Acronis

acronis.com

Cyber Protection

24.03

Panduan Pengguna

REVISI: 10/04/2024

Daftar isi

Memulai dengan Cyber Protection **19**
Mengaktifkan akun 19
Persyaratan kata sandi 19
Autentikasi dua faktor 19
Pengaturan privasi 21
Mengakses layanan Cyber Protection 22
Persyaratan perangkat lunak 23
Browser web yang didukung 23
Sistem operasi dan lingkungan yang Didukung 23
Versi Microsoft SQL Server yang didukung 30
Versi Microsoft Exchange Server yang didukung 30
Versi Microsoft SharePoint yang didukung 31
Versi Database Oracle yang didukung 31
Versi SAP HANA yang didukung 31
Versi MySQL yang didukung 31
Versi MariaDB yang didukung 32
Platform virtualisasi yang didukung 32
Kompatibilitas dengan perangkat lunak enkripsi 42
Kompatibilitas dengan penyimpanan Dell EMC Data Domain 43
Fitur perlindungan yang didukung oleh sistem operasi 44
Sistem operasi dan versi yang didukung 44
Sistem file yang didukung 53
Operasi yang didukung dengan volume logis 56
Cadangan 56
Pemulihan 57
Menginstal dan menyebarkan agen Cyber Protection **58**
Persiapan 58
Langkah 1 58
Langkah 2 58
Langkah 3 58
Langkah 4 58
Langkah 5 59
Langkah 6 60
Agen mana yang saya perlukan? 61
Pencadangan berbasis agen dan tanpa agen 65

© Acronis International GmbH, 2003-2024

Jenis cadangan apa yang saya perlukan? 65
Persyaratan sistem untuk agen 65
Paket Linux 68
Apakah paket yang diperlukan sudah diinstal? 68
Menginstal paket dari repositori 69
Menginstal paket secara manual 70
Mengonfigurasi pengaturan server proxy 71
Menginstal agen proteksi 75
Mengunduh agen proteksi 75
Menginstal agen proteksi di Windows 76
Menginstal agen proteksi di Linux 78
Menginstal agen proteksi di macOS 81
Memberikan izin sistem yang diperlukan kepada Connect Agent 82
Mengubah akun masuk pada mesin Windows 84
Instalasi dinamis dan penghapusan instalasi komponen 85
Instalasi atau penghapusan instalasi tanpa pengawasan 86
Instalasi atau penghapusan instalasi tanpa pengawasan di Windows 86
Contoh 87
Contoh 88
Contoh 89
Contoh 97
Contoh 98
Contoh 98
Instalasi atau penghapusan tanpa pengawasan di Linux 104
Instalasi dan penghapusan instalasi tanpa pengawasan di macOS 110
Mendaftarkan dan membatalkan pendaftaran beban kerja secara manual 119
Kata sandi dengan karakter spesial atau spasi kosong 122
Mengubah registrasi beban kerja 123
Penemuan manual mesin 124
Prasyarat 124
Cara kerja autodiscovery 124
Cara kerja instalasi jarak jauh agen 126
Melakukan autodiscovery dan manual discovery 127
Mengelola mesin yang ditemukan 132
Penyelesaian masalah 133
Menyebarkan Agen untuk VMware (Virtual Appliance) 135
Sebelum Anda memulai 135

© Acronis International GmbH, 2003-2024

Menyebarkan templat OVF 136
Mengonfigurasi alat virtual 136
Menyebarkan Agen untuk Scale Computing HC3 (Alat Virtual) 139
Sebelum Anda memulai 139
Menyebarkan templat QCOW2 140
Mengonfigurasi alat virtual 141
Agen untuk Scale Computing HC3 – peran yang diperlukan 143
Menyebarkan Agen untuk Virtuozzo Hybrid Infrastructure (Alat Virtual) 144
Sebelum Anda memulai 144
Mengonfigurasi jaringan di Virtuozzo Hybrid Infrastructure 145
Mengonfigurasi akun pengguna di Virtuozzo Hybrid Infrastructure 146
Menyebarkan templat QCOW2 148
Mengonfigurasi alat virtual 149
Menyebarkan Agen untuk oVirt (Alat Virtual) 152
Sebelum Anda memulai 152
Menyebarkan templat OVA 153
Mengonfigurasi alat virtual 155
Agen untuk oVirt - peran dan port yang diperlukan 157
Menyebarkan Agen untuk Synology 158
Sebelum Anda memulai 158
Mengunduh program penyiapan 159
Menginstal Agen untuk Synology 160
Memperbarui Agen untuk Synology 164
Menyebarkan agen melalui Kebijakan Grup 167
Prasyarat 167
Membuat token pendaftaran 167
Membuat file transformasi dan mengekstrak paket instalasi 170
Menyiapkan objek Kebijakan Grup 171
Koneksi SSH ke alat virtual 172
Memulai Secure Shell daemon 172
Mengatur kata sandi root pada alat virtual 172
Mengakses alat virtual melalui klien SSH 173
Memperbarui agen 173
Memperbarui agen secara manual 174
Memperbarui agen secara otomatis 176
Memperbarui agen di beban kerja yang dilindungi BitLocker 178
Mencegah penghapusan instalasi atau modifikasi agen yang tidak sah 178

© Acronis International GmbH, 2003-2024

Menghapus instalasi agen ... 180
Pengaturan perlindungan ... 181
Pembaruan otomatis komponen ... 181
Memperbarui definisi Cyber Protection sesuai jadwal ... 183
Memperbarui definisi Cyber Protection sesuai permintaan ... 183
Penyimpanan cache ... 183
Mengubah kuota layanan mesin ... 184
Layanan Cyber Protection yang diinstal di lingkungan Anda ... 185
Layanan yang diinstal di Windows ... 185
Layanan yang diinstal di macOS ... 186
Menyimpan file log agen ... 186
VPN Terbuka Situs-ke-situs - Informasi tambahan ... 186
Manajemen lisensi untuk server manajemen di lokasi ... 194
Menentukan apa yang perlu dilindungi dan cara melindunginya ... 195
Tab manajemen ... 195
Status rencana ... 195
Rencana proteksi ... 196
Rencana pencadangan untuk aplikasi awan ... 196
Rencana pemindaian cadangan ... 196
Pemrosesan data off-host ... 197
VM heartbeat ... 205
Validasi tangkapan layar ... 205
Snapshot intermediet ... 213
Modul dan rencana proteksi ... 213
Membuat rencana proteksi ... 214
Tindakan dengan rencana proteksi ... 215
Menyelesaikan pertentangan rencana ... 220
Rencana proteksi default ... 221
Rencana proteksi individu untuk integrasi panel kontrol hosting ... 227
Skor #CyberFit untuk mesin ... 227
Cara kerjanya ... 228
Menjalankan pemindaian Skor #CyberFit ... 232
Pembuatan Skrip Cyber ... 234
Prasyarat ... 234
Pembatasan ... 234
Platform yang didukung ... 234
Peran pengguna dan hak Pembuatan Skrip Cyber ... 235

© Acronis International GmbH, 2003-2024

Skrip ... 237
Repositori skrip ... 247
Rencana skrip ... 247
Jalankan cepat skrip ... 256
Perlindungan aplikasi kolaborasi dan komunikasi ... 258
Memahami tingkat proteksi Anda saat ini ... 259
Pemantauan ... 259
Dasbor Ikhtisar ... 259
Dasbor Aktivitas ... 260
Dasbor Peringatan ... 261
Jenis peringatan ... 262
Widget peringatan ... 282
Perlindungan cyber ... 282
Status proteksi ... 283
Widget Deteksi dan Tanggapan Titik Akhir (EDR) ... 284
Skor #CyberFit berdasarkan mesin ... 288
Pemantauan kesehatan disk ... 289
Peta perlindungan data ... 293
Widget penilaian kerentanan ... 294
Widget instalasi patch ... 295
Detail pemindaian cadangan ... 297
Baru-baru ini terdampak ... 297
Aplikasi awan ... 298
Widget inventaris perangkat lunak ... 299
Widget inventaris perangkat keras ... 300
Widget sesi jarak jauh ... 301
Proteksi cerdas ... 301
Tab Aktivitas ... 309
Monitor Cyber Protect ... 310
Mengonfigurasi pengaturan server proxy di Cyber Protect Monitor ... 311
Laporan ... 311
Tindakan dengan laporan ... 313
Data yang dilaporkan berdasarkan tipe widget ... 315
Mengelola beban kerja di konsol Cyber Protect ... 318
Konsol Cyber Protect ... 318
Yang baru di konsol Cyber Protect ... 319
Menggunakan konsol Cyber Protect sebagai administrator mitra ... 320

