prodotti Microsoft

Per installare gli aggiornamenti Microsoft sui sistemi selezionati, abilitare l'opzione **Aggiorna prodotti Microsoft**.

Selezionare l'opzione di installazione:

Opzione	Descrizione
Tutti gli aggiornamenti	Utilizzare questa opzione se si desidera installare tutti gli aggiornamenti approvati.
Solo aggiornamenti di sicurezza e critici	Utilizzare questa opzione se si desidera installare tutti gli aggiornamenti di sicurezza e critici approvati.
Aggiornamenti di prodotti specifici (Approvazione e test automatici della patch)	Utilizzare questa opzione se si desidera definire impostazioni personalizzate per prodotti differenti. Se si desidera aggiornare prodotti specifici, per ogni prodotto è possibile definire quali aggiornamenti installare in base a categoria, gravità o stato di approvazione. Se si desidera configurare l'approvazione e il test automatico delle patch, selezionare questa opzione.

© Acronis International GmbH, 2003-2024



Per i prodotti Microsoft, la distribuzione delle patch utilizza il servizio API di Windows. Le patch e gli aggiornamenti non vengono scaricati o archiviati internamente o su agenti di distribuzione. Invece, vengono scaricati da Microsoft CDN. Pertanto, anche se all'agente è assegnato il Ruolo di chi esegue l'aggiornamento, questo non può eseguire il download e la distribuzione delle patch.

Prodotti di terze parti per Windows

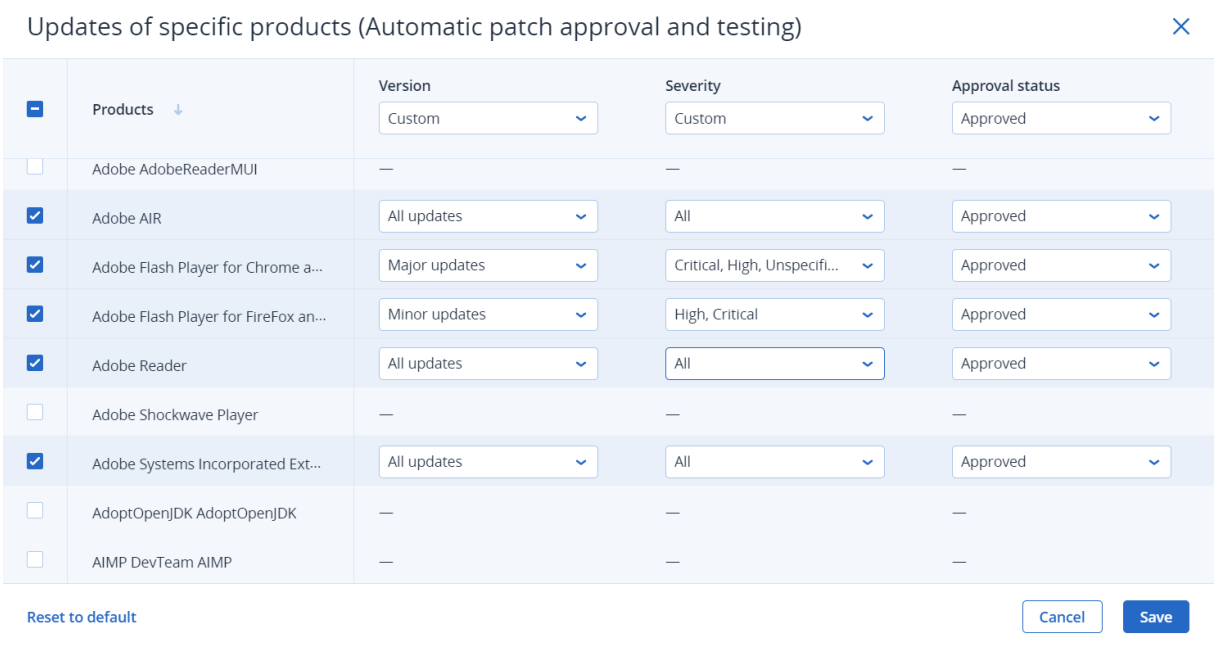
Per installare gli aggiornamenti di terze parti per i sistemi operativi Windows sui sistemi selezionati, abilitare l'opzione **Prodotti di terze parti per Windows**.

Selezionare le opzioni di installazione:

Opzione	Descrizione
Tutti gli aggiornamenti	Utilizzare questa opzione se si desidera installare tutti gli aggiornamenti approvati. *
Solo aggiornamenti principali	Utilizzare questa opzione se si desidera installare tutti gli aggiornamenti principali approvati.
Solo aggiornamenti secondari	Utilizzare questa opzione se si desidera installare gli aggiornamenti secondari approvati.
Aggiornamenti di prodotti specifici (Approvazione e test automatici della patch)	Utilizzare questa opzione se si desidera definire impostazioni personalizzate per prodotti differenti. Se si desidera aggiornare prodotti specifici, per ogni prodotto è possibile definire quali aggiornamenti installare in base a categoria, gravità o stato di approvazione. Se si desidera configurare l'approvazione e il test automatico delle patch, selezionare questa opzione.
Installare le versioni più recenti solo delle applicazioni con vulnerabilità individuate	Selezionare questa casella di controllo se si desidera installare gli aggiornamenti più recenti solo per le applicazioni che hanno vulnerabilità individuate. *

* Questa opzione richiede l'agente di Cyber Protect versione 23.11.36772 o successiva.

© Acronis International GmbH, 2003-2024



Per i prodotti di terzi per Windows, le patch vengono distribuite direttamente ai workload gestiti da un database Acronis interno. Nel caso in cui il Ruolo di chi esegue l'aggiornamento sia assegnato a un agente, questo agente verrà utilizzato per scaricare e distribuire le patch.

Pianificazione

Definire la pianificazione e le condizioni in base alle quali gli aggiornamenti verranno installati nei sistemi selezionati.

Campo	Descrizione
Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito	Questa impostazione determina quando l'attività viene eseguita. Sono disponibili i seguenti valori: • **Pianificazione oraria**: questo è il valore predefinito. L'attività viene eseguita all'orario specificato. • **Quando l'utente accede al sistema** – Per impostazione predefinita, l'accesso di qualsiasi utente determina l'avvio dell'attività. È possibile modificare questa impostazione in modo che solo un account utente specifico possa determinare l'attivazione dell'attività. • **Quando l'utente si disconnette dal sistema** – Per impostazione predefinita, la disconnessione di qualsiasi utente determina l'avvio dell'attività. È possibile modificare questa impostazione in modo che solo un account utente specifico possa determinare l'attivazione dell'attività.

© Acronis International GmbH, 2003-2024

Campo	Descrizione
	Nota L'attività non verrà eseguita allo spegnimento del sistema. Nella configurazione della pianificazione, l'arresto del sistema e la disconnessione vanno considerate come azioni differenti. • **All'avvio del sistema** – L'attività viene eseguita all'avvio del sistema operativo. • **All'arresto del sistema** – L'attività viene eseguita all'arresto del sistema operativo.
Tipo di pianificazione	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria**. Sono disponibili i seguenti valori: • **Ogni mese** – Specificare il mese e le settimane o i giorni del mese in cui verrà eseguita l'attività. • **Ogni giorno**: questo è il valore predefinito. Specificare i giorni della settimana in cui verrà eseguita l'attività. • **Ogni ora** – Specificare i giorni della settimana, il numero di ripetizioni e l'intervallo temporale in cui verrà eseguita l'attività.
Ora di avvio	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria** Specificare l'ora esatta di avvio dell'attività.
Configura la finestra di manutenzione per le patch	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria**. Selezionare questa impostazione per eseguire l'installazione delle patch solo durante l'intervallo di tempo specificato. Se il processo di installazione delle patch non viene completato entro l'orario di fine definito nella finestra di manutenzione delle patch, viene arrestato automaticamente.
Esegui entro un intervallo di date	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Pianificazione oraria**. Impostare un intervallo di validità della pianificazione configurata.
Specificare l'account utente il cui accesso al sistema operativo	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Quando l'utente accede al sistema**. Sono disponibili i seguenti valori:

© Acronis International GmbH, 2003-2024

Campo	Descrizione
avvierà l'esecuzione dell'attività	• **Tutti gli utenti**: utilizzare questa opzione per far sì che l'accesso di qualsiasi utente determini l'avvio dell'attività. • **L'utente seguente**: utilizzare questa opzione per far sì che solo l'accesso di uno specifico account utente determini l'avvio dell'attività.
Specificare l'account utente la cui disconnessione dal sistema operativo avvierà l'esecuzione dell'attività	Il campo viene visualizzato se in **Pianificare l'esecuzione dell'attività utilizzando gli eventi indicati di seguito** è stato selezionato **Quando l'utente si disconnette dal sistema**. Sono disponibili i seguenti valori: • **Tutti gli utenti**: utilizzare questa opzione per far sì che la disconnessione di qualsiasi utente determini l'avvio dell'attività. • **L'utente seguente**: utilizzare questa opzione per far sì che solo la disconnessione di uno specifico account utente determini l'avvio dell'attività.
Condizioni di avvio	Definisce tutte le condizioni che devono essere soddisfatte simultaneamente per avviare l'attività. Le condizioni di avvio per le scansioni anti-malware sono simili alle condizioni di avvio del modulo **Backup** descritte in "Condizioni di avvio". È possibile definire le seguenti condizioni di avvio aggiuntive: • **Ripartisci orari di avvio dell'attività all'interno di una finestra dell'orario** – Questa opzione consente di definire l'intervallo di tempo durante il quale deve essere eseguita l'attività in modo da evitare colli di bottiglia sulla rete. È possibile specificare il ritardo in ore o minuti. Se, ad esempio, l'orario di avvio predefinito è alle 10:00 e il ritardo è di 60 minuti, l'attività verrà avviata tra le 10:00 e le 11:00. • **Se la macchina è spenta, esegui le attività mancanti all'avvio della macchina** • **Impedisci la modalità di sospensione o ibernazione durante l'esecuzione dell'attività** – Questa opzione è valida solo per i sistemi che eseguono Windows. • **Se le condizioni di avvio non sono soddisfatte, esegui comunque l'attività dopo** – Specificare il periodo successivamente al quale l'attività verrà comunque avviata, indipendentemente dalle altre condizioni di avvio. **Nota** In Linux le condizioni di avvio non sono supportate.
Riavvia dopo l'aggiornamento	Definire se riavviare il sistema automaticamente al termine dell'installazione degli aggiornamenti. Sono disponibili i seguenti valori:

© Acronis International GmbH, 2003-2024

Campo	Descrizione
	• **Mai**: il riavvio non viene mai inizializzato dopo gli aggiornamenti. • **Se necessario**: il riavvio viene inizializzato solo se necessario per l'applicazione degli aggiornamenti. • **Sempre**: il riavvio viene sempre inizializzato dopo l'installazione degli aggiornamenti. È possibile specificare un ritardo di riavvio.
Non riavviare fino al completamento del backup	Selezionando questa opzione, se il processo di backup è in esecuzione, il riavvio del sistema verrà ritardato fino al completamento del backup.

Backup precedente all'aggiornamento

Eseguire il backup prima di installare gli aggiornamenti software – viene creato un backup incrementale del sistema prima di installare gli aggiornamenti. Se in precedenza non è stato creato alcun backup, verrà creato un backup completo del sistema. L'azione consente di prevenire quei casi in cui l'installazione degli aggiornamenti non riesce ed è quindi necessario tornare allo stato precedente. Affinché l'opzione **Backup precedente all'aggiornamento** funzioni, sui sistemi corrispondenti e nell'ambito di un piano di protezione devono essere abilitati sia il modulo Gestione patch sia il modulo Backup e gli elementi di cui eseguire il backup: intero sistema o boot e volumi di sistema. Se vengono selezionati elementi idonei all'esecuzione del backup, il sistema non consentirà l'esecuzione dell'opzione **Backup precedente all'aggiornamento**.

Visualizzazione dell'elenco delle patch disponibili

Dopo aver effettuato la scansione di vulnerability assessment, le patch disponibili vengono visualizzate in **Gestione software** > **Patch**.

Per visualizzare informazioni su una patch specifica, nell'elenco delle patch fare clic sulla patch corrispondente.

La tabella seguente descrive le informazioni relative alla patch visualizzabili nella schermata.

Campo	Descrizione
Stato di approvazione	Lo stato di approvazione è necessario principalmente per gli scenari di approvazione automatica. Per la patch è possibile definire uno dei seguenti stati: • **Approvato** – la patch è stata installata su almeno un sistema e convalidata come funzionante • **Declinato** – la patch non è sicura e può danneggiare un sistema • **Approvazione in sospeso**– lo stato della patch non è chiaro e deve essere convalidato
Contratto di licenza	• Accetto • Non accetto. Se non si accetta il contratto di licenza, lo stato della patch passa a

© Acronis International GmbH, 2003-2024

	Declinato e non verrà installato
Gravità	Lo stato di gravità della patch: • **Critico** • **Alto** • **Medio** • **Basso** • **Nessuno**
Fornitore	Il fornitore della patch
Prodotti interessati	Prodotti ai quali sono applicabili le patch
Versioni installate	Versioni del prodotto già installate
Versione	Versione della patch
Categoria	La categoria associata alla patch: • **Aggiornamento critico** – correzioni rilasciate su larga scala per problemi specifici che risolvono bug critici non correlati alla sicurezza. • **Aggiornamento di sicurezza** – correzioni rilasciate su larga scala per prodotti specifici che risolvono problemi correlati alla sicurezza. • **Aggiornamento delle definizioni** – aggiornamento dei file di definizioni dei virus o altro. • **Aggiornamento cumulativo** – insieme cumulativo di aggiornamenti rapidi, aggiornamenti di sicurezza, aggiornamenti critici e aggiornamenti raggruppati insieme per una distribuzione facilitata. In genere questo aggiornamento si concentra su un'area specifica come la sicurezza o su un componente specifico, come i servizi IIS (Internet Information Services). • **Service pack** – insiemi cumulativi di tutti gli aggiornamenti rapidi, aggiornamenti di sicurezza, aggiornamenti critici e aggiornamenti creati a partire dal rilascio del prodotto. I service pack possono inoltre contenere un numero limitato di modifiche o funzionalità progettate su richiesta dei clienti. • **Strumento** – utilità o funzionalità di supporto nel compiere un'attività o un gruppo di attività. • **Feature pack** – rilasci di nuove funzionalità che in genere vengono poi inserite nei prodotti al rilascio successivo. • **Aggiornamento** – correzioni rilasciate su larga scala per problemi specifici che risolvono bug non critici e non correlati alla sicurezza. • **Applicazioni** – patch per un'applicazione.
Data di rilascio	La data di rilascio della patch
Ultima segnalazione	La data dell'ultima segnalazione della patch

© Acronis International GmbH, 2003-2024

Prima installazione	La data della prima installazione riuscita della patch in un sistema
Microsoft KB	Se la patch è per un prodotto Microsoft, il campo fornisce l'ID dell'articolo della KB
Sistemi	Il numero di sistemi interessati
Vulnerabilità	Il numero di vulnerabilità. Facendo clic sul numero, si verrà reindirizzati all'elenco delle vulnerabilità.
Dimensione	La dimensione media della patch
Lingua	La lingua supportata dalla patch
Sito del fornitore	Il sito ufficiale del fornitore

Configurare la permanenza delle patch nell'elenco

È possibile mantenere aggiornato l'elenco delle patch configurando la permanenza delle patch nell'elenco visualizzato nella schermata **Patch**. Questa impostazione determina per quanto tempo le patch disponibili individuate resteranno visibili nell'elenco delle patch. Le patch vengono rimosse dall'elenco dopo essere state correttamente installate in tutti i sistemi in cui erano segnalate come mancanti, o al termine del periodo di permanenza indicato.

Per configurare la permanenza delle patch nell'elenco

1. Nella console di Cyber Protect, passare a **Gestione software** > **Patch**.
2. Fare clic su **Impostazioni**.
3. In **Permanenza nell'elenco** selezionare l'opzione appropriata.

Opzione	Descrizione
Per sempre	La patch non viene mai rimossa dall'elenco.
7 giorni	La patch viene rimossa dall'elenco sette giorni dopo la sua prima installazione. Si ipotizzi, ad esempio, di avere due sistemi in cui devono essere installate le patch. Uno è online, l'altro no. La patch è stata installata sul primo sistema. Dopo 7 giorni, la patch viene rimossa dall'elenco delle patch anche se non è stata installata sul secondo sistema perché questo era offline.
30 giorni	La patch viene rimossa 30 giorni dopo la sua prima installazione.

Approvazione automatica della patch

L'approvazione automatica della patch facilita il processo di installazione delle patch nei sistemi. Con l'approvazione automatica, l'installazione delle patch non viene ritardata dal processo di approvazione manuale. Gli aggiornamenti e le correzioni più importanti vengono installati più rapidamente, il che aumenta l'affidabilità del sistema.

© Acronis International GmbH, 2003-2024

È possibile utilizzare l'approvazione automatica delle patch negli scenari di test per installare automaticamente le correzioni. Se l'installazione delle patch nei sistemi di test riesce correttamente, le patch vengono installate automaticamente anche nei sistemi di produzione. Per ulteriori informazioni su questo scenario, consultare "Caso d'uso per l'approvazione e i test automatici delle patch" (pag. 994).

È anche possibile utilizzare l'approvazione automatica delle patch per installare automaticamente le correzioni nell'ambiente di produzione, saltando la fase di test. Per ulteriori informazioni su questo scenario, consultare "Caso d'uso per l'Approvazione automatica della patch senza test" (pag. 996).

Configurazione dell'approvazione automatica delle patch

È possibile configurare l'approvazione automatica delle patch e garantire che l'installazione delle patch non venga ritardata dal processo di approvazione manuale.

Per configurare l'approvazione automatica delle patch

1. Nella console di Cyber Protect, passare a **Gestione software** > **Patch**.
2. Fare clic su **Impostazioni**.
3. Abilitare **Approvazione automatica della patch**.
4. Configurare le impostazioni per l'approvazione automatica delle patch.
   a. Selezionare l'opzione di approvazione automatica della patch.

Opzione	Descrizione
Approvazione e test automatici della patch	Lo stato di approvazione della patch viene impostato su **Approvato** quando è trascorso il numero specificato di giorni dopo un tentativo riuscito di installare la patch. Si consiglia di utilizzare questa impostazione per eseguire il test delle patch installandole innanzitutto in un sistema di test, verificando che tutto funzioni come previsto e quindi installando le patch nell'ambiente di produzione.
Approvazione automatica della patch senza test	Lo stato di approvazione della patch viene impostato su **Approvato** quando è trascorso il numero specificato di giorni dopo l'individuazione della patch.

   b. Selezionare il numero di giorni che devono trascorrere da quando viene soddisfatta la condizione indicata nell'opzione di approvazione automatica della patch. Al termine del periodo, lo stato di approvazione delle patch viene automaticamente modificato da **Approvazione in sospeso** ad **Approvato**.
5. Selezionare **Accetta automaticamente i termini del contratto di licenza**.
6. Fare clic su **Applica**.

© Acronis International GmbH, 2003-2024

Caso d'uso per l'approvazione e i test automatici delle patch

Per provare le nuove patch su un sistema di test prima di installarle nei sistemi di produzione, è possibile configurare due piani di protezione: uno per l'installazione di patch con finalità di test, e uno per l'installazione di patch verificate nei sistemi di produzione. Questo approccio garantisce che le patch che vengono installate nell'ambiente di produzione sono sicure e che i sistemi di produzione funzionano correttamente dopo l'installazione delle patch.

Il caso d'uso consiste nelle fasi seguenti:

1. Configurare le impostazioni per l'Approvazione automatica delle patch. Selezionare l'opzione **Approvazione e test automatici della patch**. Per ulteriori informazioni, consultare "Configurazione dell'approvazione automatica delle patch" (pag. 993).
2. Configurare il piano di protezione per finalità di test (ad esempio "Applicazione di patch in ambiente di test") con il modulo **Gestione patch** abilitato e applicarlo ai sistemi nell'ambiente di test. Specificare la seguente condizione di installazione della patch: lo stato di approvazione della patch deve essere **Approvazione in sospeso**. Questo passaggio è necessario per convalidare le patch e controllare se i sistemi funzionano in modo adeguato dopo l'installazione della patch. Per ulteriori informazioni, consultare "Configurazione del piano di protezione Applicazione di patch in ambiente di test" (pag. 994).
3. Configurare un piano di protezione per l'ambiente di produzione (ad esempio "Applicazione di patch in ambiente di produzione") con il modulo **Gestione patch** abilitato e applicarlo ai sistemi nell'ambiente di produzione. Specificare la seguente condizione di installazione della patch: lo stato di approvazione della patch deve essere **Approvato**. Per ulteriori informazioni, consultare "Configurare il piano di protezione Applicazione di patch in ambiente di produzione" (pag. 995).
4. Eseguire il piano Applicazione di patch in ambiente di test e controllare i risultati. Lasciare lo stato di approvazione dei sistemi che non presentano problemi su **Approvazione in sospeso**, ma modificare lo stato di approvazione dei sistemi che non funzionano correttamente su **Declinato**. In base al numero di giorni configurato nell'impostazione **Approvazione automatica della patch**, lo stato delle patch viene automaticamente modificato da **Approvazione in sospeso** ad **Approvato**. Quando si esegue il piano Applicazione di patch in ambiente di produzione, solo le patch con stato **Approvato** vengono installate nei sistemi di produzione. Per ulteriori informazioni, consultare "Esecuzione del piano di protezione Applicazione di patch in ambiente di test e rifiuto delle patch non sicure" (pag. 996).
5. Eseguire di nuovo il piano Applicazione di patch in ambiente di produzione.

Configurazione del piano di protezione Applicazione di patch in ambiente di test

È possibile configurare un piano di protezione con impostazioni di installazione delle patch per i sistemi dell'ambiente di test.

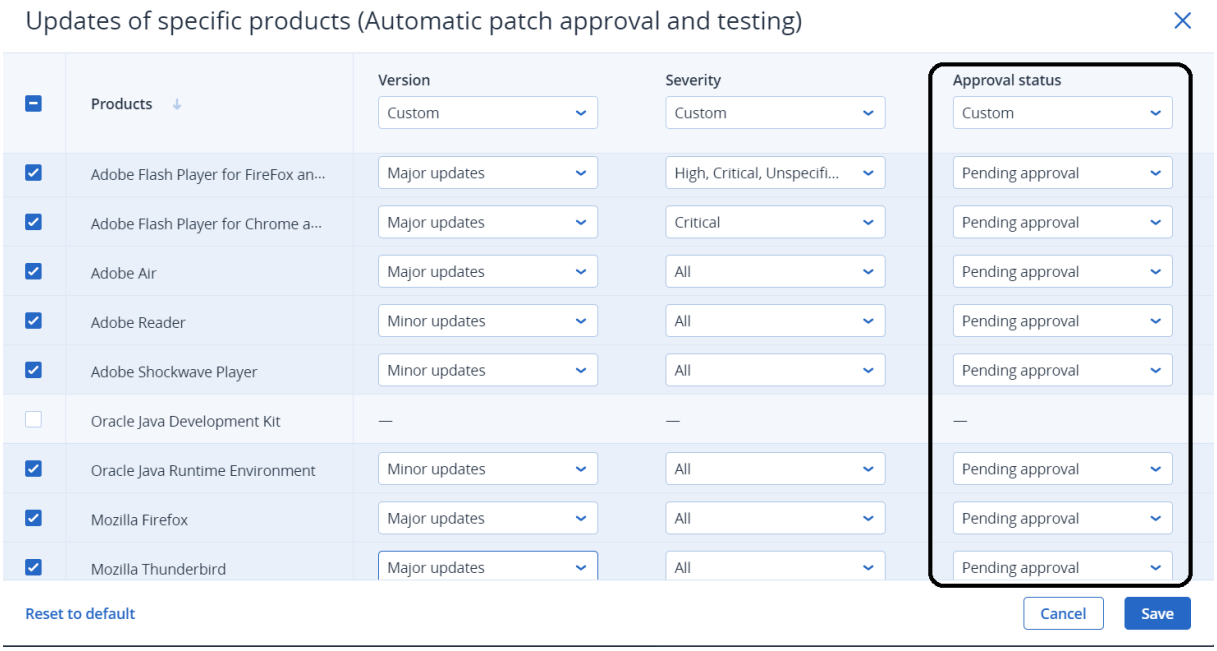
Per configurare il piano di protezione Applicazione di patch in ambiente di test

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di protezione**.
2. Fare clic su **Crea piano**.

© Acronis International GmbH, 2003-2024

3. Abilitare il modulo **Gestione patch**.
4. Definire gli aggiornamenti da installare per i prodotti Microsoft e di terze parti, le pianificazioni e i backup precedenti l'aggiornamento. Per ulteriori informazioni su queste impostazioni, consultare "Impostazioni di gestione delle patch nel piano di protezione" (pag. 985).

Importante
Affinché tutti i prodotti siano aggiornati, selezionare lo stato di approvazione **Approvazione in sospeso**. In questo modo, l'agente installerà soltanto le patch con lo stato **Approvazione in sospeso** nei sistemi selezionati dell'ambiente di test.



Configurare il piano di protezione Applicazione di patch in ambiente di produzione

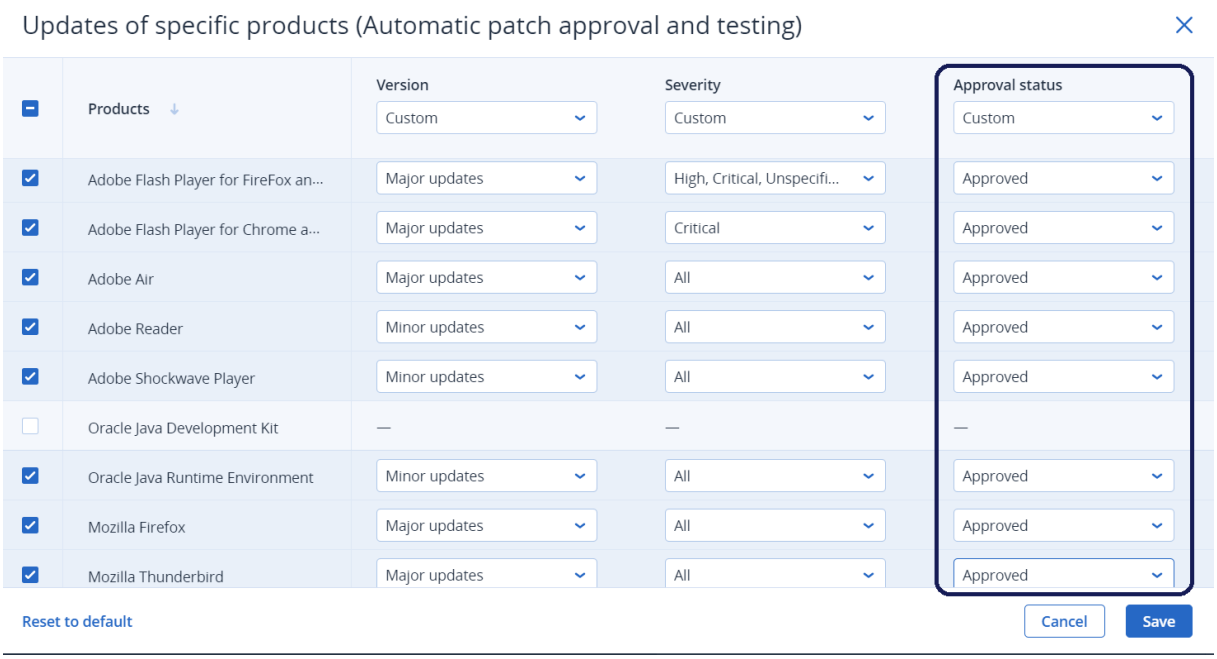
È possibile configurare un piano di protezione con impostazioni di installazione delle patch per i sistemi dell'ambiente di produzione.

Per configurare il piano di protezione Applicazione di patch in ambiente di produzione

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di protezione**.
2. Fare clic su **Crea piano**.
3. Abilitare il modulo **Gestione patch**.
4. Definire gli aggiornamenti da installare per i prodotti Microsoft e di terze parti, le pianificazioni e i backup precedenti l'aggiornamento. Per ulteriori informazioni su queste impostazioni, consultare "Impostazioni di gestione delle patch nel piano di protezione" (pag. 985).

© Acronis International GmbH, 2003-2024

Importante
Affinché tutti i prodotti siano aggiornati, impostare **Stato di approvazione** su **Approvato**. In questo modo, l'agente installerà soltanto le patch con lo stato **Approvato** nei sistemi selezionati dell'ambiente di produzione.



Esecuzione del piano di protezione Applicazione di patch in ambiente di test e rifiuto delle patch non sicure

Dopo aver installato le patch nei sistemi dell'ambiente di test, è possibile verificare che tutto funzioni come previsto. È possibile lasciare lo stato di approvazione dei sistemi che non presentano problemi su **Approvazione in sospeso**, e modificare lo stato di approvazione dei sistemi che non funzionano correttamente su **Declinato**.

Per eseguire il piano di protezione Applicazione di patch in ambiente di test e rifiutare le patch che non sono sicure

1. Eseguire il piano di protezione Applicazione di patch in ambiente di test (in base alla pianificazione o manualmente).
2. In base ai risultati ottenuti, controllare quali tra le patch installate sono sicure.
3. Passare a **Gestione software** > **Patch** e impostare lo **Stato di approvazione** su **Declinato** per le patch che non sono sicure.

Caso d'uso per l'Approvazione automatica della patch senza test

Per installare automaticamente e il prima possibile le nuove patch nei sistemi di produzione, senza prima installarle nei sistemi di test, è possibile configurare un solo piano di protezione.

Il caso d'uso consiste nelle fasi seguenti:

© Acronis International GmbH, 2003-2024

1. Configurare le impostazioni per l'Approvazione automatica delle patch. Selezionare l'opzione **Approvazione automatica della patch senza test**. Per ulteriori informazioni, consultare "Configurazione dell'approvazione automatica delle patch" (pag. 993).
2. Configurare un piano di protezione per l'ambiente di produzione (ad esempio "Applicazione di patch in ambiente di produzione") con il modulo **Gestione patch** abilitato e applicarlo ai sistemi nell'ambiente di produzione. Specificare la seguente condizione di installazione della patch: lo stato di approvazione della patch deve essere **Approvato**. Per ulteriori informazioni, consultare "Configurare il piano di protezione Applicazione di patch in ambiente di produzione" (pag. 995).
3. Eseguire di nuovo il piano Applicazione di patch in ambiente di produzione.

Approvazione manuale delle patch

È possibile approvare manualmente una patch e accelerarne l'installazione saltando la fase di test.

Prerequisiti

- Ad almeno un sistema Windows è applicato un piano di protezione al quale è applicato il modulo **Gestione patch**.
- Sono presenti patch che non sono ancora state installate nel sistema o sistemi al quale il piano di protezione è applicato.

Per approvare manualmente le patch

1. Nella console di Cyber Protect, passare a **Gestione software** > **Patch**.
2. Selezionare le patch da installare e accettare i relativi contratti di licenza.
3. Impostare lo **Stato di approvazione** delle patch su **Approvato**.
   Lo stato di approvazione delle patch è impostato su **Approvato**. Le patch vengono automaticamente installate nei sistemi in base alla pianificazione definita nel piano di protezione. Per installare le patch immediatamente, attenersi alla procedura descritta in "Installazione delle patch su richiesta" (pag. 997).

Installazione delle patch su richiesta

È possibile installare le patch su richiesta se non si desidera attendere l'orario di installazione pianificato.

È possibile avviare l'installazione manuale delle patch da tre schermate: **Patch**, **Vulnerabilità** e **Tutti i dispositivi**.

Per installare manualmente le patch

Da Patch

1. Nella console di Cyber Protect, passare a **Gestione software** > **Patch**.
2. Accettare gli accordi di licenza delle patch da installare.
3. Nella procedura guidata **Installa patch** selezionare le patch da installare e fare clic su **Installa**.

© Acronis International GmbH, 2003-2024

4. Selezionare i sistemi sui quali installare le patch.
5. Selezionare le opzioni di riavvio.
   a. Selezionare se il sistema deve essere riavviato al termine dell'installazione delle patch.

Opzione	Descrizione
No	I sistemi non vengono riavviati automaticamente al termine dell'installazione delle patch.
Se richiesto	I sistemi vengono riavviati solo se è necessario per l'applicazione delle patch.
Sì	I sistemi vengono riavviati automaticamente al termine dell'installazione delle patch. È anche possibile specificare un ritardo di riavvio.

   b. [Facoltativo] Per ritardare il riavvio di un sistema mentre è in corso il suo backup, selezionare l'opzione **Non riavviare fino al completamento del backup**.
6. Fare clic su **Installa patch**.

Da Vulnerabilità

1. Nella console di Cyber Protect, passare a **Gestione software** > **Vulnerabilità**.
2. Eseguire il processo di correzione come descritto in "Gestione delle vulnerabilità individuate" (pag. 981).

Da Tutti i dispositivi

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare il sistema nel quale installare le patch.
3. Fare clic su **Patch**.
4. Selezionare le patch da installare e fare clic su **Avanti**.
5. Selezionare le opzioni di riavvio.
   a. Selezionare se il sistema deve essere riavviato al termine dell'installazione delle patch.

Opzione	Descrizione
No	I sistemi non vengono riavviati automaticamente al termine dell'installazione delle patch.
Se richiesto	I sistemi vengono riavviati solo se è necessario per l'applicazione delle patch.
Sì	I sistemi vengono riavviati automaticamente al termine dell'installazione delle patch. È anche possibile specificare un ritardo di riavvio.

   b. [Facoltativo] Per ritardare il riavvio di un sistema mentre è in corso il suo backup, selezionare l'opzione **Non riavviare fino al completamento del backup**.
6. Fare clic su **Installa patch**.

© Acronis International GmbH, 2003-2024

Gestione dell'inventario software e hardware

Inventario software

La funzionalità Inventario software è disponibile per i dispositivi sui quali è abilitato Advanced Pack, o che dispongono della licenza Cyber Protect (Legacy). La funzionalità consente di visualizzare tutte le applicazioni software installate su tutti i dispositivi con sistema operativo Windows e macOS.

Per ottenere i dati dell'inventario software, è possibile eseguire scansioni automatiche o manuali dei dispositivi.

È possibile utilizzare i dati dell'inventario software per:

- Navigare e confrontare le informazioni su tutte le applicazioni installate nei dispositivi dell'azienda
- Stabilire se è necessario aggiornare un'applicazione
- Stabilire se è necessario rimuovere un'applicazione non utilizzata
- Verificare che sui diversi dispositivi dell'azienda sia installata la stessa versione software
- Controllare le modifiche allo stato del software tra scansioni consecutive.

Abilitazione della scansione dell'inventario software

Quando la scansione dell'inventario software è abilitata sui dispositivi, il sistema raccoglie automaticamente i dati sul software ogni 12 ore.

La funzione di scansione dell'inventario software è abilitata per impostazione predefinita per tutti i dispositivi dotati della licenza richiesta, ma è possibile modificare questa impostazione se necessario.

Nota
I tenant cliente possono abilitare o disabilitare la scansione dell'inventario software. I tenant unità possono solo visualizzare le impostazioni di scansione dell'inventario software, ma non possono modificarle.

Per abilitare la scansione dell'inventario software

1. Nella console di Cyber Protect, passare a **Impostazioni**.
2. Fare clic su **Protezione**.
3. Fare clic su **Scansione dell'inventario**.
4. Abilitare il modulo **Scansione dell'inventario software** facendo clic sull'interruttore accanto al nome del modulo.

Per disabilitare la scansione dell'inventario software

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Impostazioni**.
2. Fare clic su **Protezione**.
3. Fare clic su **Scansione dell'inventario**.
4. Disabilitare il modulo **Scansione dell'inventario software** facendo clic sull'interruttore accanto al nome del modulo.

Esecuzione manuale di una scansione dell'inventario software

È possibile eseguire in modalità manuale una scansione dell'inventario software dalla schermata **Inventario software**, oppure dalla scheda **Software** nella schermata **Inventario**.

Prerequisiti

- Il dispositivo utilizza un sistema operativo Windows o macOS.
- Il dispositivo dispone della licenza Cyber Protect (Legacy) richiesta o di un pacchetto Advanced Management attivato.

Per eseguire una scansione dell'inventario software dalla schermata Inventario software

1. Nella console di Cyber Protect, passare a **Gestione software**.
2. Fare clic su **Inventario software**.
3. Nel campo a discesa **Raggruppa per**, selezionare **Dispositivi**.
4. Individuare il dispositivo da scansionare, quindi selezionare **Esegui scansione ora**.

Per eseguire una scansione dell'inventario software dalla scheda Software nella schermata Inventario

1. Nella console di Cyber Protect, passare a **Dispositivi**.
2. Fare clic sul dispositivo da scansionare, quindi selezionare **Inventario**.
3. Nella scheda **Software**, fare clic su **Esegui scansione ora**.

Navigazione nell'inventario software

È possibile visualizzare e sfogliare i dati di tutte le applicazioni software disponibili su tutti i dispositivi fisici dell'azienda.

Prerequisiti

- I dispositivi utilizzano un sistema operativo Windows o macOS.
- I dispositivi dispongono della licenza Cyber Protect (Legacy) richiesta o di un pacchetto Advanced Management attivato.
- La scansione dell'inventario software sui dispositivi è terminata correttamente.

Per visualizzare tutte le applicazioni software disponibili sui dispositivi con sistema operativo Windows e macOS dell'azienda

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Gestione software**.
2. Fare clic su **Inventario software**.

   Per impostazione predefinita, i dati sono raggruppati per dispositivo. La tabella seguente descrive i dati visibili nella schermata **Inventario software**.

Colonna	Descrizione
Nome	Nome dell'applicazione.
Versione	Versione dell'applicazione.
Stato	Stato dell'applicazione. • **Nuova**. • **Aggiornata**. • **Rimossa**. • **Nessuna modifica**.
Fornitore	Fornitore dell'applicazione.
Data di installazione	Data e ora in cui è stata installata l'applicazione.
Ultima esecuzione	Solo per i dispositivi macOS. Data e ora dell'ultima esecuzione dell'applicazione.
Posizione	Directory in cui è installata all'applicazione.
Utente	Utente che ha installato l'applicazione.
Tipo di sistema	Solo per dispositivi Windows. Tipo di bit dell'applicazione. • **X86** per applicazioni a 32 bit. • **X64** per applicazioni a 64 bit.

3. Per raggruppare i dati in base all'applicazione, nel campo a discesa **Raggruppa per**, selezionare **Applicazioni**.
4. Utilizzare un filtro o una combinazione di filtri per limitare le informazioni visualizzate sullo schermo.
   a. Fare clic su **Filtro**.
   b. Selezionare un filtro o una combinazione di più filtri.

      La tabella seguente descrive i filtri visibili nella schermata **Inventario software**.

Filtra	Descrizione
Nome periferica	Nome del dispositivo. Consente la selezione multipla. Utilizzare questo filtro per confrontare il software di dispositivi specifici.
Applicazione	Nome dell'applicazione. Consente la selezione multipla. Utilizzare questo filtro per confrontare le informazioni di

© Acronis International GmbH, 2003-2024

Filtra	Descrizione
	un'applicazione specifica su dispositivi specifici o su tutti i dispositivi.
Fornitore	Fornitore dell'applicazione. Consente la selezione multipla. Utilizzare questo filtro per visualizzare tutte le applicazioni di un fornitore specifico su dispositivi specifici o su tutti i dispositivi.
Stato	Stato dell'applicazione. Consente la selezione multipla. Utilizzare questo filtro per visualizzare tutte le applicazioni con lo stato selezionato su dispositivi specifici o su tutti i dispositivi.
Data di installazione	Data di installazione dell'applicazione. Utilizzare questo filtro per visualizzare tutte le applicazioni installate in una data specifica su dispositivi specifici o su tutti i dispositivi.
Data scansione	Data di esecuzione della scansione dell'inventario software. Utilizzare questo filtro per visualizzare tutte le informazioni sul software installato su dispositivi specifici o su tutti i dispositivi che sono stati scansionati nella data specificata.

c. Fare clic su **Applica**.

5. Per navigare nell'intero elenco dell'inventario software, utilizzare i numeri di pagina nell'area inferiore sinistra dello schermo.

- Fare clic sul numero di pagina da aprire.
- Nel campo a discesa, selezionare il numero di pagina della pagina da aprire.

Visualizzazione dell'inventario software di un singolo dispositivo

È possibile visualizzare un elenco di tutte le applicazioni software installate su un singolo dispositivo, nonché informazioni dettagliate sulle applicazioni, ad esempio stato, versione, fornitore, data di installazione, data di ultima esecuzione e posizione.

Prerequisiti

- Il dispositivo utilizza un sistema operativo Windows o macOS.
- Il dispositivo dispone della licenza Cyber Protect (Legacy) richiesta o di un pacchetto Advanced Management attivato.
- La scansione dell'inventario software sul dispositivo è terminata correttamente.

Per visualizzare l'inventario software di un singolo dispositivo dalla schermata Inventario software

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Gestione software**.
2. Fare clic su **Inventario software**.
3. Nel campo a discesa **Raggruppa per**, selezionare **Dispositivi**.
4. Individuare il dispositivo da ispezionare utilizzando una delle opzioni seguenti.
   - Individuare il dispositivo utilizzando l'opzione **Filtro**:
     a. Fare clic su **Filtro**.
     b. Nel campo **Nome periferica**, selezionare il nome della periferica da visualizzare.
     c. Fare clic su **Applica**.
   - Individuare il dispositivo utilizzando l'opzione dinamica **Cerca**:
     a. Fare clic su **Cerca**.
     b. Digitare parte o tutto il nome del dispositivo.

Per visualizzare l'inventario software di un singolo dispositivo nella schermata Dispositivi

1. Nella console di Cyber Protect, passare a **Dispositivi**.
2. Fare clic sul dispositivo da visualizzare, quindi selezionare **Inventario**.
3. Fare clic sulla scheda **Software**.

Inventario hardware

La funzionalità Inventario hardware consente di visualizzare tutti i componenti hardware disponibili su:

- dispositivi fisici Windows e macOS dotati di licenze che supportano la funzionalità Inventario hardware.
- virtual machine Windows e macOS eseguite sulle piattaforme di virtualizzazione seguenti: VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo e Virtuozzo Hybrid Infrastructure. Per ulteriori informazioni sulle versioni supportate delle piattaforme di virtualizzazione, vedere "Piattaforme di virtualizzazione supportate" (pag. 32).

Nota
La funzionalità Inventario hardware per virtual machine non è supportata nelle edizioni legacy di Cyber Protect.

Tale funzionalità, inoltre, è supportata solo per i dispositivi nei quali è installato un agente di protezione.

Per ottenere i dati dell'inventario hardware, è possibile eseguire scansioni automatiche o manuali dei dispositivi.

È possibile utilizzare i dati dell'inventario hardware per:

© Acronis International GmbH, 2003-2024

- Individuare tutte le risorse hardware dell'organizzazione
- Navigare nell'inventario hardware di tutti i dispositivi dell'organizzazione
- Confrontare i componenti hardware di più dispositivi dell'azienda
- Visualizzare informazioni dettagliate su un componente hardware.

Abilitazione della scansione dell'inventario hardware

Quando la scansione dell'inventario hardware è abilitata su dispositivi fisici e virtual machine, il sistema raccoglie automaticamente i dati sull'hardware ogni 12 ore.

La funzione di scansione dell'inventario hardware è abilitata per impostazione predefinita, ma è possibile modificare questa impostazione se necessario.

Nota
I tenant cliente possono abilitare o disabilitare la scansione dell'inventario hardware. I tenant unità possono solo visualizzare le impostazioni di scansione dell'inventario hardware, ma non possono modificarle.

Per abilitare la scansione dell'inventario hardware

1. Nella console di Cyber Protect, passare a **Impostazioni**.
2. Fare clic su **Protezione**.
3. Fare clic su **Scansione dell'inventario**.
4. Abilitare il modulo **Scansione dell'inventario hardware** facendo clic sull'interruttore accanto al nome del modulo.

Per disabilitare la scansione dell'inventario hardware

1. Nella console di Cyber Protect, passare a **Impostazioni**.
2. Fare clic su **Protezione**.
3. Fare clic su **Scansione dell'inventario**.
4. Disabilitare il modulo **Scansione dell'inventario hardware** facendo clic sull'interruttore accanto al nome del modulo.

Esecuzione manuale di una scansione dell'inventario hardware

È possibile eseguire la scansione dell'inventario hardware in modalità manuale per un singolo dispositivo, e visualizzare i dati correnti dei componenti hardware di tale dispositivo.

© Acronis International GmbH, 2003-2024

Nota
La scansione dell'inventario hardware delle virtual machines è supportata solo se la data e l'ora correnti della virtual machine corrispondono alla data e all'ora UTC correnti. Per accertarsi che la virtual machine utilizzi le impostazioni di data e ora corrette, disabilitare l'opzione di **sincronizzazione dell'ora** della virtual machine, impostare la data, l'ora e il fuso orario correnti e quindi riavviare **Acronis Agent Core Service** e **Acronis Managed Machine Service**.

Prerequisiti

- (Per tutti i dispositivi) Il dispositivo utilizza un sistema operativo Windows o macOS.
- (Per tutti i dispositivi) I dispositivi hanno una licenza che supporta la funzionalità Inventario hardware. Si noti che la funzionalità Inventario hardware per le virtual machine non è supportata nelle edizioni di Cyber Protect (Legacy).
- (Per tutti i dispositivi) Un agente di protezione è installato nel dispositivo.
- (Per le virtual machine) La virtual machine viene eseguita in una delle piattaforme di virtualizzazione supportate. Per ulteriori informazioni, consultare "Inventario hardware" (pag. 1003).

Per eseguire una scansione dell'inventario hardware di un singolo dispositivo

1. Nella console di Cyber Protect, passare a **Dispositivi**.
2. Fare clic sul dispositivo da scansionare, quindi selezionare **Inventario**.
3. Nella scheda **Hardware**, fare clic su **Esegui scansione ora**.

Navigazione nell'inventario hardware

È possibile visualizzare e sfogliare i dati di tutti i componenti hardware disponibili su tutti i dispositivi dell'azienda.

Prerequisiti

- (Per tutti i dispositivi) I dispositivi utilizzano un sistema operativo Windows o macOS.
- (Per tutti i dispositivi) I dispositivi dispongono di una licenza che supporta la funzionalità Inventario hardware. Si noti che la funzionalità Inventario hardware per virtual machine non è supportata nelle edizioni legacy di Cyber Protect.
- (Per tutti i dispositivi) Un agente di protezione è installato nel dispositivo.
- (Per tutti i dispositivi) La scansione dell'inventario hardware sui dispositivi è terminata correttamente.
- (Per le virtual machine) La virtual machine viene eseguita in una delle piattaforme di virtualizzazione supportate. Per ulteriori informazioni, consultare "Inventario hardware" (pag. 1003).

© Acronis International GmbH, 2003-2024

Per visualizzare tutti i componenti hardware disponibili sui dispositivi Windows e macOS dell'azienda

1. Nella console di Cyber Protect, passare a **Dispositivi**.
2. Nel campo a discesa **Visualizza**, selezionare **Hardware**.

Nota
Viene visualizzata una serie di colonne con le quali è possibile determinare i dati visibili sullo schermo. Le vista predefinite sono **Standard** e **Hardware**. È possibile creare e salvare viste personalizzate che includono diversi insiemi di colonne, scegliendo quelle più adatte alle proprie esigenze.

La tabella seguente descrive i dati visibili nella vista **Hardware**.

Colonna	Descrizione
Nome	Nome del dispositivo.
Stato scansione hardware	Stato della scansione hardware. • **Completata**. • **Non avviata**. • **Non supportata**. Questo stato viene visualizzato per i carichi di lavoro per i quali non è supportata la funzionalità di inventario hardware, ad esempio macchine virtuali, dispositivi mobili, dispositivi Linux. • **Aggiorna agente**. Questo stato viene visualizzato se nel dispositivo è installata una versione non aggiornata dell'agente. Facendo clic su questa azione, verrà visualizzata la pagina Impostazioni > Agente, nella quale l'amministratore può eseguire l'aggiornamento dell'agente. • **Aggiorna quota**. Facendo clic su questa azione, verrà aperta una finestra di dialogo nella quale l'amministratore potrà sostituire la licenza attuale con una delle altre licenze disponibili per il tenant
Processore	Modelli di tutti i processori del dispositivo.
Core del processore	Numero dei core di tutti i processori del dispositivo.
Archiviazione su disco	Spazio di archiviazione utilizzato e spazio di archiviazione totale di tutti i dischi del dispositivo.
Memoria	Capacità RAM totale del dispositivo.

© Acronis International GmbH, 2003-2024

Colonna	Descrizione
Data scansione	Data e ora dell'ultima scansione dell'inventario hardware.
Scheda madre	Scheda madre del dispositivo.
Numero di serie della scheda madre	Numero di serie della scheda madre.
Versione BIOS	Versione del BIOS del sistema.
Organizzazione	Organizzazione alla quale appartiene il dispositivo.
Proprietario	Proprietario del dispositivo.
Dominio	Dominio del dispositivo.
Sistema operativo	Sistema operativo del dispositivo.
Versione sistema operativo	Versione del sistema operativo del dispositivo.

3. Per aggiungere colonne alla tabella, fare clic sull'icona delle opzioni della colonna e selezionare le colonne da visualizzare nella tabella.
4. Utilizzare uno o più filtri per limitare le informazioni visualizzate sullo schermo.
   a. Fare clic su **Cerca**.
   b. Fare clic sulla freccia e quindi su **Hardware**.
   c. Selezionare un filtro o una combinazione di più filtri.
      La tabella seguente descrive i filtri della vista **Hardware**.

Filtra	Descrizione
Modello del processore	Consente la selezione multipla. Utilizzare questo filtro per visualizzare informazioni sull'hardware dei dispositivi dotati del modello di processore specificato.
Core del processore	Utilizzare questo filtro per visualizzare informazioni sull'hardware dei dispositivi dotati del numero di core del processore specificato.
Dimensione totale dei dischi	Utilizzare questo filtro per visualizzare informazioni sull'hardware dei dispositivi dotati della dimensione di archiviazione totale specificata.
Capacità di memoria	Utilizzare questo filtro per visualizzare informazioni sull'hardware dei dispositivi dotati della capacità della RAM specificata.

   d. Fare clic su **Applica**.
5. Per ordinare i dati in ordine ascendente, fare clic sul nome di una colonna.

© Acronis International GmbH, 2003-2024

Visualizzazione dell'hardware di un singolo dispositivo

È possibile visualizzare informazioni dettagliate relative a scheda madre, processori, memoria, unità di elaborazione grafica, unità di archiviazione, rete e sistema di uno specifico dispositivo.

Prerequisiti

- (Per tutti i dispositivi) Il dispositivo utilizza un sistema operativo Windows o macOS.
- (Per tutti i dispositivi) I dispositivi dispongono di una licenza che supporta la funzionalità Inventario hardware. Si noti che la funzionalità Inventario hardware per virtual machine non è supportata nelle edizioni legacy di Cyber Protect.
- (Per tutti i dispositivi) Un agente di protezione è installato nel dispositivo.
- (Per tutti i dispositivi) La scansione dell'inventario hardware sul dispositivo è terminata correttamente.
- (Per le virtual machine) La virtual machine viene eseguita in una delle piattaforme di virtualizzazione supportate. Per ulteriori informazioni, consultare "Inventario hardware" (pag. 1003).

Per visualizzare informazioni dettagliate relative ai componenti hardware di uno specifico dispositivo

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Nel campo a discesa **Visualizza**, selezionare **Hardware**.
3. Individuare il dispositivo da ispezionare utilizzando uno dei metodi descritti di seguito.
   - Individuare il dispositivo utilizzando l'opzione **Filtro**:
     a. Fare clic su **Filtro**.
     b. Selezionare un filtro o una combinazione di più parametri filtro per individuare il dispositivo.
     c. Fare clic su **Applica**.
   - Individuare il dispositivo utilizzando l'opzione **Cerca**:
     a. Fare clic su **Cerca**.
     b. Digitare tutto il nome del dispositivo o parte di esso, e fare clic su **Invia**.
4. Selezionare la riga in cui è elencato il dispositivo e fare clic su **Inventario**.
5. Fare clic sulla scheda **Hardware**.
   Sono disponibili le seguenti informazioni sull'hardware.

Componente hardware	Informazioni visualizzate
Scheda madre	Numero, produttore, modello e numero di serie della scheda madre del dispositivo.
Processori	Produttore, modello, velocità massima di clock

© Acronis International GmbH, 2003-2024

Componente hardware	Informazioni visualizzate
	e numero dei core di ogni processore del dispositivo.
Memoria	Capacità, produttore e numero di serie della memoria del dispositivo.
Unità di elaborazione grafica	Produttore e modello della GPU del dispositivo.
Unità di archiviazione	Modello, tipo di supporto, spazio disponibile e dimensione delle unità di archiviazione del dispositivo.
Rete	Indirizzo Mac, indirizzo IP e tipo delle schede di rete del dispositivo.
Sistema	ID del prodotto, data di installazione originaria, tempo di avvio del sistema, produttore del sistema, modello del sistema, versione del BIOS, dispositivo di avvio, impostazioni locali del sistema e fuso orario del sistema.

© Acronis International GmbH, 2003-2024

Connessione a workload per attività di desktop remoto o assistenza remota

La funzionalità per desktop remoto e assistenza remota costituisce un metodo pratico per connettersi ai workload dell'organizzazione per fornire controllo o assistenza remota. A partire da dicembre 2022, la funzionalità supporta il protocolli NEAR, RDP e Condivisione schermo di Apple. Per ulteriori informazioni, consultare "Protocolli di connessione remota" (pag. 1015).

È possibile utilizzare la funzionalità desktop remoto per eseguire le attività seguenti:

- Connettersi a workload Windows, macOS e Linux remoti utilizzando il protocollo NEAR in modalità di sola visualizzazione.
- Connettersi a workload Windows remoti utilizzando il protocollo RDP.
- Connettersi a workload macOS remoti utilizzando Condivisione schermo di Apple in modalità di sola visualizzazione o tenda.
- Connettersi a workload gestiti e controllarli da remoto utilizzando connessioni remote cloud.
- Connettersi a workload non gestiti e controllarli da remoto utilizzando connessioni remote dirette.
- Connettersi a workload remoti non gestiti utilizzando Acronis Quick Assist.
- Connettersi a workload remoti utilizzando diversi metodi di autenticazione: con credenziali del workload remoto, chiedendo autorizzazioni per la modalità di osservazione o di controllo, con codice di accesso (per Quick Assist)
- Osservare più monitor simultaneamente nella modalità multivista.
- Registrare sessioni remote (se connessi tramite NEAR).
- Visualizzare il report della cronologia della sessione.

Per ulteriori informazioni sulle funzionalità incluse nei pacchetti Standard e Advanced Management, vedere "Funzionalità di desktop remoto e assistenza remota supportate" (pag. 1012).

È possibile utilizzare la funzionalità Assistenza remota per eseguire le attività seguenti:

- Connettersi a workload Windows, macOS e Linux remoti utilizzando il protocollo NEAR in modalità di controllo.
- Connettersi a workload macOS remoti utilizzando Condivisione schermo di Apple in modalità di controllo.
- Fornire assistenza remota ai workload utilizzando connessioni remote cloud.
- Trasferire file tra workload locali e remoti.
- Eseguire azioni di base sul workload remoto: riavvio, arresto, sospensione, svuotamento del cestino e disconnessione dell'utente remoto.
- Monitorare il workload remoto acquisendo periodicamente screenshot del relativo desktop.

© Acronis International GmbH, 2003-2024

Per ulteriori informazioni sulle funzionalità incluse nei pacchetti Standard protection e Advanced Management, vedere "Funzionalità di desktop remoto e assistenza remota supportate" (pag. 1012).

Importante

Per attivare la funzionalità desktop remoto e assistenza remota completa per un workload gestito, è necessario configurare e applicare al workload un piano di gestione remota. Sebbene sia possibile applicare un solo piano di gestione remota a un workload, a seconda delle esigenze è possibile configurare diversi piani di gestione remota e applicarli a diversi workload.

Ad esempio, è possibile creare un piano di gestione remota con abilitato il solo protocollo RDP e applicarlo ad alcuni workload. In questo modo, è possibile connettersi da remoto a tali workload senza attivare la licenza Advanced Management per workload e senza pagare tariffe aggiuntive.

In alternativa, è possibile creare un altro piano di gestione remota nel quale sono attivati i protocolli NEAR e Condivisione schermo di Apple. In questo caso, sarà attivata la licenza Advanced Management per workload, e verrà addebitato ogni workload al quale è applicato questo piano di gestione remota.

Per ulteriori informazioni sui piani di gestione remota e su come lavorare con essi, consultare "Piani di gestione remota" (pag. 1019).

Nota

La funzionalità desktop remoto e assistenza remota richiede:

- l'installazione una tantum di Connect Client sul workload (host) di gestione. Il sistema raccomanderà di scaricare il client al primo tentativo di eseguire un'azione remota (controllo remoto o assistenza remota) sul workload di destinazione. In alternativa, è possibile scaricare Connect Client dalla finestra di **Download** nella console di Protezione. Per ulteriori informazioni sulle impostazioni che è possibile configurare, vedere "Configurazione delle impostazioni di Connect Client" (pag. 1050).
- installazione di Connect Agent nei workload gestiti. Connect Agent è un modulo che fa parte dell'agente di Protezione a iniziare dalla versione 15.0.31266.
- per i workload remoti macOS, è necessario concedere le autorizzazioni di sistema richieste a Connect Agent. Per ulteriori informazioni, consultare "Installazione degli agenti di protezione in macOS" (pag. 82).
- eseguire l'applicazione Acronis Quick Assist nei workload non gestiti. È possibile scaricare Acronis Quick Assist dal sito web.

Per ulteriori informazioni sulle piattaforme supportate da ogni componente della funzionalità desktop remoto e assistenza remota, vedere "Piattaforme supportate" (pag. 1014).

© Acronis International GmbH, 2003-2024

Funzionalità di desktop remoto e assistenza remota supportate

La tabella seguente fornisce ulteriori informazioni sulle modifiche alle funzionalità supportate della funzionalità di desktop remoto e assistenza remota che sono state introdotte a dicembre 2022.

Caratteristiche	Standard Protection precedente a dicembre 2022	Advanced Management precedente a dicembre 2022	Standard Protection successiva a dicembre 2022	Advanced Management successiva a dicembre 2022
Assistenza remota tramite RDP per Windows	Sì	No	No	No
Condividere una connessione remota con gli utenti	No	Sì	No	No
Connessioni remote				
Azioni remote	No	No	Sì	Sì
Selezione di una sessione Windows/macOS/Linux a cui connettersi	No	No	No	Sì
Connessione diretta tramite RDP e Condivisione schermo di Apple	No	No	No	Sì
Controllo di più finestre	No	No	No	Sì
Modalità di connessione: Controllo/Solo visualizzazione/Tenda	No	No	No	Sì
Supporto di credenziali comuni per connessioni remote	No	No	Sì	Sì
Connessioni simultanee per tecnico				
tramite RDP	Sì	Sì	Sì	Sì

© Acronis International GmbH, 2003-2024

Caratteristiche	Standard Protection precedente a dicembre 2022	Advanced Management precedente a dicembre 2022	Standard Protection successiva a dicembre 2022	Advanced Management successiva a dicembre 2022
tramite NEAR	No	No	No	Sì
Trasferimento e condivisione di file				
da Windows a Windows/macOS/Linux	No	No	No	Sì
da macOS a Windows/macOS/Linux	No	No	No	Sì
da Linux a Windows/macOS/Linux	No	No	No	Sì
Connessione tramite applicazione Quick Assist				
da Windows a Windows/macOS/Linux	No	No	No	Sì
da macOS a Windows/macOS/Linux	No	No	No	Sì
da Linux a Windows/macOS/Linux	No	No	No	Sì
Connessioni remote tramite protocolli				
Connessione remota tramite NEAR				
da Windows a Windows/macOS/Linux	No	No	No	Sì
da macOS a Windows/macOS/Linux	No	No	No	Sì
da Linux a Windows/macOS/Linux	No	No	No	Sì
Connessione remota tramite RDP (client desktop)				
da Windows a Windows	Sì	Sì	Sì	Sì
da macOS a Windows	Sì	Sì	Sì	Sì
da Linux a Windows	No	No	Sì	Sì
Connessione remota tramite RDP (client web)				

© Acronis International GmbH, 2003-2024

Caratteristiche	Standard Protection precedente a dicembre 2022	Advanced Management precedente a dicembre 2022	Standard Protection successiva a dicembre 2022	Advanced Management successiva a dicembre 2022
da Windows a Windows	Sì	Sì	Sì	Sì
da macOS a Windows	Sì	Sì	Sì	Sì
da Linux a Windows	No	No	Sì	Sì
Connessione remota tramite Condivisione schermo di Apple				
da Windows/macOS/Linux a macOS	No	No	No	Sì
Gestione della sessione				
Registrazione della sessione	No	No	No	Sì
Creazione di report e monitoraggio				
Cronologia e ricerca della sessione	No	No	No	Sì
Trasmissione screenshot	No	No	No	Sì

Piattaforme supportate

La tabella seguente elenca i sistemi operativi supportati da ciascun componente della funzionalità desktop remoto e assistenza remota.

Componente della funzionalità desktop remoto	Piattaforme supportate
Connect Client	• Windows 7 o versioni successive • macOS 10.13 o versioni successive • Linux: openSUSE 8 Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20

© Acronis International GmbH, 2003-2024

Componente della funzionalità desktop remoto	Piattaforme supportate
	Manjaro 20
Connect Agent	• Windows 7 o versioni successive • Windows Server 2008 R2 o versioni successive • macOS 10.13 o versioni successive • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) - 19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1
Acronis Quick Assist	• Windows 7 o versioni successive • Windows Server 2008 R2 o versioni successive • macOS 10.13 o versioni successive • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) - 19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

Protocolli di connessione remota

La funzionalità di desktop remoto utilizza i protocolli seguenti per le connessioni remote.

NEAR

NEAR è un protocollo altamente sicuro sviluppato da Acronis che ha le caratteristiche seguenti:

- ### H.264

  NEAR implementa tre modalità di qualità: **Fluida**, **Bilanciata** e **Nitida**. Nella modalità **Fluida**, NEAR utilizza la codifica H.264 hardware su macOS e Windows per codificare l'immagine del desktop, ed esegue il failback all'encoder software se l'encoder hardware non è disponibile. Attualmente, la dimensione dell'immagine è limitata alla risoluzione Full HD (1920x1080).

© Acronis International GmbH, 2003-2024

- ### Codec Adaptive

  Nelle modalità di qualità **Bilanciata** e **Nitida**, NEAR utilizza il codec Adaptive, che fornisce una qualità dell'immagine a 32 bit, rispetto alla modalità 'video' utilizzata da H.264.

  Nella modalità **Bilanciata**, la qualità dell'immagine viene regolata automaticamente in base alle condizioni effettive della rete e conserva la frequenza di fotogrammi corrente.

  Nella modalità **Nitida**, l'immagine ha la qualità completa ma potrebbe avere una frequenza di fotogrammi ridotta nel caso in cui la rete, il processore o la scheda video siano sovraccarichi.

  Il codec Adaptive utilizza OpenCL su Windows e macOS quando è disponibile nei rispettivi driver grafici.

- ### Trasferimento audio

  NEAR è in grado di acquisire l'audio del computer remoto e di trasferirlo all'host. Per ulteriori informazioni su come abilitare il reindirizzamento dell'audio remoto su Windows, macOS e Linux, vedere "Reindirizzamento audio remoto" (pag. 1017).

- ### Altre opzioni di accesso

  Per accedere al workload remoto sono disponibili i metodi seguenti.

  Codice di accesso: l'utente connesso al workload remoto esegue Quick Assist e comunica il codice di accesso. Con questo metodo ci si collega sempre alla sessione dell'utente attualmente connesso.

  Credenziali del workload: si accede al workload remoto con le credenziali dell'amministratore registrate nel workload.

  Chiedi l'autorizzazione per osservare o per controllare: l'utente connesso al workload remoto dovrà accettare o rifiutare la connessione.

- ### Sicurezza

  I dati sono sempre crittografati in modo bidirezionali con la crittografia AES in NEAR.

RDP

Remote Desktop Protocol (RDP) è un protocollo proprietario sviluppato da Microsoft che consente di connettersi a un computer Windows remoto tramite una connessione di rete.

Condivisione schermo di Apple

Condivisione schermo di Apple è un client VNC di Apple incluso nelle versioni di macOS a partire dalla 10.5.

© Acronis International GmbH, 2003-2024

Reindirizzamento audio remoto

Connect Client supporta lo streaming audio tramite il protocollo di connessione NEAR. Per ulteriori informazioni su NEAR, vedere "Protocolli di connessione remota" (pag. 1015).

Reindirizzamento dell'audio da un workload Windows remoto

Nei workload Windows, l'audio remoto dovrebbe essere trasmesso automaticamente. Verificare che siano presenti dispositivi di output audio (altoparlanti o cuffie) connessi al workload remoto.

Reindirizzamento dell'audio da un workload macOS remoto

Per abilitare il reindirizzamento dell'audio da un workload macOS, verificare che:

- Nel workload sia stato installato l'agente di Protezione.
- Nel workload sia installato il driver di acquisizione audio.
- Il workload utilizza il protocollo NEAR per le connessioni remote.

Nota
Per macOS 10.15 Catalina, ad Connect Agent deve essere concessa l'autorizzazione Microfono. Per ulteriori informazioni su come concedere l'autorizzazione Microfono ad Connect Agent, vedere "Concedere le autorizzazioni di sistema richieste a Connect Agent" (pag. 84).

L'agente funziona con i driver di acquisizione audio seguenti: Soundflower o Blackhole.

Il processo di installazione nelle versioni più recenti è descritto nella pagina wiki di Blackhole: https://github.com/ExistentialAudio/BlackHole/wiki/Installation.

Nota
Attualmente, Connect Client supporta solo la versione a due canali di Blackhole.

Altrimenti, se nel workload è installato Homebrew, è possibile installare Blackhole con il comando seguente:

```
brew install --cask blackhole-2ch
```

Nota
Durante il reindirizzamento dell'audio di un workload macOS remoto, l'utente connesso al workload remoto non sentirà alcun suono.

Reindirizzamento dell'audio da un workload Linux remoto

Il reindirizzamento dell'audio remoto dovrebbe funzionare automaticamente nella maggior parte delle distribuzioni Linux. Se il reindirizzamento dell'audio remoto non funziona per impostazione predefinita, installare il driver PulseAudio con il comando seguente:

```
sudo apt-get install pulseaudio
```


© Acronis International GmbH, 2003-2024

Connessioni a workload remoti per desktop remoto o assistenza remota

La funzionalità di desktop remoto e assistenza remota offre diverse modalità per stabilire connessioni cloud o dirette da remoto ai workload gestiti.

Le connessioni dirette vengono stabilite tramite TCP/IP nella rete locale LAN tra Connect Client e il workload remoto sul quale non è installato alcun agente. Queste connessioni non richiedono l'accesso a Internet.

Le connessioni cloud vengono stabilite tra Connect Client e l'agente o Quick Assist sul workload, tramite Acronis Cloud.

La tabella seguente fornisce più informazioni sulle opzioni di connessione cloud.

Connessione cloud	Opzione di connessione cloud	Modalità di visualizzazione	Azione remota supportata	Disponibile per
tramite NEAR	da Connect Client a Connect Agent da Connect Client a Quick Assist	Controllo Solo visualizzazione	Desktop remoto Assistenza remota	workload gestiti
tramite RDP	da Connect Client a Connect Agent da client web a Connect Agent	Controllo	Desktop remoto	workload gestiti
tramite Condivisione schermo di Apple	da Connect Client a Connect Agent	Controllo Solo visualizzazione Tenda	Desktop remoto Assistenza remota	workload gestiti

La tabella seguente fornisce più informazioni sulle opzioni di connessione diretta.

Connessione diretta	Opzione di connessione diretta	Azione remota supportata	Disponibile per
tramite RDP	da Connect Client al server RDP	Desktop remoto	workload non gestiti
tramite Condivisione schermo di Apple	da Connect Client al server di Condivisione schermo di Apple	Desktop remoto Assistenza remota	workload non gestiti

© Acronis International GmbH, 2003-2024

Piani di gestione remota

I piani di gestione remota sono piani applicati all'agente di Protezione per abilitare e configurare la funzionalità di desktop remoto e assistenza remota nei workload gestiti.

Se al workload non è applicato alcun piano di gestione remota, le funzionalità di desktop remoto e di assistenza remota saranno limitate alle azioni remote (riavvio, arresto, sospensione, svuotamento del cestino, e disconnessione dell'utente remoto).

Nota
La disponibilità delle impostazioni che è possibile configurare nel piano di gestione remota dipende dal pacchetto di servizi applicato al tenant. Per accedere a tutte le impostazioni, attivare il pacchetto Advanced Management. Per ulteriori informazioni sulle funzionalità incluse nei pacchetti Standard e Advanced Management, vedere "Funzionalità di desktop remoto e assistenza remota supportate" (pag. 1012).

Creazione di un piano di gestione remota

È possibile creare un piano di gestione remota e quindi assegnarlo a un workload per configurare la funzionalità di desktop remoto e assistenza remota sul workload gestito.

Nota
La disponibilità delle impostazioni del piano di gestione remota dipende dalla quota di servizio assegnata al tenant. Se si utilizza la funzionalità standard, è possibile configurare solo connessioni tramite RDP.

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per creare un piano di gestione remota

Da Piani di gestione remota

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di gestione remota**.
2. Creare un piano di gestione remota utilizzando una delle due opzioni.
   - Se l'elenco non contiene piani di gestione remota, fare clic su **Crea**.
   - Se l'elenco contiene piani di gestione remota, fare clic su **Crea piano**.
3. [Facoltativo] Per cambiare il nome predefinito del piano, fare clic sull'icona a forma di matita, immettere il nome del piano, quindi fare clic su **Procedi**.
4. Fare clic su **Protocolli di connessione** e abilitare i protocolli che si desidera rendere disponibili in questo piano di gestione remota per le connessioni remote: NEAR, RDP o Condivisione schermo di Apple.

© Acronis International GmbH, 2003-2024

5. [Facoltativo] Per il protocollo NEAR, nella sezione **Impostazioni di sicurezza** selezionare o deselezionare le caselle di controllo per abilitare o disabilitare l'impostazione corrispondente, quindi fare clic su **Fine**.

Impostazione	Descrizione	Disponibile per
Blocca il workload quando l'utente si disconnette dalla sessione della console	Selezionando questa impostazione, il workload remoto verrà bloccato quando l'utente si disconnette dalla sessione della console.	Windows, macOS
Consenti solo a un utente alla volta di connettersi tramite NEAR o di trasferire file	Selezionando questa impostazione le connessioni tramite NEAR e i trasferimenti di file non saranno possibili mentre è attiva una connessione remota al workload.	Windows, macOS, Linux
Consenti agli amministratori del workload di connettersi a qualsiasi sessione di utenti non amministratori	Selezionando questa impostazione, l'amministratore potrà connettersi a qualsiasi sessione utente standard nel workload. Se sono deselezionate entrambe le opzioni **Consenti agli amministratori del workload di connettersi a qualsiasi sessione di utenti non amministratori** e **Consenti la creazione della sessione di sistema**, non sarà possibile connettersi alle sessioni di amministrazione attive sui workload remoti macOS.	Windows, macOS
Consenti la creazione della sessione di sistema	Selezionando questa impostazione, quando si stabiliscono connessioni remote l'amministratore si connetterà a una nuova sessione, invece che a una delle sessioni attive esistenti.	macOS

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione	Disponibile per
Consenti sincronizzazione degli appunti	Selezionando questa impostazione, sarà possibile trasferire dati tra gli appunti del sistema in uso e gli appunti del workload remoto. Ad esempio, sarà possibile copiare del testo da un file sul workload remoto e copiarlo in un file nel workload dell'utente e viceversa.	Windows, macOS, Linux

6. Fare clic su **Impostazioni di sicurezza**, selezionare o deselezionare le caselle di controllo per abilitare o disabilitare l'impostazione corrispondente, quindi fare clic su **Fine**.

Impostazione	Descrizione
Mostra se il workload è controllato da remoto	Selezionando questa opzione, nel desktop del workload remoto viene visualizzata una notifica quando è presente una connessione desktop remoto attiva al workload.
Chiedi l'autorizzazione dell'utente per acquisire screenshot del workload	Selezionando questa impostazione, l'utente del workload remoto riceve una notifica quando l'amministratore richiede la trasmissione dello screenshot dal workload.

7. Fare clic su **Gestione workload**, selezionare le funzionalità da rendere disponibili nei workload remoti, quindi fare clic su **Fine**.

Impostazione	Descrizione	Disponibile su
Trasferimento di file	Abilita i trasferimenti di file tra workload locali e remoti.	Windows, macOS, Linux
Trasmissione screenshot	Abilita la trasmissione di screenshot del desktop del workload remoto nella console di Cyber Protect.	Windows, macOS, Linux

8. Fare clic su **Impostazioni di visualizzazione**, selezionare o deselezionare le caselle di controllo per abilitare o disabilitare l'impostazione corrispondente, quindi fare clic su **Fine**.

Nota
Le **Impostazioni di visualizzazione** sono disponibili solo per le connessioni tramite NEAR.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione	Disponibile su
Utilizza Deduplicazione desktop per l'acquisizione del desktop	La duplicazione Desktop è uno dei metodi di acquisizione dello schermo disponibili in Windows. Potrebbe non essere stabile in alcuni ambienti. Se non si utilizza Deduplicazione desktop, potrà essere utilizzato il metodo di base BitBlt, che risulta molto più lento, ma anche più stabile.	Windows
Utilizza accelerazione OpenCL	L'accelerazione OpenCL può velocizzare il codec adattivo, responsabile della modalità di qualità **Bilanciato**, eseguendo parte dell'elaborazione nell'unità di elaborazione grafica (GPU). Richiede l'installazione di un driver OpenCL nel sistema Linux remoto. Il codec Adaptive utilizza OpenCL su Windows e macOS quando è disponibile nei rispettivi driver grafici.	Linux
Utilizza codifica H.264 hardware	NEAR supporta tre modalità di qualità: **Fluida**, **Bilanciata** e **Nitida**. La modalità **Fluida** utilizza la codifica H.264 hardware per codificare l'immagine del desktop. La modalità **Bilanciata** utilizza il codec Adaptive, che fornisce una qualità dell'immagine a 32 bit, rispetto alla modalità 'video' utilizzata da H.264. La qualità dell'immagine viene regolata automaticamente in base alle condizioni effettive della rete e conserva la frequenza di fotogrammi corrente.	Windows, macOS

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione	Disponibile su
	La modalità **Nitida** utilizza il codec Adaptive, che fornisce una qualità dell'immagine a 32 bit, rispetto alla modalità 'video' utilizzata da H.264. Con questa modalità si ottiene sempre la qualità completa dell'immagine, ma potrebbe essere ridotta la frequenza dei fotogrammi nel caso in cui la rete, il processore o la scheda video siano sovraccarichi.	

9. Per visualizzare le informazioni sugli ultimi utenti connessi ai workload nei dettagli del workload, fare clic su **Set di strumenti**, selezionare **Mostra gli ultimi utenti connessi**, quindi fare clic su **Fine**.