© Acronis International GmbH, 2003-2024

Prasyarat ... 324
Beban kerja ... 328
Menambahkan beban kerja ke konsol Cyber Protect ... 329
Menghapus beban kerja dari konsol Cyber Protect ... 334
Grup perangkat ... 338
Grup bawaan dan grup khusus ... 338
Grup statis dan grup dinamis ... 339
Grup awan-ke-awan dan grup non-awan-ke-awan ... 340
Membuat grup statis ... 340
Menambahkan beban kerja ke grup statis ... 342
Membuat grup dinamis ... 342
Mengedit grup dinamis ... 360
Menghapus grup ... 360
Menerapkan rencana ke grup ... 361
Batalkan rencana dari grup ... 362
Bekerja dengan modul kontrol Perangkat ... 362
Menggunakan kontrol perangkat ... 365
Pengaturan akses ... 372
Daftar izin jenis perangkat ... 378
Daftar izin perangkat USB ... 379
Mengecualikan proses dari kontrol akses ... 384
Peringatan kontrol perangkat ... 386
Penghapusan aman data dari beban kerja yang terkelola ... 389
Beban kerja CyberApp ... 390
Beban kerja terakumulasi ... 391
Bekerja dengan beban kerja CyberApp ... 391
Bekerja dengan beban kerja yang terkumpul ... 392
Temukan pengguna yang terakhir masuk ... 393
Mengelola pencadangan serta pemulihan beban kerja dan file ... 395
Cadangan ... 395
Referensi cepat rencana proteksi ... 397
Memilih data yang akan dicadangkan ... 400
Memilih keseluruhan mesin ... 400
Memilih disk atau volume ... 401
Memilih file atau folder ... 404
Memilih status sistem ... 407
Memilih konfigurasi ESXi ... 407

© Acronis International GmbH, 2003-2024

Perlindungan data berkelanjutan (CDP) ... 408
Cara kerjanya ... 408
Sumber data yang didukung ... 410
Tujuan yang didukung ... 411
Mengonfigurasi cadangan CDP ... 411
Memilih tujuan ... 412
Opsi penyimpanan lanjutan ... 413
Tentang Secure Zone ... 414
Jadwal pencadangan ... 417
Skema cadangan ... 417
Jenis cadangan ... 419
Menjalankan pencadangan sesuai jadwal ... 420
Menjalankan pencadangan secara manual ... 433
Aturan retensi ... 434
Kiat penting ... 435
Aturan retensi sesuai dengan skema pencadangan ... 435
Mengonfigurasi aturan retensi ... 438
Replikasi ... 439
Contoh penggunaan ... 439
Lokasi yang didukung ... 440
Enkripsi ... 441
Mengonfigurasi enkripsi dalam rencana proteksi ... 441
Mengonfigurasi enkripsi sebagai properti mesin ... 442
Notarisasi ... 444
Cara menggunakan notarisasi ... 444
Cara kerjanya ... 444
Opsi cadangan default ... 445
Opsi cadangan ... 445
Ketersediaan opsi pencadangan ... 445
Peringatan ... 448
Konsolidasi cadangan ... 449
Nama file cadangan ... 450
Format cadangan ... 454
Validasi cadangan ... 456
Pelacakan perubahan blok (CBT) ... 456
Mode cadangan klaster ... 456
Tingkat kompresi ... 458

© Acronis International GmbH, 2003-2024

Penanganan eror ... 458
Cadangan inkremental/diferensial cepat ... 459
Filter file (Penyertaan/Pengecualian) ... 460
Snapshot pencadangan tingkat file ... 462
Data forensik ... 462
Pemotongan log ... 471
Membuat snapshot LVM ... 471
Titik mount ... 472
Snapshot multivolume ... 473
Pemulihan sekali klik ... 473
Pengaturan kinerja dan cadangan jendela ... 478
Pengiriman Data Fisik ... 482
Perintah pra/pasca ... 483
Perintah pengambilan data pra/pasca ... 485
Penjadwalan ... 488
Pencadangan sektor demi sektor ... 489
Pembagian ... 489
Penanganan kegagalan tugas ... 490
Syarat mulai tugas ... 490
Layanan Menyalin Bayangan Volume (VSS) ... 491
Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual ... 493
Pencadangan mingguan ... 494
Log event Windows ... 495
Pemulihan ... 495
Referensi cepat pemulihan ... 495
Pemulihan aman ... 497
Memulihkan mesin ... 498
Siapkan driver ... 508
Cek akses ke driver pada lingkungan yang dapat di-boot ... 508
Pencarian driver otomatis ... 508
Driver penyimpanan massal akan tetap diinstal ... 509
Memulihkan beberapa file ... 510
Memulihkan status sistem ... 517
Memulihkan konfigurasi ESXi ... 517
Opsi pemulihan ... 518
Operasi dengan pencadangan ... 526
Tab Penyimpanan cadangan ... 526

© Acronis International GmbH, 2003-2024

Mounting volume dari cadangan 528
Memvalidasi cadangan 530
Mengekspor cadangan 531
Menghapus beberapa cadangan 532
Memahami deteksi kemacetan 534
Mencadangkan beban kerja ke cloud publik 538
Menentukan lokasi cadangan di Microsoft Azure 538
Mendefinisikan lokasi cadangan di Amazon S3 541
Mendefinisikan lokasi cadangan di Wasabi 543
Melihat dan memperbarui lokasi cadangan cloud publik 545
Mengelola akses akun cloud publik 546
Melindungi aplikasi Microsoft 557
Melindungi Microsoft SQL Server dan Microsoft Exchange Server 557
Melindungi Microsoft SharePoint 557
Melindungi pengontrol domain 558
Memulihkan aplikasi 558
Prasyarat 559
Cadangan database 561
Cadangan keberadaan aplikasi 567
Pencadangan kotak surat 569
Memulihkan database SQL 571
Memulihkan database Exchange 579
Memulihkan kotak surat Exchange dan item kotak surat 581
Mengubah kredensial akses SQL Server atau Exchange Server 588
Melindungi perangkat seluler 588
Perangkat seluler yang didukung 589
Apa yang dapat Anda cadangkan 589
Apa yang perlu Anda ketahui 589
Tempat untuk mendapatkan aplikasi Cyber Protect 590
Cara memulai pencadangan data Anda 590
Cara memulihkan data ke perangkat seluler 590
Cara meninjau data melalui konsol Cyber Protect 591
Melindungi data Exchange yang Dihosting 592
Apa saja item yang dapat dicadangkan? 592
Apa saja item yang dapat dipulihkan? 592
Memilih kotak surat Exchange Online 593
Memulihkan kotak surat dan item kotak surat 593

© Acronis International GmbH, 2003-2024

Melindungi data Microsoft 365 596
Mengapa perlu mencadangkan data Microsoft 365? 596
Agen cloud dan agen lokal 596
Hak pengguna yang diperlukan 599
Pembatasan 600
Laporan pelisensian kursi Microsoft 365 600
Pencatatan 601
Menggunakan Agen untuk Office 365 yang diinstal secara lokal 601
Menggunakan versi awan Agen untuk Microsoft 365 605
Melindungi data Google Workspace 638
Apa definisi perlindungan Google Workspace? 638
Hak pengguna yang diperlukan 639
Tentang jadwal pencadangan 639
Pembatasan 640
Pencatatan 640
Menambahkan organisasi Google Workspace 640
Membuat proyek Google Cloud pribadi. 641
Menemukan sumber daya Google Workspace 645
Pengaturan frekuensi pencadangan Google Workspace 645
Melindungi data Gmail 646
Melindungi file Google Drive 650
Melindungi file drive Shared 654
Notarisasi 658
Pencarian dalam cadangan cloud ke cloud 659
Pencarian teks lengkap 660
Indeks pencarian 660
Memeriksa ukuran indeks pencarian 661
Memperbarui, membangun ulang, atau menghapus indeks 661
Mengaktifkan pencarian yang ditingkatkan dalam cadangan yang dienkripsi 662
Mengaktifkan atau menonaktifkan pencarian yang ditingkatkan dalam rencana yang ada 663
Menonaktifkan pencarian teks lengkap untuk cadangan Gmail 664
Melindungi Database Oracle 664
Perlindungan SAP HANA 664
Melindungi data MySQL dan MariaDB 665
Mengonfigurasi cadangan keberadaan aplikasi 666
Memulihkan data dari cadangan keberadaan aplikasi 667
Melindungi situs web dan server hosting 671

© Acronis International GmbH, 2003-2024

Melindungi situs web ... 671
Melindungi server hosting web ... 675
Operasi khusus dengan mesin virtual ... 676
Menjalankan mesin virtual dari cadangan (Pemulihan Instan) ... 676
Bekerja di VMware vSphere ... 680
Mencadangkan mesin Hyper-V klaster ... 699
Membatasi jumlah total mesin virtual yang dicadangkan secara simultan ... 699
Migrasi mesin ... 701
Mesin virtual Microsoft Azure and Amazon EC2 ... 705
Membuat media yang dapat di-boot untuk memulihkan sistem operasi ... 705
Media yang dapat di-boot kustom atau siap pakai? ... 705
Media yang dapat di-boot berbasis Linux atau WinPE/WinRE? ... 706
Membuat media fisik yang dapat di-boot ... 706
Pembangun Media Yang Dapat Di-Boot ... 707
Pemulihan dari penyimpanan awan ... 711
Pemulihan dari berbagi jaringan ... 712
File skrip ... 712
Struktur autostart.json ... 713
Objek level atas ... 713
Objek variabel ... 713
Jenis kontrol ... 715
Menghubungkan ke mesin yang di-boot dari media yang dapat di-boot ... 722
Operasi lokal dengan media yang dapat di-boot ... 723
Operasi jarak jauh dengan media yang dapat di-boot ... 724
Startup Recovery Manager ... 727
Menerapkan pemulihan bencana ... 730
Tentang Cyber Disaster Recovery Cloud ... 730
Fungsi utama ... 730
Persyaratan perangkat lunak ... 731
Sistem Operasi yang Didukung ... 731
Platform virtualisasi yang didukung ... 731
Pembatasan ... 732
Versi percobaan Cyber Disaster Recovery Cloud ... 733
Keterbatasan saat menggunakan Penyimpanan Cloud Geo-redundan ... 734
Kesesuaian Pemulihan Bencana dengan perangkat lunak enkripsi ... 734
Titik komputasi ... 734
Mengatur fungsi pemulihan bencana ... 736

© Acronis International GmbH, 2003-2024

Membuat rencana proteksi pemulihan bencana ... 736
Mengedit Parameter default server pemulihan ... 738
Infrastruktur jaringan awan ... 739
Mengatur konektivitas ... 740
Konsep pengaturan jaringan ... 740
Konfigurasi konektivitas awal ... 751
Prasyarat ... 754
Manajemen jaringan ... 760
Prasyarat ... 775
Mengatur server pemulihan ... 776
Membuat server pemulihan ... 776
Cara kerja failover ... 779
Cara kerja failback ... 787
Prasyarat ... 789
Prasyarat ... 794
Bekerja dengan cadangan yang dienkripsi ... 797
Operasi dengan mesin virtual Microsoft Azure ... 798
Mengatur server utama ... 798
Membuat server utama ... 799
Operasi dengan server utama ... 801
Mengelola server awan ... 801
Aturan firewall untuk server awan ... 802
Menetapkan aturan firewall untuk server awan ... 803
Memeriksa aktivitas firewall awan ... 806
Mencadangkan server awan ... 806
Orkestrasi (runbook) ... 807
Mengapa menggunakan runbook? ... 807
Membuat runbook ... 807
Operasi dengan runbook ... 811
Mengonfigurasi proteksi antivirus dan antimalware Anda ... 814
Platform yang didukung ... 814
Fitur yang didukung per platform ... 815
Perlindungan antivirus and antimalware ... 817
Fitur antimalware ... 818
Jenis pemindaian ... 818
Pengaturan perlindungan Antivirus dan antimalware ... 819
Active Protection di Cyber Backup edisi Standard ... 835

© Acronis International GmbH, 2003-2024

Pengaturan Active Protection di Cyber Backup Standard ... 835
Pemfilteran URL ... 842
Cara kerjanya ... 843
Alur kerja konfigurasi pemfilteran URL ... 845
Pengaturan pemfilteran URL ... 845
Deskripsi ... 852
Microsoft Defender Antivirus dan Microsoft Security Essentials ... 852
Jadwalkan pemindaian ... 853
Tindakan default ... 853
Perlindungan waktu nyata ... 854
Tingkat lanjut ... 854
Pengecualian ... 855
Manajemen firewall ... 855
Karantina ... 856
Bagaimana file masuk ke folder karantina? ... 856
Mengelola file yang dikarantina ... 857
Lokasi karantina di mesin ... 857
Folder kustom layanan mandiri sesuai permintaan ... 858
Daftar putih perusahaan ... 858
Penambahan otomatis ke daftar putih ... 859
Penambahan manual ke daftar putih ... 859
Menambahkan file yang dikarantina ke daftar putih ... 859
Pengaturan daftar putih ... 859
Melihat detail tentang item dalam daftar putih ... 860
Pemindaian antimalware pada cadangan ... 860
Pembatasan ... 861
Bekerja dengan fitur proteksi Tingkat Lanjut ... 862
Advanced Data Loss Prevention ... 864
Membuat kebijakan alur data dan aturan kebijakan ... 864
Mengaktifkan Advanced Data Loss Prevention di rencana proteksi ... 874
Deteksi tujuan mandiri ... 877
Definisi data sensitif ... 878
Peristiwa Pencegahan Kehilangan Data ... 884
Widget Advanced Data Loss Prevention dalam dasbor Ikhtisar ... 885
Kategori sensitivitas kustom ... 886
Peta organisasi ... 888
Masalah dan batasan yang diketahui ... 891

© Acronis International GmbH, 2003-2024

Deteksi dan Tanggapan Titik Akhir (EDR) ... 892
Alasan Anda memerlukan Deteksi dan Tanggapan Titik Akhir (EDR) ... 892
Mengaktifkan fungsionalitas Deteksi dan Tanggapan Titik Akhir (EDR) ... 895
Cara menggunakan Deteksi dan Tanggapan Titik Akhir (EDR) ... 897
Melihat insiden mana yang saat ini tidak dimitigasi ... 901
Memahami ruang lingkup dan dampak insiden ... 902
Cara menavigasi tahapan serangan ... 911
Mengaktifkan mode monitoring untuk Endpoint Detection and Response (EDR) ... 946
Cara menguji apakah Deteksi dan Tanggapan Titik Akhir (EDR) bekerja dengan baik ... 948
Menilai kerentanan dan mengelola patch ... 950
Penilaian kerentanan ... 950
Produk Microsoft dan produk pihak ketiga yang didukung ... 951
Produk Apple dan pihak ketiga yang didukung ... 952
Produk Linux yang didukung ... 953
Pengaturan penilaian kerentanan ... 953
Penilaian kerentanan untuk mesin Windows ... 956
Penilaian kerentanan untuk mesin Linux ... 956
Penilaian kerentanan untuk perangkat macOS ... 957
Mengelola kerentanan yang ditemukan ... 957
Manajemen patch ... 959
Alur kerja manajemen patch ... 959
Pengaturan manajemen patch dalam rencana proteksi ... 960
Melihat daftar patch yang tersedia ... 965
Persetujuan patch otomatis ... 967
Menyetujui patch secara manual ... 972
Menginstal patch sesuai permintaan ... 972
Mengelola inventaris perangkat keras dan perangkat lunak Anda ... 974
Inventaris perangkat lunak ... 974
Mengaktifkan pemindaian inventaris perangkat lunak ... 974
Menjalankan pemindaian inventaris perangkat lunak secara manual ... 975
Menjelajahi inventaris perangkat lunak ... 975
Menampilkan inventaris perangkat lunak dari satu perangkat ... 977
Inventaris perangkat keras ... 978
Mengaktifkan pemindaian inventaris perangkat keras ... 979
Menjalankan pemindaian inventaris perangkat keras secara manual ... 979
Menjelajahi inventaris perangkat keras ... 980
Menampilkan perangkat keras dari satu perangkat ... 982

© Acronis International GmbH, 2003-2024

Menghubungkan ke beban kerja untuk desktop jarak jauh atau bantuan jarak jauh 984
Fitur desktop dan bantuan jarak jauh yang didukung 986
Platform yang didukung 988
Protokol koneksi jarak jauh 989
NEAR 989
RDP 990
Berbagi Layar Apple 990
Pengalihan suara jarak jauh 990
Koneksi ke beban kerja jarak jauh untuk desktop jarak jauh atau bantuan jarak jauh 991
Rencana manajemen jarak jauh 992
Membuat rencana manajemen jarak jauh 993
Menambahkan beban kerja ke rencana manajemen jarak jauh 1000
Menghapus beban kerja dari rencana manajemen jarak jauh 1001
Operasi tambahan dengan rencana manajemen jarak jauh yang ada 1002
Masalah kompatibilitas dengan rencana manajemen jarak jauh 1004
Menyelesaikan masalah kompatibilitas dengan rencana manajemen jarak jauh 1005
Kredensial beban kerja 1006
Menambahkan kredensial 1006
Menetapkan kredensial ke beban kerja 1007
Menghapus kredensial 1007
Membatalkan penetapan kredensial dari beban kerja 1008
Bekerja dengan beban kerja terkelola 1008
Mengonfigurasi pengaturan RDP 1009
Menghubungkan ke beban kerja terkelola untuk desktop jarak jauh atau bantuan jarak jauh 1009
Menghubungkan ke beban kerja terkelola melalui klien web 1012
Mentransfer file 1013
Melakukan tindakan kontrol pada beban kerja terkelola 1014
Pemantauan beban kerja melalui transmisi tangkapan layar 1015
Mengamati beberapa beban kerja terkelola secara bersamaan 1016
Bekerja dengan beban kerja tidak terkelola 1017
Menghubungkan ke beban kerja tidak terkelola melalui Acronis Bantuan Cepat 1018
Menghubungkan ke beban kerja yang tidak terkelola melalui alamat IP 1019
Mentransfer file melalui Acronis Bantuan Cepat 1019
Menggunakan toolbar di jendela Penampil 1020
Merekam dan memutar sesi jarak jauh 1023
Mengonfigurasi pengaturan Hubungkan Klien 1023
Pemberitahu desktop jarak jauh 1025