   Per ulteriori informazioni sugli ultimi utenti connessi, consultare "Trovare l'ultimo utente connesso" (pag. 403).
10. [Facoltativo] Per aggiungere workload al piano:
    a. Fare clic su **Aggiungi workload**.
    b. Selezionare i workload e quindi fare clic su **Aggiungi**.
    c. Se si riscontrano problemi di compatibilità che devono essere risolti, attenersi alla procedura descritta in "Risoluzione dei problemi di compatibilità con i piani di gestione remota" (pag. 1031).
11. Fare clic su **Crea**.

Da Tutti i dispositivi

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic sul workload al quale applicare il piano di gestione remota.
3. Fare clic su **Proteggi**, quindi su **Aggiungi piano**.
4. Fare clic su **Crea piano**, quindi selezionare **Gestione remota**.
5. [Facoltativo] Per cambiare il nome predefinito del piano, fare clic sull'icona a forma di matita, immettere il nome del piano, quindi fare clic su **Procedi**.
6. Fare clic su **Protocolli di connessione** e abilitare i protocolli che si desidera rendere disponibili in questo piano di gestione remota per le connessioni remote: NEAR, RDP o Condivisione schermo di Apple.
7. [Facoltativo] Per il protocollo NEAR, nella sezione **Impostazioni di sicurezza** selezionare o deselezionare le caselle di controllo per abilitare o disabilitare l'impostazione corrispondente, quindi fare clic su **Fine**.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione	Disponibile per
Blocca il workload quando l'utente si disconnette dalla sessione della console	Selezionando questa impostazione, il workload remoto verrà bloccato quando l'utente si disconnette dalla sessione della console.	Windows, macOS
Consenti solo a un utente alla volta di connettersi tramite NEAR o di trasferire file	Selezionando questa impostazione le connessioni tramite NEAR e i trasferimenti di file non saranno possibili mentre è attiva una connessione remota al workload.	Windows, macOS, Linux
Consenti agli amministratori del workload di connettersi a qualsiasi sessione di utenti non amministratori	Selezionando questa impostazione, l'amministratore potrà connettersi a qualsiasi sessione utente standard nel workload. Se sono deselezionate entrambe le opzioni **Consenti agli amministratori del workload di connettersi a qualsiasi sessione di utenti non amministratori** e **Consenti la creazione della sessione di sistema**, non sarà possibile connettersi alle sessioni di amministrazione attive sui workload remoti macOS.	Windows, macOS
Consenti la creazione della sessione di sistema	Selezionando questa impostazione, quando si stabiliscono connessioni remote l'amministratore si connetterà a una nuova sessione, invece che a una delle sessioni attive esistenti.	macOS
Consenti sincronizzazione degli appunti	Selezionando questa impostazione, sarà possibile	Windows, macOS, Linux

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione	Disponibile per
	trasferire dati tra gli appunti del sistema in uso e gli appunti del workload remoto. Ad esempio, sarà possibile copiare del testo da un file sul workload remoto e copiarlo in un file nel workload dell'utente e viceversa.	

8. Fare clic su **Impostazioni di sicurezza**, selezionare o deselezionare le caselle di controllo per abilitare o disabilitare l'impostazione corrispondente, quindi fare clic su **Fine**.

Impostazione	Descrizione
Mostra se il workload è controllato da remoto	Selezionando questa opzione, nel desktop del workload remoto viene visualizzata una notifica quando è presente una connessione desktop remoto attiva al workload.
Chiedi l'autorizzazione dell'utente per acquisire screenshot del workload	Selezionando questa impostazione, l'utente del workload remoto riceve una notifica quando l'amministratore richiede la trasmissione dello screenshot dal workload.

9. Fare clic su **Gestione workload**, selezionare le funzionalità da rendere disponibili nei workload remoti, quindi fare clic su **Fine**.

Impostazione	Descrizione	Disponibile su
Trasferimento di file	Abilita i trasferimenti di file tra workload locali e remoti.	Windows, macOS, Linux
Trasmissione screenshot	Abilita la trasmissione di screenshot del desktop del workload remoto nella console di Cyber Protect.	Windows, macOS, Linux

10. Fare clic su **Impostazioni di visualizzazione**, selezionare o deselezionare le caselle di controllo per abilitare o disabilitare l'impostazione corrispondente, quindi fare clic su **Fine**.

Nota
Le **Impostazioni di visualizzazione** sono disponibili solo per le connessioni tramite NEAR.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione	Disponibile su
Utilizza Deduplicazione desktop per l'acquisizione del desktop	La duplicazione Desktop è uno dei metodi di acquisizione dello schermo disponibili in Windows. Potrebbe non essere stabile in alcuni ambienti. Se non si utilizza Deduplicazione desktop, potrà essere utilizzato il metodo di base BitBlt, che risulta molto più lento, ma anche più stabile.	Windows
Utilizza accelerazione OpenCL	L'accelerazione OpenCL può velocizzare il codec adattivo, responsabile della modalità di qualità **Bilanciato**, eseguendo parte dell'elaborazione nell'unità di elaborazione grafica (GPU). Richiede l'installazione di un driver OpenCL nel sistema Linux remoto. Il codec Adaptive utilizza OpenCL su Windows e macOS quando è disponibile nei rispettivi driver grafici.	Linux
Utilizza codifica H.264 hardware	NEAR supporta tre modalità di qualità: **Fluida**, **Bilanciata** e **Nitida**. La modalità **Fluida** utilizza la codifica H.264 hardware per codificare l'immagine del desktop. La modalità **Bilanciata** utilizza il codec Adaptive, che fornisce una qualità dell'immagine a 32 bit, rispetto alla modalità 'video' utilizzata da H.264. La qualità dell'immagine viene regolata automaticamente in base alle condizioni effettive della rete e conserva la frequenza di fotogrammi corrente.	Windows, macOS

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione	Disponibile su
	La modalità **Nitida** utilizza il codec Adaptive, che fornisce una qualità dell'immagine a 32 bit, rispetto alla modalità 'video' utilizzata da H.264. Con questa modalità si ottiene sempre la qualità completa dell'immagine, ma potrebbe essere ridotta la frequenza dei fotogrammi nel caso in cui la rete, il processore o la scheda video siano sovraccarichi.	

11. Per visualizzare le informazioni sugli ultimi utenti connessi ai workload nei dettagli del workload, fare clic su **Set di strumenti**, selezionare **Mostra gli ultimi utenti connessi**, quindi fare clic su **Fine**.

    Per ulteriori informazioni sugli ultimi utenti connessi, consultare "Trovare l'ultimo utente connesso" (pag. 403).
12. Fare clic su **Crea**.

Aggiunta di un workload a un piano di gestione remota

A seconda delle esigenze, è possibile aggiungere dei workload a un piano di gestione remota, successivamente alla creazione del piano.

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per aggiungere un workload a un piano di gestione remota

Da Piani di gestione remota

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di gestione remota**.
2. Fare clic sul piano di gestione remota.
3. A seconda che il piano sia già stato applicato o meno a un workload, procedere come segue:
   - Fare clic su **Aggiungi workload** se il piano non è ancora stato applicato ad alcun workload.
   - Fare clic su **Gestisci workload** se il piano è già stato applicato ad altri workload.
4. Selezionare un workload dall'elenco, quindi fare clic su **Aggiungi**.
5. Fare clic su **Salva**.
6. Fare clic su **Conferma** per applicare la quota di servizio richiesta al workload.

Da Tutti i dispositivi

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic sul workload al quale applicare il piano di gestione remota.
3. Fare clic su **Proteggi**, quindi su **Aggiungi piano**.
4. In **Selezionare un piano dall'elenco seguente**, selezionare **Gestione remota** per visualizzare solo i piani di gestione remota.
5. Fare clic su **Applica**.
6. Fare clic su **Conferma** per applicare la quota di servizio richiesta al workload.

Rimozione di workload da un piano di gestione remota

A seconda delle esigenze, è possibile rimuovere workload da un piano di gestione remota.

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per rimuovere workload da un piano di gestione remota

1. Nella console di Cyber Protect, passare a **Gestione** > **Piani di gestione remota**.
2. Fare clic sul piano di gestione remota.
3. Fare clic su **Gestisci workload**.
4. Selezionare uno o più workload da eliminare dal piano di gestione remota, quindi fare clic su **Rimuovi**.
5. Fare clic su **Fine**.
6. Fare clic su **Salva**.

Ulteriori operazioni con i piani di gestione remota esistenti

Nella schermata **Piani di gestione remota** è possibile eseguire le azioni aggiuntive seguenti sui piani di gestione remota: visualizzazione dei dettagli, modifica, visualizzazione delle attività, visualizzazione degli avvisi, ridenominazione, abilitazione, disabilitazione, clonazione, esportazione ed eliminazione.

Visualizza dettagli

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per visualizzare i dettagli di un piano di gestione remota

1. Nella schermata **Piani di gestione remota**, fare clic sull'icona **Altre azioni** del piano di gestione remota.
2. Fare clic su **Visualizza dettagli**.

Modifica

© Acronis International GmbH, 2003-2024

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per modificare un piano

1. Nella schermata **Piani di gestione remota**, fare clic sull'icona **Altre azioni** del piano di gestione remota.
2. Fare clic su **Modifica**.

Attività

Per visualizzare le attività relative a un piano di gestione remota

1. Nella schermata **Piani di gestione remota**, fare clic sull'icona **Altre azioni** del piano di gestione remota.
2. Fare clic su **Attività**.
3. Fare clic sull'attività per visualizzarne ulteriori dettagli.

Avvisi

Per visualizzare gli avvisi

1. Nella schermata **Piani di gestione remota**, fare clic sull'icona **Altre azioni** del piano di gestione remota.
2. Fare clic su **Avvisi**.

Rinomina

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per ridenominare un piano di gestione remota

1. Nella schermata **Piani di gestione remota**, fare clic sull'icona **Altre azioni** del piano di gestione remota.
2. Fare clic su **Rinomina**.
3. Immettere il nuovo nome per il piano, quindi fare clic su **Procedi**.

Abilita

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per abilitare un piano di gestione remota

1. Nella schermata **Piani di gestione remota**, fare clic sull'icona **Altre azioni** del piano di gestione remota.

© Acronis International GmbH, 2003-2024

2. Fare clic su **Abilita**.

Disabilita

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per disabilitare un piano di gestione remota

1. Nella schermata **Piani di gestione remota**, fare clic sull'icona **Altre azioni** del piano di gestione remota.
2. Fare clic su **Disabilita**.

Clona

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per clonare un piano di gestione remota

1. Nella schermata **Piani di gestione remota**, fare clic sull'icona **Altre azioni** del piano di gestione remota.
2. Fare clic su **Clona**.
3. Fare clic su **Crea**.

Esporta

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per esportare un piano di gestione remota

1. Nella schermata **Piani di gestione remota**, fare clic sull'icona **Altre azioni** del piano di gestione remota.
2. Fare clic su **Esporta**.
   La configurazione del piano viene esportata in formato JSON nel sistema locale.

Elimina

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per eliminare un piano di gestione remota

1. Nella schermata **Piani di gestione remota**, fare clic sull'icona **Altre azioni** del piano di gestione remota.

© Acronis International GmbH, 2003-2024

2. Fare clic su **Elimina**.
3. Selezionare **Confermo**, quindi fare clic su **Elimina**.

Problemi di compatibilità con i piani di gestione remota

In alcuni casi, applicare un piano di gestione remota a un workload può causare problemi di compatibilità. Potrebbero registrarsi i problemi di compatibilità seguenti:

- Piani in conflitto: questo problema si verifica quando al workload è già applicato un altro piano di gestione remota, poiché a ogni workload può essere applicato un solo piano di gestione remota.
- Sistema operativo non compatibile: questo problema si verifica quando il sistema operativo del workload non è supportato.
- Agente non supportato: questo problema si verifica quando una versione dell'agente di protezione nel workload è obsoleta e non supporta la funzionalità di desktop remoto.
- Quota non sufficiente: questo problema si verifica quando la quota di servizio nel tenant non è sufficiente per essere assegnata ai workload selezionati.

Se il piano di gestione remota è applicato a un massimo di 150 workload selezionati singolarmente, verrà richiesto di risolvere i conflitti esistenti prima di salvare il piano. Per risolvere i conflitti, rimuovere la causa principale che li causa oppure rimuovere i workload interessati dal piano. Per ulteriori informazioni, consultare "Risoluzione dei problemi di compatibilità con i piani di gestione remota" (pag. 1031). Se si salva il piano senza risolvere i conflitti, il piano verrà automaticamente disabilitato per i workload non compatibili e verranno mostrati i relativi avvisi.

Se il piano di gestione remota è applicato a più di 150 workload o a gruppi di dispositivi, prima verrà salvato e quindi ne verrà controllata la compatibilità. Il piano verrà automaticamente disabilitato per i workload incompatibili e verranno visualizzati i relativi avvisi.

Risoluzione dei problemi di compatibilità con i piani di gestione remota

A seconda della causa che li provoca, è possibile eseguire azioni differenti per risolvere i problemi di compatibilità durante il processo di creazione di un nuovo piano di gestione remota.

Nota
Quando si tenta di risolvere un problema di compatibilità rimuovendo i workload da un piano, non è possibile rimuovere i workload che fanno parte di un gruppo di dispositivi.

Per risolvere i problemi di compatibilità

1. Fare clic su **Rivedi problemi**.
2. [Per risolvere i problemi di compatibilità con i piani di gestione remota esistenti rimuovendo i workload dal nuovo piano]

© Acronis International GmbH, 2003-2024

a. Nella scheda **Piani in conflitto** selezionare i workload da eliminare.

b. Fare clic su **Rimuovi i workload dal piano**.

c. Fare clic su **Rimuovi** e quindi su **Chiudi**.

3. [Per risolvere i problemi di compatibilità con i piani di gestione remota disabilitando i piani già applicati ai workload]
   a. Fare clic su **Disabilita i piani applicati**.
   b. Fare clic su **Disabilita** e quindi su **Chiudi**.
4. [Per risolvere i problemi di compatibilità con sistemi operativi incompatibili]
   a. Nella scheda **Sistema operativo incompatibile** selezionare i workload da eliminare.
   b. Fare clic su **Rimuovi i workload dal piano**.
   c. Fare clic su **Rimuovi** e quindi su **Chiudi**.
5. [Per risolvere i problemi di compatibilità con agenti non supportati rimuovendo i workload dal piano]
   a. Nella scheda **Agenti non supportati** selezionare i workload da eliminare.
   b. Fare clic su **Rimuovi i workload dal piano**.
   c. Fare clic su **Rimuovi** e quindi su **Chiudi**.
6. [Per risolvere i problemi di compatibilità con agenti non supportati aggiornando la versione dell'agente] Fare clic su **Passare all'elenco degli agenti**.

   Nota
   Questa opzione è disponibile solo per gli amministratori del cliente.

7. [Per risolvere i problemi di compatibilità con quote insufficienti rimuovendo i workload dal piano]
   a. Nella scheda **Quota insufficiente** selezionare i workload da eliminare.
   b. Fare clic su **Rimuovi i workload dal piano**.
   c. Fare clic su **Rimuovi** e quindi su **Chiudi**.
8. [Per risolvere i problemi di compatibilità con quote insufficienti aumentando la quota del tenant]

   Nota
   Questa opzione è disponibile solo per gli amministratori del partner.

   a. Nella scheda **Quota insufficiente**, fare clic su **Vai al portale di gestione**.
   b. Aumentare la quota di servizio per il cliente.

Credenziali del workload

È possibile aggiungere credenziali amministrative o non amministrative per i workload remoti (nome utente e password o password VNC), salvarle nell'archivio delle credenziali nel cloud e quindi

© Acronis International GmbH, 2003-2024

utilizzarle per l'autenticazione automatica quando ci si connette ai workload che si gestiscono. In questo modo, invece di inserire ogni volta manualmente le credenziali durante il passaggio di autenticazione della connessione, è possibile salvarle nell'archivio delle credenziali una volta, assegnarle a più workload, e quindi Connect Client potrà utilizzarle ogni volta che dovrà connettersi ai workload remoti.

Nota
Le credenziali archiviate nell'archivio delle credenziali non sono condivise tra i diversi livelli di tenant. Vengono condivise solo allo stesso livello di tenant, per lo stesso tenant cliente o tenant partner.

Ciò significa che se un tenant cliente ha numerosi amministratori questi vedranno e condivideranno le credenziali nell'archivio delle credenziali, mentre qualsiasi altro amministratore del partner, o amministratore del cliente di altri tenant, non potrà visualizzare né utilizzare tali credenziali.

Aggiunta di credenziali

È possibile aggiungere credenziali e utilizzare per le connessioni remote a diversi workload.

Per aggiungere le credenziali a un workload e salvarle nell'archivio delle credenziali

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic sul workload al quale aggiungere le credenziali.
3. Accedere al menu **Impostazioni** in uno dei modi seguenti:
   - Fare clic su **Desktop remoto**, quindi su **Impostazioni**.
   - Fare clic su **Gestisci**, quindi su **Impostazioni**.
4. Fare clic su **Aggiungi credenziali**.
5. In **Archivio credenziali**, fare clic su **Aggiungi credenziali**.
6. Immettere le credenziali.

Campo	Descrizione
Nome credenziali	Identificatore delle credenziali che sarà visibile nell'archivio delle credenziali.
Nome utente	Nome utente che verrà utilizzato per le connessioni remote al workload di destinazione.
Password	Password che verrà utilizzata per le connessioni remote al workload di destinazione.
Password VNC	Questo campo è disponibile solo per la Condivisione schermo di Apple.

7. Fare clic su **Salva**.

© Acronis International GmbH, 2003-2024

Assegnazione di credenziali a un workload

Dopo aver aggiunto le credenziali, queste possono essere utilizzate per l'autenticazione automatica quando l'utente si connette a un workload che gestisce.

Per assegnare a un workload le credenziali salvate per l'autenticazione automatica

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Accedere al menu **Impostazioni** in uno dei modi seguenti:
   - Fare clic su **Desktop remoto**, quindi su **Impostazioni**.
   - Fare clic su **Gestisci**, quindi su **Impostazioni**.
3. Nella scheda dei protocolli supportati (NEAR, RDP o Condivisione schermo di Apple), fare clic su **Aggiungi credenziali**.
4. Nell'**Archivio delle credenziali**, selezionare le credenziali dall'elenco, quindi fare clic su **Seleziona credenziali**.

Eliminazione delle credenziali

È possibile eliminare le credenziali che non sono più necessarie.

Per eliminare le credenziali dall'archivio delle credenziali

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Accedere al menu **Impostazioni** in uno dei modi seguenti:
   - Fare clic su **Desktop remoto**, quindi su **Impostazioni**.
   - Fare clic su **Gestisci**, quindi su **Impostazioni**.
3. Nella scheda dei protocolli supportati (NEAR, RDP o Condivisione schermo di Apple), fare clic su **Elimina**.
4. Nella finestra di conferma, fare clic su **Elimina**.

Annullamento dell'assegnazione di credenziali da un workload

È possibile annullare l'assegnazione di credenziali da un workload continuando a conservarle nell'archivio delle credenziali.

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Accedere al menu **Impostazioni** in uno dei modi seguenti:
   - Fare clic su **Desktop remoto**, quindi su **Impostazioni**.
   - Fare clic su **Gestisci**, quindi su **Impostazioni**.
3. Nella scheda dei protocolli supportati (NEAR, RDP o Condivisione schermo di Apple), fare clic su **Annulla assegnazione**.
4. Nella finestra di conferma, fare clic su **Annulla assegnazione**.

© Acronis International GmbH, 2003-2024

Operare con workload gestiti

I workload gestiti sono workload nei quali è installato l'agente di Protezione.

È possibile eseguire le seguenti operazioni nei workload remoti gestiti:

- connettersi per assistenza remota o desktop remoto utilizzando NEAR in modalità di controllo o sola visualizzazione
- connettersi per desktop remoto utilizzando RDP in modalità di controllo
- connettersi per assistenza remota o desktop remoto utilizzando Condivisione schermo di Apple in modalità di controllo, sola visualizzazione o tenda
- connettersi per desktop remoto tramite un client web
- eseguire azioni come riavvio, arresto, sospensione, svuotamento del cestino e disconnessione dell'utente remoto dai workload remoti
- trasferire file tra il workload di gestione e quelli remoti
- monitorarli acquisendo screenshot

Nota
Le connessioni desktop remoto ai workload gestiti richiedono l'installazione di un agente di Protezione e l'applicazione di un piano di gestione remota al workload.

Configurazione delle impostazioni RDP

È possibile configurare le impostazioni che verranno applicate automaticamente per il controllo remoto delle connessioni RDP al workload gestito.

Per configurare le impostazioni RDP di un workload

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Accedere al menu **Impostazioni** in uno dei modi seguenti:
   - Fare clic su **Desktop remoto**, quindi su **Impostazioni**.
   - Fare clic su **Gestisci**, quindi su **Impostazioni**.

© Acronis International GmbH, 2003-2024

3. Configurare le impostazioni nella scheda **RDP**.

Impostazione	Descrizione
Riproduzione audio	Questa impostazione abilita o disabilita il reindirizzamento dell'audio del workload remoto verso il workload locale.
Registrazione audio	Questa impostazione determina se la registrazione dell'audio (parlando al microfono) verrà trasferita al workload remoto.
Reindirizza stampanti	Selezionando questa impostazione, le stampanti del workload dell'utente saranno disponibili nel workload remoto.
Reindirizza file	Questa impostazione determina se i file del workload locale saranno condivisi con il workload remoto.
Intensità colore	Questa impostazione determina il numero di colori nell'immagine che verrà trasferita da RDP. Valori più elevati richiedono una larghezza di banda più elevata. **Modalità 65.536 colori**: 16 bit **Modalità 16,8 milioni di colori**: • 24 bit per le connessioni RDP tramite client web • 32 bit per le connessioni RDP tramite Connect Client

4. Fare clic sul pulsante Chiudi.

Connessione a workload gestiti per desktop remoto o assistenza remota

Nota
La disponibilità dei protocolli di connessione utilizzabili per le connessioni remote dipende dalla configurazione del piano di gestione remota e dal sistema operativo del workload remoto.

Prerequisiti

- Al workload gestito è applicato un piano di gestione remota con il protocollo di connessione corrispondente abilitato.
- Al workload è assegnata la quota di servizio richiesta. (La quota di servizio viene acquisita automaticamente quando si applica un piano di gestione remota al workload.)
- [Per le connessioni Condivisione schermo di Apple] Condivisione schermo di Apple è abilitata sul workload macOS.
- L'autenticazione a due fattori è abilitata per l'account utente in Acronis Cyber Protect Cloud.

Per connettersi da remoto a un workload gestito per desktop remoto o assistenza remota

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Fare clic sul workload al quale connettersi.

© Acronis International GmbH, 2003-2024

3. Fare clic su **Desktop remoto**.
   Per impostazione predefinita, NEAR è selezionato come protocollo di connessione.
4. [Facoltativo] Nell'elenco a discesa **Protocollo di connessione**, selezionare il protocollo di connessione da utilizzare.
5. Fare clic sulla modalità di visualizzazione da utilizzare.

Protocollo	Connessioni remote a	Modalità di visualizzazione	Azione remota supportata
NEAR	Windows Linux macOS	**Controllo** - In questa modalità, l'utente può osservare ed eseguire operazioni sul workload remoto. **Solo visualizzazione** - In questa modalità, l'utente può solo osservare quanto avviene sul workload remoto.	Desktop remoto Assistenza remota
RDP	Windows	**Controllo** - In questa modalità, l'utente può visualizzare ed eseguire operazioni sul workload remoto. **Nota** Se RDP è disabilitato nelle impostazioni del sistema operativo del workload, verrà visualizzata una finestra a comparsa. Utilizzare questa finestra per abilitare RDP per il workload per la sessione in corso o in generale: • Per abilitare RDP per questo workload solo per la sessione in corso, selezionare **Disabilita dopo la fine della sessione**, quindi fare clic su **Consenti**. • Per abilitare RDP per questo workload, fare clic su **Consenti**.	Desktop remoto
Condivisione schermo di Apple	macOS	**Controllo** - In questa modalità, l'utente può osservare ed eseguire operazioni sul workload remoto. **Solo visualizzazione** - In questa modalità, l'utente può solo osservare quanto avviene sul workload remoto. **Tenda** - Disponibile soltanto per i workload macOS. Se ci si connette al workload remoto in modalità Tenda, il monitor di tale workload viene visualizzato in grigio, impedendo	Desktop remoto Assistenza remota

© Acronis International GmbH, 2003-2024

Protocollo	Connessioni remote a	Modalità di visualizzazione	Azione remota supportata
		all'utente remoto di vedere le azioni eseguite sul workload.	

6. A seconda che Connect Client sia installato o meno nel workload in uso, procedere come segue:
   - Se Connect Client non è installato, scaricarlo, installarlo e, nella finestra di conferma popup visualizzata, selezionare **Consenti**.
   - Se Connect Client è già installato, nella finestra di conferma popup visualizzata selezionare **Apri Connect Client**.
7. Nella finestra **Autenticazione**, selezionare un'opzione di autenticazione e quindi fornire le credenziali richieste.

Nota
Se al workload sono state assegnate delle credenziali, l'autenticazione verrà eseguita automaticamente e questo passaggio verrà ignorato. Per ulteriori informazioni, consultare "Assegnazione di credenziali a un workload" (pag. 1034).

Opzione di autenticazione	Descrizione
Con credenziali del workload remoto	L'utente può stabilire la connessione remota dopo aver fornito nome utente e password di un utente amministratore del workload remoto. Questa opzione è disponibile per NEAR, RDP e Condivisione schermo di Apple. È possibile utilizzare questa opzione per l'autenticazione per desktop remoto e assistenza remota.
Chiedi l'autorizzazione per osservare	È possibile stabilire la connessione remota in modalità di osservazione se l'utente connesso al workload remoto fornisce il suo consenso. Questa opzione è disponibile per NEAR e Condivisione schermo di Apple. È possibile utilizzare questa opzione per l'autenticazione per assistenza remota.
Chiedi l'autorizzazione per controllare	L'utente può stabilire la connessione remota in modalità di controllo se l'utente che ha fatto accesso al workload remoto fornisce il suo consenso. Questa opzione è disponibile per NEAR e Condivisione schermo di Apple. È possibile utilizzare questa opzione per l'autenticazione per assistenza remota.

8. Fare clic su **Connettere** e quindi sulla sessione da visualizzare (se sono presenti più sessioni utente nel workload).

© Acronis International GmbH, 2003-2024

Connect Client apre una nuova finestra del visualizzatore nella quale sarà visibile il desktop del workload remoto. Il visualizzatore è dotato di una barra degli strumenti con azioni aggiuntive che è possibile eseguire sul workload remoto dopo aver stabilito la connessione remota. Per ulteriori informazioni, consultare "Utilizzo della barra degli strumenti nella finestra del visualizzatore" (pag. 1047).

Connetti a un workload gestito tramite client web

È possibile stabilire una connessione desktop remoto a un workload gestito tramite client web.

Prerequisiti

- Al workload è assegnata una quota di servizio standard.
- Al workload gestito è applicato un piano di gestione remota con RDP abilitato.
- Sul workload gestito è abilitato RDP.
- Il browser in uso supporta il protocollo HTML5.
- L'autenticazione a due fattori è abilitata per l'account utente in Acronis Cyber Protect Cloud.

Per connettersi da remoto a un workload gestito tramite client web

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic sul workload al quale connettersi in modalità remota, quindi fare clic su **Desktop remoto**>**Connetti tramite client web**.
3. Immettere il login e la password per accedere al workload e fare clic su **Connettere**.

Nota
Se al workload sono state assegnate delle credenziali, l'autenticazione verrà eseguita automaticamente e questo passaggio verrà ignorato. Per ulteriori informazioni, consultare "Assegnazione di credenziali a un workload" (pag. 1034).

Trasferimento di file

È possibile trasferire con semplicità file tra il workload locale e un workload gestito.

Prerequisiti

- Al workload è applicato un piano di gestione remota con il protocollo NEAR e la funzionalità Trasferimento di file abilitata.
- Al workload è applicata la quota Advanced Management.
- L'autenticazione a due fattori è abilitata per l'account utente in Acronis Cyber Protect Cloud.

Per trasferire in modalità remota i file tra il workload locale e un workload gestito

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Fare clic sul workload al quale trasferire i file.

© Acronis International GmbH, 2003-2024

3. Fare clic su **Gestisci**, quindi su **Trasferisci file**.
4. A seconda che Connect Client sia installato o meno nel workload in uso, procedere come segue:
   - Se Connect Client non è installato, scaricarlo, installarlo e, nella finestra di conferma a comparsa visualizzata, fare clic su **Consenti**.
   - Se Connect Client è già installato, nella finestra di conferma popup visualizzata selezionare **Apri Connect Client**.
5. Nella finestra **Autenticazione**, selezionare un'opzione di autenticazione e quindi fornire le credenziali richieste.

Opzione di autenticazione	Descrizione
Con credenziali del workload remoto	L'utente può stabilire la connessione remota dopo aver fornito nome utente e password di un utente amministratore del workload remoto.
Chiedi l'autorizzazione per trasferire i file	È possibile trasferire i file dopo che l'utente connesso al workload remoto fornisce il suo consenso.

6. Nella finestra **Trasferimento di file**, selezionare i file necessari e trascinarli sulla destinazione desiderata.

   Nota
   I file del workload locale sono elencati nel pannello a sinistra e i file del workload remoto sono elencati nel pannello a destra.
   Quando ha inizio un trasferimento di file, viene visualizzato nel pannello **Attività**.

7. [Facoltativo] Se si desidera rimuovere le attività completate dal pannello **Attività**, fare clic su **Cancella attività completate**.
8. Quando tutti i trasferimenti sono stati completati, chiudere la finestra.

Esecuzione di azioni di controllo sui workload gestiti

È possibile gestire un workload remoto eseguendo su questo le seguenti azioni di controllo di base: svuota cestino, sospendi, riavvia, arresta e disconnetti utente remoto.

Prerequisiti

- Al workload è applicata una quota di servizio standard.
- L'autenticazione a due fattori è abilitata per l'account utente in Acronis Cyber Protect Cloud.

Svuota cestino

Per svuotare il cestino nel workload remoto

© Acronis International GmbH, 2003-2024

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Fare clic sul workload sul quale eseguire questa azione.
3. Fare clic su **Gestisci**, quindi su **Svuota cestino**.
4. Selezionare la sessione utente per la quale eseguire questa azione, quindi fare clic su **Svuota cestino**.

Sospendi

Per attivare la modalità sospensione del workload remoto

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Fare clic sul workload sul quale eseguire questa azione.
3. Fare clic su **Gestisci**, quindi su **Sospendi**.

Riavvia

Per riavviare un workload remoto

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Fare clic sul workload sul quale eseguire questa azione.
3. Fare clic su **Gestisci**, quindi su **Riavvia**.
   - Per i workload Windows, scegliere se consentire all'utente attualmente connesso al workload in locale di salvare le modifiche prima che il workload venga riavviato; selezionare l'utente, quindi fare di nuovo clic su **Riavvia**.
   - Per i workload macOS, scegliere se consentire all'utente attualmente connesso al workload in locale di salvare le modifiche prima che il workload venga riavviato, quindi fare di nuovo clic su **Riavvia**.
   - Per i workload Linux, fare clic su **Riavvia**.

Spegni

Per arrestare un workload remoto

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Fare clic sul workload sul quale eseguire questa azione.
3. Fare clic su **Gestisci**, quindi su **Spegni**.
   - Per i workload Windows, scegliere se consentire all'utente attualmente connesso al workload in locale di salvare le modifiche prima che il workload venga arrestato; selezionare l'utente, quindi fare di nuovo clic su **Arresta**.
   - Per i workload MacOS, scegliere se consentire all'utente attualmente connesso al workload in locale di salvare le modifiche prima che il workload venga arrestato, quindi fare di nuovo clic su **Arresta**.
   - Per i workload Linux, fare clic su **Spegni**.

Disconnetti utente remoto

© Acronis International GmbH, 2003-2024

Per disconnettere l'utente da un workload remoto

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Fare clic sul workload sul quale eseguire questa azione.
3. Fare clic su **Gestisci**, quindi su **Disconnetti utente remoto**.
4. Selezionare l'utente da disconnettere, quindi fare clic su **Disconnetti**.

Monitoraggio dei workload tramite la trasmissione di screenshot

È possibile monitorare lo stato di un workload utilizzando la funzionalità Trasmissione screenshot.

Prerequisiti

- Al workload è applicato un piano di gestione remota con la funzionalità Trasmissione screenshot abilitata.
- La versione dell'agente di protezione è aggiornata e supporta la funzionalità Trasmissione screenshot.
- Al workload è applicata la quota di servizio Advanced Management.
- Il workload è online.
- L'autenticazione a due fattori è abilitata per l'account utente in Acronis Cyber Protect Cloud.

Monitoraggio di un workload tramite la trasmissione di screenshot

Per monitorare un workload tramite la trasmissione di screenshot

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Trasmissione screenshot**.
2. Fare clic sul workload che si desidera monitorare.
3. Selezionare la sessione utente.
4. Selezionare il monitor.
5. Selezionare la frequenza di aggiornamento con la quale acquisire un nuovo screenshot del desktop.
6. Selezionare la qualità dell'immagine.
7. Per scaricare lo screenshot, fare clic sull'icona di download.

Acquisire uno screenshot di un workload

Per acquisire uno screenshot di un workload gestito

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Macchine con agenti**.
2. Selezionare il workload di cui acquisire lo screenshot.
3. Fare clic su **Gestisci**, quindi fare clic su **Acquisisci uno screenshot del desktop**.
   Viene visualizzata la schermata **Trasmissione screenshot**, con il workload preselezionato. A seconda delle impostazioni del piano di gestione remota applicato al workload, lo screenshot viene visualizzato subito oppure dopo che l'utente del workload remoto approva la richiesta.

© Acronis International GmbH, 2003-2024

Osservazione di più workload gestiti simultaneamente

È possibile osservare simultaneamente i desktop di più workload remoti in un'unica finestra.

Nota
Il numero di desktop visualizzati simultaneamente nella finestra dipende dalla dimensione del monitor.

Prerequisiti

- I protocolli NEAR/Condivisione schermo di Apple sono abilitati nei piani di gestione remota applicati ai workload.
- Al workload è applicata la quota di servizio Advanced Management.
- L'autenticazione a due fattori è abilitata per l'account utente in Acronis Cyber Protect Cloud.

Per osservare più workload simultaneamente

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare i workload da osservare.
3. Fare clic su **Multivista**.
4. A seconda che Connect Client sia installato o meno nel workload in uso, procedere come segue:
   - Se Connect Client non è installato, scaricarlo, installarlo e, nella finestra di conferma popup visualizzata, selezionare **Consenti**.
   - Se Connect Client è già installato, nella finestra di conferma popup visualizzata selezionare **Apri Connect Client**.
5. Nella finestra **Autenticazione**, selezionare un'opzione di autenticazione e quindi fornire le credenziali richieste.

Opzione di autenticazione	Descrizione
Con credenziali del workload remoto	L'utente può stabilire la connessione remota dopo aver fornito nome utente e password di un utente amministratore del workload remoto.
Chiedi l'autorizzazione per osservare	È possibile stabilire la connessione remota in modalità di osservazione se l'utente connesso al workload remoto fornisce il suo consenso.

6. Se si desidera utilizzare lo stesso codice di autenticazione e le stesse credenziali per la connessione a tutti i workload remoti selezionati nel passaggio 2, selezionare **Utilizzare su altri computer**.
7. Fare clic su **Connettere**.

© Acronis International GmbH, 2003-2024

Nella barra degli strumenti della finestra multivista, è possibile selezionare una modalità di visualizzazione con la quale connettersi a un workload. Questa azione apre una finestra del visualizzatore distinta per il workload selezionato.

Nota
Se uno qualsiasi dei workload selezionati è offline, o ha una versione obsoleta dell'agente installato, non verrà visualizzato nella finestra multivista.
Tutte le connessioni multivista ai workload remoti sono in modalità **Solo visualizzazione**.

Operare con workload non gestiti

I workload non gestiti sono workload nei quali è non installato l'agente di Protezione.

È possibile eseguire le seguenti operazioni nei workload remoti non gestiti:

- connettersi per assistenza remota utilizzando Acronis Quick Assist
- connettersi per desktop remoto o assistenza remota utilizzando un indirizzo IP
- trasferire file tra il workload di gestione e quello remoto utilizzando Quick Assist

Nota
Per connettersi ai workload non gestiti utilizzando Quick Assist, verificare che:

- Il pacchetto Advanced Management sia attivato per il tenant cliente.
- L'applicazione Quick Assist è in esecuzione sul workload remoto al quale ci si connette.

Connessione a workload non gestiti tramite Acronis Quick Assist

È possibile utilizzare la funzionalità Quick Assist per la connessione remota on demand a workload non gestiti e per fornire assistenza temporanea.

Prerequisiti

- Il pacchetto Advanced Management è assegnato al tenant cliente.
- L'autenticazione a due fattori è abilitata per l'account utente in Acronis Cyber Protect Cloud.
- L'utente remoto ha fornito l'ID del workload e il codice di accesso mostrati in Quick Assist.
- L'utente remoto ha scaricato e sta eseguendo Acronis Quick Assist.

Per connettersi a un workload per assistenza remota utilizzando Quick Assist

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic su **Quick Assist**.
3. Nella finestra **Quick Assist**, immettere l'ID del workload fornito dall'utente finale, quindi selezionare **Connettere**.
4. Fare clic su **Connettere**.