© Acronis International GmbH, 2003-2024

Pemantauan kesehatan dan kinerja beban kerja **1027**
Rencana pemantauan 1027
Jenis pemantauan 1027
Pemantauan berbasis anomali 1028
Platform yang didukung untuk pemantauan 1028
Monitor yang dapat dikonfigurasi 1028
Pengaturan monitor ruang Disk 1033
Pengaturan monitor suhu CPU 1035
Pengaturan monitor suhu GPU 1037
Pengaturan monitor Perubahan perangkat keras 1038
Pengaturan monitor penggunaan CPU 1039
Pengaturan monitor Penggunaan memori 1041
Pengaturan monitor kecepatan transfer Disk 1043
Pengaturan monitor Penggunaan jaringan 1045
Pengaturan penggunaan CPU berdasarkan monitor proses 1048
Pengaturan penggunaan Memori berdasarkan monitor proses 1049
Pengaturan kecepatan transfer Disk berdasarkan monitor proses 1050
Pengaturan penggunaan Jaringan berdasarkan monitor proses 1051
Pengaturan monitor status layanan Windows 1052
Pengaturan monitor Status proses 1053
Pengaturan monitor Perangkat lunak yang diinstal 1053
Pengaturan monitor Mulai ulang sistem terakhir 1054
Pengaturan monitor log peristiwa Windows 1054
Pengaturan monitor ukuran File dan folder 1056
Pengaturan monitor status Pembaruan Windows 1057
Pengaturan monitor status Firewall 1057
Pengaturan monitor upaya masuk gagal 1057
Pengaturan status monitor perangkat lunak antimalware 1058
Pengaturan monitor status fitur AutoRun 1059
Pengaturan monitor Kustom 1059
Rencana pemantauan 1061
Membuat rencana pemantauan 1061
Menambahkan beban kerja ke rencana pemantauan 1063
Membatalkan rencana pemantauan 1064
Mengonfigurasi tindakan respons otomatis 1064
Operasi tambahan dengan rencana pemantauan 1067
Masalah kompatibilitas dengan rencana pemantauan 1069

© Acronis International GmbH, 2003-2024

Menyelesaikan masalah kompatibilitas dengan rencana pemantauan 1070
Memulai ulang model pembelajaran mesin 1071
Peringatan pemantauan 1071
Mengonfigurasi peringatan pemantauan 1072
Variabel peringatan pemantauan 1073
Tindakan respons manual 1075
Melihat peringatan monitoring untuk beban kerja 1078
Melihat log peringatan dari peringatan pemantauan 1078
Mengonfigurasi kebijakan notifikasi email 1079
Melihat data monitor 1080
Widget monitor 1081
Alat bantu Cyber Protection tambahan 1083
Mode kepatuhan 1083
Pembatasan 1083
Fitur yang tidak didukung 1083
Mengatur kata sandi enkripsi 1084
Mengubah kata sandi enkripsi 1084
Memulihkan cadangan untuk penyewa dalam mode Kepatuhan 1085
Penyimpanan yang tidak dapat diubah 1085
Mode penyimpanan yang tidak dapat diubah 1085
Penyimpanan dan agen yang didukung 1086
Mengaktifkan penyimpanan yang tidak dapat diubah 1086
Menonaktifkan penyimpanan yang tidak dapat diubah 1087
Mengakses cadangan yang dihapus dalam penyimpanan yang tidak dapat diubah 1087
Penyimpanan geo-redundan 1088
Mengaktifkan dan menonaktifkan penyimpanan geo-redundan 1088
Status Geo-replikasi 1089
Pembatasan 1089
Glosarium 1090
Indeks 1095

© Acronis International GmbH, 2003-2024

Memulai dengan Cyber Protection

Mengaktifkan akun

Ketika administrator membuat akun untuk Anda, sebuah pesan email akan dikirimkan ke alamat email Anda. Pesan tersebut berisi informasi berikut:

- **Login Anda.** Ini adalah nama pengguna yang Anda gunakan untuk masuk. Login Anda juga ditampilkan di halaman aktivasi akun.
- Tombol **Aktifkan akun**. Klik tombol dan atur kata sandi untuk akun Anda. Pastikan kata sandi Anda setidaknya sepanjang sembilan karakter. Untuk informasi lebih lanjut tentang kata sandi, lihat "Persyaratan kata sandi" (hlm. 19).

Jika administrator Anda telah mengaktifkan autentikasi dua-faktor, Anda akan diminta untuk menyiapkan akun Anda. Untuk informasi lebih lanjut, lihat "Autentikasi dua faktor" (hlm. 19).

Persyaratan kata sandi

Panjang maksimum kata sandi untuk akun pengguna adalah 9 karakter. Kata sandi juga diperiksa kerumitannya, dan masuk ke dalam salah satu dari kategori berikut:

- Lemah
- Sedang
- Kuat

Anda tidak bisa menyimpan kata sandi yang lemah, meskipun berisi 9 karakter atau lebih. Kata sandi yang menggunakan nama pengguna, login, surel pengguna, atau nama penyewa pemilik akun pengguna selalu dianggap lemah. Sebagian besar kata sandi paling umum juga dianggap lemah.

Untuk memperkuat kata sandi, tambahkan lebih banyak karakter. Menggunakan jenis karakter yang berbeda, seperti digit, huruf besar dan huruf kecil, dan karakter khusus tidak diwajibkan, tetapi akan menghasilkan kata sandi yang kuat dan juga lebih pendek.

Autentikasi dua faktor

Autentikasi dua faktor (2FA) memberikan perlindungan ekstra dari akses tidak sah ke akun Anda. Ketika 2FA diatur, Anda diminta memasukkan kata sandi Anda (faktor pertama) dan kode satu kali (faktor kedua) untuk masuk ke konsol Cyber Protect. Kode satu kali dihasilkan dari aplikasi khusus yang harus diinstal di ponsel atau perangkat lain yang Anda miliki. Meskipun seseorang mengetahui login dan kata sandi Anda, mereka tidak akan dapat masuk ke akun Anda tanpa memiliki akses ke perangkat faktor kedua Anda.

Guna mengatur autentikasi dua faktor untuk akun Anda

© Acronis International GmbH, 2003-2024

Anda harus menyiapkan 2FA untuk akun Anda jika administrator telah mengaktifkannya untuk organisasi Anda. Jika administrator mengaktifkan 2FA saat Anda masuk ke konsol Cyber Protect, Anda harus mengaturnya ketika sesi Anda saat ini berakhir.

Prasyarat

- Autentikasi dua faktor diaktifkan untuk organisasi Anda oleh administrator.

Guna mengatur autentikasi dua faktor untuk akun Anda

1. Instal aplikasi autentikator di perangkat seluler Anda.
   Contoh aplikasi autentikator:
   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
2. Pindai kode QR menggunakan aplikasi autentikator Anda, lalu masukkan kode 6 digit yang ditampilkan pada aplikasi autentikator di jendela **Siapkan autentikasi dua faktor**.
3. Klik **Berikutnya**.
   Petunjuk tentang cara memulihkan akses Anda ke akun Anda jika Anda kehilangan perangkat 2FA atau mencopot pemasangan aplikasi autentikator ditampilkan.
4. Simpan atau cetak file PDF.

   Catatan
   Pastikan Anda menyimpan file PDF di tempat yang aman atau mencetaknya untuk referensi lebih lanjut. Ini adalah cara terbaik untuk memulihkan akses Anda.

5. Kembali ke halaman masuk konsol Cyber Protect dan masukkan kode yang dihasilkan.
   Kode satu kali berlaku selama 30 detik. Jika Anda menunggu lebih dari 30 detik, gunakan kode berikutnya yang dihasilkan.

Saat berikutnya Anda login, Anda dapat memilih kotak centang **Percayai browser ini...**. Dalam hal ini, kode tidak akan diperlukan untuk login berikutnya dengan menggunakan browser ini di mesin ini.

Catatan
Kami menyarankan Anda membiarkan kotak centang ini kosong. Jika tidak, Anda akan kehilangan akses ke 2FA untuk akun Anda.

Untuk memulihkan autentikasi dua faktor pada perangkat baru (2FA)

Jika Anda memiliki akses ke aplikasi autentikasi seluler yang telah diatur sebelumnya

1. Instal aplikasi autentikator di perangkat baru Anda.
2. Gunakan file PDF yang Anda simpan saat Anda mengonfigurasi 2FA di perangkat Anda. File ini berisi kode 32 digit yang harus Anda masukkan di aplikasi autentikator untuk menautkan kembali aplikasi autentikator ke akun Acronis Anda.

© Acronis International GmbH, 2003-2024

Penting
Jika kode tidak berfungsi, pastikan waktu di aplikasi seluler autentikator disinkronkan dengan perangkat Anda.

Jika Anda tidak menyimpan file PDF selama pengaturan:

a. Klik **Atur ulang 2FA**, lalu masukkan kata sandi satu kali yang ditampilkan di aplikasi autentikator seluler.
b. Ikuti petunjuk di layar.

Jika Anda tidak memiliki akses ke aplikasi autentikator seluler yang telah diatur sebelumnya

1. Ambil perangkat seluler baru.
2. Gunakan file PDF yang disimpan untuk menautkan perangkat baru (nama default file tersebut adalah `cyberprotect-2fa-backupcode.pdf`).
3. Pulihkan akses ke akun Anda dari cadangan. Pastikan pencadangan didukung oleh aplikasi seluler Anda.
4. Buka aplikasi dengan akun yang sama dari perangkat seluler lain jika didukung oleh aplikasi.

Pengaturan privasi

Pengaturan privasi membantu Anda menunjukkan apakah Anda memberikan izin pengumpulan, penggunaan, dan pengungkapan informasi pribadi atau tidak.

Bergantung pada negara tempat Anda menggunakan pusat data Cyber Protect Cloud dan Cyber Protect Cloud yang memberikan layanan untuk Anda, pada peluncuran awal Cyber Protect Cloud, Anda mungkin diminta mengonfirmasi apakah Anda setuju menggunakan Google Analytics di Cyber Protect Cloud.

Google Analytics membantu kami memahami perilaku pengguna dengan lebih baik dan meningkatkan pengalaman pengguna di Cyber Protect Cloud dengan mengumpulkan data pseudonim.

Jika Anda mengaktifkan atau menolak mengaktifkan Google Analytics di peluncuran awal Cyber Protect Cloud, Anda dapat mengubah keputusan kapan saja.

Untuk mengaktifkan atau menonaktifkan Google Analytics

1. Di konsol Cyber Protect, klik **Kelola akun**.
2. Klik ikon akun di sudut kanan atas.
3. Pilih **Pengaturan privasi saya**. Jendela **Pengaturan privasi saya** ditampilkan.
4. Di bagian **Pengumpulan data Google Analytics**, klik salah satu tombol berikut:
   - **Aktif** untuk mengaktifkan Google Analytics
   - **Nonaktif** untuk menonaktifkan Google Analytics

© Acronis International GmbH, 2003-2024

Di bagian **Cara menghapus cookie**, Anda dapat mengontrol dan mengelola cookie langsung di browser Anda.

Catatan
Jika Anda tidak melihat bagian Google Analytics, berarti Google Analytics tidak digunakan di negara Anda.

Di bagian **Onboarding dalam produk dan bantuan interaktif** yang awalnya ditampilkan selama masa uji coba, Anda dapat berhenti atau tetap menerima informasi tentang peningkatan dan fitur baru dalam program di masa mendatang. Fitur ini diaktifkan secara default, tetapi Anda dapat menonaktifkannya dengan mengalihkan tombol ke **Off**.

Mengakses layanan Cyber Protection

Setelah mengaktifkan akun, Anda dapat mengakses layanan Cyber Protection dengan masuk ke konsol Cyber Protect atau melalui portal manajemen.

Untuk masuk ke konsol Cyber Protect

1. Buka halaman masuk layanan Cyber Protection.
2. Ketik login Anda, lalu klik **Lanjutkan**.
3. Ketik kata sandi Anda, lalu klik **Lanjutkan**.
4. [Jika Anda menggunakan lebih dari satu layanan Cyber Protect Cloud] Klik **Perlindungan Cyber**.
   Pengguna yang hanya memiliki akses ke layanan Cyber Protection, masuk langsung ke konsol Cyber Protect.
   Jika **Perlindungan Cyber** bukan satu-satunya layanan yang dapat Anda akses, Anda dapat beralih antarlayanan dengan menggunakan ikon di sudut kanan atas. Administrator juga dapat menggunakan ikon ini untuk beralih ke portal manajemen.

Periode batas waktu untuk konsol Cyber Protect adalah 24 jam untuk sesi aktif dan 1 jam untuk sesi idle.

Anda dapat mengubah bahasa antarmuka web dengan cara mengeklik ikon akun pada sudut kanan atas.

Untuk mengakses konsol Cyber Protect melalui portal manajemen

1. Di portal manajemen, buka **Pemantauan** > **Penggunaan**.
2. Di bawah **Cyber Protect**, pilih **Perlindungan**, dan kemudian klik **Kelola layanan**.
   Atau, di bawah **Klien**, pilih pelanggan, lalu klik **Kelola layanan**.

Hasilnya, Anda dialihkan ke konsol Cyber Protect.

© Acronis International GmbH, 2003-2024

Penting
Jika pelanggan dalam mode manajemen **Layanan mandiri**, Anda tidak dapat mengelola layanan untuk pelanggan. Hanya administrator pelanggan yang dapat mengubah mode pelanggan menjadi **Dikelola oleh penyedia layanan**, lalu mengelola layanan.

Untuk mengatur ulang kata sandi Anda

1. Buka halaman masuk layanan Cyber Protection.
2. Ketik login Anda, lalu klik **Lanjutkan**.
3. Klik **Lupa kata sandi?**
4. Konfirmasi bahwa Anda menginginkan informasi lebih lanjut dengan mengeklik **Kirim**.
5. Ikuti petunjuk dalam email yang telah Anda terima.
6. Atur kata sandi baru Anda.

Persyaratan perangkat lunak

Browser web yang didukung

Konsol Cyber Protect menggunakan protokol TLS 1.2 dan memberikan dukungan untuk browser web berikut:

- Google Chrome 29 ke atas
- Mozilla Firefox 23 ke atas
- Opera 16 ke atas
- Microsoft Edge 25 ke atas
- Safari 8 ke atas yang berjalan di sistem operasi macOS dan iOS

Di browser web lain (termasuk browser Safari yang berjalan di sistem operasi lain), antarmuka pengguna mungkin akan ditampilkan dengan tidak tepat atau beberapa fungsi mungkin tidak tersedia.

Sistem operasi dan lingkungan yang Didukung

Agen untuk Windows

Agen ini mencakup komponen untuk perlindungan Antivirus & Antimalware dan pemfilteran URL. Lihat "Fitur perlindungan yang didukung oleh sistem operasi" (hlm. 44) untuk detail tentang fungsi yang didukung oleh sistem operasi.

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows Server 2003 SP1/2003 R2 ke atas – Standard dan Enterprise edition (x86, x64)

© Acronis International GmbH, 2003-2024

- Windows Small Business Server 2003/2003 R2
- Windows Server 2008, Windows Server 2008 SP2* – edisi Standard, Enterprise, Datacenter, Foundation, dan Web (x86, x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7 – semua edisi

Catatan
Untuk menggunakan Cyber Protection dengan Windows 7, Anda harus menginstal pembaruan berikut dari Microsoft sebelum menginstal agen proteksi:

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

Untuk informasi lebih lanjut mengenai pembaruan yang diperlukan, lihat artikel basis pengetahuan ini.

- Windows Server 2008 R2* – edisi Standard, Enterprise, Datacenter, Foundation, dan Web
- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011* – semua edisi
- Windows 8/8.1 – semua edisi (x86, x64), kecuali untuk Windows RT edition
- Windows Server 2012/2012 R2 – semua edisi
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – edisi Home, Pro, Education, Enterprise, IoT Enterprise dan LTSC (sebelumnya LTSB)
- Windows Server 2016 – semua opsi instalasi, kecuali untuk Nano Server
- Windows Server 2019 – semua opsi instalasi, kecuali untuk Nano Server
- Windows 11 – semua edisi
- Windows Server 2022 – semua opsi instalasi, kecuali untuk Nano Server

Catatan
* Untuk menggunakan Cyber Protection dengan versi Windows ini, Anda harus menginstal pembaruan dukungan penandatanganan kode SHA2 dari Microsoft (KB4474419) sebelum menginstal agen proteksi.

Untuk informasi tentang masalah yang terkait dengan pembaruan dukungan penandatanganan kode SHA2, lihat artikel basis pengetahuan ini.