© Acronis International GmbH, 2003-2024

5. A seconda che Connect Client sia installato o meno nel workload in uso, procedere come segue:
   - Se Connect Client non è installato, scaricarlo, installarlo e, nella finestra di conferma popup visualizzata, selezionare **Consenti**.
   - Se Connect Client è già installato, nella finestra di conferma popup visualizzata selezionare **Apri Connect Client**.
6. Nella finestra **Autenticazione**, immettere il codice di accesso.
7. Connect Client apre una nuova finestra del visualizzatore nella quale sarà visibile il desktop del workload remoto. Il visualizzatore è dotato di una barra degli strumenti con azioni aggiuntive che è possibile eseguire sul workload remoto dopo aver stabilito la connessione remota. Per ulteriori informazioni, consultare "Utilizzo della barra degli strumenti nella finestra del visualizzatore" (pag. 1047).

Connessione a workload non gestiti tramite indirizzo IP

Se un workload non gestito è presente nella LAN, è possibile connettersi ad esso per il desktop remoto o l'assistenza remota utilizzandone l'indirizzo IP. Questa connessione non richiede l'accesso a Internet.

Prerequisiti

- Il pacchetto Advanced Management è assegnato al tenant cliente.
- L'autenticazione a due fattori è abilitata per l'account utente in Acronis Cyber Protect Cloud.

Per connettersi a un workload per desktop remoto o assistenza remota utilizzando l'indirizzo IP

1. Nella console di Cyber Protect, passare a **Tutti i dispositivi**.
2. Fare clic su **Quick Assist**.
3. Fare clic sulla scheda **Tramite indirizzo IP**.
4. Immettere l'indirizzo IP e la porta del workload.
5. Selezionare un protocollo di connessione - RDP (workload Windows) o Condivisione schermo di Apple (per workload macOS), in base al sistema operativo del workload remoto.

   Nota
   Le connessioni tramite RDP supportano l'azione di desktop remoto, e le connessioni tramite Condivisione schermo di Apple supportano sia le azioni di desktop remoto che quelle di assistenza remota.

6. Fare clic su **Connettere**.
7. Nella finestra **Autenticazione** fornire le credenziali richieste.

Per le connessioni Condivisione schermo di Apple, Connect Client apre una nuova finestra del visualizzatore nella quale sarà possibile vedere il desktop del workload remoto. Il visualizzatore è dotato di una barra degli strumenti con azioni aggiuntive che è possibile eseguire sul workload

© Acronis International GmbH, 2003-2024

remoto dopo aver stabilito la connessione remota. Per ulteriori informazioni, consultare "Utilizzo della barra degli strumenti nella finestra del visualizzatore" (pag. 1047).

Trasferimento di file tramite Acronis Quick Assist

È possibile utilizzare la funzionalità Quick Assist per trasferire file tra il workload di gestione e i workload non gestiti.

Prerequisiti

- Il pacchetto Advanced Management è assegnato al tenant cliente.
- L'autenticazione a due fattori è abilitata per l'account utente in Acronis Cyber Protect Cloud.
- L'utente remoto ha scaricato e sta eseguendo Acronis Quick Assist.
- L'utente remoto ha fornito l'ID del computer e il codice di accesso mostrati in Quick Assist.

Per trasferire file a un workload utilizzando Quick Assist

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic su **Quick Assist**.
3. Nella finestra **Quick Assist**, immettere l'ID del workload fornito dall'utente finale, quindi selezionare **Trasferimento di file**.
4. Fare clic su **Connettere**.
5. A seconda che Connect Client sia installato o meno nel workload in uso, procedere come segue:
   - Se Connect Client non è installato, scaricarlo, installarlo e, nella finestra di conferma popup visualizzata, selezionare **Consenti**.
   - Se Connect Client è già installato, nella finestra di conferma popup visualizzata selezionare **Apri Connect Client**.
6. Nella finestra **Autenticazione**, immettere il codice di accesso.
7. Nella finestra **Trasferimento di file**, selezionare i file necessari e trascinarli sulla destinazione desiderata.

   Nota
   I file del workload locale sono elencati nel pannello a sinistra e i file del workload remoto sono elencati nel pannello a destra.
   Quando ha inizio un trasferimento di file, viene visualizzato nel pannello **Attività**.

8. [Facoltativo] Se si desidera rimuovere le attività completate dal pannello **Attività**, fare clic su **Cancella attività completate**.
9. Quando tutti i trasferimenti sono stati completati, chiudere la finestra.

© Acronis International GmbH, 2003-2024

Utilizzo della barra degli strumenti nella finestra del visualizzatore

Dopo aver effettuato la connessione a un workload remoto, è possibile utilizzare la barra degli strumenti nella finestra del visualizzatore per eseguire rapidamente le varie azioni.

Icona	Descrizione
	Dimensioni effettive Ridimensiona il desktop del workload remoto in modo che un pixel di quest'ultimo corrisponda a un pixel nella finestra del visualizzatore.
	Zoom per adattare Ridimensiona il desktop del workload remoto in modo che si adatti alla finestra del visualizzatore.
	Blocca e **Sblocca schermo** Mostra un segnaposto nel display del workload remoto in modo che l'utente remoto non visualizzi le azioni compiute dall'esterno.
	Acquisisci uno screenshot Salva l'immagine del desktop del server remoto in un file locale.
	Selezionare il display Selezionare il display del workload remoto da visualizzare e la risoluzione desiderata. Disponibile per connessioni di Condivisione schermo di Apple verso macOS e per connessioni NEAR verso qualsiasi sistema operativo.
	Qualità dell'immagine Regola la qualità dell'immagine dello schermo remoto da bianco e nero alla migliore possibile nelle connessioni di Condivisione schermo di Apple.
	Qualità dell'immagine NEAR Regola il rapporto qualità/prestazioni nelle connessioni NEAR. Il lato sinistro del dispositivo di scorrimento (Fluido) da priorità alle prestazioni rispetto alla qualità dell'immagine, mentre il lato destro (Nitido) indica la migliore qualità dello schermo del desktop remoto, ma potenzialmente le prestazioni peggiori.
	Invia Ctrl+Alt+Canc Invia una sequenza Ctrl+Alt+Canc al workload remoto.

© Acronis International GmbH, 2003-2024

Icona	Descrizione
	Disponibile per workload Windows e Linux.
	Trasferimento di file Apre la finestra del file manager per lo scambio di file tra il workload remoto e quello locale. Disponibile per le connessioni NEAR.
	Blocca barra degli strumenti Disattiva la visualizzazione automatica della barra degli strumenti del visualizzatore. Disponibile per workload Windows.
	Schermo intero Passa alla modalità schermo intero e ridimensiona il workload remoto affinché si adatti completamente allo schermo locale. Disponibile per workload Windows.
	Chiudi Chiude la finestra del visualizzatore e termina la sessione di controllo remoto. Disponibile per workload Windows.

A seconda del tipo di connessione, possono essere disponibili opzioni aggiuntive che vengono visualizzate facendo clic sull'icona **Altro**.

Opzione	Descrizione
Avvia registrazione/Interrompi registrazione	Registra la sessione desktop remoto corrente. Le registrazioni delle sessioni vengono salvate come file .crec sul workload locale. È possibile aprire i file .crec con Acronis Connect Client. Disponibile per le connessioni NEAR.
Sincronizzazione automatica degli appunti	Quando questa opzione è attiva, il client sincronizza automaticamente gli appunti del computer locale e quelli del computer remoto. Disponibile per le connessioni NEAR e Condivisione schermo di Apple
Invia appunti **Recupera appunti**	**Invia appunti** sostituisce il contenuto degli appunti del computer remoto con il contenuto degli appunti locali. **Recupera appunti** trasferisce il contenuto degli appunti del computer remoto negli appunti locali.

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
Tastiera intelligente/Tasti non elaborati/Tasti non elaborati con tutte le scelte rapide	Modifica la modalità di input della tastiera per la connessione corrente. **Tastiera intelligente**- il client trasmette codice Unicode dei simboli digitati in locale al computer remoto **Tasti non elaborati**- il client utilizza i tasti non elaborati dei pulsanti della tastiera premuti. **Tasti non elaborati con tutte le scelte rapide**- il client disabilita le scelte rapide del sistema locale in modo che vengano trasmesse anche al sistema operativo remoto.
Tastiera attiva al passaggio del mouse	Se abilitata, il client acquisisce l'input da tastiera solo quando il cursore del mouse locale viene posizionato sopra la finestra del visualizzatore. Quando disabilitata, il client acquisisce l'input da tastiera ogni volta che la finestra è attiva.
Mostra informazioni sulla connessione/Nascondi informazioni sulla connessione	Quando è selezionata **Mostra informazioni sulla connessione**, sullo schermo del desktop remoto viene visualizzato un piccolo riquadro informativo che contiene le informazioni di base sulla connessione corrente.
Audio da remoto	Abilita il client a reindirizzare l'audio dal computer remoto a quello locale. Disponibile per le connessioni NEAR.
Preferenze	Configurare le impostazioni di Connect Client. Per ulteriori informazioni, consultare "Configurazione delle impostazioni di Connect Client" (pag. 1050).

Registrazione e riproduzione di sessioni remote

È possibile registrare una sessione remota tramite NEAR in Acronis Connect Client.

Per registrare una sessione remota

1. Nella barra degli strumenti del Visualizzatore nel Connect Client, fare clic su **Altro** e selezionare **Avvia registrazione**.
2. Selezionare un nome e una posizione per la registrazione.
   Per impostazione predefinita, il nome del file contiene la data e l'ora correnti e viene posizionato nella cartella **Documenti** nella home directory dell'utente corrente. Mentre la registrazione è attiva, nella barra degli strumenti del **Visualizzatore** sono visibili un cerchio rosso lampeggiante nell'angolo in alto a destra dello schermo remoto e il timer di registrazione.
3. Per interrompere la registrazione, fare clic su **Altro**, quindi su **Interrompi registrazione**. In un sistema Mac è anche possibile fare clic sul pulsante di **arresto** nella barra degli strumenti.

© Acronis International GmbH, 2003-2024

Per impostazione predefinita, tutti i file .crec creati da Acronis Connect Client vengono aperti con Acronis Connect Client.

Per riprodurre una registrazione

1. Localizzare un file di registrazione.
2. Aprire il file.
   Viene aperto il lettore registrazioni di Acronis Connect Client. Non è possibile spostarsi nella registrazione. Per trovare un momento specifico nella registrazione, attendere finché il lettore non lo raggiunge.
3. [Facoltativo] Per regolare la velocità di riproduzione, utilizzare le icone **<<** e **>>** nella sezione dei comandi della riproduzione.
   La registrazione viene archiviata come una sequenza di eventi trasmessi da e verso il server remoto durante una connessione. Ciò garantisce una migliore qualità della registrazione e la dimensione minima del file. Tuttavia, ciò implica anche l'impossibilità di spostarsi all'interno della registrazione stessa. Attualmente non è possibile neanche convertire le registrazioni in un formato video.

Configurazione delle impostazioni di Connect Client

Dopo aver installato Connect Client nel workload in uso, è possibile configurarne le impostazioni in base alle preferenze dell'utente.

Per configurare le impostazioni di Connect Client

1. Nel menu di avvio, individuare **Connect Client** e avviarlo.
2. Configurare le impostazioni nella scheda **Informazioni generali**.

Opzione	Descrizione
Scrivi registri dettagliati	Selezionare questa opzione per consentire a Connect Client di scrivere registri dettagliati. Se l'opzione è disabilitata, il client scriverà solo informazioni generiche nel file di registro.
Impostazioni del proxy	Selezionare se utilizzare il proxy di sistema predefinito o configurare un proxy SOCKSS personalizzato.

3. Configurare le impostazioni nella scheda **Visualizzatore**.

Opzione	Descrizione
Chiedi conferma quando viene chiuso un visualizzatore	Selezionare questa opzione affinché Connect Client visualizzi un messaggio di conferma quando si tenta di chiudere la finestra del visualizzatore in modo da prevenirne la chiusura accidentale.
Quando ridotto a icona	Selezionare se sospendere l'attività del visualizzatore quando viene ridotto a icona, in modo da ridurre il carico sulla CPU.

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
Quando ingrandito	Selezionare se abilitare lo schermo intero quando il visualizzatore è ingrandito.
Trasferimento appunti	Abilita la visualizzazione dell'indicatore di trasferimento degli appunti nella finestra del visualizzatore ogni volta che vengono copiati o incollati testi e immagini.
Modalità tastiera	Abilita la visualizzazione dell'indicatore di input nel titolo della finestra del visualizzatore ogni volta che vengono inviati al sistema remoto eventi relativi al mouse o alla tastiera.
Appunti	Selezionare **Abilita sincronizzazione automatica degli appunti** per abilitare la sincronizzazione al sistema remoto degli appunti se disponibile.
Invia eventi tastiera	Scegliere se acquisire l'input dalla tastiera locale ogni volta che la finestra di Connect Client è attiva o solo al passaggio del puntatore del mouse locale.
Colore di sfondo del visualizzatore	Consente di modificare il colore di sfondo del visualizzatore.
Riconnetti automaticamente	Selezionare **Abilita riconnessione automatica** affinché Connect Client ristabilisca automaticamente la connessione nel caso in cui venga interrotta.
H.264	Consente di disabilitare i decodificatori hardware.
Chiudi quando inattivo	Selezionare l'intervallo di tempo di inattività dopo il quale la finestra del visualizzatore verrà chiusa.

4. Configurare le impostazioni nella scheda **Tastiera**.

Opzione	Descrizione
Mapping modificatori	Consente di modificare il comportamento dei tasti modificatori con un menu a comparsa. Queste impostazioni sono archiviate in modo distinto per le connessioni NEAR, Condivisione schermo di Apple e RDP.
Modalità di input	Per ogni tipo di connessione (selezionata nell'intestazione del pannello), selezionare la modalità di input da tastiera predefinita.

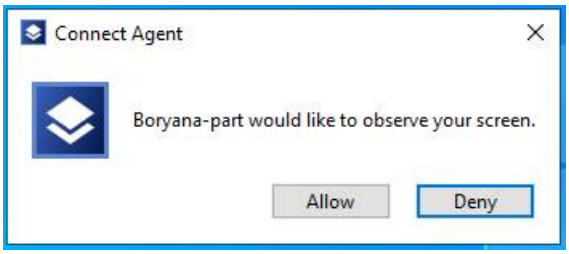
5. Fare clic su **OK**.

Notifier del desktop remoto

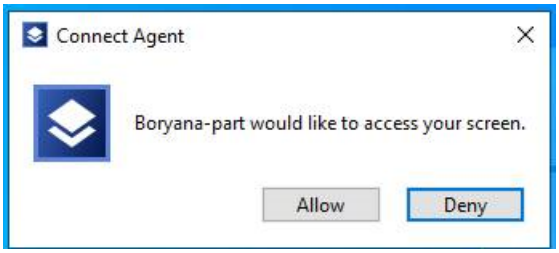
Connect Agent visualizza finestre di dialogo di azione (notifier) nel desktop del workload remoto nei casi seguenti:

© Acronis International GmbH, 2003-2024

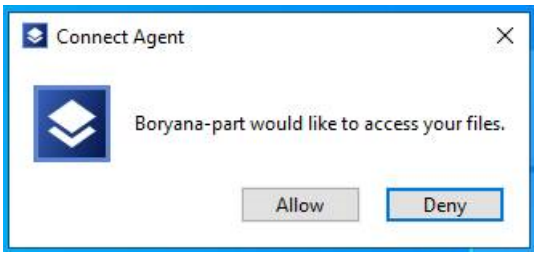
- quando si tenta la connessione al workload da remoto chiedendo l'autorizzazione per l'attività di osservazione. L'utente connesso al workload remoto in locale può accettare o rifiutare la richiesta.



- quando si tenta la connessione al workload da remoto chiedendo l'autorizzazione per l'attività di controllo. L'utente connesso al workload remoto in locale può accettare o rifiutare la richiesta.



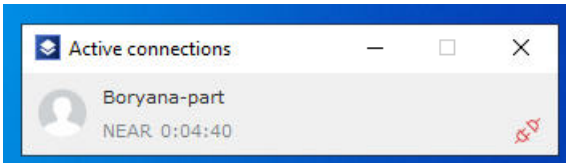
- quando si tenta di scambiare file tra il workload di gestione e quello remoto chiedendo l'autorizzazione per il trasferimento dei file. L'utente connesso al workload remoto in locale può accettare o rifiutare la richiesta.



Quando si stabilisce una connessione desktop remoto con un workload, l'utente connesso al workload visualizzerà un notifier di connessione differente, che contiene le informazioni seguenti:

- nome dell'utente connesso in modalità remota
- protocollo di connessione utilizzato per stabilire la connessione remota
- durata della connessione remota

L'utente connesso al workload remoto in locale può terminare la connessione in qualsiasi momento facendo clic sull'icona **Disconnetti** o sull'icona **Chiudi**.



© Acronis International GmbH, 2003-2024

Monitoraggio dell'integrità e delle prestazioni dei workload

È possibile monitorare i parametri di sistema e l'integrità dei workload dell'organizzazione. Se un parametro non è a norma, l'utente riceverà una notifica immediata e potrà risolvere rapidamente il problema. È inoltre possibile configurare avvisi personalizzati e azioni di risposta automatiche. Sono le azioni che verranno eseguite automaticamente per risolvere le anomalie nel comportamento del workload.

Nota
La funzionalità di monitoraggio richiede l'installazione nel workload dell'agente Protezione versione 15.0.35324 o successiva.

Piani di monitoraggio

Per iniziare a monitorare i parametri relativi alle prestazioni, all'hardware, al software, al sistema e alla sicurezza dei workload gestiti, applicare a ognuno di questi elementi un piano di monitoraggio. I piani di monitoraggio sono costituiti da diversi monitor che è possibile abilitare e configurare. Alcuni monitor supportano il tipo di monitoraggio basato su anomalia. Per ulteriori informazioni sui piani di monitoraggio, vedere "Piani di monitoraggio" (pag. 1088). Per ulteriori informazioni sui monitor disponibili che è possibile configurare nei piani di monitoraggio, vedere "Monitor configurabili" (pag. 1054).

Se, per qualsiasi ragione, l'agente non può acquisire i dati da un workload, il sistema genera un avviso.

Tipi di monitoraggio

È necessario configurare il tipo di monitoraggio di ogni monitor abilitato nel piano. Il tipo di monitoraggio determina l'algoritmo che viene utilizzato dal monitor per valutare il comportamento normale e la deviazione del workload. Esistono due tipi di monitoraggio: il monitoraggio basato su soglia e il monitoraggio basato su anomalia. Alcuni monitor supportano solo il tipo di monitoraggio basato su soglia.

Il monitoraggio basato su soglia registra i valori dei parametri che sono superiori o inferiori a un valore soglia configurato dall'utente. Con questo tipo di monitoraggio, l'utente è responsabile della definizione dei valori soglia corretti per i workload. Il sistema determina il comportamento normale in base a questi valori soglia statici, senza considerare altre condizioni specifiche che possono essere causa del comportamento. Per questa ragione, il monitoraggio basato su soglia potrebbe essere meno preciso rispetto al monitoraggio basato su anomalia.

Il monitoraggio basato su anomalia si avvale di modelli di machine learning per definire i normali schemi di comportamento di un workload e rilevarne quindi un comportamento anomalo. Per ulteriori informazioni, consultare "Monitoraggio basato sulle anomalie" (pag. 1054).

© Acronis International GmbH, 2003-2024

Monitoraggio basato sulle anomalie

Il monitoraggio basato sull'anomalia si avvale di modelli di machine learning per definire i normali schemi di comportamento di un workload e rilevarne quindi le anomalie, ovvero i picchi non previsti in dati in serie temporali. Quando si attiva questa tipologia di monitoraggio, il sistema crea un modello e ne avvia l'addestramento, adeguando il modello al workload specifico in base ai dati che raccoglie dal workload. Ciò significa che all'inizio del periodo di addestramento i dati potrebbero non essere completamente corretti. La creazione di un modello affidabile richiede almeno tre settimane di addestramento del modello. Mano a mano che il sistema raccoglie più dati e analizza i set di dati cronologici, affina gradualmente il modello e crea le soglie dinamiche superiore e inferiore per ogni metrica del workload. Questo tipo di monitoraggio è più flessibile rispetto al monitoraggio basato su soglia, in quanto il sistema monitora i valori dei parametri e il loro contesto. Ad esempio, potrebbe essere normale che un workload specifico abbia un carico maggiore in alcune ore del giorno. Un tipo di monitoraggio basato su soglia interpreta erroneamente questo comportamento come anormale e genera un avviso.

È possibile reimpostare i modelli di machine learning di un workload. In questo caso, il sistema elimina tutti i dati e i modelli dei monitor applicati al workload. Per ulteriori informazioni, consultare "Reimpostazione dei modelli di machine learning" (pag. 1098).

Piattaforme supportate per il monitoraggio

La funzionalità di monitoraggio è supportata dai seguenti sistemi operativi.

Versioni supportate di Windows	Versioni supportate di macOS
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x (Big Sur) • macOS 12.x (Monterey) • macOS 13.x (Ventura)

Monitor configurabili

La funzionalità di monitoraggio supporta i monitor seguenti, divisi in sei categorie: Hardware, Prestazioni, Software, Sistema, Sicurezza, Personalizzato.

© Acronis International GmbH, 2003-2024

Monitor	Descrizione	Sistemi operativi supportati	Frequenza della raccolta di dati	Supporto del monitoraggio basato su anomalia	Disponibilità in Standard Protection o in Advanced Management
Hardware					
Spazio su disco	Monitora lo spazio libero su un'unità specifica del workload.	Windows macOS	1 minuto	Sì	Standard Protection
Temperatura CPU	Monitora la temperatura della CPU.	Windows macOS	30 sec	Sì	Advanced Management
Temperatura GPU	Monitora la temperatura della GPU.	Windows macOS	30 sec	Sì	Advanced Management
Modifiche hardware	Monitora le modifiche hardware, come l'aggiunta, la rimozione o la sostituzione dell'hardware in un workload	Windows macOS	24 ore	No	Standard Protection
Prestazioni					
Utilizzo CPU	Monitora l'utilizzo complessivo della memoria (da parte di tutte le CPU nel workload).	Windows macOS	30 sec	Sì	Advanced Management
Utilizzo della memoria	Monitora l'utilizzo complessivo della memoria (da parte di tutti gli slot di memoria nel	Windows macOS	30 sec	Sì	Advanced Management

© Acronis International GmbH, 2003-2024

Monitor	Descrizione	Sistemi operativi supportati	Frequenza della raccolta di dati	Supporto del monitoraggio basato su anomalia	Disponibilità in Standard Protection o in Advanced Management
	workload).				
Velocità di trasferimento disco	Monitora la velocità di lettura e scrittura di ogni disco fisico nel workload.	Windows macOS	30 sec	Sì	Advanced Management
Utilizzo della rete	Monitora il traffico in entrata e in uscita per ogni adattatore di rete del workload.	Windows macOS	30 sec	Sì	Advanced Management
Utilizzo della CPU per processo	Monitora l'utilizzo della CPU da parte di determinati processi.	Windows macOS	30 sec	No	Advanced Management
Utilizzo della memoria per processo	Monitora l'utilizzo della memoria da parte del processo selezionato.	Windows macOS	30 sec	No	Advanced Management
Velocità di trasferimento disco per processo	Monitora la velocità di lettura e scrittura del processo selezionato.	Windows macOS	30 sec	No	Advanced Management
Utilizzo della rete per processo	Monitora il traffico in entrata e in uscita del	Windows macOS	30 sec	No	Advanced Management

© Acronis International GmbH, 2003-2024

Monitor	Descrizione	Sistemi operativi supportati	Frequenza della raccolta di dati	Supporto del monitoraggio basato su anomalia	Disponibilità in Standard Protection o in Advanced Management
	processo selezionato.				
Software					
Stato dei servizi Windows	Monitora lo stato del servizio Windows selezionato (In esecuzione o Arrestato).	Windows	30 sec	No	Advanced Management
Stato del processo	Monitora lo stato del processo selezionato (In esecuzione o Arrestato).	Windows macOS	30 sec	No	Advanced Management
Software installato	Monitora l'installazione, l'aggiornamento o l'eliminazione di applicazioni software.	Windows macOS	24 ore	No	Advanced Management
Sistema					
Ultimo riavvio del sistema	Monitora se il workload è stato riavviato.	Windows macOS	1 ora	No	Standard Protection
Registro eventi di Windows	Monitora specifici eventi critici per l'azienda nel registro degli eventi di Windows.	Windows	10 min	No	Advanced Management
Dimensione	Monitora la	Windows	10 min	No	Standard

© Acronis International GmbH, 2003-2024

Monitor	Descrizione	Sistemi operativi supportati	Frequenza della raccolta di dati	Supporto del monitoraggio basato su anomalia	Disponibilità in Standard Protection o in Advanced Management
file e cartelle	dimensione totale dei file o delle cartelle selezionati.	macOS			Protection
Sicurezza					
Stato di Windows Update	Monitora lo stato di Windows Update del workload e se gli aggiornamenti più recenti sono stati installati.	Windows	15 min	No	Advanced Management
Stato del firewall	Monitora lo stato del firewall integrato o di terzi installato nel workload.	Windows macOS	5 min	No	Advanced Management
Stato del software anti-malware	Monitora lo stato del software anti-malware integrato o di terzi installato nel workload.	Windows macOS	5 min	No	Advanced Management
Accessi non riusciti	Monitora i tentativi di accesso non riusciti al workload.	Windows	1 ora	No	Advanced Management
Stato della funzionalità di esecuzione	Monitora se la funzionalità di esecuzione	Windows	1 ora	No	Advanced Management

© Acronis International GmbH, 2003-2024

Monitor	Descrizione	Sistemi operativi supportati	Frequenza della raccolta di dati	Supporto del monitoraggio basato su anomalia	Disponibilità in Standard Protection o in Advanced Management
automatica	automatica per il supporto di storage rimovibile è abilitata.				
Personalizzato					
Personalizzato	Monitora gli oggetti personalizzati tramite script in esecuzione.	Windows macOS	personalizzato	No	Advanced Management

Impostazioni del monitor Spazio su disco

Il monitor **Spazio su disco** controlla lo spazio libero su un'unità specifica del workload.

Nota
Nel calcolo dello spazio, il monitor utilizza byte binari (1024 byte per KB, 1024 KB per MB e 1024 MB per GB) sia per i workload Windows che per quelli macOS.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Monitoraggio basato su soglia	
Unità	L'unità che si desidera monitorare. Sono disponibili i seguenti valori. • **Unità di sistema** —Questo è il valore predefinito. • **Qualsiasi unità**
Operatore	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Meno di** —Questo è il valore predefinito. • **Minore o uguale a**
Soglia dello	Il valore soglia e il valore **Operatore** determinano la prestazione normale

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
spazio libero su disco	della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero incluso nell'intervallo 1-100 (min). Il valore predefinito è 20.
Includere unità rimovibili	Questa impostazione è disponibile se il valore **Unità** è impostato su **Qualsiasi unità**. Selezionare questa impostazione per aggiungere al monitoraggio unità rimovibili come un'unità flash USB. Per impostazione predefinita, questa impostazione è disabilitata.
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 30.
Monitoraggio basato sulle anomalie	
Unità	L'unità che si desidera monitorare. Sono disponibili i seguenti valori. • **Unità di sistema** —Questo è il valore predefinito. • **Qualsiasi unità**
Periodo di addestramento del modello	Il periodo in cui il sistema addestra i modelli di machine learning utilizzando i dati raccolti dagli agenti e crea i modelli di comportamento normale del workload. Più è lungo il periodo di addestramento del modello e più precisi saranno i modelli di comportamento a lungo termine che verranno creati dal sistema. Il periodo minimo consigliato per la formazione del modello è di 21 giorni. Inserire un valore intero (giorni). Il valore predefinito è 21.
Ricevi avvisi su anomalie durante il periodo di addestramento	Se si seleziona questa impostazione, si riceveranno avvisi relativi alle anomalie rilevate durante il periodo di addestramento del modello. Questi avvisi potrebbero essere falsati, perché i modelli sono ancora in fase di addestramento e potrebbero non essere sufficientemente precisi. Per impostazione predefinita, l'impostazione è selezionata.
Livello di sensibilità	Il livello di sensibilità funge da filtro preliminare per le anomalie se i valori di queste rientrano in un intervallo specifico. Questo filtro opera in modo indipendente dall'algoritmo di rilevamento dell'anomalia. La sua finalità è quella di arrestare le anomalie che rientrano nell'intervallo specificato evitando che vengano elaborate dall'algoritmo di rilevamento. Durante il periodo di addestramento:

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	1. L'algoritmo viene addestrato utilizzando i dati acquisiti durante l'addestramento. 2. L'algoritmo esegue il rilevamento delle anomalie sui dati di addestramento. 3. Viene applicato un processo di filtraggio basato sulla deviazione media e standard. 4. Viene filtrata qualsiasi anomalia che rientra nell'intervallo specificato. 5. Dai punti dati anomali rimanenti, viene selezionata l'anomalia con il livello più basso. Questo livello (un numero a virgola mobile compreso tra 0 e 1) viene registrato nel modello. Durante la fase di previsione: 1. L'algoritmo prevede le anomalie mediante i dati di inferenza. 2. Le anomalie previste vengono filtrate in base alla deviazione media e standard, secondo il livello di sensibilità. 3. Le anomalie rimanenti vengono ulteriormente filtrate in base al principio seguente: i valori superiori al livello soglia vengono considerati anomalie, mentre i valori al di sotto del livello soglia vengono considerati comportamenti normali. Sono disponibili i seguenti valori. • **Basso**. Il livello basso equivale al valore medio e al valore della deviazione standard. • **Normale**. Questo è il valore predefinito. Il livello normale equivale al valore medio e al doppio del valore della deviazione standard. • **Alto**. Il livello alto equivale al valore medio e al triplo del valore della deviazione standard.
Durata dell'anomalia	Il sistema genera un avviso per l'anomalia rilevata solo se il comportamento anomalo persiste per il periodo specificato. Il valore predefinito è 30 minuti.

Impostazioni del monitor Temperatura CPU

Il monitor **Temperatura CPU** controlla la temperatura della CPU.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Monitoraggio basato su soglia	
La temperatura CPU è stata superata (°C)	Il valore massimo della metrica monitorata. Se il valore viene superato, il sistema genera un avviso. Inserire un valore intero (°C). Il valore predefinito è 80.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.
Monitoraggio basato sulle anomalie	
Periodo di addestramento del modello	Il periodo in cui il sistema addestra i modelli di machine learning utilizzando i dati raccolti dagli agenti e crea i modelli di comportamento normale del workload. Più è lungo il periodo di addestramento del modello e più precisi saranno i modelli di comportamento a lungo termine che verranno creati dal sistema. Il periodo minimo consigliato per la formazione del modello è di 21 giorni. Inserire un valore intero (giorni). Il valore predefinito è 21.
Livello di sensibilità	Il livello di sensibilità funge da filtro preliminare per le anomalie se i valori di queste rientrano in un intervallo specifico. Questo filtro opera in modo indipendente dall'algoritmo di rilevamento dell'anomalia. La sua finalità è quella di arrestare le anomalie che rientrano nell'intervallo specificato evitando che vengano elaborate dall'algoritmo di rilevamento. Durante il periodo di addestramento: 1. L'algoritmo viene addestrato utilizzando i dati acquisiti durante l'addestramento. 2. L'algoritmo esegue il rilevamento delle anomalie sui dati di addestramento. 3. Viene applicato un processo di filtraggio basato sulla deviazione media e standard. 4. Viene filtrata qualsiasi anomalia che rientra nell'intervallo specificato. 5. Dai punti dati anomali rimanenti, viene selezionata l'anomalia con il livello più basso. Questo livello (un numero a virgola mobile compreso tra 0 e 1) viene registrato nel modello. Durante la fase di previsione: 1. L'algoritmo prevede le anomalie mediante i dati di inferenza. 2. Le anomalie previste vengono filtrate in base alla deviazione media e standard, secondo il livello di sensibilità. 3. Le anomalie rimanenti vengono ulteriormente filtrate in base al principio seguente: i valori superiori al livello soglia vengono considerati anomalie, mentre i valori al di sotto del

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	livello soglia vengono considerati comportamenti normali. Sono disponibili i seguenti valori. • **Basso**. Il livello basso equivale al valore medio e al valore della deviazione standard. • **Normale**. Questo è il valore predefinito. Il livello normale equivale al valore medio e al doppio del valore della deviazione standard. • **Alto**. Il livello alto equivale al valore medio e al triplo del valore della deviazione standard.
Durata dell'anomalia	Il sistema genera un avviso per l'anomalia rilevata solo se il comportamento anomalo persiste per il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 15.

Impostazioni del monitor Temperatura GPU

Il monitor **Temperatura GPU** controlla la temperatura della GPU del workload.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Monitoraggio basato su soglia	
La temperatura GPU è stata superata	Il valore massimo della metrica monitorata. Se il valore viene superato, il sistema rileva un'anomalia. Inserire un valore intero (°C). Il valore predefinito è 80.
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.
Monitoraggio basato sulle anomalie	
Periodo di addestramento del modello	Il periodo in cui il sistema addestra i modelli di machine learning utilizzando i dati raccolti dagli agenti e crea i modelli di comportamento normale del workload. Più è lungo il periodo di addestramento del modello e più precisi saranno i modelli di comportamento a lungo termine che verranno creati dal sistema. Il periodo minimo consigliato per la formazione del modello è di 21 giorni. Inserire un valore intero (giorni). Il valore predefinito è 21.
Livello di	Il livello di sensibilità funge da filtro preliminare per le anomalie se i valori

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
sensibilità	di queste rientrano in un intervallo specifico. Questo filtro opera in modo indipendente dall'algoritmo di rilevamento dell'anomalia. La sua finalità è quella di arrestare le anomalie che rientrano nell'intervallo specificato evitando che vengano elaborate dall'algoritmo di rilevamento. Durante il periodo di addestramento: 1. L'algoritmo viene addestrato utilizzando i dati acquisiti durante l'addestramento. 2. L'algoritmo esegue il rilevamento delle anomalie sui dati di addestramento. 3. Viene applicato un processo di filtraggio basato sulla deviazione media e standard. 4. Viene filtrata qualsiasi anomalia che rientra nell'intervallo specificato. 5. Dai punti dati anomali rimanenti, viene selezionata l'anomalia con il livello più basso. Questo livello (un numero a virgola mobile compreso tra 0 e 1) viene registrato nel modello. Durante la fase di previsione: 1. L'algoritmo prevede le anomalie mediante i dati di inferenza. 2. Le anomalie previste vengono filtrate in base alla deviazione media e standard, secondo il livello di sensibilità. 3. Le anomalie rimanenti vengono ulteriormente filtrate in base al principio seguente: i valori superiori al livello soglia vengono considerati anomalie, mentre i valori al di sotto del livello soglia vengono considerati comportamenti normali. Sono disponibili i seguenti valori. • **Basso**. Il livello basso equivale al valore medio e al valore della deviazione standard. • **Normale**. Questo è il valore predefinito. Il livello normale equivale al valore medio e al doppio del valore della deviazione standard. • **Alto**. Il livello alto equivale al valore medio e al triplo del valore della deviazione standard.
Durata dell'anomalia	Il sistema genera un avviso per l'anomalia rilevata solo se il comportamento anomalo persiste per il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 15.

Impostazioni del monitor Modifiche hardware

Il monitor **Modifiche hardware** controlla le modifiche hardware, come l'aggiunta, la rimozione o la sostituzione dell'hardware in un workload.

Per il monitor sono configurabili le impostazioni indicate di seguito.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
Componenti hardware	Selezionare uno o più componenti hardware di cui monitorare le modifiche. Sono disponibili i seguenti valori. • **Tutti** - Questo è il valore predefinito. • **Scheda madre** • **CPU** • **RAM** • **Disco** • **GPU** • **Adattatore di rete**
Aspetti da monitorare	Specificare le modifiche da monitorare nei componenti hardware selezionati. È possibile selezionare più elementi dall'elenco. Sono disponibili i seguenti valori. • **Qualsiasi modifica** -Questo è il valore predefinito. • **Componente aggiunto** • **Componente sostituito** • **Componente rimosso**

Impostazioni del monitor Utilizzo della CPU

Il monitor **Utilizzo CPU** controlla l'utilizzo totale della CPU (utilizzo del processore) da parte del workload. Se il workload ha più CPU, l'utilizzo di CPU totale sarà dato dalla somma dell'utilizzo della CPU di ogni CPU.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Monitoraggio basato su soglia	
Operatore	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito. • **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia di utilizzo della CPU	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero incluso nell'intervallo 1-100 (min). Il valore

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	predefinito è 90.
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.
Monitoraggio basato sulle anomalie	
Periodo di addestramento del modello	Il periodo in cui il sistema addestra i modelli di machine learning utilizzando i dati raccolti dagli agenti e crea i modelli di comportamento normale del workload. Più è lungo il periodo di addestramento del modello e più precisi saranno i modelli di comportamento a lungo termine che verranno creati dal sistema. Il periodo minimo consigliato per la formazione del modello è di 21 giorni. Inserire un valore intero (giorni). Il valore predefinito è 21.
Ricevi avvisi su anomalie durante il periodo di addestramento	Se si seleziona questa impostazione, si riceveranno avvisi relativi alle anomalie rilevate durante il periodo di addestramento del modello. Questi avvisi potrebbero essere falsati, perché i modelli sono ancora in fase di addestramento e potrebbero non essere sufficientemente precisi. Per impostazione predefinita, l'impostazione è selezionata.
Livello di sensibilità	Il livello di sensibilità funge da filtro preliminare per le anomalie se i valori di queste rientrano in un intervallo specifico. Questo filtro opera in modo indipendente dall'algoritmo di rilevamento dell'anomalia. La sua finalità è quella di arrestare le anomalie che rientrano nell'intervallo specificato evitando che vengano elaborate dall'algoritmo di rilevamento. Durante il periodo di addestramento: 1. L'algoritmo viene addestrato utilizzando i dati acquisiti durante l'addestramento. 2. L'algoritmo esegue il rilevamento delle anomalie sui dati di addestramento. 3. Viene applicato un processo di filtraggio basato sulla deviazione media e standard. 4. Viene filtrata qualsiasi anomalia che rientra nell'intervallo specificato. 5. Dai punti dati anomali rimanenti, viene selezionata l'anomalia con il livello più basso. Questo livello (un numero a virgola mobile compreso tra 0 e 1) viene registrato nel modello. Durante la fase di previsione: 1. L'algoritmo prevede le anomalie mediante i dati di inferenza. 2. Le anomalie previste vengono filtrate in base alla deviazione media e standard, secondo il livello di sensibilità.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	3. Le anomalie rimanenti vengono ulteriormente filtrate in base al principio seguente: i valori superiori al livello soglia vengono considerati anomalie, mentre i valori al di sotto del livello soglia vengono considerati comportamenti normali. Sono disponibili i seguenti valori. • **Basso**. Il livello basso equivale al valore medio e al valore della deviazione standard. • **Normale**. Questo è il valore predefinito. Il livello normale equivale al valore medio e al doppio del valore della deviazione standard. • **Alto**. Il livello alto equivale al valore medio e al triplo del valore della deviazione standard.
Durata dell'anomalia	Il sistema genera un avviso per l'anomalia rilevata solo se il comportamento anomalo persiste per il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 15.