© Acronis International GmbH, 2003-2024

Agen untuk SQL, Agen untuk Active Directory, Agen untuk Exchange (untuk cadangan database dan cadangan keberadaan aplikasi)

Setiap agen berikut dapat diinstal di mesin yang menjalankan sistem operasi apa pun yang ada dalam daftar di atas dan versi yang didukung dari masing-masing aplikasi.

Agen untuk Pencegahan Kebocoran Data

Kontrol perangkat

- Microsoft Windows 7 Service Pack 1 dan versi lebih baru
- Microsoft Windows Server 2008 R2 dan versi lebih baru
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

Catatan
Agen untuk Pencegahan Kehilangan Data untuk macOS hanya mendukung prosesor x64. Prosesor berbasis Apple silicon ARM tidak didukung.

Pencegah kehilangan data

- Microsoft Windows 7 Service Pack 1 dan versi lebih baru
- Microsoft Windows Server 2008 R2 dan versi lebih baru

Catatan
Agen untuk Pencegahan Kehilangan Data dapat diinstal pada sistem macOS yang tidak didukung karena merupakan bagian integral dari Agen untuk Mac. Pada kasus ini, konsol Cyber Protect akan mengindikasikan bahwa Agen untuk Pencegahan Kehilangan Data sudah diinstal di komputer, tetapi fungsionalitas kontrol perangkat dan pencegahan kehilangan data tidak akan berfungsi. Fungsionalitas kontrol perangkat hanya akan berfungsi pada sistem macOS yang didukung oleh Agen untuk Pencegahan Kehilangan Data.

Agen untuk Advanced Data Loss Prevention

- Microsoft Windows 7 Service Pack 1 dan versi lebih baru
- Microsoft Windows Server 2008 R2 dan versi lebih baru

Agen untuk File Sync & Share

Untuk daftar sistem operasi yang didukung, lihat Cyber Files Cloud panduan pengguna.

© Acronis International GmbH, 2003-2024

Agen untuk Exchange (untuk pencadangan kotak surat)

- Windows Server 2008 – edisi Standard, Enterprise, Datacenter, Foundation, dan Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 – semua edisi
- Windows Server 2008 R2 – edisi Standard, Enterprise, Datacenter, Foundation, dan Web
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – semua edisi
- Windows 8/8.1 – semua edisi (x86, x64), kecuali untuk Windows RT edition
- Windows Server 2012/2012 R2 – semua edisi
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – edisi Home, Pro, Education, dan Enterprise
- Windows Server 2016 – semua opsi instalasi, kecuali untuk Nano Server
- Windows Server 2019 – semua opsi instalasi, kecuali untuk Nano Server
- Windows 11 – semua edisi
- Windows Server 2022 – semua opsi instalasi, kecuali untuk Nano Server

Agen untuk Microsoft 365

- Windows Server 2008 – edisi Standard, Enterprise, Datacenter, Foundation, dan Web (hanya x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2 – edisi Standard, Enterprise, Datacenter, Foundation, dan Web
- Windows Home Server 2011
- Windows Small Business Server 2011 – semua edisi
- Windows 8/8.1 – semua edisi (hanya x64), kecuali Windows RT edition
- Windows Server 2012/2012 R2 – semua edisi
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (hanya x64)
- Windows 10 – Home, Pro, Education, dan Enterprise edition (hanya x64)
- Windows Server 2016 – semua opsi instalasi (hanya x64), kecuali untuk Nano Server
- Windows Server 2019 – semua opsi instalasi (hanya x64), kecuali untuk Nano Server
- Windows 11 – semua edisi
- Windows Server 2022 – semua opsi instalasi, kecuali untuk Nano Server

© Acronis International GmbH, 2003-2024

Agen untuk Oracle

- Windows Server 2008R2 – edisi Standard, Enterprise, Datacenter, dan Web (x86, x64)
- Windows Server 2012R2 – edisi Standard, Enterprise, Datacenter, dan Web (x86, x64)
- Linux – kernel dan distribusi apa pun yang didukung oleh Agen untuk Linux (tercantum di bawah)

Agen untuk MySQL/MariaDB

- Linux – kernel dan distribusi apa pun yang didukung oleh Agen untuk Linux (tercantum di bawah)

Agen untuk Linux

Agen ini mencakup komponen untuk perlindungan Antivirus & Antimalware dan pemfilteran URL. Lihat "Fitur perlindungan yang didukung oleh sistem operasi" (hlm. 44) untuk detail tentang fungsi yang didukung oleh sistem operasi.

Distribusi dan versi kernel Linux telah diuji secara khusus. Akan tetapi, bahkan jika distribusi atau versi kernel Linux Anda tidak tercantum di bawah ini, distribusi atau versi kernel tersebut masih dapat berfungsi dengan baik dalam semua skenario wajib karena karakteristik sistem operasi Linux.

Jika Anda mengalami masalah saat menggunakan Cyber Protection dengan kombinasi distribusi Linux dan versi kernel Anda, hubungi tim Dukungan untuk investigasi lebih lanjut.

Linux dengan kernel dari 2.6.9 hingga 5.19 dan glibc 2.3.4 atau lebih baru, termasuk distribusi x86 dan x86_64 berikut:

- 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

Penting
Konfigurasi dengan Btrfs tidak didukung untuk SUSE Linux Enterprise Server 12 dan 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* – Unbreakable Enterprise Kernel dan Red Hat Compatible Kernel

© Acronis International GmbH, 2003-2024

Catatan
Menginstal agen perlindungan di Oracle Linux 8.6 dan versi yang lebih baru, dengan Boot Aman yang aktif, memerlukan penandatanganan manual modul kernel. Untuk informasi lebih lanjut tentang penandatanganan modul kernel, lihat artikel basis pengetahuan ini.

- 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

* Mulai dari versi 8.4, hanya didukung dengan kernel dari 4.18 hingga 5.19

Agen untuk Mac

Agen ini mencakup komponen untuk perlindungan Antivirus & Antimalware dan pemfilteran URL. Lihat "Fitur perlindungan yang didukung oleh sistem operasi" (hlm. 44) untuk detail tentang fungsi yang didukung oleh sistem operasi.

Arsitektur x64 dan ARM (digunakan dalam prosesor silikon Apple seperti Apple M1 dan M2) didukung.

Catatan
Anda tidak dapat memulihkan cadangan tingkat disk dari Mac berbasis Intel ke Mac yang menggunakan prosesor silikon Apple, dan sebaliknya. Anda dapat memulihkan file dan folder.

- 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

Penting
Mulai dari versi C23.07, Cyber Protect Cloud tidak mendukung sistem operasi berikut: OS X Yosemite 10.10, OS X El Capitan 10.11, dan macOS Sierra 10.12.

Kami sangat menganjurkan agar Anda meningkatkan sistem operasi Anda ke versi yang didukung untuk memastikan kompatibilitas dan dapat menggunakan fungsionalitas penuh dari Cyber Protect Cloud.

© Acronis International GmbH, 2003-2024

Agen untuk VMware (Virtual Appliance)

Agen ini dikirim sebagai alat virtual untuk berjalan di host ESXi.

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

Agen untuk VMware (Windows)

Agen ini dikirim sebagai aplikasi Windows untuk menjalankan sistem operasi apa pun yang ada dalam daftar di atas sebagai Agen untuk Windows dengan pengecualian berikut:

- Sistem operasi 32-bit tidak didukung.
- Windows XP, Windows Server 2003/2003 R2, dan Windows Small Business Server 2003/2003 R2 tidak didukung.

Agen untuk Hyper-V

- Windows Server 2008 (hanya x64) dengan peran Hyper-V, termasuk mode instalasi Server Core
- Windows Server 2008 R2 dengan peran Hyper-V, termasuk mode instalasi Server Core
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 dengan peran Hyper-V, termasuk mode instalasi Server Core
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (hanya x64) dengan Hyper-V
- Windows 10 – Pro, Education, dan Enterprise edition dengan Hyper-V
- Windows Server 2016 dengan peran Hyper-V – semua opsi instalasi, kecuali untuk Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 dengan peran Hyper-V – semua opsi instalasi, kecuali untuk Nano Server
- Microsoft Hyper-V Server 2019
- Windows Server 2022 – semua opsi instalasi, kecuali untuk Nano Server

Agen untuk Virtuozzo

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

Agen untuk 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

Agen untuk Scale Computing HC3

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

© Acronis International GmbH, 2003-2024

Agen untuk oVirt

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agen untuk Synology

DiskStation Manager 6.2.x, 7.x

Agen untuk Synology hanya mendukung perangkat NAS dengan prosesor x86_64. Prosesor ARM tidak didukung.

Monitor Cyber Protect

- Windows 7 dan versi lebih baru
- Windows Server 2008 R2 dan versi lebih baru
- Semua versi macOS yang didukung oleh Agen untuk Mac

Versi Microsoft SQL Server yang didukung

- 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

SQL Server Express editions dari versi SQL Server di atas juga didukung.