Impostazioni del monitor Utilizzo della memoria

Il monitor **Utilizzo della memoria** controlla l'utilizzo totale della memoria da parte di tutti i moduli di memoria del workload.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Monitoraggio basato su soglia	
Operatore	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito. • **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia di utilizzo della memoria	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero incluso nell'intervallo 1-100 (min). Il valore predefinito è 90.
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.
Monitoraggio basato sulle anomalie	
Periodo di addestramento del modello	Il periodo in cui il sistema addestra i modelli di machine learning utilizzando i dati raccolti dagli agenti e crea i modelli di comportamento normale del workload. Più è lungo il periodo di addestramento del modello e più precisi saranno i modelli di comportamento a lungo termine che verranno creati dal sistema. Il periodo minimo consigliato per la formazione del modello è di 21 giorni. Inserire un valore intero (giorni). Il valore predefinito è 21.
Ricevi avvisi su anomalie durante il periodo di addestramento	Se si seleziona questa impostazione, si riceveranno avvisi relativi alle anomalie rilevate durante il periodo di addestramento del modello. Questi avvisi potrebbero essere falsati, perché i modelli sono ancora in fase di addestramento e potrebbero non essere sufficientemente precisi. Per impostazione predefinita, l'impostazione è selezionata.
Livello di sensibilità	Il livello di sensibilità funge da filtro preliminare per le anomalie se i valori di queste rientrano in un intervallo specifico. Questo filtro opera in modo indipendente dall'algoritmo di rilevamento dell'anomalia. La sua finalità è quella di arrestare le anomalie che rientrano nell'intervallo specificato evitando che vengano elaborate dall'algoritmo di rilevamento. Durante il periodo di addestramento: 1. L'algoritmo viene addestrato utilizzando i dati acquisiti durante l'addestramento. 2. L'algoritmo esegue il rilevamento delle anomalie sui dati di addestramento. 3. Viene applicato un processo di filtraggio basato sulla deviazione media e standard. 4. Viene filtrata qualsiasi anomalia che rientra nell'intervallo specificato. 5. Dai punti dati anomali rimanenti, viene selezionata l'anomalia con il livello più basso. Questo livello (un numero a virgola mobile compreso tra 0 e 1) viene registrato nel modello. Durante la fase di previsione: 1. L'algoritmo prevede le anomalie mediante i dati di inferenza. 2. Le anomalie previste vengono filtrate in base alla deviazione media e standard, secondo il livello di sensibilità. 3. Le anomalie rimanenti vengono ulteriormente filtrate in base al principio seguente: i valori superiori al livello soglia vengono considerati anomalie, mentre i valori al di sotto del livello soglia vengono considerati comportamenti normali.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	Sono disponibili i seguenti valori. • **Basso**. Il livello basso equivale al valore medio e al valore della deviazione standard. • **Normale**. Questo è il valore predefinito. Il livello normale equivale al valore medio e al doppio del valore della deviazione standard. • **Alto**. Il livello alto equivale al valore medio e al triplo del valore della deviazione standard.
Durata dell'anomalia	Il sistema genera un avviso per l'anomalia rilevata solo se il comportamento anomalo persiste per il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 30 minuti.

Impostazioni del monitor Velocità di trasferimento disco

Il monitor **Velocità di trasferimento disco** controlla la velocità di lettura e scrittura di ogni disco fisico nel workload.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Monitoraggio basato su soglia	
Aspetti da monitorare	Selezionare la velocità da monitorare. Sono disponibili i seguenti valori. • **Velocità di lettura e velocità di scrittura**. Questo è il valore predefinito. • **Velocità di lettura** • **Velocità di scrittura**
Operatore velocità di lettura	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di**. Questo è il valore predefinito. • **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia velocità di lettura	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero (kb/sec). Il valore predefinito è 0 kb/sec.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
Periodo di tempo della velocità di lettura	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.
Operatore velocità di scrittura	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito. • **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia velocità di scrittura	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero (kb/sec). Il valore predefinito è 0 kb/sec.
Periodo di tempo della velocità di scrittura	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.
Monitoraggio basato sulle anomalie	
Periodo di addestramento del modello	Il periodo in cui il sistema addestra i modelli di machine learning utilizzando i dati raccolti dagli agenti e crea i modelli di comportamento normale del workload. Più è lungo il periodo di addestramento del modello e più precisi saranno i modelli di comportamento a lungo termine che verranno creati dal sistema. Il periodo minimo consigliato per la formazione del modello è di 21 giorni. Inserire un valore intero (giorni). Il valore predefinito è 21.
Ricevi avvisi su anomalie durante il periodo di addestramento	Se si seleziona questa impostazione, si riceveranno avvisi relativi alle anomalie rilevate durante il periodo di addestramento del modello. Questi avvisi potrebbero essere falsati, perché i modelli sono ancora in fase di addestramento e potrebbero non essere sufficientemente precisi. Per impostazione predefinita, l'impostazione è selezionata.
Aspetti da monitorare	Selezionare la velocità da monitorare. Sono disponibili i seguenti valori. • **Velocità di lettura e velocità di scrittura**. Questo è il valore predefinito.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	• **Velocità di lettura** • **Velocità di scrittura**
Livello di sensibilità	Il livello di sensibilità funge da filtro preliminare per le anomalie se i valori di queste rientrano in un intervallo specifico. Questo filtro opera in modo indipendente dall'algoritmo di rilevamento dell'anomalia. La sua finalità è quella di arrestare le anomalie che rientrano nell'intervallo specificato evitando che vengano elaborate dall'algoritmo di rilevamento. Durante il periodo di addestramento: 1. L'algoritmo viene addestrato utilizzando i dati acquisiti durante l'addestramento. 2. L'algoritmo esegue il rilevamento delle anomalie sui dati di addestramento. 3. Viene applicato un processo di filtraggio basato sulla deviazione media e standard. 4. Viene filtrata qualsiasi anomalia che rientra nell'intervallo specificato. 5. Dai punti dati anomali rimanenti, viene selezionata l'anomalia con il livello più basso. Questo livello (un numero a virgola mobile compreso tra 0 e 1) viene registrato nel modello. Durante la fase di previsione: 1. L'algoritmo prevede le anomalie mediante i dati di inferenza. 2. Le anomalie previste vengono filtrate in base alla deviazione media e standard, secondo il livello di sensibilità. 3. Le anomalie rimanenti vengono ulteriormente filtrate in base al principio seguente: i valori superiori al livello soglia vengono considerati anomalie, mentre i valori al di sotto del livello soglia vengono considerati comportamenti normali. Sono disponibili i seguenti valori. • **Basso**. Il livello basso equivale al valore medio e al valore della deviazione standard. • **Normale**. Questo è il valore predefinito. Il livello normale equivale al valore medio e al doppio del valore della deviazione standard. • **Alto**. Il livello alto equivale al valore medio e al triplo del valore della deviazione standard.
Durata dell'anomalia (velocità di lettura)	Il sistema genera un avviso per l'anomalia rilevata solo se il comportamento anomalo persiste per il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 25.
Durata	Il sistema genera un avviso per l'anomalia rilevata solo se il comportamento anomalo persiste per il periodo specificato.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
dell'anomalia (velocità di scrittura)	Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 25.

Impostazioni del monitor Utilizzo della rete

Il monitor **Utilizzo della rete** controlla il traffico in entrata e in uscita per ogni adattatore di rete del workload.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Monitoraggio basato su soglia	
Direzione del traffico	La direzione del traffico da monitorare. Sono disponibili i seguenti valori. • **Traffico in entrata e in uscita**. Questo è il valore predefinito. • **Traffico in entrata** • **Traffico in uscita**
Operatore traffico in entrata	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito. • **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia traffico in entrata	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero (kb/sec). Il valore predefinito è 0 kb/sec.
Periodo di tempo traffico in entrata	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.
Operatore traffico in uscita	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	• **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia traffico in uscita	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero (kb/sec). Il valore predefinito è 0 kb/sec.
Periodo di tempo traffico in uscita	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.
Monitoraggio basato sulle anomalie	
Periodo di addestramento del modello	Il periodo in cui il sistema addestra i modelli di machine learning utilizzando i dati raccolti dagli agenti e crea i modelli di comportamento normale del workload. Più è lungo il periodo di addestramento del modello e più precisi saranno i modelli di comportamento a lungo termine che verranno creati dal sistema. Il periodo minimo consigliato per la formazione del modello è di 21 giorni. Inserire un valore intero (giorni). Il valore predefinito è 21.
Ricevi avvisi su anomalie durante il periodo di addestramento	Se si seleziona questa impostazione, si riceveranno avvisi relativi alle anomalie rilevate durante il periodo di addestramento del modello. Questi avvisi potrebbero essere falsati, perché i modelli sono ancora in fase di addestramento e potrebbero non essere sufficientemente precisi. Per impostazione predefinita, l'impostazione è selezionata.
Direzione del traffico	• **Traffico in entrata e in uscita**. Questo è il valore predefinito. • **Traffico in entrata** • **Traffico in uscita**
Livello di sensibilità	Il livello di sensibilità funge da filtro preliminare per le anomalie se i valori di queste rientrano in un intervallo specifico. Questo filtro opera in modo indipendente dall'algoritmo di rilevamento dell'anomalia. La sua finalità è quella di arrestare le anomalie che rientrano nell'intervallo specificato evitando che vengano elaborate dall'algoritmo di rilevamento. Durante il periodo di addestramento: 1. L'algoritmo viene addestrato utilizzando i dati acquisiti durante l'addestramento. 2. L'algoritmo esegue il rilevamento delle anomalie sui dati di

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	addestramento. 3. Viene applicato un processo di filtraggio basato sulla deviazione media e standard. 4. Viene filtrata qualsiasi anomalia che rientra nell'intervallo specificato. 5. Dai punti dati anomali rimanenti, viene selezionata l'anomalia con il livello più basso. Questo livello (un numero a virgola mobile compreso tra 0 e 1) viene registrato nel modello. Durante la fase di previsione: 1. L'algoritmo prevede le anomalie mediante i dati di inferenza. 2. Le anomalie previste vengono filtrate in base alla deviazione media e standard, secondo il livello di sensibilità. 3. Le anomalie rimanenti vengono ulteriormente filtrate in base al principio seguente: i valori superiori al livello soglia vengono considerati anomalie, mentre i valori al di sotto del livello soglia vengono considerati comportamenti normali. Sono disponibili i seguenti valori. • **Basso**. Il livello basso equivale al valore medio e al valore della deviazione standard. • **Normale**. Questo è il valore predefinito. Il livello normale equivale al valore medio e al doppio del valore della deviazione standard. • **Alto**. Il livello alto equivale al valore medio e al triplo del valore della deviazione standard.
Durata dell'anomalia (in ingresso)	Il sistema genera un avviso per l'anomalia rilevata solo se il comportamento anomalo persiste per il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 25.
Durata dell'anomalia (in uscita)	Il sistema genera un avviso per l'anomalia rilevata solo se il comportamento anomalo persiste per il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 25.

Impostazioni del monitor Utilizzo della CPU per processo

Il monitor **Utilizzo della CPU per processo** controlla l'utilizzo della CPU da parte del processo selezionato. In presenza di più istanze dello stesso processo, il sistema monitora l'utilizzo totale di tutte le istanze del processo e genera un avviso quando vengono soddisfatte le condizioni specificate.

Per il monitor sono configurabili le impostazioni indicate di seguito.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
Nome del processo	Il nome del processo da monitorare. Inserire il nome del processo senza estensione.
Operatore	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito. • **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero incluso nell'intervallo 1-100 (min). Il valore predefinito è 90.
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.

Impostazioni del monitor Utilizzo della memoria per processo

Il monitor **Utilizzo della memoria per processo** controlla l'utilizzo della memoria da parte del processo selezionato. In presenza di più istanze dello stesso processo, il sistema monitora l'utilizzo totale di tutte le istanze del processo e genera un avviso quando vengono soddisfatte le condizioni specificate.

Nota
Gli agenti utilizzano il working set complessivo del processo (privato e condiviso) per quantificare la dimensione dell'utilizzo di memoria da parte del processo stesso. Per questo motivo la dimensione che il widget mostra potrebbe differire dalla dimensione dell'utilizzo di memoria che mostra Gestione attività di Windows (working set privato).

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Nome del processo	Il nome del processo da monitorare. Inserire il nome del processo senza estensione.
Operatore	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito. • **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero (kb). Il valore predefinito è 1.
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.

Impostazioni del monitor Velocità di trasferimento disco per processo

Il monitor **Velocità di trasferimento disco per processo** controlla la velocità di lettura e scrittura del processo selezionato. In presenza di più istanze dello stesso processo, il sistema monitora l'utilizzo totale di tutte le istanze del processo e genera un avviso quando vengono soddisfatte le condizioni specificate.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Nome del processo	Il nome del processo da monitorare. Inserire il nome del processo senza estensione.
Aspetti da monitorare	La velocità da monitorare. Sono disponibili i seguenti valori. • **Velocità di lettura e velocità di scrittura**. Questo è il valore predefinito. • **Velocità di lettura** • **Velocità di scrittura**
Operatore velocità di lettura	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	• **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia velocità di lettura	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero (kb/sec). Il valore predefinito è 0 kb/sec.
Periodo di tempo della velocità di lettura	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.
Operatore velocità di scrittura	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito. • **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia velocità di scrittura	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero (kb/sec). Il valore predefinito è 0 kb/sec.
Periodo di tempo della velocità di scrittura	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.

Impostazioni del monitor Utilizzo della rete per processo

Il monitor **Utilizzo della rete per processo** controlla il traffico in entrata e in uscita del processo selezionato. In presenza di più istanze dello stesso processo, il sistema monitora l'utilizzo totale di tutte le istanze del processo e genera un avviso quando vengono soddisfatte le condizioni specificate per tutte le istanze.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Nome del	Il nome del processo da monitorare. Inserire il nome del processo senza

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
processo	estensione.
Direzione del traffico	La direzione del traffico da monitorare. Sono disponibili i seguenti valori. • **Traffico in entrata e in uscita**. Questo è il valore predefinito. • **Traffico in entrata** • **Traffico in uscita**
Operatore traffico in entrata	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito. • **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia traffico in entrata	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero (kb/sec). Il valore predefinito è 0 kb/sec.
Periodo di tempo traffico in entrata	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.
Operatore traffico in uscita	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito. • **Maggiore o uguale a** • **Minore di** • **Minore o uguale a**
Soglia traffico in uscita	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero (kb/sec). Il valore predefinito è 0 kb/sec.
Periodo di tempo traffico in uscita	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 5.

© Acronis International GmbH, 2003-2024

Impostazioni del monitor Stato dei servizi Windows

Il monitor **Stato dei servizi Windows** controlla se il servizio Windows selezionato è in esecuzione o è stato arrestato.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Nome del servizio	Il nome del servizio Windows da monitorare. È possibile selezionare il nome di un servizio dall'elenco dei servizi Windows. Questo elenco viene compilato da tutti gli agenti del tenant quando la scansione dell'inventario software sui workload viene completata correttamente. È anche possibile aggiungere un nome di servizio non presente nell'elenco. È l'unica opzione disponibile se la scansione dell'inventario software non è stata eseguita nei workload.
Stato servizio	Se il servizio è nello stato selezionato, il sistema genera un evento. Sono disponibili i seguenti valori. • **In esecuzione** • **Interrotto**—Questo è il valore predefinito.
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 1.

Impostazioni del monitor Stato del processo

Il monitor **Stato del processo** controlla se il processo selezionato è in esecuzione o se è stato interrotto. In presenza di più istanze dello stesso processo, il sistema monitora ogni istanza e genera l'avviso quando vengono soddisfatte le condizioni per tutte le istanze del processo.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Nome del processo	Il nome del processo da monitorare. Specificare il nome del file eseguibile senza estensione.
Stato del processo	Se il processo è nello stato selezionato, il sistema genererà un evento. Sono disponibili i seguenti valori. • **In esecuzione** • **Interrotto**—Questo è il valore predefinito.
Periodo di	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
tempo	metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-60 (min). Il valore predefinito è 1.

Impostazioni del monitor Software installato

Il monitor **Software installato** controlla l'installazione, l'aggiornamento o l'eliminazione di applicazioni software dal workload.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Software da monitorare	Specificare il software da monitorare. Sono disponibili i seguenti valori. • **Qualsiasi software** -Questo è il valore predefinito. • **Software specifico**
Nome software	Questa impostazione diventa disponibile se si seleziona il valore **Software specifico** per la voce **Software da monitorare**. Inserire il nome di una o di diverse applicazioni software. È possibile selezionare il nome di un'applicazione software dall'elenco dei servizi Windows. Questo elenco viene compilato da tutti gli agenti del tenant quando la scansione dell'inventario software sui workload viene completata correttamente. È anche possibile aggiungere un nome di applicazione software non presente nell'elenco. È l'unica opzione disponibile se la scansione dell'inventario software non è stata eseguita nei workload.
Stato installazione	Specificare se monitorare il software installato, non installato o aggiornato. Sono disponibili i seguenti valori. • **Installato**: Questo è il valore predefinito. Se si seleziona questo valore, il monitor genera un avviso quando viene installata una nuova applicazione software sul workload. • **Aggiornato**: Se si seleziona questo valore, il monitor genera un avviso quando viene aggiornata un'applicazione software. • **Non installato**: Se si seleziona questo valore, il monitor genera un avviso quando un'applicazione software viene disinstallata o non è disponibile sul workload.

Impostazioni del monitor Ultimo riavvio del sistema

Il monitor **Ultimo riavvio del sistema** controlla l'ultimo avvio del workload.

Per il monitor è configurabile l'impostazione indicata di seguito.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
Il workload non è stato riavviato per	Il periodo (espresso in numero di giorni) trascorso dall'ultimo riavvio del workload. Se il workload non è stato riavviato per un periodo più lungo di quello specificato, il sistema genera un avviso. Inserire un valore intero incluso nell'intervallo 1-180 (giorni). Il valore predefinito è 30.

Impostazioni del monitor Registro eventi di Windows

Il monitor **Registro eventi di Windows** monitora specifici eventi critici per l'azienda nel registro degli eventi di Windows.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Nome registro eventi	Selezionare un registro eventi specifico dall'elenco dei Registri eventi di Windows disponibile nel Visualizzatore eventi. Sono disponibili i seguenti valori. • **Qualsiasi** —Questo è il valore predefinito. • **Applicazione** • **Sicurezza** • **Sistema**
Origine evento	Nome origine evento È possibile selezionare il valore dall'elenco delle origini degli eventi acquisite da tutti gli agenti del tenant o inserire manualmente un nuovo nome origine. Se per il tenant è disabilitata la scansione dell'inventario software, l'elenco delle origini degli eventi sarà vuoto.
Modalità di corrispondenza	In questo campo è possibile specificare se connettere le impostazioni **ID evento**, **Tipo di evento** e **Descrizione evento** utilizzando l'operatore **Qualsiasi** o l'operatore **Tutti**. Sono disponibili i seguenti valori. • **Qualsiasi** -Questo è il valore predefinito. L'avviso viene generato solo se uno qualsiasi dei criteri selezionati viene soddisfatto. • **Tutti** L'avviso viene generato solo se tutti i criteri selezionati sono soddisfatti.
ID evento	Inserire uno o più ID evento separati da una virgola. Il sistema genera un avviso se individua nel registro eventi uno qualsiasi dei codici evento inseriti in questo campo.

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
Tipo di evento	Selezionare uno o più tipi di evento da monitorare. Sono disponibili i seguenti valori. • **Qualsiasi** —Questo è il valore predefinito. • **Errore** • **Attenzione** • **Informazioni** • **Riuscito-audit** • **Non riuscito-audit**
Descrizione evento	Specificare parole chiave o frasi da cercare nella descrizione dell'evento. Ogni parola chiave o frase inserita deve essere racchiusa tra virgolette e separata da una virgola. Il sistema genera un avviso se individua una qualsiasi delle parole chiave o frasi inserite in questo campo.
Numero di occorrenze	Il numero minimo di occorrenze di un evento nel registro durante il periodo di tempo specificato affinché il sistema generi un avviso. Inserire un valore intero incluso nell'intervallo 1-1000.
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero e quindi selezionare l'unità utilizzata: minuti o ore. Il valore predefinito è 60 minuti.

Impostazioni del monitor Dimensione file e cartelle

Il monitor **Dimensione file e cartelle** controlla la dimensione totale dei file e delle cartelle selezionati.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
File o cartelle da monitorare	I percorsi dei file o delle cartelle da monitorare. È anche possibile specificare i file o le cartelle da escludere dall'attività di monitoraggio. È possibile utilizzare i seguenti caratteri jolly: • * sostituisce zero o più caratteri nel nome di un file o di una cartella • ? sostituisce esattamente un carattere nel nome di un file o di una cartella Per i workload Windows: • Il percorso completo deve iniziare con la lettera di unità, seguita dal separatore :\. • È possibile utilizzare la barra o la barra rovesciata come carattere

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	separatore del percorso. • Il nome del file o della cartella non deve terminare con uno spazio o un punto. Per i workload macOS: • Il percorso completo deve iniziare con la directory radice. • È possibile utilizzare la barra come carattere separatore del percorso. • Il nome del file o della cartella non deve terminare con uno spazio o un punto. Non è obbligatorio indicare una posizione specifica per i filtri di esclusione. I file immessi senza una posizione specifica verranno esclusi dalle cartelle monitorate.
Operatore	L'operatore è una funzione condizionale che definisce come misurare le prestazioni della metrica. Sono disponibili i seguenti valori. • **Maggiore di** —Questo è il valore predefinito. • **Minore di**
Valore soglia	Il valore soglia e il valore **Operatore** determinano la prestazione normale della metrica monitorata. Quando il valore della metrica monitorata è fuori norma, il sistema genera un avviso. Inserire un valore intero (MB).
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 10-60 (min). Il valore predefinito è 10.

Impostazioni del monitor Stato di Windows Update

Il monitor **Stato di Windows Update** controlla lo stato di Windows Update per il workload e verifica che gli aggiornamenti più recenti siano stati installati.

Abilitando il monitor, il sistema genera un avviso nei casi seguenti.

- Windows Update è disabilitato nel workload.
- Windows Update è abilitato nel workload, ma gli aggiornamenti più recenti non sono stati installati.

Impostazioni del monitor Stato del firewall

Il monitor **Stato del firewall** controlla lo stato del firewall integrato o di terzi installato nel workload.

© Acronis International GmbH, 2003-2024

Abilitando il monitor, il sistema genera un avviso nei casi seguenti.

- Il firewall del sistema operativo integrato (Windows Defender Firewall o firewall macOS) è disabilitato e nessun firewall di terzi è in esecuzione.
- Il firewall di Windows Defender è disabilitato per le reti pubbliche.
- Il firewall di Windows Defender è disabilitato per le reti private.
- Il firewall di Windows Defender è disabilitato per le reti di dominio.

Impostazioni del monitor Accessi non riusciti

Il monitor **Accessi non riusciti** controlla i tentativi di accesso non riusciti al workload.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Soglia di tentativi di accesso non riusciti	Il valore soglia determina i limiti della prestazione normale della metrica monitorata. Quando il valore soglia viene superato, il valore viene considerato fuori norma. Inserire un valore intero. Il valore predefinito è 60.
Periodo di tempo	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato. Inserire un valore intero incluso nell'intervallo 1-24 e selezionare un'unità: ore o giorni. Il valore predefinito è 12.

Impostazioni del monitor Stato del software anti-malware

Il monitor **Stato del software anti-malware** controlla lo stato del software anti-malware integrato o di terzi installato nel workload.

Abilitando il monitor, il sistema genera un avviso quando identifica una delle condizioni seguenti.

- Il software anti-malware non è installato nel workload.
- Il software anti-malware è installato ma non in esecuzione.
- Il software anti-malware è installato e in esecuzione, ma le definizioni del malware non sono aggiornate.

Nota
Questa condizione viene verificata per i sistemi operativi Windows e Windows Server.

Sistema operativo	Software anti-malware supportati
Windows	• Acronis Cyber Protect • Windows Defender

© Acronis International GmbH, 2003-2024

Sistema operativo	Software anti-malware supportati
	• Symantec Endpoint Security • Norton 360 • Norton AntiVirus • SentinelOne • Trend Micro Endpoint Security con Apex One • Trend Micro Worry-Free Business • McAfee Endpoint Security • McAfee Endpoint Protection for SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud • BitDefender Antivirus • Sophos Intercept X Endpoint • Avast Business Antivirus • AVG Antivirus Business Edition • AVG Internet Security Business Edition • Panda Endpoint Protection • Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security • Avira Antivirus • Comodo Internet Security • Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security **Nota** Il monitor può funzionare con altre applicazioni anti-malware, ma ciò non è garantito.
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Anti-virus for Mac

© Acronis International GmbH, 2003-2024

Sistema operativo	Software anti-malware supportati
	• Sophos Home • Sophos Endpoint Protection • Avast Security for Mac • AVG AntiVirus for Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus for Mac • Comodo Antivirus for Mac • K7 Antivirus for Mac • Vipre Advanced Security • Total AV for Mac **Nota** Il monitor può funzionare con altre applicazioni anti-malware, ma ciò non è garantito.

Impostazioni del monitor Stato della funzionalità di esecuzione automatica

Il monitor **Stato della funzionalità di esecuzione automatica** controlla se la funzionalità di esecuzione automatica per il supporto rimovibile è abilitata.

Per ragioni di sicurezza, si consiglia di disabilitare la funzionalità di esecuzione automatica del supporto rimovibile nel workload. Se la funzionalità è abilitata, il sistema genera un avviso.

Impostazioni del monitor personalizzato

Il monitor **Personalizzato** controlla oggetti personalizzati tramite l'esecuzione di script.

Per il monitor sono configurabili le impostazioni indicate di seguito.

Impostazione	Descrizione
Script da eseguire	Elenco di script predefiniti dal repository degli script.
Pianificazione	Orario in cui lo script viene eseguito e, facoltativamente, le condizioni aggiuntive da soddisfare per la sua esecuzione. Sono disponibili i seguenti valori. • **Pianificazione oraria**. Lo script viene eseguito esattamente all'ora, nel giorno, nella settimana o nel mese specificati dall'utente. Questo è il valore predefinito. **Tipo di pianificazione**. **Ogni ora**, **Ogni giorno** o **Ogni mese**

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	Esegui entro un intervallo di date. Un intervallo di date entro cui eseguire lo script. • **Quando l'utente accede al sistema**. Lo script viene eseguito quando un utente accede al workload. • **Quando l'utente si disconnette dal sistema**. Lo script viene eseguito quando un utente si disconnette dal workload. • **All'avvio del sistema**. Lo script viene eseguito all'avvio del sistema operativo del workload. • **Quando il sistema viene arrestato**. Lo script viene eseguito quando il workload viene arrestato. • **Quando il sistema è online**. Lo script viene eseguito quando il workload diventa disponibile online. **Condizioni di avvio**. Lo script viene eseguito all'ora o all'evento specificati solo se la condizione è soddisfatta. In caso di più condizioni, è necessario che tutte vengano soddisfatte contemporaneamente per consentire l'avvio dell'attività. Per impostazione predefinita, la condizione **Impedisci alla modalità di sospensione o ibernazione di avviare un'attività pianificata** è selezionata. **Se le condizioni di avvio non sono soddisfatte, esegui comunque l'attività dopo**. Per impostazione predefinita, questa condizione è abilitata. Il valore predefinito è 1 ora.
Account che esegue lo script	L'account per il quale viene eseguito lo script. Sono disponibili i seguenti valori. • **Account di sistema** — Questo è il valore predefinito. • **Account attualmente connesso**
Durata massima	Il periodo massimo durante il quale lo script può essere eseguito nel workload. Se l'esecuzione dello script non si completa durante il periodo specificato, l'operazione non riesce. Inserire un valore intero incluso nell'intervallo 1-1440 (min). Il valore predefinito è 3 minuti.
Policy di esecuzione di PowerShell	La policy di esecuzione di PowerShell. Sono disponibili i seguenti valori. • **Undefined** • **AllSigned** • **Bypass** — Questo è il valore predefinito. • **RemoteSigned**

© Acronis International GmbH, 2003-2024

Impostazione	Descrizione
	• **Restricted** • **Unrestricted** Per ulteriori informazioni su questi valori, consultare la documentazione Microsoft.

Piani di monitoraggio

I piani di monitoraggio sono piani applicati ai workload gestiti per abilitare e configurare la funzionalità di monitoraggio.

Se al workload non è applicato alcun piano di monitoraggio, le funzionalità di monitoraggio non saranno disponibili per il workload.

Nota
La disponibilità delle impostazioni che è possibile configurare nel piano di monitoraggio dipende dal pacchetto di servizi applicato al tenant. Per accedere a tutte le impostazioni, attivare il pacchetto Advanced Management.

Creazione di un piano di monitoraggio

È possibile creare un piano di monitoraggio e quindi aggiungervi dei workload per configurare la funzionalità di monitoraggio sui workload gestiti.

Prerequisiti

La versione dell'agente installata nel workload supporta la funzionalità di monitoraggio.

Per creare un piano di monitoraggio

Da Piani di monitoraggio

1. Nella console di Protezione, passare a **Gestione** > **Piani di monitoraggio**.
2. Creare un piano di monitoraggio utilizzando una delle due opzioni.
   - Se l'elenco non contiene piani di monitoraggio, fare clic su **Crea**.
   - Se l'elenco contiene piani monitoraggio, fare clic su **Crea piano**.
3. A seconda che il pacchetto Advanced Management sia abilitato o meno per il tenant, nella finestra **Crea piano di monitoraggio** procedere come segue:
   - Se il tenant utilizza la protezione Standard, al piano di monitoraggio vengono automaticamente aggiunti i quattro monitor seguenti: Spazio su disco, Modifiche hardware, Ultimo riavvio del sistema, Dimensione file e cartelle.
   - Se il pacchetto Advanced Management è abilitato per il tenant, selezionare una delle opzioni del modello e quindi fare clic su **Avanti**.

© Acronis International GmbH, 2003-2024

Opzione	Descrizione
Consigliato	Selezionare questa opzione per creare un piano di monitoraggio con la configurazione di monitoraggio predefinita.
Personalizzato	Utilizzare questa opzione per creare un piano di monitoraggio da zero.

4. [Facoltativo] Per cambiare il nome predefinito del piano, fare clic sull'icona a matita, inserire il nome del piano, quindi fare clic su **OK**.
5. [Facoltativo] Per aggiungere un monitor al piano, fare clic su **Aggiungi monitor**, fare clic sul monitor nell'elenco, quindi su **Aggiungi**.

   Nota
   Le impostazioni del monitor vengono compilate automaticamente con i valori predefiniti.
   È possibile aggiungere fino a tre monitor dello stesso tipo e fino a 30 monitor in totale a un piano di monitoraggio.

6. [Facoltativo] Nella schermata dei parametri del monitor, modificare le impostazioni predefinite del monitor e degli avvisi, quindi fare clic su **Fine**.

   Nota
   È possibile configurare impostazioni differenti per ciascun monitor. Per ulteriori informazioni, consultare "Monitor configurabili" (pag. 1054) e "Configurazione degli avvisi di monitoraggio" (pag. 1099).

7. [Facoltativo] Per eliminare un monitor, fare clic sull'icona a cestino, quindi su **Elimina**.
8. [Facoltativo] Per aggiungere workload al piano:
   a. Fare clic su **Aggiungi workload**.
   b. Selezionare i workload e quindi fare clic su **Aggiungi**.
   c. Se si riscontrano problemi di compatibilità che devono essere risolti, attenersi alla procedura descritta in "Risoluzione dei problemi di compatibilità con i piani monitoraggio" (pag. 1097).
9. Fare clic su **Crea**.

Da Tutti i dispositivi

1. Nella console di Protezione, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic sul workload al quale applicare il piano di monitoraggio.
3. Fare clic su **Proteggi**.
4. A seconda che al workload sia applicato o meno un piano di monitoraggio, procedere come segue.
   - Se al workload è già applicato un piano di monitoraggio, fare clic su **Crea piano**, quindi selezionare **Monitoraggio**.

© Acronis International GmbH, 2003-2024

- Se al workload non è applicato alcuno piano di monitoraggio, fare clic su **Aggiungi piano**, quindi **Crea piano** e infine selezionare **Monitoraggio**.

5. Nella finestra **Crea piano di monitoraggio**, selezionare una delle opzioni del modello e quindi fare clic su **Avanti**.

Opzione	Descrizione
Consigliato	Selezionare questa opzione per creare un piano di monitoraggio con la configurazione di monitoraggio predefinita.
Personalizzato	Utilizzare questa opzione per creare un piano di monitoraggio da zero.

6. [Facoltativo] Per cambiare il nome predefinito del piano, fare clic sull'icona a matita, inserire il nome del piano, quindi fare clic su **OK**.
7. [Facoltativo] Per modificare le impostazioni predefinite del monitor e degli avvisi, configurare i nuovi valori e quindi fare clic su **Fine**.

   Nota
   È possibile aggiungere fino a tre monitor dello stesso tipo e fino a 30 monitor in totale a un piano di monitoraggio.

8. [Facoltativo] Nella schermata dei parametri del monitor, modificare le impostazioni predefinite del monitor e degli avvisi, quindi fare clic su **Fine**.

   Nota
   È possibile configurare impostazioni differenti per ciascun monitor. Per ulteriori informazioni, consultare "Monitor configurabili" (pag. 1054) e "Configurazione degli avvisi di monitoraggio" (pag. 1099).

9. [Facoltativo] Per eliminare un monitor, fare clic sull'icona a cestino, quindi su **Elimina**.
10. Fare clic su **Crea**.

Aggiunta di workload ai piani di monitoraggio

A seconda delle esigenze, è possibile aggiungere dei workload a un piano di monitoraggio, successivamente alla creazione del piano.

Prerequisiti

- L'autenticazione a due fattori è abilitata per l'account utente.
- La versione dell'agente installata nel workload supporta la funzionalità di monitoraggio.
- È disponibile almeno un piano di monitoraggio.

Per aggiungere un workload a un piano di monitoraggio

Da Piani di monitoraggio

© Acronis International GmbH, 2003-2024

1. Nella console di Protezione, passare a **Gestione** > **Piani di monitoraggio**.
2. Fare clic sul piano di monitoraggio.
3. A seconda che il piano sia già stato applicato o meno a un workload, procedere come segue:
   - Fare clic su **Aggiungi workload** se il piano non è ancora stato applicato ad alcun workload.
   - Fare clic su **Gestisci workload** se il piano è già stato applicato a un qualsiasi workload.
4. Selezionare un workload dall'elenco, quindi fare clic su **Aggiungi**.
5. Fare clic su **Salva**.
6. Se necessario, fare clic su **Conferma** per applicare la quota di servizio richiesta al workload.

Da Tutti i dispositivi

1. Nella console di Protezione, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic sul workload al quale applicare il piano di monitoraggio.
3. Fare clic su **Proteggi**.
4. Individuare il piano di monitoraggio da aggiungere al workload, quindi fare clic su **Applica**.
5. Se necessario, fare clic su **Conferma** per applicare la quota di servizio richiesta al workload.

Revoca di piani di monitoraggio

È possibile revocare un piano di monitoraggio da un workload a cui il piano è applicato.

Prerequisiti

Almeno un piano di monitoraggio è applicato al workload.

Per revocare un piano di monitoraggio

1. Nella console di Protezione, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare il workload e quindi fare clic su **Proteggi**.
3. Fare clic sull'icona **Più azioni** del piano di monitoraggio da revocare, quindi fare clic su **Revoca**.

Configurazione delle azioni di risposta automatica

Le azioni di risposta automatica relative agli eventi con avvisi sono azioni predefinite o misure attivate automaticamente in risposta a eventi o incidenti rilevati. Queste azioni sono progettate per contenere le potenziali minacce e ridurre al minimo i danni.

È possibile configurare una o più azioni di risposta automatica per gli eventi con avvisi. Il numero massimo di azioni di risposta automatica per monitor è 20.

Per configurare le azioni di risposta automatica

1. Nella console di Protezione, passare a **Gestione** > **Piani di monitoraggio**.
2. Selezionare il piano di monitoraggio per il quale configurare le azioni di risposta automatica.

© Acronis International GmbH, 2003-2024

3. Selezionare il monitor per il quale configurare le azioni di risposta automatica, oppure, se ancora non è stato aggiunto alcun monitor, fare clic su **Aggiungi monitor**, fare clic sul monitor nell'elenco, fare clic su **Aggiungi** e selezionare il monitor.
4. Fare clic sul link accanto ad **Azioni di risposta automatica**.
5. Nella finestra **Azioni di risposta automatica**, aggiungere una o più azioni di risposta da eseguire automaticamente all'attivazione di un avviso.
6. Configurare ogni azione di risposta. Ad esempio, se è stata aggiunta l'azione di risposta **Avvia un servizio Windows**, procedere come segue:
   a. Accanto a **Servizio Windows**, fare clic su **Specificare**.
   b. Nel campo **Servizio**, selezionare un servizio da avviare come azione di risposta.
   c. Fare clic su **Fine**.
7. Nell'elenco di tutte le azioni di risposta aggiunte, utilizzare le frecce su e giù oppure trascinare e rilasciate per definire la sequenza di azioni di risposta.
8. Configurare come gestire le azioni di risposta successive se una delle precedenti non ha esito positivo. Selezionare una delle seguenti opzioni:
   a. **Prosegui con l'azione di risposta successiva**.
   b. **Non proseguire con l'azione di risposta successiva**.
9. Fare clic su **Fine**.

   Il numero di azioni configurate viene visualizzato accanto all'impostazione **Azioni di risposta automatica** del piano di monitoraggio. È possibile modificare o eliminare queste azioni, così come le nuove, in qualsiasi momento successivo.

La tabella seguente elenca e descrive tutte le azioni di risposta automatica disponibili nelle impostazioni dei monitor.

Azione di risposta automatica	Descrizione	Sistema operativo supportato
Esegui uno script	Se si aggiunge questa azione, è possibile: 1. Selezionare un determinato script da eseguire nel workload. 2. Specificare l'account per il quale eseguire lo script. 3. Specificare la durata massima dell'operazione. 4. Specificare la policy di esecuzione di PowerShell. 5. Esegui uno script. Per eseguire questa azione, è necessaria una licenza Advanced Management Pack per il workload (se non è ancora stata assegnata).	Windows, macOS

© Acronis International GmbH, 2003-2024

Azione di risposta automatica	Descrizione	Sistema operativo supportato
	Quando vengono soddisfatte le condizioni, il sistema esegue lo script remoto selezionato con i parametri specificati.	
Riavvia il workload	Se si aggiunge questa azione, quando vengono soddisfatte le condizioni, il sistema riavvia il workload da remoto.	Windows, macOS
Arresta il processo	Se si aggiunge questa azione, è possibile specificare il processo da arrestare inserendo manualmente il nome del processo. Quando vengono soddisfatte le condizioni, il sistema arresta il processo.	Windows, macOS
Avvia il servizio Windows	Se si aggiunge questa azione, è possibile selezionare il servizio Windows da avviare dall'elenco dinamico dei servizi popolato dagli agenti. Quando vengono soddisfatte le condizioni, il sistema avvia il servizio.	Windows
Arresta il servizio Windows	Se si aggiunge questa azione, è possibile selezionare il servizio Windows da arrestare dall'elenco dinamico dei servizi popolato dagli agenti. Quando vengono soddisfatte le condizioni, il sistema arresta il servizio.	Windows
Abilita Windows Update	Se si aggiunge questa azione, quando vengono soddisfatte le condizioni il sistema abilita Windows Update. Questa azione è disponibile solo per il monitor dello stato di Windows Update.	Windows
Disabilita l'esecuzione automatica nelle unità rimovibili	Se si aggiunge questa azione, quando vengono soddisfatte le condizioni, il sistema disabilita l'esecuzione automatica nei supporti di storage rimovibili del workload. Questa azione è disponibile solo per il monitor dello stato della funzionalità di esecuzione automatica.	Windows

© Acronis International GmbH, 2003-2024

Ulteriori operazioni con i piani monitoraggio

Nella schermata **Piani di monitoraggio** è possibile eseguire le azioni aggiuntive seguenti sui piani monitoraggio: visualizzazione dei dettagli, modifica, visualizzazione delle attività, visualizzazione degli avvisi, ridenominazione, abilitazione, disabilitazione, clonazione, esportazione ed eliminazione.

Visualizza dettagli

Per visualizzare i dettagli di un piano di monitoraggio

1. Nella schermata **Piani di monitoraggio**, fare clic sull'icona **Altre azioni** del piano di monitoraggio.
2. Fare clic su **Visualizza dettagli**.
3. [Facoltativo] Per visualizzare i dettagli di un monitor abilitato nel piano, fare clic sul nome del monitor.

Modifica

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per modificare un piano

1. Nella schermata **Piani di monitoraggio**, fare clic sull'icona **Altre azioni** del piano di monitoraggio.
2. Fare clic su **Modifica**.
3. [Facoltativo] Per eliminare un monitor dal piano, fare clic sull'icona del cestino posizionata a destra del nome del monitor.
4. [Facoltativo] Per abilitare o disabilitare un monitor nel piano, fare clic sull'interruttore accanto al nome del monitor.
5. [Facoltativo] Per modificare i parametri del monitor, procedere come segue.
   a. Fare clic sul nome del monitor.
   b. Fare clic sulla panoramica dei parametri del monitor.
   c. Nella schermata **Parametri del monitor**, configurare i parametri, quindi fare clic su **Fine**.

      Nota
      È possibile configurare impostazioni differenti per ciascun monitor. Per ulteriori informazioni, consultare "Monitor configurabili" (pag. 1054) e "Configurazione degli avvisi di monitoraggio" (pag. 1099).

   d. Chiudere la schermata e confermare le modifiche.
6. [Facoltativo] Per aggiungere un monitor, fare clic su **Aggiungi monitor**, quindi, se necessario, modificare i parametri come illustrato nel passaggio precedente.
7. Fare clic su **Salva**.

© Acronis International GmbH, 2003-2024

Attività

Per visualizzare le attività relative a un piano di monitoraggio

1. Nella schermata **Piani di monitoraggio**, fare clic sull'icona **Altre azioni** del piano di monitoraggio.
2. Fare clic su **Attività**.
3. Fare clic sull'attività per visualizzarne ulteriori dettagli.

Avvisi

Per visualizzare gli avvisi

1. Nella schermata **Piani di monitoraggio**, fare clic sull'icona **Altre azioni** del piano di monitoraggio.
2. Fare clic su **Avvisi**.

Rinomina

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per ridenominare un piano di monitoraggio

1. Nella schermata **Piani di monitoraggio**, fare clic sull'icona **Altre azioni** del piano di monitoraggio.
2. Fare clic su **Rinomina**.
3. Inserire il nuovo nome del piano, quindi fare clic su **OK**.

Abilita

Prerequisiti

- L'autenticazione a due fattori è abilitata per l'account utente.
- Il piano di monitoraggio è applicato ad almeno un workload.

Per abilitare un piano di monitoraggio

1. Nella schermata **Piani di monitoraggio**, fare clic sull'icona **Altre azioni** del piano di monitoraggio.
2. Fare clic su **Abilita**.

Disabilita

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per disabilitare un piano di monitoraggio

© Acronis International GmbH, 2003-2024

1. Nella schermata **Piani di monitoraggio**, fare clic sull'icona **Altre azioni** del piano di monitoraggio.
2. Fare clic su **Disabilita**.

Clona

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per clonare un piano di monitoraggio

1. Nella schermata **Piani di monitoraggio**, fare clic sull'icona **Altre azioni** del piano di monitoraggio.
2. Fare clic su **Clona**.
3. Fare clic su **Crea**.

Esporta

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per esportare un piano di monitoraggio

1. Nella schermata **Piani di monitoraggio**, fare clic sull'icona **Altre azioni** del piano di monitoraggio.
2. Fare clic su **Esporta**.
   La configurazione del piano viene esportata in formato JSON nel sistema locale.

Elimina

Prerequisiti

L'autenticazione a due fattori è abilitata per l'account utente.

Per eliminare un piano di monitoraggio

1. Nella schermata **Piani di monitoraggio**, fare clic sull'icona **Altre azioni** del piano di monitoraggio.
2. Fare clic su **Elimina**.
3. Selezionare **Confermo**, quindi fare clic su **Elimina**.

Problemi di compatibilità con i piani monitoraggio

In alcuni casi, applicare un piano di monitoraggio a un workload può causare problemi di compatibilità. Potrebbero registrarsi i problemi di compatibilità seguenti:

- Sistema operativo non compatibile: questo problema si verifica quando il sistema operativo del workload non è supportato.

© Acronis International GmbH, 2003-2024

- Agente non supportato: questo problema si verifica quando una versione dell'agente di protezione nel workload è obsoleta e non supporta la funzionalità di monitoraggio.
- Quota non sufficiente: questo problema si verifica quando la quota di servizio nel tenant non è sufficiente per essere assegnata ai workload selezionati.

Se il piano monitoraggio è applicato a un massimo di 150 workload selezionati singolarmente, verrà richiesto di risolvere i conflitti esistenti prima di salvare il piano. Per risolvere i conflitti, rimuovere la causa principale che li causa oppure rimuovere i workload interessati dal piano. Per ulteriori informazioni, consultare "Risoluzione dei problemi di compatibilità con i piani monitoraggio" (pag. 1097). Se si salva il piano senza risolvere i conflitti, il piano verrà automaticamente disabilitato per i workload non compatibili e verranno mostrati i relativi avvisi.

Se il piano monitoraggio è applicato a più di 150 workload o a gruppi di dispositivi, prima verrà salvato e quindi ne verrà controllata la compatibilità. Il piano verrà automaticamente disabilitato per i workload incompatibili e verranno visualizzati i relativi avvisi.

Risoluzione dei problemi di compatibilità con i piani monitoraggio

A seconda della causa che provoca i problemi di compatibilità, è possibile eseguire azioni differenti per risolvere tali problemi durante il processo di creazione di un nuovo piano di monitoraggio.

Per risolvere i problemi di compatibilità

1. Fare clic su **Rivedi problemi**.
2. [Facoltativo] Per risolvere i problemi di compatibilità con sistemi operativi incompatibili rimuovendo i workload dal piano:
   a. Nella scheda **Sistema operativo incompatibile** selezionare i workload da eliminare.
   b. Fare clic su **Rimuovi i workload dal piano**.
   c. Fare clic su **Rimuovi** e quindi su **Chiudi**.
3. [Facoltativo] Per risolvere i problemi di compatibilità con sistemi operativi incompatibili disabilitando un monitor nel piano:
   a. Nella scheda **Sistema operativo incompatibile** selezionare i monitor da eliminare.
   b. Fare clic su **Disabilita monitor**.
   c. Fare clic su **Disabilita** e quindi su **Chiudi**.
4. [Facoltativo] Per risolvere i problemi di compatibilità con agenti non supportati rimuovendo i workload dal piano:
   a. Nella scheda **Agenti non supportati** selezionare i workload da eliminare.
   b. Fare clic su **Rimuovi i workload dal piano**.
   c. Fare clic su **Rimuovi** e quindi su **Chiudi**.
5. [Facoltativo] Per risolvere i problemi di compatibilità con agenti non supportati aggiornando la versione dell'agente, fare clic su **Passare all'elenco degli agenti**.

© Acronis International GmbH, 2003-2024

Nota
Questa opzione è disponibile solo per gli amministratori del cliente.

6. [Facoltativo] Per risolvere i problemi di compatibilità con quote insufficienti rimuovendo i workload dal piano:
   a. Nella scheda **Quota insufficiente** selezionare i workload da eliminare.
   b. Fare clic su **Rimuovi i workload dal piano**.
   c. Fare clic su **Rimuovi** e quindi su **Chiudi**.
7. [Facoltativo] Per risolvere i problemi di compatibilità con quote insufficienti aumentando la quota del tenant:
   a. Nella scheda **Quota insufficiente**, fare clic su **Vai al portale di gestione**.
   b. Aumentare la quota di servizio per il cliente.

   Nota
   Questa opzione è disponibile solo per gli amministratori del partner.

Reimpostazione dei modelli di machine learning

È possibile reimpostare i modelli di un workload che per qualsiasi motivo diventano obsoleti o non sono più validi. Questa azione elimina i modelli creati e i dati raccolti per il workload dai monitor che eseguono il tipo di monitoraggio basato sulle anomalie; l'addestramento dei modelli di machine learning relativi al workload verrà quindi riavviato da zero.

Per reimpostare i modelli di machine learning di un workload

1. Nella console di Protezione, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Fare clic su un workload nell'elenco, quindi fare clic sulla scheda **Dettagli**.
3. Nella sezione **Reimposta modelli di machine learning**, selezionare **Reimposta**.
4. Nella finestra di conferma, fare di nuovo clic su **Reimposta**.

Monitoraggio avvisi

Gli avvisi di monitoraggio vengono visualizzati nella console di Protezione e inviati tramite e-mail quando il comportamento monitorato dei workload è fuori norma. Gli avvisi assicurano che le parti interessate siano informate al più presto di eventuali problemi nell'ambiente IT dell'organizzazione.

Nota
Per abilitare gli avvisi di monitoraggio tramite e-mail, è necessario configurare almeno una policy di notifica e-mail per il tipo di avviso corrispondente. Per ulteriori informazioni, consultare "Configurazione delle policy di notifica e-mail" (pag. 1106).

© Acronis International GmbH, 2003-2024

Configurazione degli avvisi di monitoraggio

È possibile configurare le impostazioni di avviso di un monitor quando si aggiunge un monitor a un piano di monitoraggio o quando si modifica un monitor già disponibile in un piano di monitoraggio.

Per configurare gli avvisi di monitoraggio

1. Nella finestra **Parametri del monitor**, passare alla sezione **Genera un avviso**.
2. In **Gravità avviso**, selezionare la gravità corrispondente alla priorità dell'avviso.

Opzione	Descrizione
Critico	Questi avvisi hanno la più alta priorità e sono correlati a problemi critici per il funzionamento del workload. Risolvere questi problemi il prima possibile.
Errore	Un avviso di errore è meno grave e indica la presenza di qualcosa di sbagliato o che non si comporta normalmente. Risolvere questi problemi tempestivamente per impedire che possano causare problemi più gravi.
Attenzione	Un avviso di attenzione indica che si è verificata una condizione della quale l'utente deve essere a conoscenza, ma che ancora non sta causando alcun problema. Risolvere questi problemi dopo aver corretto le cause degli avvisi critici e di errore. Questo è il valore predefinito.
Informativo	Questi avvisi hanno la priorità più bassa. La categoria di gravità 'Informativa' non segnala un problema. Avvisi di questo tipo forniscono informazioni sulle azioni relative a un oggetto monitorato.

3. In **Frequenza dell'avviso**, selezionare quanto spesso il sistema deve generare un avviso quando viene soddisfatta la condizione specificata.

Opzione	Descrizione
Una volta fino al superamento del controllo	Il sistema genera un avviso una volta fino al corretto completamento del controllo. Questo è il valore predefinito.
Dopo X errori consecutivi	Il sistema genera un avviso dopo il numero specificato di controlli consecutivi non riusciti. X indica un valore intero.

4. In **Messaggio di allarme**, fare clic sull'icona a matita per modificare il messaggio di avviso predefinito che verrà utilizzato quando il sistema genera un avviso. È possibile specificare un messaggio di avviso personalizzato che contiene variabili. Per ulteriori informazioni sulle variabili che è possibile utilizzare, vedere "Variabili del monitoraggio avvisi" (pag. 1100).

Nota
Per alcuni monitor è possibile configurare più di un messaggio di avviso.

© Acronis International GmbH, 2003-2024

5. Abilitare l'**Avviso di risoluzione automatica** affinché il sistema risolva automaticamente l'avviso quando la metrica e il comportamento monitorati tornano in uno stato di normalità. Per impostazione predefinita, questa impostazione è abilitata.

Variabili del monitoraggio avvisi

Per i diversi monitor è possibile configurare diverse variabili di avviso. Per utilizzare una variabile, questa deve essere racchiusa tra parentesi graffe {{}}.

La tabella seguente fornisce più informazioni sulle variabili disponibili.

Variabile	Descrizione	Disponibile per il monitor
plan_name	Il nome della policy	Tutti i monitor
monitor_name	Il nome della policy secondaria nel piano di monitoraggio	Tutti i monitor
workload_ name	Il nome del workload	Tutti i monitor
threshold_ value	Specifica le condizioni di monitoraggio o le soglie per la generazione di un avviso	Tutti i monitor che supportano il monitoraggio basato su soglia.
threshold_unit	L'unità di misura associata al valore soglia. Ad esempio, %, MB o mb/sec.	Tutti i monitor che supportano il monitoraggio basato su soglia.
time_period	Il sistema genera un avviso per l'anomalia rilevata solo se il valore della metrica è fuori norma durante tutto il periodo specificato.	Tutti i monitor che supportano il monitoraggio basato su soglia.
time_unit	L'unità di misura che sarà associata al periodo di tempo (sec/min/ore/giorni).	Tutti i monitor che supportano il monitoraggio basato su soglia.
anomaly_value	Il valore dell'anomalia	Tutti i monitor che supportano il monitoraggio basato su anomalia.
anomaly_unit	L'unità che sarà associata al valore dell'anomalia	Tutti i monitor che supportano il monitoraggio basato su anomalia.

© Acronis International GmbH, 2003-2024

Variabile	Descrizione	Disponibile per il monitor
deviation_value	Il valore della deviazione	Tutti i monitor che supportano il monitoraggio basato su anomalia.
deviation_unit	L'unità che sarà associata al valore della deviazione	Tutti i monitor che supportano il monitoraggio basato su anomalia.
drive_name	L'unità per Windows o la partizione per macOS	Spazio su disco,
CPU_model	Il modello della CPU monitorata	Temperatura CPU
GPU_model	Il modello della GPU monitorata	Temperatura GPU
hardware_model	Il modello del componente monitorato	Modifiche hardware
hardware_component	Il tipo di hardware monitorato	Modifiche hardware
hardware_model_old	Il modello di componente monitorato che è stato sostituito	Modifiche hardware
hardware_model_new	Il modello di componente monitorato che è stato aggiunto	Modifiche hardware
disk_model	Il modello del disco	Velocità di trasferimento disco
network_adapter_model	Il modello dell'adattatore di rete	Utilizzo di rete
process_name	Il nome del processo	Utilizzo della CPU per processo Utilizzo della memoria per processo Velocità di trasferimento disco per processo Utilizzo della rete per processo Stato del processo
service_name	Il nome del servizio	Stato dei servizi Windows

© Acronis International GmbH, 2003-2024

Variabile	Descrizione	Disponibile per il monitor
software_name	Il nome dell'applicazione software	Software installato
software_ version	La versione dell'applicazione software	Software installato
software_ version_old	La versione dell'applicazione software prima dell'aggiornamento	Software installato
software_ version_new	La versione dell'applicazione software nuova o aggiornata	Software installato
number_of_ occurrences	Il numero di volte che un evento appare nel registro	Registro eventi di Windows
event_types	Il tipo di evento	Registro eventi di Windows
event_source	L'origine dell'evento	Registro eventi di Windows
event_log_ name	Il nome dell'evento	Registro eventi di Windows
firewall_ software_name	Il nome del software del firewall	Stato del firewall
antimalware_ software_name	Il nome del software anti-malware	Stato del software anti-malware
user_name	Il nome dell'utente	Stato della funzionalità di esecuzione automatica
script_name	Il nome dello script	Personalizzato

Azioni di risposta manuali

Quando viene visualizzato un avviso, è possibile selezionare un'azione di risposta da eseguire sugli eventi segnalati.

Per eseguire un'azione di risposta manuale

1. Nella console di Protezione, passare a **Avvisi**.
2. Aprire l'avviso da visualizzare.
3. Fare clic su **Azione di risposta**, quindi selezionare una delle azioni di risposta dall'elenco a discesa.

© Acronis International GmbH, 2003-2024

L'elenco delle azioni di risposta disponibili per uno specifico avviso dipende dal tipo di avviso, dalla disponibilità delle funzionalità per uno specifico tenant e dal sistema operativo del workload.

La tabella seguente elenca e descrive tutte le azioni di risposta manuale disponibili, per riferimento.

Azione di risposta manuale	Descrizione	Sistema operativo supportato
Sfoglia le tendenze di utilizzo dello spazio su disco	Apre una finestra con il grafico **Utilizzo dello spazio su disco**, nella quale è possibile: • Osservare come l'utilizzo dello spazio su disco si è modificato nel tempo (per gli ultimi 1 giorno/7 giorni/1 mese). • Osservare il delta dell'utilizzo dello spazio su disco espresso con un valore relativo (%) per il periodo selezionato.	Windows, macOS
Sfoglia le tendenze di crescita delle dimensioni dei file	Apre una finestra con il grafico **Crescita delle dimensioni dei file**, nella quale è possibile: • Osservare come la dimensione totale dei file e delle cartelle monitorate si è modificata nel tempo (per gli ultimi 1 giorno/7 giorni/1 mese). • Osservare il delta della dimensione totale dei file espresso con un valore relativo (%) per il periodo selezionato.	Windows, macOS
Esegui uno script	Apre una finestra nella quale è possibile: 1. Selezionare un determinato script da eseguire nel workload. 2. Specificare l'account per il quale eseguire lo script. 3. Specificare la durata massima dell'operazione. 4. Specificare la policy di esecuzione di PowerShell. 5. Esegui uno script. Per eseguire questa azione, è necessaria una licenza Advanced Management Pack per il workload (se non è ancora stata assegnata).	Windows, macOS
Connetti tramite NEAR	Acronis Connect Client stabilisce una connessione remota.	Windows, macOS
Connetti tramite RDP	Acronis Connect Client stabilisce una connessione remota.	Windows

© Acronis International GmbH, 2003-2024

Azione di risposta manuale	Descrizione	Sistema operativo supportato
Apri inventario hardware	L'utente viene reindirizzato alla scheda **Inventario hardware** del workload corrente.	Windows, macOS
Sfoglia i primi 10 processi che hanno caricato la CPU	Apre una finestra con i primi dieci processi che hanno caricato la CPU e possono averne causato il surriscaldamento (snapshot del sistema al momento della generazione dell'avviso).	Windows, macOS
Sfoglia i primi 10 processi che hanno caricato la GPU	Apre una finestra con i primi dieci processi che hanno caricato la GPU e possono averne causato il surriscaldamento (snapshot del sistema al momento della generazione dell'avviso).	Windows, macOS
Sfoglia i primi 10 processi che hanno caricato la memoria	Apre una finestra con i primi dieci processi che hanno caricato la memoria (snapshot del sistema al momento della generazione dell'avviso).	Windows, macOS
Sfoglia i primi 10 processi che hanno caricato il disco	Apre una finestra con i primi dieci processi che hanno caricato il disco (snapshot del sistema al momento della generazione dell'avviso).	Windows, macOS
Sfoglia i primi 10 processi che hanno caricato la rete	Apre una finestra con i primi dieci processi che hanno caricato l'adattatore dell'interfaccia di rete (snapshot del sistema al momento della generazione dell'avviso).	Windows, macOS
Sfoglia l'utilizzo delle risorse per processo	Apre una finestra con informazioni dettagliate sull'utilizzo delle risorse hardware da parte del processo relativo: Utilizzo della CPU, Utilizzo della memoria, I/O del disco, Utilizzo della rete.	Windows, macOS
Riavvia workload	Apre una finestra di conferma. Dopo l'invio della conferma, riavvia il workload.	Windows, macOS
Avvia servizio Windows	Apre una finestra di conferma. Dopo l'invio della conferma, avvia il servizio Windows.	Windows
Arresta servizio Windows	Apre una finestra di conferma. Dopo l'invio della conferma, arresta il servizio Windows.	Windows
Arresta processo	Apre una finestra di conferma. Dopo l'invio della conferma, arresta il processo a cui fa	Windows, macOS

© Acronis International GmbH, 2003-2024

Azione di risposta manuale	Descrizione	Sistema operativo supportato
	riferimento l'avviso.	
Abilita Windows Update	Apre una finestra di conferma. Dopo l'invio della conferma, abilita Windows Update.	Windows
Disabilita la funzionalità di esecuzione automatica nelle unità rimovibili	Apre una finestra di conferma. Dopo l'invio della conferma, disabilita la funzionalità di esecuzione automatica al livello del sistema del workload.	Windows

Importante
Per ragioni di sicurezza, è necessario utilizzare l'autenticazione a due fattori per eseguire le seguenti azioni di risposta manuale:

- Esegui uno script
- Connetti tramite NEAR
- Connetti tramite RDP
- Riavvia workload
- Avvia servizio Windows
- Arresta servizio Windows
- Arresta processo
- Abilita Windows Update
- Disabilita la funzionalità di esecuzione automatica nelle unità rimovibili

Visualizzazione degli avvisi di monitoraggio di un workload

Nella scheda **Avvisi**, è possibile visualizzare gli avvisi di monitoraggio di uno specifico workload ed eseguire diverse azioni.

Per visualizzare gli avvisi di monitoraggio di un workload

1. Nella console di Protezione, passare a **Tutti i dispositivi**.
2. Fare clic sul workload e quindi selezionare la scheda **Avvisi**.
3. [Facoltativo] Nel pannello degli avvisi di monitoraggio, eseguire una delle seguenti azioni:
   - Per cancellare l'avviso, fare clic su **Cancella**.
   - Per avviare un'azione di risposta, fare clic su **Azione di risposta**, quindi fare clic sull'azione.
   - Per contattare il team di supporto, fare clic su **Richiedi supporto**.

© Acronis International GmbH, 2003-2024

4. [Facoltativo] Per cancellare tutti gli avvisi di monitoraggio del workload, fare clic su **Cancella tutto**.

Visualizzazione del registro degli avvisi di monitoraggio

È possibile visualizzare tutti gli eventi correlati a un avviso di monitoraggio in ordine cronologico: le azioni di risposta (sia automatiche che manuali) che sono state eseguite e le notifiche e-mail che sono state inviate.

Per visualizzare il registro di audit di un avviso di monitoraggio

1. Nella console di Protezione, passare a **Avvisi**.
2. Aprire la **Visualizzazione tabella**.
3. Nell'elenco degli avvisi, selezionare l'avviso di monitoraggio da visualizzare.
4. Fare clic su **Dettagli**, quindi su **Registro avvisi**.

Configurazione delle policy di notifica e-mail

Le policy di notifica e-mail consentono di specificare quali utenti riceveranno le notifiche e-mail dai diversi monitor.

Nella schermata **Notifiche e-mail**, è possibile aggiungere, modificare, abilitare, disabilitare ed eliminare le notifiche e-mail.

Aggiungi

Per aggiungere una nuova policy di notifica e-mail

1. Nella console di Protezione, passare a **Impostazioni** > **Notifiche e-mail**.
2. Fare clic su **Aggiungi policy**.
3. Fare clic su **Seleziona destinatari**.
4. Nella schermata **Seleziona destinatari**, selezionare gli utenti a quali inviare gli avvisi e-mail, quindi fare clic su **Seleziona**.
5. In **Tipi di avvisi**, selezionare i monitor per i quali il sistema deve inviare gli allarmi e-mail.
6. Fare clic su **Aggiungi**.

Modifica

Per modificare una policy di notifica e-mail

1. Nella console di Protezione, passare a **Impostazioni** > **Notifiche e-mail**.
2. Fare clic sull'icona dei puntini di sospensione della policy di notifica, quindi su **Modifica**.
3. [Facoltativo] Per modificare i destinatari, fare clic su **Modifica destinatari**, aggiungere o rimuovere gli utenti dall'elenco, quindi fare clic su **Seleziona**.

© Acronis International GmbH, 2003-2024

4. [Facoltativo] In **Tipi di avviso**, selezionare i tipi di avvisi di monitoraggio da inviare ai destinatari selezionati.
5. Fare clic su **Salva**.

Abilita

Per abilitare una policy di notifica e-mail

1. Nella console di Protezione, passare a **Impostazioni** > **Notifiche e-mail**.
2. Nella schermata **Notifiche e-mail**, fare clic sull'icona **...** della policy di notifica e-mail.
3. Fare clic su **Abilita**.

Disabilita

Per disabilitare una policy di notifica e-mail

1. Nella console di Protezione, passare a **Impostazioni** > **Notifiche e-mail**.
2. Nella schermata **Notifiche e-mail**, fare clic sull'icona**...** della policy di notifica e-mail.
3. Fare clic su **Disabilita**.

Elimina

Per eliminare una policy di notifica e-mail

1. Nella console di Protezione, passare a **Impostazioni** > **Notifiche e-mail**.
2. Nella schermata **Notifiche e-mail**, fare clic sull'icona**...** della policy di notifica e-mail.
3. Fare clic su **Elimina**, quindi su **Conferma**.

Visualizzazione dei dati di monitoraggio

Per ogni workload, è possibile visualizzare l'elenco dei monitor applicati, lo stato corrente dei monitor e i dettagli cronologici delle prestazioni in una vista grafica. È possibile utilizzare queste informazioni per analizzare lo stato del workload e il modo in cui è cambiato nel tempo.

Prerequisiti

- Al workload è applicato un piano di monitoraggio.
- Il workload è online e presenta i dati per il monitor corrispondente.
- La versione dell'agente installato nel workload supporta i piani di monitoraggio.

Per visualizzare i monitor applicati a un workload e i relativi dati

1. Nella console di Protezione, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare il workload e quindi fare clic sulla scheda **Monitoraggio**.
   La scheda **Monitoraggio** visualizza un widget per ogni monitor abilitato per il workload. Ogni widget visualizza le informazioni indicate di seguito.

© Acronis International GmbH, 2003-2024

Informazioni visualizzate	Descrizione
Nome monitor	Nome del monitor
Ultimo risultato	Valore più recente della metrica monitorata o stato più recente dell'evento
Ultimo controllo	Data e ora in cui il monitor ha acquisito i dati più recenti
Avvisi	Il numero di avvisi generati dal monitor e ancora non risolti. Se è presente almeno un avviso non risolto generato da questo monitor, fare clic sul numero per aprire la scheda **Avvisi**. Gli avvisi vengono filtrati e vengono elencati solo gli avvisi relativi a questo monitor.

Nota
Il widget diventa visibile nella scheda dopo 15 minuti (o dopo la frequenza di monitoraggio minima impostata per un monitor) dall'applicazione di un piano di monitoraggio al workload.

3. [Facoltativo] Per visualizzare ulteriori dettagli sul monitor e, se applicabile, i dati cronologici che sono stati acquisiti per la metrica monitorata, nel widget del monitor, fare clic sull'icona dei puntini di sospensione e quindi su **Dettagli**.
   Per ulteriori informazioni sui dettagli dei monitor che è possibile visualizzare nei widget, vedere "Widget dei monitor" (pag. 1108).

Widget dei monitor

Nei widget dei monitor è possibile visualizzare le seguenti informazioni sul monitor.

Dettaglio	Descrizione
Piano di monitoraggio	Il nome del piano di monitoraggio che contiene il monitor. Il nome del piano di monitoraggio è un link che apre il piano di monitoraggio in modalità di visualizzazione.
Frequenza del monitor	L'intervallo di tempo nel quale il monitor raccoglie i dati dal workload
Ultimo risultato	Valore più recente della metrica monitorata o stato più recente dell'evento
Ultimo controllo	Data e ora in cui il monitor ha acquisito i dati più recenti
Ultimo avviso	La data e l'ora in cui è stato generato l'ultimo avviso. Il campo viene visualizzato solo se per il monitor è stato generato almeno un avviso.
Grafico cronologico	Per i monitor che raccolgono dati in serie temporale, il widget mostra con un grafico i dati cronologici riferiti al periodo selezionato (1 ora, 6 ore, 12

© Acronis International GmbH, 2003-2024

Dettaglio	Descrizione
	ore, 1 giorno, 1 settimana o 1 mese). Il grafico mostra i valori correnti delle metriche durante un periodo selezionato. Se per qualche ragione l'agente non ha inviato i dati raccolti al cloud, i valori mancanti vengono visualizzati come linea punteggiata che collega i punti dati ai valori correnti che precedono e seguono il valore mancante. Per i monitor che utilizzano il monitoraggio **Basato su anomalia**, il grafico visualizza l'area di riferimento, una riga che mostra i valori correnti della metrica e le anomalie. Le anomalie sono rappresentate dai picchi o dai valori che si discostano dalle linee di riferimento e vengono visualizzate come punti rossi sul grafico. Passando il mouse sul grafico, è possibile visualizzare il valore corrente e i valori soglia di uno specifico momento. **Nota** I dati nei grafici vengono visualizzati con il fuso orario del sistema locale. Corrisponde al fuso orario del browser del workload dal quale si accede alla console di Protezione.

© Acronis International GmbH, 2003-2024

Strumenti Cyber Protection aggiuntivi

Modalità Conformità

La modalità Conformità è progettata per clienti con esigenze di sicurezza più elevate. Tale modalità richiede la crittografia obbligatoria di tutti i backup e consente soltanto l'uso di password di crittografia impostate a livello locale.

In modalità Conformità, tutti i backup creati in un tenant cliente e nelle relative unità vengono crittografati automaticamente con l'algoritmo AES e una chiave a 256 bit. Gli utenti possono impostare le proprie password di crittografia soltanto nei dispositivi protetti, e non possono impostarle nei piani di protezione.

Importante
Non è possibile disabilitare la modalità Conformità.

Limitazioni

- La modalità Conformità è compatibile solo con gli agenti la cui versione è 15.0.26390 o superiore.
- La modalità Conformità non è disponibile per i dispositivi che eseguono Red Hat Enterprise Linux 4.x o 5.x e i loro derivati.
- I servizi cloud non possono accedere alle password di crittografia. A causa di questa limitazione, alcune funzionalità non sono disponibili ai tenant in modalità Conformità.

Funzionalità non supportate

Le funzionalità seguenti non sono disponibili ai tenant in modalità Conformità:

- Ripristino mediante la console di Cyber Protect
- Esplorazione dei backup a livello di file mediante la console di Cyber Protect
- Backup da cloud a cloud
- Backup di siti web
- Backup applicazione
- Backup di dispositivi mobili
- Scansione anti-malware dei backup
- Ripristino sicuro
- Creazione automatica di elenchi degli elementi consentiti aziendali
- Mappa di protezione dati
- Disaster Recovery
- Report e dashboard correlati alle funzionalità non disponibili

© Acronis International GmbH, 2003-2024

Impostare la password di crittografia

È necessario impostare questa password di crittografia in locale, nel dispositivo protetto. Non è possibile impostare la password di crittografia in un piano di protezione. Senza una password, la creazione dei backup non ha esito positivo.

Attenzione!
Impossibile recuperare i backup crittografati se si perde o si dimentica la password.

È possibile impostare la password di crittografia nei modi indicati di seguito:

1. Durante l'installazione di un agente di protezione (per Windows, macOS e Linux).
2. Utilizzando la riga di comando (per Windows e Linux).
   Questo è l'unico modo per impostare una password di crittografia su un'appliance virtuale.
   Per ulteriori informazioni su come impostare una password di crittografia con lo strumento **Acropsh**, fare riferimento a "Crittografia" (pag. 449).
3. In Cyber Protect Monitor (per Windows e macOS).

Per impostare la password di crittografia in Cyber Protect Monitor

1. Nel dispositivo protetto, accedere come amministratore.
2. Fare clic sull'icona Cyber Protect Monitor nell'area di notifica (in Windows) o nella barra dei menu (in macOS).
3. Fare clic sull'icona ingranaggio.
4. Fare clic su **Crittografia**
5. Impostare la password di crittografia.
6. Fare clic su **OK**.

Modifica della password di crittografia

È possibile modificare le impostazioni di crittografia prima della creazione dei backup da parte del relativo piano di protezione.

Non è consigliabile modificare la password di crittografia dopo la creazione dei backup, perché i backup successivi non avranno esito positivo. Per continuare a proteggere lo stesso sistema, è necessario creare un nuovo piano di protezione apposito. Modificare sia la password di crittografia sia il piano di protezione ha come conseguenza la creazione di nuovi backup che vengono crittografati con la password modificata. I backup creati prima di queste modifiche non subiranno modifiche.

In alternativa, è possibile mantenere il piano di protezione applicato e modificare soltanto il nome del file di backup in esso contenuto. Inoltre, in questo modo i nuovi backup creati saranno crittografati con la password modificata. Per ulteriori informazioni sul nome del file di backup, fare riferimento a "Nome file di backup" (pag. 457).

© Acronis International GmbH, 2003-2024

È possibile modificare la password di crittografia nei modi indicati di seguito:

1. In Cyber Protect Monitor (per Windows e macOS).
2. Utilizzando la riga di comando (per Windows e Linux).
   Per ulteriori informazioni su come impostare una password di crittografia con lo strumento **Acropsh**, fare riferimento a "Crittografia" (pag. 449).

Ripristino dei backup per i tenant in modalità Conformità

In modalità Conformità, non è possibile ripristinare i backup nella console di Cyber Protect.

Sono disponibili le seguenti opzioni:

- Ripristino dell'intero sistema e dei relativi dischi o file mediante un supporto di avvio.
- Estrazione di file dai backup locali di sistemi Windows con agente installato, utilizzando Esplora file di Windows.

Archivio immutabile

Lo storage immutabile consente di accedere ai backup eliminati durante un periodo di conservazione specificato. Sarà possibile ripristinare il contenuto da questi backup, ma non sarà possibile modificarli, spostarli o eliminarli. Al termine del periodo di conservazione, i backup eliminati verranno eliminati definitivamente.

Lo storage immutabile contiene i backup seguenti:

- Backup eliminati manualmente.
- Backup eliminati automaticamente in base alle impostazioni indicate nella sezione **Tempo di conservazione** di un piano di protezione o della sezione **Regole di conservazione** di un piano di pulizia.

I backup eliminati nello storage immutabile utilizzano comunque uno spazio di storage il cui consumo viene addebitato.

Lo spazio di storage utilizzato dai tenant eliminati, incluso quello per lo storage immutabile, non viene addebitato.

Modalità dell'archivio immutabile

Per i tenant cliente, l'archivio immutabile è disponibile nelle modalità seguenti:

L'archivio immutabile è disponibile nelle modalità seguenti:

- **Modalità Governance**
  Questa modalità consente di disabilitare e abilitare di nuovo l'archivio immutabile, modificare il periodo di conservazione o passare alla modalità Compliance.
- **Modalità Conformità**

© Acronis International GmbH, 2003-2024

Attenzione!
La selezione della modalità Compliance è irreversibile.