Catatan
Cadangan Microsoft SQL hanya didukung untuk database yang berjalan pada sistem file NFTS, REFS, dan FAT32. ExFat tidak didukung.

Versi Microsoft Exchange Server yang didukung

- Microsoft Exchange Server 2019 – semua edisi.
- Microsoft Exchange Server 2016 – semua edisi.
- Microsoft Exchange Server 2013 – semua edisi, Pembaruan Kumulatif 1 (CU1) ke atas.
- Microsoft Exchange Server 2010 – semua edisi, semua paket layanan. Pencadangan kotak surat dan pemulihan granular dari cadangan database didukung mulai dengan Service Pack 1 (SP1).

© Acronis International GmbH, 2003-2024

- Microsoft Exchange Server 2007 – semua edisi, semua paket layanan. Pencadangan kotak surat dan pemulihan granular dari cadangan database tidak didukung.

Versi Microsoft SharePoint yang didukung

Cyber Protection mendukung versi Microsoft SharePoint berikut:

- 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*

*Untuk menggunakan SharePoint Explorer dengan versi ini, Anda memerlukan farm pemulihan SharePoint untuk menyertakan database.

Cadangan atau database yang datanya Anda ekstrak harus berasal dari versi SharePoint yang sama dengan versi di mana SharePoint Explorer diinstal.

Versi Database Oracle yang didukung

- Database Oracle versi 11g, semua edisi
- Database Oracle versi 12c, semua edisi
- Database Oracle versi 19c, semua edisi
- Database Oracle versi 21c, semua edisi

Hanya konfigurasi instans tunggal yang didukung.

Versi SAP HANA yang didukung

HANA 2.0 SPS 03 diinstal di RHEL 7.6 yang beroperasi di mesin fisik atau mesin virtual VMware ESXi.

Dikarenakan SAP HANA tidak mendukung pemulihan kontainer basis data multipenyewa dengan menggunakan snapshot penyimpanan, solusi ini mendukung kontainer SAP HANA dengan hanya satu basis data penyewa.

Versi MySQL yang didukung

- 5.5.x − Edisi Community Server, Enterprise, Standard, dan Classic
- 5.6.x − Edisi Community Server, Enterprise, Standard, dan Classic
- 5.7.x − Edisi Community Server, Enterprise, Standard, dan Classic
- 8.0.x − Edisi Community Server, Enterprise, Standard, dan Classic

© Acronis International GmbH, 2003-2024

Versi MariaDB yang didukung

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

Platform virtualisasi yang didukung

Tabel berikut merangkum bagaimana berbagai platform virtualisasi didukung.

Untuk informasi selengkapnya tentang perbedaan antara cadangan berbasis agen dan tanpa agen, lihat "Pencadangan berbasis agen dan tanpa agen" (hlm. 65).

Catatan
Jika Anda menggunakan platform virtualisasi atau versi yang tidak terdaftar di bawah ini, metode **Pencadangan berbasis Agen (Pencadangan dari dalam OS tamu)** mungkin masih dapat bekerja dengan benar dalam semua skenario yang diperlukan. Jika Anda mengalami masalah dengan backup berbasis agen, hubungi tim Dukungan untuk penyelidikan lebih lanjut.

VMware

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Versi VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 **Edisi VMware vSphere:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **VMware ESXi** > **Agen untuk instalasi di Windows** atau **Perangkat** > **Tambah** > **Host virtualisasi** > **VMware ESXi** > **Perangkat virtual (OVF)**	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

© Acronis International GmbH, 2003-2024

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
VMware vSphere Hypervisor (ESXi Gratis)**	Tidak didukung	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**
VMware Server (Server VMware Virtual) VMware Workstation VMware ACE VMware Player	Tidak didukung	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

* Dalam edisi ini, transportasi HotAdd untuk disk virtual didukung pada vSphere 5.0 ke atas. Di versi 4.1, pencadangan mungkin berjalan lebih lambat.

** Pencadangan pada tingkat hypervisor tidak didukung untuk vSphere Hypervisor karena produk ini membatasi akses ke Remote Command Line Interface (RCLI) ke mode hanya baca. Agen berfungsi selama periode evaluasi vSphere Hypervisor sementara tidak ada kunci seri yang dimasukkan. Setelah Anda memasukkan kunci seri, agen akan berhenti berfungsi.

Catatan
Cyber ProtectCloud secara resmi mendukung pembaruan apa pun dalam versi vSphere utama yang didukung.

Sebagai contoh, dukungan vSphere 8.0 mencakup dukungan untuk setiap pembaruan dalam versi ini, kecuali dinyatakan sebaliknya. Artinya, vSphere 8.0 Perbarui 1 juga didukung bersama dengan vSphere 8.0 yang dirilis pertama kali.

Didukung untuk versi VMware vSphere yang artinya vSAN versi bersangkutan juga didukung. Misalnya, mendukung vSphere 8.0 berarti vSAN 8.0 juga dapat didukung.

Pembatasan

- **Mesin toleransi kegagalan**
  Agen untuk VMware mencadangkan mesin toleransi kegagalan hanya jika toleransi kesalahan diaktifkan di VMware vSphere 6.0 ke atas. Jika Anda meningkatkan dari versi vSphere sebelumnya, cukup nonaktifkan dan aktifkan toleransi kegagalan untuk setiap mesin. Jika Anda menggunakan versi vSphere sebelumnya, instal agen di sistem operasi tamu.
- **Disk independen dan RDM**
  Agen untuk VMware tidak mencadangkan disk Raw Device Mapping (RDM) dalam mode kompatibilitas fisik atau disk independen. Agen melewatkan disk ini dan menambahkan peringatan ke log. Anda dapat menghindari peringatan dengan mengecualikan disk independen

© Acronis International GmbH, 2003-2024

dan RDM dalam mode kompatibilitas fisik dari rencana proteksi. Jika Anda ingin mencadangkan disk atau data ini pada disk ini, instal agen di sistem operasi tamu.

- **Koneksi iSCSI tamu**
  Agen untuk VMware tidak mencadangkan volume LUN yang dihubungkan oleh inisiator iSCSI yang bekerja dalam sistem operasi tamu. Karena hypervisor ESXi tidak mengetahui volume tersebut, volume tersebut tidak disertakan dalam snapshot tingkat hypervisor dan dihilangkan dari cadangan tanpa peringatan. Jika Anda ingin mencadangkan volume ini atau data pada volume ini, instal agen dalam sistem operasi tamu.
- **Mesin virtual terenkripsi** (diperkenalkan di VMware vSphere 6.5)
  - Mesin virtual terenkripsi dicadangkan dalam status tidak terenkripsi. Jika enkripsi sangat penting untuk Anda, aktifkan enkripsi cadangan ketika membuat rencana proteksi.
  - Mesin virtual yang dipulihkan selalu tidak terenkripsi. Anda dapat mengaktifkan enkripsi secara manual setelah pemulihan selesai.
  - Jika Anda mencadangkan mesin virtual terenkripsi, kami sarankan Anda juga mengenkripsi mesin virtual di mana Agen untuk VMware berjalan. Jika tidak, operasi dengan mesin terenkripsi mungkin lebih lambat dari yang diharapkan. Terapkan **Kebijakan Enkripsi VM** ke mesin agen menggunakan Klien Web vSphere.
  - Mesin virtual terenkripsi akan dicadangkan melalui LAN, meskipun Anda mengonfigurasi mode transpor SAN untuk agen tersebut. Agen akan melakukan fallback pada transpor NBD karena VMware tidak mendukung transpor SAN untuk mencadangkan disk virtual terenkripsi.
- **Boot Aman**
  - Mesin virtual VMware (diperkenalkan di VMware vSphere 6.5) **Booot Aman** dinonaktifkan setelah mesin virtual dipulihkan sebagai mesin virtual baru. Anda dapat mengaktifkan secara manual opsi ini setelah pemulihan selesai. Pembatasan ini berlaku untuk VMware.
  - Mesin virtual Hyper-V: Untuk semua VM GEN2, Boot Aman dinonaktifkan setelah mesin virtual dipulihkan ke mesin virtual baru atau mesin virtual yang sudah ada.
- **Pencadangan konfigurasi ESXi** tidak didukung untuk VMware vSphere 7.0.
- **Operasi yang didukung untuk mesin dengan volume logis**
  Pencadangan dan pemulihan beban kerja dengan volume logis, seperti LDM di Windows (disk dinamis) dan LVM di Linux, didukung dengan beberapa keterbatasan. Untuk informasi lebih lanjut tentang keterbatasan, lihat "Operasi yang didukung dengan volume logis" (hlm. 56).