Non è possibile disabilitare l'archivio immutabile né modificare il periodo di conservazione e non è possibile tornare alla modalità Governance.

Storage e agenti supportati

- Lo storage immutabile è supportato solo nel cloud storage.

  Lo storage immutabile è disponibile per i cloud storage su hosting di Acronis e dei partner che utilizzano Acronis Cyber Infrastructure versione 4.7.1 o successiva.

  Sono supportati tutti gli storage che possono essere utilizzati con Acronis Cyber Infrastructure Backup Gateway, ad esempio lo storage Acronis Cyber Infrastructure, lo storage Amazon S3 ed EC2 e lo storage Microsoft Azure.

  Lo storage immutabile richiede che la porta TCP 40440 sia aperta per il servizio Backup Gateway in Acronis Cyber Infrastructure. Nella versione 4.7.1 e successive, la porta TCP 40440 è aperta automaticamente in presenza del tipo di traffico **Backup (ABGW) public**. Per ulteriori informazioni sui tipi di traffico, consultare la documentazione di Acronis Cyber Infrastructure.
- L'archivio immutabile richiede un agente di protezione versione 21.12 (build 15.0.28532) o successive.
- Sono supportati solo i backup TIBX (Versione 12).

Abilitazione dell'archivio immutabile

È possibile configurare le impostazioni dell'archivio immutabile nella console di Cyber Protect o nel portale di gestione. Entrambi forniscono l'accesso alle stesse funzionalità. La procedura sottostante utilizza la console di Cyber Protect. Per ulteriori informazioni su come configurare le impostazioni dell'archivio immutabile nel portale di gestione, consultare Configurazione dell'archivio immutabile nel manuale dell'amministratore.

Per la configurazione delle impostazioni dello storage immutabile è necessario aver abilitato l'autenticazione a due fattori per il tenant al quale appartiene l'account amministratore.

Per abilitare l'archivio immutabile

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Impostazioni** > **Impostazioni di sistema**.
3. Scorrere l'elenco delle opzioni di backup predefinite, quindi fare clic su **Archivio immutabile**.
4. Abilitare l'opzione **Archivio immutabile**.
5. Specificare un periodo di conservazione tra 14 e 3650 giorni.

   Il periodo di conservazione predefinito è di 14 giorni. Un periodo di conservazione più lungo implica un maggiore utilizzo dello storage.
6. Selezionare la modalità Archivio immutabile, quindi confermare la scelta se richiesto.

© Acronis International GmbH, 2003-2024

In modalità Governance, è possibile abilitare o disabilitare l'archivio immutabile e modificare il periodo di conservazione. È possibile passare dalla modalità Governance alla modalità Conformità.

Attenzione!
Il passaggio alla modalità Conformità è irreversibile. Dopo aver selezionato questa modalità, non sarà più possibile disabilitare l'archivio immutabile, modificarne la modalità o il periodo di conservazione.

7. Fare clic su **Salva**.
8. Per far sì che un archivio esistente supporti lo storage immutabile, creare un nuovo backup in tale archivio.
   Per creare un nuovo backup, eseguire il piano di protezione in modo manuale o in base alla pianificazione.

   Attenzione!
   Se si elimina un backup prima che l'archivio supporti lo storage immutabile, tale backup verrà cancellato definitivamente.

Disabilitazione dell'archivio immutabile

Nota
È possibile disabilitare l'archivio immutabile solo nella modalità Governance.

Per disabilitare l'archivio immutabile

1. Accedere alla console di Cyber Protect come amministratore.
2. Nel menu di navigazione, fare clic su **Impostazioni** > **Impostazioni di sistema**.
3. Scorrere l'elenco delle opzioni di backup predefinite, quindi fare clic su **Archivio immutabile**.
4. Disabilitare l'opzione **Archivio immutabile**.
5. Confermare la selezione facendo clic su **Disabilita**.

Attenzione!
La disabilitazione dello storage immutabile non ha effetto immediato. Durante il grace period di 14 giorni, lo storage immutabile è ancora attivo e sarà possibile accedere ai backup eliminati in base al loro periodo di conservazione originale. Al termine del grace period, tutti i backup contenuti nello storage immutabile verranno eliminati definitivamente.

Accesso ai backup eliminati nell'archivio immutabile

Durante il periodo di conservazione, è possibile accedere ai backup eliminati e ripristinare dati da questi.

© Acronis International GmbH, 2003-2024

Nota
Per consentire l'accesso ai backup eliminati, la porta 40440 dello storage di backup deve essere abilitata per le connessioni in entrata.

Per accedere a un backup eliminato

1. Nella scheda **Archivio di backup**, selezionare il cloud storage che contiene il backup eliminato.
2. [Solo per archivi eliminati] Per visualizzare gli archivi eliminati, fare clic su **Mostra eliminati**.
3. Selezionare l'archivio che contiene il backup da recuperare.
4. Fare clic su **Mostra backup** quindi su **Mostra eliminati**.
5. Selezionare il backup da ripristinare.
6. Procedere con l'operazione di ripristino come descritto in "Ripristino" (pag. 503).

Storage con geo-ridondanza

Lo storage con geo-ridondanza aumenta la durata dei dati copiandoli in modo asincrono in una posizione secondaria e geograficamente distante dalla posizione primaria. La geo-ridondanza rende accessibili i dati anche in caso di mancata disponibilità della posizione primaria.

Importante
I dati replicati occupano lo stesso spazio di storage dei dati originari.

Abilitazione e disabilitazione dello storage con geo-ridondanza

Prerequisiti

- Lo storage con geo-ridondanza diventa disponibile nella console di Cyber Protect solo dopo essere stato abilitato da un amministratore del Partner nel portale di gestione o tramite API.
- Solo gli amministratori possono abilitare o disabilitare lo storage con geo-ridondanza nella console di Cyber Protect. Verificare di disporre dei diritti di amministratore.

Per abilitare lo storage con geo-ridondanza

1. [Solo se lo storage con geo-ridondanza è stato abilitato tramite API] Nell'avviso visibile in alto: "La geo-ridondanza è disponibile per tutti i dati dell'utente nel cloud", fare clic su **Abilita Geo-redundant Cloud Storage**.
2. Nella console di Cyber Protect, passare a **Impostazioni** > **Impostazioni di sistema**.
3. Scorrere l'elenco delle opzioni di backup predefinite, quindi fare clic su **Geo-redundant Cloud Storage**.
4. Abilitare l'opzione **Geo-redundant Cloud Storage**.
5. Fare clic su **Salva**.
   In questo modo i dati vengono replicati in una posizione secondaria e restano disponibili anche in caso di indisponibilità della posizione primaria.

© Acronis International GmbH, 2003-2024

Per disabilitare lo storage con geo-ridondanza

Attenzione!
I dati replicati vengono eliminati entro un giorno dalla disabilitazione della geo-ridondanza.

1. Nella console di Cyber Protect, passare a **Impostazioni** > **Impostazioni di sistema**.
2. Scorrere l'elenco delle opzioni di backup, quindi fare clic su **Geo-redundant Cloud Storage**.
3. Disabilitare l'opzione **Geo-redundant Cloud Storage**.
4. Confermare la scelta facendo clic su **Disabilita** e quindi su **Disabilita**.

Stato della geo-replica

La geo-ridondanza implica che i dati vengono replicati su una posizione secondaria. Lo stato della geo-replica mostra le fasi di questo processo. Sono possibili gli stati seguenti:

- **Sincronizzata**: i dati sono stati replicati nella posizione secondaria.
- **In corso di sincronizzazione**: è in corso la replica dei dati nella posizione secondaria. La durata di questa operazione dipende dalla dimensione dei dati.
- **In attesa**: la replica dei dati è stata temporaneamente sospesa.
- **Disabilitata**: la replica dei dati è disabilitata.

Per controllare lo stato della replica nella console di Cyber Protect

1. Nella console di Cyber Protect, passare a **Archivio di backup**.
2. Selezionare la posizione e il set di backup.
3. Fare clic su **Dettagli**, quindi controllare lo stato in **Stato della geo-replica**.

Limitazioni

- Al momento, le posizioni secondarie per i dati replicati sono disponibili solo negli Stati Uniti e in Canada.
- Per informazioni sui limiti del servizio di Disaster Recovery quando si utilizza la geo-ridondanza, consultare la documentazione di Disaster Recovery.

© Acronis International GmbH, 2003-2024

Glossario

A

Agente di prevenzione della perdita di dati

Componente del sistema del cliente per la prevenzione della perdita di dati, che impedisce l'utilizzo non autorizzato del computer host per la trasmissione e l'archiviazione di dati sensibili, riservati o protetti applicando una combinazione di tecniche di analisi del contesto e dei contenuti e criteri per la prevenzione della perdita di dati gestiti a livello centralizzato. Cyber Protection offre un agente di prevenzione della perdita di dati ricco di funzionalità. Tuttavia, la funzionalità dell'agente in un computer protetto è limitata all'insieme di funzionalità di prevenzione della perdita di dati disponibile con le licenze di Cyber Protection, e dipende dal piano di protezione applicato a tale computer.

Agente di protezione

È l'agente che viene installato nei sistemi per la protezione dati.

Appliance VPN

[Disaster Recovery] Una macchina virtuale speciale che abilita la connessione tra la rete locale e il sito nel cloud tramite un tunnel VPN sicuro. L'appliance VPN viene distribuita nel sito locale.

B

Backup completo

Un backup autosufficiente contenente tutti i dati selezionati per il backup. Non è necessario accedere ad altri backup per ripristinare i dati da un backup completo.

Backup differenziale

In un backup differenziale vengono memorizzate le modifiche apportate ai dati rispetto all'ultimo backup completo. È necessario accedere al backup completo corrispondente per ripristinare i dati da un backup differenziale.

Backup incrementale

Un backup che memorizza le modifiche dei dati rispetto all'ultimo backup. È necessario accedere ad altri backup per ripristinare i dati da un backup incrementale.

Backup orfano

Si definisce orfano un backup che non è più associato a un piano di protezione.

C

Connessione da punto a sito (P2S)

[Disaster Recovery] Una connessione VPN sicura dall'esterno che usa i dispositivi endpoint (ad esempio un computer o laptop) per collegarsi al cloud e ai siti locali.

Connessione da sito a sito (S2S)

[Disaster Recovery] Una connessione che estende la rete locale nel cloud tramite un tunnel VPN sicuro.

Convalida

Un'operazione che controlla la possibilità di ripristino dei dati da un backup. La convalida di un backup di file imita il ripristino di tutti i file dal backup a un destinazione non operativa. La convalida di un backup del disco calcola una

© Acronis International GmbH, 2003-2024

somma di controllo per ogni blocco dei dati salvato nel backup. Entrambe le procedure hanno un elevato dispendio di risorse. Sebbene una convalida eseguita correttamente implichi un'elevata probabilità di riuscita del ripristino, essa non controlla tutti i fattori che influenzano la procedura di ripristino.

D

Database dei dispositivi USB

[Controllo dispositivo] Il modulo Controllo dispositivo gestisce un database di dispositivi USB dal quale questi ultimi possono essere aggiunti all'elenco delle esclusioni per il controllo degli accessi ai dispositivi. Nel database, i dispositivi USB vengono registrati con l'ID dispositivo, che può essere immesso manualmente o selezionato dai dispositivi noti nella console di Cyber Protect.

F

Failback

Passaggio di un carico di lavoro da un server di riserva (ad esempio la replica di una macchina virtuale o un server di ripristino in esecuzione nel cloud) al server di produzione.

Failover

Passaggio di un carico di lavoro da un server di produzione a un server di riserva (ad esempio la replica di una macchina virtuale o un server di ripristino in esecuzione nel cloud).

Finalizzazione

L'operazione che trasforma una macchina virtuale temporanea eseguita da un backup in una macchina virtuale permanente. Dal punto di vista fisico, ciò significa ripristinarne tutti i dischi virtuali, nonché le modifiche apportate durante l'esecuzione della macchina, nel datastore in cui sono archiviate tali modifiche.

Formato di backup a file singolo

Un nuovo formato di backup, in cui i backup incrementali completi e successivi vengono salvati su un unico file .tibx. Questo formato consente di sfruttare la velocità del metodo di backup incrementale, evitando tuttavia il suo principale svantaggio ovvero la difficoltà di eliminazione dei backup obsoleti. Il software contrassegna i blocchi utilizzati dai backup obsoleti come "liberi" e li utilizza per scrivere i nuovi backup. Ne consegue una pulizia estremamente rapida, con un consumo minimo delle risorse. Il formato di backup a file singolo non è disponibile quando si esegue il backup in posizioni che non supportano le modalità di lettura e scrittura con accesso casuale.

G

Gateway VPN (in precedenza noto come server VPN o gateway di connessione)

[Disaster Recovery] Una macchina virtuale speciale che fornisce la connessione tra il sito locale e il sito nel cloud tramite un tunnel VPN sicuro. Il gateway VPN viene distribuito nel sito cloud.

I

Indirizzo IP di prova

[Disaster Recovery] Un indirizzo IP necessario in caso di failover di prova, per impedire la duplicazione dell'indirizzo IP di produzione.

Indirizzo IP pubblico

[Disaster Recovery] Un indirizzo IP necessario per rendere i server cloud disponibili da

© Acronis International GmbH, 2003-2024

Internet.

M

Macchina fisica

Una macchina il cui backup viene eseguito ad opera di un agente installato nel sistema operativo.

Macchina virtuale

Una virtual machine il cui backup viene eseguito a livello di hypervisor da un agente esterno, come l'Agente per VMware o l'Agente per Hyper-V. Dal punto di vista del backup, una virtual machine con un agente interno viene considerata come un sistema fisico.

Modulo

Il modulo è un componente di un piano di protezione che fornisce una specifica funzionalità di protezione dati. Ne sono esempi il modulo Backup, il modulo Protezione antivirus e anti-malware e così via.

Modulo Controllo dispositivo

Componente di un piano di protezione, il modulo Controllo dispositivo si avvale di un sottoinsieme delle funzioni dell'agente di prevenzione della perdita di dati su ogni computer protetto, per rilevare e prevenire l'accesso non autorizzato ai dati e la loro trasmissione tramite i canali dei computer locali, quali, ad esempio, l'accesso degli utenti a periferiche e porte, la stampa di documenti, operazioni di copia/incolla da appunti, operazioni di formattazione ed espulsione di supporti e di sincronizzazione con dispositivi mobile connessi in locale. Il modulo Controllo dispositivo offre un controllo granulare e contestuale dei tipi di dispositivi e porte a cui gli utenti possono accedere sul computer protetto e sulle azioni che gli utenti possono intraprendere su tali dispositivi.

O

Obiettivo punto di ripristino (RPO)

[Disaster Recovery] Quantità di dati perduta a causa di un'interruzione, misurata come la quantità di tempo a partire da un'interruzione pianificata o da un’emergenza. La soglia RPO definisce l'intervallo di tempo massimo consentito tra l'ultimo punto di ripristino idoneo per un failover e l’ora corrente.

P

Piano di protezione

Il piano di protezione combina diversi moduli di protezione dati, incluso Backup, Protezione antivirus e antimalware, Filtro URL, Windows Defender Antivirus, Microsoft Security Essentials, Valutazione delle vulnerabilità, Gestione patch, Mappa di protezione dei dati.

Prevenzione della perdita di dati

Un sistema di tecnologie integrate e di misure organizzative intese a individuare e a prevenire la diffusione e/o l'accesso accidentale o intenzionale a dati riservati, protetti o sensibili da parte di entità non autorizzate interne o esterne all'organizzazione, o il trasferimento di tali dati in ambienti non attendibili.

R

Rete di produzione

[Disaster Recovery] La rete interna estesa per mezzo di un tunnel VPN, a copertura dei siti locali e cloud. I server locali e i server cloud possono comunicare tra loro nella rete di produzione.

© Acronis International GmbH, 2003-2024

Rete di prova

[Disaster Recovery] Rete virtuale isolata utilizzata per testare il processo di failover.

Runbook

[Disaster Recovery] Uno scenario pianificato costituito da passaggi configurabili che automatizzano le azioni da intraprendere in caso di disaster recovery.

S

Server cloud

[Disaster Recovery] Riferimenti generali per il ripristino di un server primario.

Server di ripristino

[Disaster Recovery] Una replica virtuale della macchina di origine, basata sui backup dei server protetti archiviati nel cloud. I server di ripristino sono utilizzati per trasferire i carichi di lavoro dai server originali in caso di emergenza.

Server primario

[Disaster Recovery] Una macchina virtuale che non dispone di un sistema collegato nel sito locale (ad esempio un server di ripristino). I server primari sono utilizzati per proteggere un'applicazione o per eseguire diversi servizi ausiliari, ad esempio un server web.

Set backup

Un gruppo di backup a cui è possibile applicare una singola regola di conservazione. Per lo schema di backup Personalizzato, i set di backup corrispondono ai metodi di backup (Completo, Differenziale e Incrementale). In tutti gli altri casi, i set di backup sono Mensile, Giornaliero, Settimanale e Ogni ora. Un backup mensile è il primo backup creato dopo l'inizio di un mese. Un backup settimanale è il primo backup creato nel giorno della settimana selezionato nell'opzione Backup settimanale (fare clic sull'icona dell'ingranaggio, quindi su Opzioni di backup > Backup settimanale). Se il primo backup creato dopo l'inizio di un mese è un backup settimanale, verrà considerato mensile. In questo caso, il backup settimanale verrà creato nel giorno selezionato della settimana successiva. Un backup giornaliero è il primo backup creato dopo l'inizio di un giorno, a meno che tale backup non rientri nella definizione di backup mensile o settimanale. Un backup eseguito ogni ora è il primo backup creato dopo l'inizio di un'ora, a meno che tale backup non rientri nella definizione di backup mensile, settimanale o giornaliero.

Sito cloud (o sito DR)

[Disaster Recovery] Sito remoto con hosting nel cloud, utilizzato per l'esecuzione dell'infrastruttura di ripristino in caso di emergenza.

Sito locale

[Disaster Recovery] L'infrastruttura locale distribuita nella sede dell'azienda.

© Acronis International GmbH, 2003-2024

Indice

#

#CyberFit Score dei sistemi 233

#CyberFit Score per sistema 295

3

32 o 64 bit? 727

A

Abilita backup completo VSS 501

Abilitare la funzionalità Endpoint Detection and Response (EDR) 918

Abilitare o disabilitare il controllo dispositivo 374

Abilitare o disabilitare le notifiche e gli avvisi di servizio del sistema operativo 377

Abilitazione dell'archivio immutabile 1113

Abilitazione dell'utilizzo del modulo Controllo dispositivo su macOS 374

Abilitazione della modalità di monitoraggio per Endpoint Detection and Response (EDR) 970

Abilitazione della ricerca avanzata nei backup crittografati 680

Abilitazione della scansione dell'inventario hardware 1004

Abilitazione della scansione dell'inventario software 999

Abilitazione di Advanced Data Loss Prevention nei piani di protezione 896

Abilitazione di One-click Recovery 482

Abilitazione e disabilitazione della connessione da sito a sito 784

Abilitazione e disabilitazione dello storage con geo-ridondanza 1115

Abilitazione e disabilitazione di Gestione firewall 878

Abilitazione o disabilitazione della ricerca avanzata nei piani esistenti 680

Abilitazione o disabilitazione di un piano di protezione 223

Accesso a siti web dannosi 867

Accesso a un'appliance virtuale tramite un client SSH 178

Accesso ai backup eliminati nell'archivio immutabile 1114

Accesso al servizio Cyber Protection 22

Accesso VPN al sito locale 789

Accesso VPN remoto da punto a sito 768

Acquisizione dei certificato per i backup con dati forensi 474

Acquisizione di pacchetti di rete 792

Active Protection 841

Active Protection nell'edizione Cyber Backup Standard 857

Adeguamento delle autorizzazioni nelle regole della policy di flusso dei dati 891

Advanced Antimalware 842

Advanced Data Loss Prevention 886

Agente cloud e agente locale 608

Agente per Advanced Data Loss Prevention 25

Agente per Exchange (per il backup delle caselle di posta) 26

Agente per File Sync & Share 25

Agente per Hyper-V 29

© Acronis International GmbH, 2003-2024

Agente per la prevenzione della perdita di dati 25

Agente per Linux 27

Agente per Mac 28

Agente per Microsoft 365 26

Agente per MySQL/MariaDB 27

Agente per Oracle 27

Agente per oVirt 30

Agente per oVirt – ruoli e porte richiesti 162

Agente per Scale Computing HC3 30

Agente per Scale Computing HC3 - ruoli necessari 147

Agente per SQL, Agente per Active Directory, Agente per Exchange (per il backup di database e il backup application-aware) 25

Agente per Synology 30

Agente per Virtuozzo 29

Agente per Virtuozzo Hybrid Infrastructure 29

Agente per VMware - Backup senza LAN 704

Agente per VMware (appliance virtuale) 29

Agente per VMware (Windows) 29

Agente per Windows 23

Aggiornamenti automatici dei componenti 187

Aggiornamenti non effettuati per categorie 304

Aggiornamento automatico degli agenti 181

Aggiornamento degli agenti sui workload protetti da BitLocker 183

Aggiornamento delle definizioni di Cyber Protection in base alla pianificazione 188

Aggiornamento delle definizioni di Cyber Protection su richiesta 188

Aggiornamento di Agente per Synology 169

Aggiornamento di agenti 178

Aggiornamento manuale degli agenti 179

Aggiornare, ricompilare o eliminare gli indici 678

Aggiungere o rimuovere i dispositivi USB dal database 378

Aggiungere o rimuovere un processo, un file o una rete nell'elenco degli elementi consentiti o nell'elenco degli elementi bloccati del piano di protezione 968

Aggiunta automatica all'elenco degli elementi consentiti 880

Aggiunta dell'accesso a un abbonamento Microsoft Azure 560

Aggiunta dell'accesso a una connessione al cloud pubblico 564

Aggiunta di credenziali 1033

Aggiunta di file in quarantena all'elenco degli elementi consentiti 881

Aggiunta di un workload a un piano di gestione remota 1027

Aggiunta di un’organizzazione di Microsoft 365 613, 618

Aggiunta di un’organizzazione Google Workspace 656

Aggiunta di VLAN 741

Aggiunta di workload a un gruppo statico 349

Aggiunta di workload ai piani di monitoraggio 1090

Aggiunta di workload alla console di Cyber Protect 336

Aggiunta manuale all'elenco degli elementi consentiti 881

Algoritmo di distribuzione 708

© Acronis International GmbH, 2003-2024

All'evento Registro eventi di Windows 433

Altre opzioni di accesso 1016

Amazon 41

Amministrazione di organizzazioni di Microsoft 365 aggiunte su diversi livelli 619

Analisi dei dettagli del problema 926

Analisi del rilevamento dei colli di bottiglia 544

Analisi riepilogativa dei problemi 920

Annullamento dell'assegnazione di credenziali da un workload 1034

Appliance VPN 764

Applicare una patch a un workload 956

Applicazione di un piano a gruppo 369

Applicazione di un piano di protezione a un workload 221

Applicazione di un piano di protezione predefinito 231

Applicazioni cloud 305

Approvazione automatica della patch 992

Approvazione manuale delle patch 997

Archiviazione cache 188

Archiviazione degli eventi di sicurezza per 180 giorni 918

Archivio immutabile 1112

Arresto dell’esecuzione di un runbook 833

Arresto failover 701

Assegnare la priorità ai problemi che richiedono un intervento immediato 922

Assegnazione di credenziali a un workload 1034

Assegnazione indirizzo IP di prova 764

Associazione delle macchine virtuali 708

Associazione manuale 709

Attendi che le condizioni della pianificazione siano soddisfatte 499

Attivazione dell'account 19

Attivazione di Startup Recovery Manager 746

Attributi di ricerca per i workload cloud-to-cloud 352

Attributi di ricerca per i workload non cloud-to-cloud 353

Autenticazione 452, 675

Autenticazione a due fattori 19

Autenticazione dei backup con dati forensi 473

Auto-protezione 844

Autorizzazioni 892

Autorizzazioni delle policy 557-558

Autorizzazioni richieste per l'installazione automatica in macOS 114

Avanzato 876

Avvia la macchina virtuale di destinazione quando il ripristino è completo 536

Avvio del daemon Secure Shell 177

Avvisi 456

Avvisi di Backup 269

Avvisi di Controllo dispositivo 287, 394

Avvisi di Disaster recovery 273

Avvisi di EDR 286

Avvisi di Filtro URL 286

Avvisi di Licensing 284

Avvisi di Protezione anti-malware 279

Avvisi di Sistema 288

Avvisi di stato dell'integrità del disco 300

Azione al rilevamento 858

Azioni 893

© Acronis International GmbH, 2003-2024

Azioni di risposta manuali 1102

Azioni di risposta per singoli nodi della sequenza di attacco informatico 949

Azioni eseguibili con i piani di protezione 220

Azioni predefinite 875

B

Backup 57, 404

Backup caselle di posta 579

Backup compatibile con i cluster 575

Backup compatibile con l'applicazione 577

Backup con agente e agentless 66

Backup dei database compresi in un AAG 574

Backup dei dati dei cluster di Exchange 576

Backup dei server cloud 827

Backup di database 571

Backup di sistemi Hyper-V in cluster 717

Backup di un sito Web 689

Backup di virtual machine Microsoft Azure e Amazon EC2 723

Backup di workload su cloud pubblici 548

Backup incrementale/differenziale veloce 467

Backup precedente all'aggiornamento 990

Backup settimanale 503

Backup settore per settore 497

Backup su Amazon S3 556

Backup su Wasabi 558

Basato su Linux 725

Basato su WinPE/WinRE 725

Browser Web supportati 23

Burndown dei problemi di sicurezza 294

C

calculate hash 477

Cancellazione dei dati da un workload gestito 398

Caratteristiche 916

Cartella personalizzata self-service su richiesta 880

Caso d'uso per l'Approvazione automatica della patch senza test 996

Caso d'uso per l'approvazione e i test automatici delle patch 994

Categorie da filtrare 867

Categorie di riservatezza personalizzate 909

Changed block tracking (CBT) 464

Changed Block Tracking (CBT) 702

Che cos'è un file di backup? 457

Chiavi di accesso 558-559

Citrix 37

Classi di storage supportate 557

Clonazione di uno script 248

Codec Adaptive 1016

Collegamento di database di SQL Server 589

Collegare workload a utenti specifici 402

Comandi post-acquisizione dei dati 495

Comandi post-backup 493

Comandi post ripristino 534

Comandi pre-acquisizione dei dati 494

Comandi pre-backup 492

Comandi pre-ripristino 533

Comandi pre/post 491, 533, 702-703

Comandi prima/dopo la cattura dei dati 493

© Acronis International GmbH, 2003-2024

Combinare le regole della policy di flusso dei dati 892

Come assegnare i diritti utente 86

Come capire quali problemi di sicurezza richiedono un intervento immediato 922

Come creare Secure Zone 423

Come eliminare Secure Zone 424

Come eseguire il failover di server utilizzando il server DNS locale 806

Come eseguire il failover di un server DHCP 807

Come funziona 233, 297, 309, 312, 417, 452, 473, 676, 857, 865

Come funziona il routing 760, 763, 768

Come funziona? 912

Come indagare sui problemi rilevati nella sequenza di attacco 929

Come orientarsi nelle fasi di attacco 934

Come ottenere i dati forensi da un backup 472

Come ottenere l'ID e il segreto dell'applicazione 614

Come ridurre i colli di bottiglia 545

Come rivedere i dati tramite la console di Cyber Protect 603

Come utilizzare l'autenticazione 452, 675

Come utilizzare la funzionalità Endpoint Detection and Response (EDR) 920

Come vengono spostati i file nella cartella Quarantena? 878

Come verificare il corretto funzionamento della funzionalità Endpoint Detection and Response (EDR) 972

Compatibilità con gli storage Dell EMC Data Domain 43

Compatibilità con il software di crittografia 42

Compatibilità del formato del backup tra diverse versioni del prodotto 463

Compatibilità di Disaster Recovery con il software di crittografia 753

Componenti per l'installazione automatica (EXE) 95

Componenti per l'installazione automatica (MSI) 104

Comprendere e personalizzare la visualizzazione della sequenza dell'attacco informatico 931

Comprendere le azioni intraprese per mitigare un problema 937

Comprensione del livello attuale di protezione 265

Comprensione dell'ambito e dell'impatto dei problemi 925

Concedere le autorizzazioni di sistema richieste a Connect Agent 84

Concetti sulla rete 759

Condivisione schermo di Apple 1016

Condizioni di avvio 256, 434

Condizioni di avvio dell'attività 498

Configurare il piano di protezione Applicazione di patch in ambiente di produzione 995

Configurare la permanenza delle patch nell'elenco 992

Configurare le impostazioni di VPN IPsec multisito 772

Configurare un backup application-aware 683

Configurazione degli account utente in Virtuozzo Hybrid Infrastructure 149

Configurazione degli avvisi di monitoraggio 1099

Configurazione dei server di ripristino 796

© Acronis International GmbH, 2003-2024

Configurazione dei server primari 819

Configurazione del failover di prova automatizzato 803

Configurazione del numero di nuovi tentativi in caso di errore 211

Configurazione del piano di protezione Applicazione di patch in ambiente di test 994

Configurazione del routing locale 788

Configurazione dell'accesso VPN remoto da punto a sito 778

Configurazione dell'appliance virtuale 139, 144, 153, 159

Configurazione dell'approvazione automatica delle patch 993

Configurazione della connessione 759

Configurazione della connessione iniziale 770

Configurazione della crittografia come proprietà del sistema 450

Configurazione della crittografia nel piano di protezione 449

Configurazione della funzionalità di disaster recovery 755

Configurazione della modalità solo cloud 770

Configurazione della protezione antivirus e anti-malware 835

Configurazione delle azioni di risposta automatica 1091

Configurazione delle impostazioni del server proxy 72

Configurazione delle impostazioni del server proxy in Cyber Protect Monitor 318

Configurazione delle impostazioni di Connect Client 1050

Configurazione delle impostazioni di rete 741

Configurazione delle impostazioni RDP 1035

Configurazione delle policy di notifica e-mail 1106

Configurazione delle regole di conservazione 446

Configurazione delle reti in Virtuozzo Hybrid Infrastructure 149

Configurazione di rete del gateway VPN 763

Configurazione di server DNS personalizzati 787

Configurazione di un backup CDP 419

Configurazione di una connessione Open VPN da sito a sito 770

Configurazione di una connessione VPN IPsec multisito 772

Configurazione di una Open VPN da sito a sito 770

Configurazioni cluster supportate 574-575

Conflitto tra un piano individuale e un piano di gruppo 225

Conflitto tra un piano nuovo e uno esistente 225

Confronto tra conversione regolare in virtual machine ed esecuzione di una virtual machine da un backup 216

Confronto tra i piani di protezione predefiniti 226

Confronto tra replica e backup 698

Confronto tra versioni di uno script 251

Connessione a un sistema avviato da un supporto di avvio 740

Connessione a workload gestiti per desktop remoto o assistenza remota 1036

Connessione a workload non gestiti tramite Acronis Quick Assist 1044

© Acronis International GmbH, 2003-2024

Connessione a workload non gestiti tramite indirizzo IP 1045

Connessione a workload per attività di desktop remoto o assistenza remota 1010

Connessione locale 740

Connessione Open VPN da sito a sito 761, 779

Connessione remota a un workload 960

Connessione VPN IPsec multisito 767

Connessioni a workload remoti per desktop remoto o assistenza remota 1018

Connessioni da punto a sito attive 790

Connessioni SSH a un'appliance virtuale 177

Connetti a un workload gestito tramite client web 1039

Consegna fisica dei dati 490

Consentire il traffico DHCP su L2 VPN 788

Consigli e raccomandazioni di correzione 917

Consolidamento backup 456

Contrassegnato come Riservato 905

Controlla gli indirizzi IP del dispositivo 440

Controllare la presenza di indicatori di compromissione di attacchi pubblicamente noti nei workload 940

Controller di dominio Active Directory per la connessione Open VPN L2 777

Controller di dominio Active Directory per la connessione VPN IPsec L3 778

Controllo delle attività del firewall cloud 827

Controllo dello stato di convalida di un backup 212

Convalida 205

Convalida del backup 463, 529

Convalida di backup 540

Convalida screenshot 210

Conversione in macchina virtuale 213

Copiare le librerie di Microsoft Exchange 599

Correggere un intero problema 944

Correggere un problema falso positivo 948

Correzione dei problemi 944

Cos'è un collo di bottiglia? 544

Cosa attiva una regola di policy? 891

Cosa si intende con protezione dei dati di Google Workspace? 654

Creare un piano di protezione di disaster recovery 755

Creazione del file di trasformazione ed estrazione dei pacchetti di installazione 175

Creazione della policy di flusso dei dati e delle regole della policy 886

Creazione di backup in un archivio di backup esistente 461

Creazione di runbook 829

Creazione di un gruppo di dispositivi dinamico a livello del partner 330

Creazione di un gruppo di dispositivi statico a livello del partner 330

Creazione di un gruppo dinamico 350

Creazione di un gruppo statico 348

Creazione di un piano di convalida 206

Creazione di un piano di gestione remota 1019

Creazione di un piano di monitoraggio 1088

Creazione di un piano di protezione 218

Creazione di un piano di replica 699

Creazione di un piano di replica del backup 202

© Acronis International GmbH, 2003-2024

Creazione di un piano di scripting 254

Creazione di un progetto personale Google Cloud 657

Creazione di un server di ripristino 796

Creazione di un server primario 819

Creazione di un supporto di avvio fisico 725

Creazione di un supporto di avvio per recuperare i sistemi operativi 724

Creazione di un supporto di avvio WinPE o WinRE 736

Creazione di uno script 243

Creazione di uno script utilizzando l'IA 245

Creazione snapshot LVM 480

Credenziali del workload 1032

Criteri di selezione 469

Crittografia 449

Cronologia di installazione patch 303

Cronologia gravità problema 293

Cyber Protect Monitor 30, 317

Cyber Protection 290

Cyber Scripting 239

D

Da macchina fisica a macchina virtuale 509

Dashboard Attività 266

Dashboard Avvisi 267

Dashboard con panoramica rapida 917

Data e ora dei file 531

Database dei dispositivi USB 389

Dati considerati Informazioni che consentono l'identificazione personale dell'utente (PII) 903

Dati considerati Informazioni sanitarie protette (PHI) 901

Dati considerati PCI DSS 905

Dati forensi 470

Dati inseriti nel report in base al tipo di widget 322

Dati soggetti allo standard Payment Card Industry Data Security Standard (PCI DSS) 905

Deduplicazione dei dati 56

Deduplicazione negli archivi 463

Definire le azioni di risposta per un file sospetto 966

Definire le azioni di risposta per un processo sospetto 962

Definire le azioni di risposta per un workload interessato 951

Definire le azioni di risposta per una voce del Registro di sistema sospetta 968

Definire le impostazioni del feed sulle minacce 941

Definizione degli elementi da proteggere e delle modalità di protezione 199

Definizione di una posizione di backup in Amazon S3 551

Definizione di una posizione di backup in Microsoft Azure 548

Definizione di una posizione di backup in Wasabi 553

Definizioni di dati sensibili 900

Descrizione 874

Descrizione delle opzioni 478

Destinazioni supportate 419

Di quale agente occorre disporre? 62

© Acronis International GmbH, 2003-2024

Di quali elementi è possibile eseguire il backup? 604, 616, 622, 633, 638, 642, 662, 666, 671, 689

Diritti utente necessari 581, 611, 654

Diritti utente necessari per i backup application-aware 578

Disabilitare il servizio DRS automatico per l'agente 139

Disabilitazione del failover di prova automatizzato 804

Disabilitazione dell'archivio immutabile 1114

Disabilitazione dell'assegnazione automatica per un agente 710

Disabilitazione della ricerca a tutto testo per i backup di Gmail 681

Disabilitazione di One-click Recovery 484

Disattivazione di Startup Recovery Manager 747

Disinstallazione di agenti 185

Disponibilità delle opzioni di backup 453

Disponibilità delle opzioni di ripristino 528

Disponibilità elevata di un sistema ripristinato 717

Dispositivi mobili supportati 600

Distribuzione dei principali problemi per workload 292

Distribuzione del modello OVA 158

Distribuzione del modello OVF 139

Distribuzione del modello QCOW2 143, 152

Distribuzione dell'Agente per oVirt (Virtual Appliance) 156

Distribuzione dell'Agente per Scale Computing HC3 (appliance virtuale) 142

Distribuzione dell'Agente per Synology 163

Distribuzione dell'Agente per Virtuozzo Hybrid Infrastructure (appliance virtuale) 148

Distribuzione dell'Agente per VMware (Virtual Appliance) 138

Distribuzione di agenti tramite i Criteri di gruppo 171

Dove posso vedere i nomi dei file di backup? 458

Download degli agenti di protezione 77

Download dei dati relativi ai workload recentemente interessati 305

Download dei file di registro della connessione VPN IPsec 795

Download del programma di installazione 164

Download di file dall'archivio nel cloud 521

Driver di archiviazione di massa da installare in ogni caso 518

E

Elaborazione dei dati al di fuori dell'host 201

Elementi da scansionare 977

Elementi della replica 203

Elementi di cui è possibile eseguire il backup 600

Elenco degli elementi consentiti aziendale 880

Eliminare un'organizzazione di Microsoft 365 620

Eliminare un gruppo 369

Eliminazione automatica degli ambienti del cliente non utilizzati dal sito cloud 769

Eliminazione dei backup fuori dalla console di Cyber Protect 543

Eliminazione della macchina 696

Eliminazione delle credenziali 1034

© Acronis International GmbH, 2003-2024

Eliminazione di backup 542

Eliminazione di server DNS personalizzati 787

Eliminazione di tutti gli avvisi 312

Eliminazione di un piano di protezione 224

Eliminazione di workload dalla console di Cyber Protect 341

Endpoint Detection and Response (EDR) 915

Escludere i singoli dispositivi USB dal controllo dell'accesso 378

Escludere sottoclassi di dispositivo dal controllo dell'accesso 377

Esclusione di processi dal controllo dell'accesso 392

Esclusione di URL 873

Esclusioni 877

Esclusioni dalla protezione 853

Esclusioni file 532

Esecuzione automatica degli script di pre blocco e post sblocco 710

Esecuzione del backup su Microsoft Azure 556

Esecuzione del failback in un sistema fisico 814

Esecuzione del failback in una virtual machine 810

Esecuzione del piano di protezione Applicazione di patch in ambiente di test e rifiuto delle patch non sicure 996

Esecuzione del sistema 694

Esecuzione dell'individuazione automatica dei sistemi a livello del tenant partner 331

Esecuzione dell'individuazione automatica e dell'individuazione manuale 130

Esecuzione di azioni di controllo sui workload gestiti 1040

Esecuzione di un backup da una pianificazione 428

Esecuzione di un failback manuale 817

Esecuzione di un failover 804

Esecuzione di un failover di prova 800

Esecuzione di un failover permanente 701

Esecuzione di un runbook 833

Esecuzione di una macchina virtuale da un backup (Ripristino istantaneo) 693

Esecuzione di una scansione #CyberFit Score 237

Esecuzione manuale dei backup da cloud a cloud 200

Esecuzione manuale di un backup 442

Esecuzione manuale di una scansione dell'inventario hardware 1004

Esecuzione manuale di una scansione dell'inventario software 1000

Esecuzione rapida dello script 262

Esegui come macchina virtuale 209

Eseguire l'indagine sul problema 928

Eseguire un backup forense su richiesta su un workload 959

Esempi 89-90, 98, 100, 111

Esempi di utilizzo 447, 693, 698, 710

Esempio 90, 100, 113, 150-151, 435-440, 445

Backup di emergenza in caso di blocchi danneggiati sul disco rigido 433

Installazione manuale dei pacchetti in Fedora 14 72

Esportazione di backup 541

Espressione logica per tutte le lingue supportate ad eccezione del giapponese 903

Espressioni logiche per il giapponese 904

© Acronis International GmbH, 2003-2024

Espressioni logiche utilizzate per l'individuazione di contenuti 902-903, 905

Estrazione dei file MSI, MST e CAB 97

Estrazione di file dai backup locali 525

Eventi di prevenzione della perdita di dati 907

F

Failback 701

Failback in un sistema fisico di destinazione 813

Failback in una virtual machine di destinazione 808

Failback manuale 817

Failover di disaster recovery 961

Failover di produzione 799

Failover di prova automatizzato 800, 803

Failover in una copia 700

Feed minacce 309

File di registro della VPN IPsec multisito 795

File di uno script 731

File system supportati 54

Filtri di inclusione ed esclusione 468

Filtri file (Inclusioni/Esclusioni) 468

Filtro URL 865

Finalizzazione del sistema 696

Finalizzazione di sistemi in esecuzione dai backup nel cloud 697

Finalizzazione e normale ripristino a confronto 697

Finestra di backup 487

Firma di file con ASign 522

Flashback 532

Flusso di lavoro di configurazione del filtro URL 867

Flusso di lavoro di gestione delle patch 984

Formato backup 462

Formato e file di backup 462

Funzionalità anti-malware 839

Funzionalità di desktop remoto e assistenza remota supportate 1012

Funzionalità di protezione supportate in base al sistema operativo 44

Funzionalità non supportate 1110

Funzionalità principali 749

Funzionalità supportate per piattaforma 836

Funzionamento del processo di failback 807

Funzionamento del processo di failover 799

Funzionamento dell'individuazione automatica 128

Funzionamento dell'installazione remota di agenti 130

Funzionamento della conversione regolare in virtual machine 216

G

Gateway VPN 763, 768

Generatore di supporti riavviabili 726

Generazione del token di registrazione 172

Gestione degli errori 466, 531, 702-703

Gestione dei file in quarantena 879

Gestione dei file non protetti individuati 313

Gestione dei problemi nella pagina Problemi 916

Gestione dei server cloud 822

Gestione dei sistemi individuati 136

© Acronis International GmbH, 2003-2024

Gestione dei workload di destinazione di un piano 258

Gestione del backup e del ripristino di workload e file 404

Gestione dell'accesso ad altri servizi di cloud storage pubblico 563

Gestione dell'accesso agli abbonamenti Microsoft Azure 559

Gestione dell'accesso agli account di cloud pubblico 556

Gestione dell'inventario software e hardware 999

Gestione della rete 779

Gestione delle impostazioni dell'appliance VPN 783

Gestione delle impostazioni di connessioni da punto a sito 789

Gestione delle licenze per i management server in locale 198

Gestione delle reti 779

Gestione delle vulnerabilità individuate 981

Gestione di ambienti di virtualizzazione 712

Gestione di workload nella console di Cyber Protect 325

Gestione energetica MV 535, 703

Gestione fallimento dell'attività 498

Gestione firewall 877

Gestione patch 983

Gestire l'isolamento della rete di un workload 952

get content 477

Gruppi cloud-to-cloud e gruppi non cloud-to-cloud 347

Gruppi di parole chiave 906

Gruppi dinamici 347

Gruppi dispositivi 345

Gruppi integrati 346

Gruppi integrati e gruppi personalizzati 346

Gruppi personalizzati 346

Gruppi statici 346

Gruppi statici e gruppi dinamici 346

H

H.264 1015

Heartbeat MV 209

Host della posizione di backup disponibile 436

I

I pacchetti richiesti sono già installati? 69

Ignora l'esecuzione dell'attività 499

Ignora settori danneggiati 467

Ignora writer VSS non riusciti 500

Immagini WinPE 736

Immagini WinRE 736

Impedire la disinstallazione o la modifica non autorizzate degli agenti 183

Implementazione del disaster recovery 749

Impostare la password di crittografia 1111

Impostazione dell'oggetto Criteri di gruppo 176

Impostazione della frequenza dei backup di Google Workspace 661

Impostazione della frequenza dei backup di Microsoft 365 621

Impostazione della password radice su un'appliance virtuale 177

© Acronis International GmbH, 2003-2024

Impostazione delle regole del firewall per server cloud 824

Impostazione di una modalità di visualizzazione 742

Impostazioni avanzate 899

Impostazioni del bucket 558-559

Impostazioni del monitor Accessi non riusciti 1084

Impostazioni del monitor Dimensione file e cartelle 1082

Impostazioni del monitor Modifiche hardware 1064

Impostazioni del monitor personalizzato 1086

Impostazioni del monitor Registro eventi di Windows 1081

Impostazioni del monitor Software installato 1080

Impostazioni del monitor Spazio su disco 1059

Impostazioni del monitor Stato dei servizi Windows 1079

Impostazioni del monitor Stato del firewall 1083

Impostazioni del monitor Stato del processo 1079

Impostazioni del monitor Stato del software anti-malware 1084

Impostazioni del monitor Stato della funzionalità di esecuzione automatica 1086

Impostazioni del monitor Stato di Windows Update 1083

Impostazioni del monitor Temperatura CPU 1061

Impostazioni del monitor Temperatura GPU 1063

Impostazioni del monitor Ultimo riavvio del sistema 1080

Impostazioni del monitor Utilizzo della CPU 1065

Impostazioni del monitor Utilizzo della CPU per processo 1074

Impostazioni del monitor Utilizzo della memoria 1067

Impostazioni del monitor Utilizzo della memoria per processo 1075

Impostazioni del monitor Utilizzo della rete 1072

Impostazioni del monitor Utilizzo della rete per processo 1077

Impostazioni del monitor Velocità di trasferimento disco 1069

Impostazioni del monitor Velocità di trasferimento disco per processo 1076

Impostazioni dell'elenco degli elementi consentiti 881

Impostazioni di accesso 381

Impostazioni di Active Protection in Cyber Backup Standard 857

Impostazioni di gestione delle patch nel piano di protezione 985

Impostazioni di Mappa di protezione dati 313

Impostazioni di privacy 21

Impostazioni di protezione 186

Impostazioni di Protezione antivirus e anti-malware 840

Impostazioni di rete 739

Impostazioni di sicurezza IPsec/IKE 775

Impostazioni di Universal Restore 517

Impostazioni di Valutazione delle vulnerabilità 977

© Acronis International GmbH, 2003-2024

Impostazioni Filtro URL 867

In 611

In che modo la creazione di Secure Zone trasforma il disco 423

In cosa consiste esattamente un problema? 922

In Cyber Protection 654

In Google Workspace 654

In Microsoft 365 611

Indagare su singoli nodi nella sequenza di attacco 936

Indagare sulle fasi di attacco di un problema 932

Indici di ricerca 678

Individuazione automatica dei sistemi 127

Individuazione dei processi di mining delle criptovalute 845

Informazioni che consentono l'identificazione personale dell'utente (PII) 902

Informazioni fondamentali 600

Informazioni per gli amministratori di Partner 341

Informazioni sanitarie protette (PHI) 901

Informazioni su Cyber Disaster Recovery Cloud 749

Informazioni su Secure Zone 422

Informazioni sul servizio di Consegna fisica dei dati 490

Informazioni sulla conversione 215

Informazioni sulla finalizzazione 697

Informazioni sulla pianificazione dei backup 655

Informazioni sulla scansione del backup 304

Infrastruttura di rete cloud 758

Installare agenti e componenti (combinazione di MSI e MST) 97

Installare e disinstallare agenti e componenti (EXE) 88

Installare e disinstallare agenti e componenti (MSI e selezione diretta) 98

Installazione 80

Installazione degli agenti di protezione 76

Installazione degli agenti di protezione in Linux 80

Installazione degli agenti di protezione in macOS 82

Installazione degli agenti di protezione in Windows 77

Installazione dell'Agente per Synology 164

Installazione delle patch su richiesta 997

Installazione di pacchetti dal repository 70

Installazione e deployment di agenti Cyber Protection 59

Installazione e disinstallazione automatica con un file EXE 88

Installazione e disinstallazione automatica con un file MSI 96

Installazione e disinstallazione automatica in macOS 112

Installazione e disinstallazione dinamica di componenti 87

Installazione manuale dei pacchetti 71

Installazione o disinstallazione automatica 88

Installazione o disinstallazione automatica in Linux 106

Installazione o disinstallazione automatica in Windows 88

Integrazioni per DirectAdmin, cPanel e Plesk 692

© Acronis International GmbH, 2003-2024

Interazione con altre opzioni di backup 494

Introduzione a Cyber Protection 19

Inventario hardware 1003

Inventario software 999

Istantanea di backup a livello di file 470

L

L'utente è inattivo 435

La console di Cyber Protect 325

La scheda Archivio di backup 536

Lavorare con i registri 790

Lavorare con il modulo Controllo dispositivo 371

Lavorare con le funzionalità di protezione avanzata 884

Lavorare con workload aggregati 401

Lavorare con workload CyberApp 400

Lavorare in VMware vSphere 697

Limitare il numero totale di macchine virtuali di cui viene eseguito il backup simultaneo 718

Limitazioni 34, 36-38, 40-41, 149, 157, 164, 216, 239, 296, 409-410, 413, 416, 423, 506, 521, 530, 612, 633, 638, 642, 655, 663, 666-667, 671-672, 682, 689, 699, 705, 746, 751, 883, 1110

Limitazioni durante l'utilizzo di Geo-redundant Cloud Storage 753

Limitazioni e problemi noti 652

Limitazioni per i nomi del file di backup 459

Limiti al ripristino di file nella console di Cyber Protect 525

Lingue supportate 901-902, 905

Linux 411

list backups 476

list content 476

Lista dei dispositivi USB in un computer 392

Lista di dispositivi USB consentiti 387

Lista di tipi di dispositivo consentiti 386

Livello del tenant cliente 327

Livello del tenant partner (Tutti i clienti) 327

Livello del tenant partner nella console di Cyber Protect 328

Livello di compressione 466

M

Mac 411

Macchine individuate 291

Mappa dell'organizzazione 911

Mappa di protezione dati 300, 312

McAfee Endpoint Encryption e PGP Whole Disk Encryption 43

Meccanismo di assegnazione del Punteggio #CyberFit 233

Metodi di convalida 208

Microsoft 35

Microsoft Azure 42

Microsoft BitLocker Drive Encryption 43

Microsoft Defender Antivirus 874

Microsoft Defender Antivirus e Microsoft Security Essentials 874

Microsoft Exchange Server 465

Microsoft Security Essentials 874

Microsoft SQL Server 464

Migrazione della macchina 719

Migrazione tramite un supporto di avvio 723

© Acronis International GmbH, 2003-2024

Modalità backup cluster 464

Modalità Conformità 1110

Modalità dell'archivio immutabile 1112

Modalità di avvio 529

Modalità di utilizzo di Secure Zone 42

Modalità solo cloud 760, 781

Modifica dei parametri predefiniti del server di ripristino 757

Modifica del formato di backup alla versione 12 (TIBX) 463

Modifica del timeout per l'heartbeat della VM e convalida degli screenshot 210

Modifica dell'account di accesso su sistemi Windows 85

Modifica della password di crittografia 1111

Modifica della quota di servizio dei sistemi 189

Modifica della registrazione di un workload 126

Modifica delle credenziali di accesso di Microsoft 365 615

Modifica delle porte utilizzate dall'agente di protezione 61

Modifica dello stato dello script 250

Modifica di un gruppo dinamico 368

Modifica di un piano di protezione 222

Modifica di un piano di protezione predefinito 232

Modifica o eliminazione di uno script 249

Modifica SID 535

Modificare le credenziali di accesso a SQL Server o al server di Exchange 599

Monitor configurabili 1054

Monitoraggio 265

Monitoraggio avvisi 1098

Monitoraggio basato sulle anomalie 1054

Monitoraggio dei workload tramite la trasmissione di screenshot 1042

Monitoraggio dell'integrità e delle prestazioni dei workload 1053

Monitoraggio integrità del disco 296

Montaggio di database di Exchange Server 592

Montaggio di volumi da un backup 538

Motore comportamentale 846

MTTR dei problemi di sicurezza 293

N

Navigazione nell'inventario hardware 1005

Navigazione nell'inventario software 1000

NEAR 1015

Nome file di backup 457

Nome file di backup predefinito 459

Nomi senza variabili 460

Non avviare se è attiva la connessione alle reti Wi-Fi seguenti 439

Non avviare se è attiva una connessione a consumo 438

Non ci sono backup completati per un numero specifico di giorni consecutivi 456

Non visualizzare i messaggi e le finestre di dialogo durante l'elaborazione (modalità nascosta) 467, 531

Note per gli utenti di Mac 505

Notifiche e avvisi di servizio del sistema operativo 385

Notifier del desktop remoto 1051

Novità della console di Cyber Protect 326

© Acronis International GmbH, 2003-2024

Nuova configurazione dell'indirizzo IP 782

Nutanix 40

O

Oggetto di livello superiore 732

Oggetto variabile 732

One-click Recovery 482

Open VPN site-to-site - Informazioni aggiuntive 192

Operare con backup crittografati 818

Operare con workload gestiti 1035

Operare con workload non gestiti 1044

Operatori di ricerca 366

Operazioni con backup 536

Operazioni con i runbook 832

Operazioni con un server primario 822

Operazioni con virtual machine di Microsoft Azure 819

Operazioni locali con un supporto di avvio 741

Operazioni remoto con un supporto di avvio 743

Operazioni speciali con le macchine virtuali 693

Operazioni supportate con i volumi logici 57

Opzione di archiviazione avanzata 421

Opzioni aggiuntive 429

Opzioni di backup 453

Opzioni di backup predefinite 453

Opzioni di failback 703

Opzioni di replica 702

Opzioni di ripristino 528

Oracle 39

Orchestrazione (runbook) 828

Origini dati supportate 418

Osservazione di più workload gestiti simultaneamente 1043

oVirt/Red Hat Virtualization 4.2 e 4.3/Oracle Virtualization Manager 4.3 162

oVirt/Red Hat Virtualization 4.4, 4.5 162

P

Pacchetti di Linux 69

Pagina di gestione del database dei dispositivi USB 389

Pannello di controllo Panoramica 265

Panoramica dei cluster di Exchange Server 575

Panoramica del piano di protezione 406

Panoramica del ripristino 503

Panoramica del servizio di Consegna fisica dei dati 490

Panoramica delle soluzioni a disponibilità elevata di SQL Server 573

Parallels 39

Parametri 728

Parametri aggiuntivi 110

Parametri del kernel 728

Parametri del runbook 831

Parametri di base 108

Parametri di disinstallazione 111

Parametri di installazione 108

Parametri di registrazione 109

Parametri evento 433

Parametri informativi 110

Parametri per funzionalità già esistenti 111

© Acronis International GmbH, 2003-2024

Parametri per l'installazione automatica (EXE) 90

Parametri per l'installazione automatica (MSI) 100

Parametri per l'installazione o la disinstallazione automatica 107

Passaggi successivi 756

Passaggio 1 59

Passaggio 2 59

Passaggio 3 59

Passaggio 4 59

Passaggio 5 60

Passaggio 6 61

Passaggio al tipo di connessione da sito a sito 785

Password con caratteri speciali o spazi 126

Per avviare il backup dei dati 602

Per quali workload, agenti e posizioni di backup vengono visualizzati i colli di bottiglia? 547

Per ripristinare i dati in un dispositivo mobile 602

Per scaricare l'app Cyber Protect 601

Perché è necessario eseguire il backup di un sito Web? 689

Perché Endpoint Detection and Response (EDR) è una soluzione necessaria 915

Perché eseguire il backup dei dati di Microsoft 365? 608

Perché sono presenti backup mensili con uno schema orario? 445

Perché utilizzare Generatore di supporti riavviabili? 726

Perché utilizzare i runbook? 828

Perché utilizzare il backup compatibile con l'applicazione? 577

Perché utilizzare Secure Zone? 422

Piani ai diversi livelli di amministrazione 259

Piani di backup per applicazioni cloud 200

Piani di gestione remota 1019

Piani di monitoraggio 1053, 1088

Piani di protezione 200

Piani di protezione individuali per le integrazioni con pannelli di controllo per l'hosting 232

Piani di protezione predefiniti 225

Piani di scansione del backup 200

Piani di scripting 253

Piani e moduli di protezione 217

Piani supportati per gruppi di dispositivi 347

Pianifica scansione 849, 874

Pianificazione 256, 313, 978, 987

Pianificazione del backup 425

Pianificazione e condizioni di avvio 256

Pianificazione oraria 429

Pianificazione per eventi 431

Piattaforme di virtualizzazione supportate 32, 750

Piattaforme supportate 239, 835, 1014

Piattaforme supportate per il monitoraggio 1054

Porte 770

Porte necessarie per il componente Downloader 61

Porte richieste 162

Porte TCP necessarie per il backup e la replica di macchine virtuali VMware 60

© Acronis International GmbH, 2003-2024

Posizione della cartella Quarantena nei sistemi 879

Posizioni supportate 204-205, 212, 448

Possibili utilizzi di una copia 698

Preconfigurazione di più connessioni di rete 740

Preparazione 59, 80, 517

WinPE 2.x e 3.x 738

WinPE 4.0 e versioni successive 738

Preparazione delle unità 517

Preparazione di un sistema per l'installazione remota 133

Prerequisiti 127, 165, 167, 169, 171, 178-179, 239, 250, 327, 331, 400-402, 416, 484, 525, 569, 683, 694, 711, 773, 778, 784, 787, 795-796, 810, 814, 819, 997, 1000, 1002, 1005, 1008, 1019, 1027-1030, 1036, 1039-1040, 1042-1046, 1088, 1090-1091, 1094-1096, 1107

Prestazioni 533, 703

Prestazioni e finestra di backup 486

Prevenzione degli exploit 846

Prima di iniziare 138, 142, 148, 156, 163

Priorità CPU 488

Privilegi necessari per l'Agente per VMware 714

Privilegi richiesti per l'account di accesso 86

Problema con le licenze 225

Problemi di compatibilità con i piani di gestione remota 1031

Problemi di compatibilità con i piani monitoraggio 1096

Problemi di compatibilità con piani di scripting 260

Problemi noti 683

Problemi noti e limitazioni 914

Procedura di Universal Restore 518

Procedure di ripristino specifiche per il software 43

Processo di backup con dati forensi 471

Prodotti Apple e prodotti di terze parti supportati 976

Prodotti Apple supportati 976

Prodotti di terze parti per Windows 986

Prodotti di terze parti supportati per i sistemi operativi Windows 976

Prodotti di terze parti supportati per macOS 977

Prodotti Linux supportati 977

Prodotti Microsoft 985

Prodotti Microsoft e prodotti di terze parti supportati 975

Prodotti Microsoft supportati 975

Programmazione 496

Protezione antivirus e anti-malware 839

Protezione continua dei dati (CDP) 416

Protezione dei dati di Exchange Online 622

Protezione dei dati di Gmail 662

Protezione dei dati di Google Workspace 654

Protezione dei dati di Microsoft 365 608

Protezione dei dati di MySQL e MariaDB 682

Protezione dei dati per Exchange ospitato 604

Protezione dei dispositivi mobili 600

Protezione dei gruppi di disponibilità Always On (AAG) 573

Protezione dei gruppi di disponibilità del database (DAG) 575

Protezione delle applicazioni Microsoft 567

© Acronis International GmbH, 2003-2024

Protezione delle cartelle di rete 842

Protezione delle caselle di posta di Exchange Online 616

Protezione delle utenze delle app di collaborazione di Microsoft 365 653

Protezione di applicazioni di collaborazione e comunicazione 263

Protezione di file di Google Drive 666

Protezione di file di OneDrive 633

Protezione di file di unità condivise 671

Protezione di Microsoft 365 Teams 642

Protezione di Microsoft SharePoint 567

Protezione di Microsoft SQL Server e Microsoft Exchange Server 567

Protezione di notebook OneNote 652

Protezione di SAP HANA 681

Protezione di server di hosting su Web 692

Protezione di siti di SharePoint Online 638

Protezione di siti Web 689

Protezione di siti Web e di server di hosting 689

Protezione di un controller di dominio 568

Protezione in tempo reale 839, 848, 875

Protezione intelligente 309

Protezione lato server 843

Protezione per Oracle Database 681

Protocolli di connessione remota 1015

Prova di una copia 700

Prova failover 800

Provisioning disco 702

Pulizia 212

Punti di calcolo 753

Punti di montaggio 480, 532

Q

Qual è la differenza tra un supporto di avvio basato su Linux o uno basato su WinPE? 725

Qual è la differenza tra un supporto di avvio personalizzato e uno pronto all'uso? 724

Quale tipo di backup scegliere? 66

Quali elementi è possibile ripristinare? 604, 616, 622, 633, 638, 642, 662, 667, 671

Quali elementi non è possibile ripristinare? 639

Quali informazioni sono incluse in una fase di attacco? 934

Quali informazioni vengono memorizzate dal backup di un disco o un volume? 410

Quanti agenti sono necessari per il backup e ripristino dei dati compatibile con i cluster? 576

Quanti agenti sono necessari per il backup e ripristino dei dati del cluster? 574

Quanti agenti sono necessari? 139, 143, 148, 157

Quarantena 845, 878

Quote 692

R

Raccolta dei dati di replica iniziali 703

Raccomandazioni 530

Raccomandazioni generiche per i siti locali 774

Raccomandazioni per la disponibilità dei Servizi di dominio Active Directory 777

RDP 1016

Recentemente interessato 305

Recupero delle routine archiviate 688

© Acronis International GmbH, 2003-2024

Red Hat e Linux 38

Registrare il supporto di avvio 739

Registrazione e annullamento della registrazione di workload in modalità manuale 122

Registrazione e riproduzione di sessioni remote 1049

Registro eventi di Windows 503, 536

Regole dei criteri per dischi e volumi 411

Regole dei criteri per file e cartelle 414

Regole del firewall per i server cloud 823

Regole di backup comuni 43

Regole di conservazione 443

Regole di conservazione in base allo schema di backup 444

Regole di estensione ed eccezione 315

Regole di installazione comuni 42

Reimpostazione dei modelli di machine learning 1098

Reindirizzamento audio remoto 1017

Reindirizzamento dell'audio da un workload Linux remoto 1017

Reindirizzamento dell'audio da un workload macOS remoto 1017

Reindirizzamento dell'audio da un workload Windows remoto 1017

Reinstallazione del gateway VPN 783

Replica 447

Replica di backup 202

Replica di macchine virtuali 698

Report 319

Report sul licensing delle utenze di Microsoft 365 613

Repository di script 252

Requisiti 525, 538

Requisiti aggiuntivi per i backup compatibili con l'applicazione 570

Requisiti aggiuntivi per i sistemi che eseguono Windows 579

Requisiti aggiuntivi per le macchine virtuali 579

Requisiti comuni 569

Requisiti di accesso necessari per il backup su cloud storage pubblico 556

Requisiti di rete per Agente per Virtuozzo Hybrid Infrastructure (appliance virtuale) 149

Requisiti di sistema 770

Requisiti di sistema per agenti 66

Requisiti di sistema per l'agente 138, 143, 148, 156

Requisiti per Controllo account utente (UAC) 134

Requisiti per l'utilizzo di backup compatibili con le applicazioni 577

Requisiti per l'appliance VPN 770

Requisiti per la password 19

Requisiti per le macchine virtuali ESXi 570

Requisiti per le macchine virtuali Hyper-V 570

Requisiti software 23, 750, 918

Requisiti sugli account utente 593

Revisione e gestione delle policy 893

Revoca di piani di monitoraggio 1091

Revoca di un piano di protezione 223

Revocare un piano da un gruppo 370

Riassegnazione di indirizzi IP 786

Riavvia un workload 957

© Acronis International GmbH, 2003-2024

Ricerca automatica dei driver 517

Ricerca nei backup cloud-to-cloud 676

Ricerca testo completo 677

Ricezione di notifiche di avviso in caso di violazione 916

Ridistribuzione 709

Rientra nell'intervallo di tempo 437

Riepilogo di installazione patch 303

Rigenera file di configurazione 789

Rilevamento automatico della destinazione 900

Rilevamento per tattica 294

Rimozione dell'accesso a un abbonamento Microsoft Azure 562

Rimozione dell'accesso a una connessione al cloud pubblico 566

Rimozione di workload da un piano di gestione remota 1028

Rinnovare la policy per un'azienda o un'unità 894

Rinnovare la policy per uno o più utenti dell'azienda o dell'unità 894

Rinnovo dell'accesso a un abbonamento Microsoft Azure 561

Rinnovo dell'accesso a una connessione al cloud pubblico 565

Rinnovo della policy di flusso dei dati 894

Ripristino 57, 503

Ripristino con riavvio 507

Ripristino con supporto di avvio in locale 742

Ripristino da backup 960

Ripristino da una condivisione di rete 730

Ripristino dall'archiviazione cloud 730

Ripristino dei backup per i tenant in modalità Conformità 1112

Ripristino dei canali dei team o di file nei canali dei team 645

Ripristino dei database compresi in un AAG 574

Ripristino dei database di Exchange 590

Ripristino dei dati da un backup application-aware 684

Ripristino dei dati del cluster di Exchange 576

Ripristino del database master 589

Ripristino del disco RAM originale iniziale 519

Ripristino dell'intero server 685

Ripristino della casella di posta del team 647

Ripristino della configurazione ESXi 527

Ripristino delle applicazioni 568

Ripristino delle caselle postali 594, 605, 617, 624, 664

Ripristino dello stato del sistema 526

Ripristino di cartelle pubbliche e di elementi della cartella 631

Ripristino di caselle di posta di Exchange e relativi elementi 592

Ripristino di caselle postali e di elementi delle caselle postali 605, 617, 624, 664

Ripristino di database 686

Ripristino di database di sistema 588

Ripristino di database SQL 581

Ripristino di database SQL come file 586

Ripristino di database SQL in un sistema diverso dall'originale 584

Ripristino di database SQL nel sistema originale 582

Ripristino di dati di SharePoint Online 640

© Acronis International GmbH, 2003-2024

Ripristino di dischi mediante i supporti di avvio 514

Ripristino di elementi della casella di posta del team su file PST 648

Ripristino di elementi di casella di posta 596, 606, 617, 626, 665

Ripristino di elementi di caselle di posta in file PST 629

Ripristino di file 519

Ripristino di file di Google Drive 669

Ripristino di file di OneDrive 636

Ripristino di file di unità condivise 674

Ripristino di file mediante i supporti di avvio 524

Ripristino di file nella console di Cyber Protect 519

Ripristino di Google Drive e di file di Google Drive 668

Ripristino di intere caselle di posta in file di dati PST 628

Ripristino di istanze 685

Ripristino di messaggi e-mail e riunioni 650

Ripristino di notebook OneNote oggetto di backup 652

Ripristino di OneDrive e di file di OneDrive 635

Ripristino di sistemi fisici 507

Ripristino di tabelle 687

Ripristino di un intero Google Drive 668

Ripristino di un intero OneDrive 635

Ripristino di un sito del team o di elementi specifici di un sito 651

Ripristino di un sito Web 691

Ripristino di un team completo 644

Ripristino di un'intera unità condivisa 673

Ripristino di una macchina 507

Ripristino di una macchina con One-click Recovery 484

Ripristino di una macchina virtuale 512

Ripristino di unità condivise e di file di unità condivise 673

Ripristino in container o virtual machine Virtuozzo 526

Ripristino percorso completo 532

Ripristino sicuro 506

Ripristino tra piattaforme 505

Riprova se si verifica un errore 466, 531

Riprova se si verifica un errore durante la creazione dello snapshot MV 467

Risoluzione dei conflitti tra piani 224

Risoluzione dei problemi 137

Risoluzione dei problemi di compatibilità con i piani di gestione remota 1031

Risoluzione dei problemi di compatibilità con i piani monitoraggio 1097

Risoluzione dei problemi di compatibilità con piani di scripting 261

Risparmia carica della batteria 438

Rivedere e analizzare gli indicatori di compromissione individuati 943

Rivedere e mitigare gli indicatori di compromissione sui workload interessati 942

Ruoli richiesti 162

Ruoli utente e diritti di Cyber Scripting 240

S

Salva le informazioni di sistema se il ripristino con riavvio non riesce 531

© Acronis International GmbH, 2003-2024

Salvataggio di un file del registro agente 191
Scale Computing 37
Scansione anti-malware dei backup 882
Scansione pianificata 840
Scarica configurazione per OpenVPN 789
Scaricare i registri del gateway VPN 791
Scaricare i registri dell'appliance VPN 791
Scaricare l'output di un'operazione di scripting 252
Scenari di utilizzo 539
Scheda Attività 316, 329
Scheda Avvisi 328
Scheda Dispositivi 329
Scheda Gestione 199
Scheda Gestione software 329
Schemi di backup 425
Script 242
Script nel supporto di avvio 730
Script personalizzati 731
Script predefiniti 730
Se si sceglie di creare la macchina virtuale su un server di virtualizzazione 217
Se si sceglie di salvare la macchina virtuale come set di file 217
Selezionare il provider di snapshot 500
Selezione dei componenti per l'installazione 135
Selezione dei dati del backup 409
Selezione dei team 643
Selezione della configurazione ESXi 415
Selezione delle caselle di posta 623
Selezione delle caselle di posta di Exchange Online 605
Selezione delle caselle di posta di Exchange Server 580
Selezione delle caselle di posta di Gmail 663
Selezione delle caselle di posta di Microsoft 365 616
Selezione dello stato di sistema 415
Selezione di cartelle pubbliche 624
Selezione di database SQL 571
Selezione di dati di Exchange Server 572
Selezione di dati di SharePoint Online 639
Selezione di dischi o volumi 409
Selezione di file di Google Drive 667
Selezione di file di OneDrive 634
Selezione di file di unità condivise 672
Selezione di file e cartelle 412
Selezione di un intero sistema 409
Selezione di un livello tenant 327
Selezione di una destinazione 420
Server di ripristino 764
Server primari 766
Servizi di Cyber Protection installati nell'ambiente 190
Servizi installati in macOS 191
Servizi installati in Windows 191
Servizio Copia Shadow del volume (VSS) 499
Servizio Copia Shadow del volume per macchine virtuali 501, 703
Sicurezza 1016
Sicurezza a livello di file 532
Sistemi operativi e ambienti supportati 23

© Acronis International GmbH, 2003-2024

Sistemi operativi e versioni supportati 45

Sistemi operativi supportati 750

Sistemi operativi Windows supportati 877

Sistemi vulnerabili 301

Snapshot intermedi 217

Snapshot multivolume 481

Soluzione dei problemi della configurazione VPN IPsec 792

Soluzione dei problemi di configurazione di VPN IPsec 793

Spegni le macchine virtuali di destinazione quando viene avviato il ripristino 535

Startup Recovery Manager 746

Stati del piano 199

Stato della geo-replica 1116

Stato della rete dei workload 295

Stato di convalida 206

Stato di installazione patch 303

Stato minaccia 292

Stato protezione 290

Storage con geo-ridondanza 1115

Strumenti Cyber Protection aggiuntivi 1110

Strumento "tibxread" per l'acquisizione dei dati di cui è stato eseguito il backup 474

Struttura della policy di flusso dei dati 888

Struttura della regola 889

Struttura di autostart.json 732

Suddivisione 497

Suggerimenti importanti 443

Suggerimenti utili 619, 656

Supporto di avvio basato su Linux 727

Supporto di avvio basato su WinPE e WinRE 735

Supporto per ambienti multitenant 334

Supporto per la migrazione di virtual machine 711

T

Tenant in modalità Conformità 525

Tipi di avviso 268

Tipi di backup 427

Tipi di macchina virtuale supportati 215

Tipi di monitoraggio 1053

Tipi di scansione 839

Tipo di Controllo 733

Trasferimento audio 1016

Trasferimento di file 1039

Trasferimento di file tramite Acronis Quick Assist 1046

Troncamento registro 479

Trovare l'ultimo utente connesso 403

U

Ulteriori operazioni con i piani di gestione remota esistenti 1028

Ulteriori operazioni con i piani monitoraggio 1094

Ulteriori opzioni di pianificazione 441

Universal Restore in Linux 518

Universal Restore in Windows 517

Utenti disconnessi 436

Utilizzo del modulo Controllo dispositivo 374

Utilizzo dell'Agente cloud per Microsoft 365 618

© Acronis International GmbH, 2003-2024

Utilizzo dell’Agente installato in locale per Office 365 613

Utilizzo della barra degli strumenti nella finestra del visualizzatore 1047

Utilizzo della console di Cyber Protect come amministratore di partner 327

Utilizzo della modalità di Applicazione adattiva per il rinnovo di una policy utente 895

Utilizzo della modalità di osservazione per il rinnovo di una policy utente 895

Utilizzo delle variabili 460

Utilizzo di un archivio collegato localmente 707

Utilizzo di Universal Restore 516

V

Valori del campo Azione 396

Valutazione della vulnerabilità per dispositivi macOS 981

Valutazione delle vulnerabilità 974

Valutazione delle vulnerabilità e gestione delle patch 974

Valutazione delle vulnerabilità per sistemi Linux 980

Valutazione delle vulnerabilità per sistemi Windows 980

Variabili del monitoraggio avvisi 1100

Velocità di output durante il backup 489

Verifica checksum 209

Verifica degli attacchi resi pubblici ai workload utilizzando i feed sulle minacce 917

Verifica dell'autenticità dei file con Notary Service 522, 676

Verifica della dimensione di un indice di ricerca 678

Verificare l'accesso ai driver nell'ambiente di avvio 517

Versione in trial di Cyber Disaster Recovery Cloud 752

Versioni dello script 249

Versioni di MariaDB supportate 32

Versioni di Microsoft SharePoint supportate 31

Versioni di MySQL supportate 32

Versioni di Oracle Database supportate 31

Versioni di SAP HANA supportate 31

Versioni supportate 652

Versioni supportate di Microsoft Exchange Server 30

Versioni supportate di Microsoft SQL Server 30

Virtuozzo 40

Virtuozzo Hybrid Infrastructure 41

Visualizzare gli avvisi di Controllo dispositivo 380

Visualizzare informazioni sugli elementi dell'elenco degli elementi consentiti 881

Visualizzare o modificare le impostazioni di accesso 376

Visualizzazione degli avvisi di monitoraggio di un workload 1105

Visualizzazione dei dati di monitoraggio 1107

Visualizzazione dei dettagli sui colli di bottiglia 546

Visualizzazione dei problemi attualmente non risolti 924

Visualizzazione dei risultati della distribuzione 709

Visualizzazione del registro degli avvisi di monitoraggio 1106

Visualizzazione dell'elenco delle patch

© Acronis International GmbH, 2003-2024

disponibili 990

Visualizzazione dell'hardware di un singolo dispositivo 1008

Visualizzazione dell'inventario software di un singolo dispositivo 1002

Visualizzazione della cronologia dell’esecuzione 833

Visualizzazione dello stato del backup stato nel client vSphere 713

Visualizzazione dello stato del failover di prova automatizzato 804

Visualizzazione di workload di clienti specifici 329

Visualizzazione di workload gestiti dalle integrazioni RMM 399

Visualizzazione e aggiornamento delle posizioni di backup nel cloud pubblico 555

Visualizzazione intuitiva della sequenza di attacco 917

VMware 32

Vulnerabilità esistenti 302

W

Widget dei monitor 1108

Widget di Advanced Data Loss Prevention nella dashboard Panoramica 908

Widget di avviso 289

Widget di Endpoint Detection and Response (EDR) 291

Widget di installazione patch 303

Widget di integrità del disco 297

Widget di valutazione delle vulnerabilità 301

Widget Inventario hardware 307

Widget Inventario software 306

Widget sessioni remote 308

Windows 410

Workload 335

Workload aggregati 400

Workload CyberApp 400

© Acronis International GmbH, 2003-2024