Microsoft

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Windows Server 2008 (x64) dengan Hyper-V Windows Server 2008 R2 dengan Hyper-V	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Hyper-V**	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

© Acronis International GmbH, 2003-2024

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 dengan Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) dengan Hyper-V Windows 10 dengan Hyper-V Windows Server 2016 dengan Hyper-V – semua opsi instalasi, kecuali untuk Nano Server Microsoft Hyper-V Server 2016 Windows Server 2019 dengan Hyper-V – semua opsi instalasi, kecuali untuk Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 dengan Hyper-V – semua opsi instalasi, kecuali untuk Nano Server		
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	Tidak didukung	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**
Microsoft Virtual Server 2005	Tidak didukung	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

Catatan

Mesin virtual Hyper-V yang berjalan pada klaster hyper-converged dengan Storage Spaces Direct (S2D) didukung. Storage Spaces Direct juga didukung sebagai penyimpanan cadangan.

© Acronis International GmbH, 2003-2024

Pembatasan

- **Disk akses lewat**
  Agen untuk Hyper-V tidak mencadangkan disk akses lewat. Selama pencadangan, agen akan melewatkan disk ini dan menambahkan peringatan ke log. Anda dapat menghindari peringatan dengan mengecualikan disk akses lewat dari rencana proteksi. Jika Anda ingin mencadangkan disk atau data ini pada disk ini, instal agen di sistem operasi tamu.
- **Pengklusteran tamu Hyper-V**
  Agen untuk Hyper-V tidak mendukung cadangan mesin virtual Hyper-V yang merupakan simpul dari Kluster Failover Windows Server. Snapshot VSS di tingkat host dapat sementara memutus koneksi disk kuorum eksternal dari kluster. Jika Anda ingin mencadangkan mesin ini, instal agen di sistem operasi tamu.
- **Koneksi iSCSI tamu**
  Agen untuk Hyper-V tidak mencadangkan volume LUN yang dihubungkan oleh inisiator iSCSI yang bekerja dalam sistem operasi tamu. Karena hypervisor Hyper-V tidak mengetahui volume tersebut, volume tersebut tidak disertakan dalam snapshot tingkat hypervisor dan dihilangkan dari cadangan tanpa peringatan. Jika Anda ingin mencadangkan volume ini atau data pada volume ini, instal agen dalam sistem operasi tamu.
- **Boot Aman**
  Untuk semua VM GEN2, Boot Aman dinonaktifkan setelah mesin virtual dipulihkan ke mesin virtual baru atau mesin virtual yang sudah ada.
- **Operasi yang didukung untuk mesin dengan volume logis**
  Pencadangan dan pemulihan beban kerja dengan volume logis, seperti LDM di Windows (disk dinamis) dan LVM di Linux, didukung dengan beberapa keterbatasan. Untuk informasi lebih lanjut tentang keterbatasan, lihat "Operasi yang didukung dengan volume logis" (hlm. 56).
- **Nama file VHD/VHDX dengan simbol ampersand**
  Pada host Hyper-V yang menjalankan Windows Server 2016 atau lebih baru, Anda tidak dapat mencadangkan mesin virtual lama (versi 5.0) yang awalnya dibuat dengan Hyper-V 2012 R2 atau lebih lama, jika nama file VHD/VHDX berisi simbol ampersand (&).
  Untuk dapat mencadangkan mesin tersebut, di Hyper-V Manager, lepaskan disk virtual yang sesuai dari mesin virtual, edit nama file VHD/VHDX dengan menghapus simbol ampersand, lalu pasang kembali disk ke mesin virtual.
- **Depedensi pada subsistem Microsoft WMI**
  Cadangan tanpa agen dari mesin virtual Hyper-V bergantung pada subsistem Microsoft WMI, dan khususnya pada kelas `Msvm_VirtualSystemManagementService`. Jika query WMI gagal, cadangan juga akan gagal. Untuk informasi lebih lanjut tentang kelas `Msvm_VirtualSystemManagementService`, lihat dokumen Microsoft.

© Acronis International GmbH, 2003-2024

Scale Computing

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Scale Computing HC3**	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

Pembatasan

Operasi yang didukung untuk mesin dengan volume logis

Pencadangan dan pemulihan beban kerja dengan volume logis, seperti LDM di Windows (disk dinamis) dan LVM di Linux, didukung dengan beberapa keterbatasan. Untuk informasi lebih lanjut tentang keterbatasan, lihat "Operasi yang didukung dengan volume logis" (hlm. 56).

Citrix

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
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	Tidak didukung	Didukung hanya untuk tamu yang sepenuhnya tervirtualisasi (alias HVM). Tamu paravirtualized (disebut juga PV) tidak didukung. **Perangkat** > **Tambah** > **Host virtualisasi** > **Citrix XenServer** > **Windows** atau **Linux**

Red Hat dan Linux

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
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	Tidak didukung	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

© Acronis International GmbH, 2003-2024

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Red Hat Virtualization (dikelola oleh oVirt) 4.2, 4.3, 4.4, 4.5	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Red Hat Virtualization (oVirt)**	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**
Mesin Virtual berbasis Kernel (KVM)	Tidak didukung	Didukung **Perangkat** > **Tambah** > **KVM** > **Windows** atau **Linux**
Mesin Virtual berbasis Kernel (KVM) yang dikelola oleh oVirt 4.3 yang berjalan di Red Hat Enterprise Linux 7.6, 7.7, atau CentOS 7.6, 7.7	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Red Hat Virtualization (oVirt)**	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**
Mesin Virtual berbasis Kernel (KVM) yang dikelola oleh oVirt 4.4 yang berjalan di Red Hat Enterprise Linux 8.x atau CentOS Stream 8.x	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Red Hat Virtualization (oVirt)**	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**
Mesin Virtual berbasis Kernel (KVM) yang dikelola oleh oVirt 4.5 yang berjalan di Red Hat Enterprise Linux 8.x atau CentOS Stream 8.x	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Red Hat Virtualization (oVirt)**	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

Pembatasan

Operasi yang didukung untuk mesin dengan volume logis

Pencadangan dan pemulihan beban kerja dengan volume logis, seperti LDM di Windows (disk dinamis) dan LVM di Linux, didukung dengan beberapa keterbatasan. Untuk informasi lebih lanjut tentang keterbatasan, lihat "Operasi yang didukung dengan volume logis" (hlm. 56).

Parallels

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Parallels Workstation	Tidak didukung	Didukung **Perangkat** > **Tambah** >

© Acronis International GmbH, 2003-2024

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
		Stasiun Kerja atau **Server** > **Windows** atau **Linux**
Parallels Server 4 Bare Metal	Tidak didukung	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

Oracle

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Oracle Virtualization Manager (berdasarkan oVirt)* 4.3	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Red Hat Virtualization (oVirt)**	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**
Oracle VM Server 3.0, 3.3, 3.4	Tidak didukung	Didukung hanya untuk tamu yang sepenuhnya tervirtualisasi (alias HVM). Tamu paravirtualized (disebut juga PV) tidak didukung. **Perangkat** > **Tambah** > **Host virtualisasi** > **Oracle** > **Windows** atau **Linux**
Oracle VM VirtualBox 4.x	Tidak didukung	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Oracle** > **Windows** atau **Linux**

*Oracle Virtualization Manager didukung oleh Agen untuk oVirt.

Pembatasan

Operasi yang didukung untuk mesin dengan volume logis

Pencadangan dan pemulihan beban kerja dengan volume logis, seperti LDM di Windows (disk dinamis) dan LVM di Linux, didukung dengan beberapa keterbatasan. Untuk informasi lebih lanjut tentang keterbatasan, lihat "Operasi yang didukung dengan volume logis" (hlm. 56).

© Acronis International GmbH, 2003-2024

Nutanix

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Nutanix Acropolis Hypervisor (AHV) 20160925.x hingga 20180425.x	Tidak didukung	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Nutanix AHV** > **Windows** atau **Linux**

Virtuozzo

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Virtuozzo**	Didukung hanya untuk mesin virtual. Kontainer tidak didukung. **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**
Virtuozzo 7.0.13, 7.0.14	Didukung untuk wadah ploop saja. Mesin virtual tidak didukung. **Perangkat** > **Tambah** > **Host virtualisasi** > **Virtuozzo**	Didukung hanya untuk mesin virtual. Kontainer tidak didukung. **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**
Virtuozzo Hybrid Server 7.5	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **Virtuozzo**	Didukung hanya untuk mesin virtual. Kontainer tidak didukung. **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

Pembatasan

Operasi yang didukung untuk mesin dengan volume logis

Pencadangan dan pemulihan beban kerja dengan volume logis, seperti LDM di Windows (disk dinamis) dan LVM di Linux, didukung dengan beberapa keterbatasan. Untuk informasi lebih lanjut tentang keterbatasan, lihat "Operasi yang didukung dengan volume logis" (hlm. 56).

© Acronis International GmbH, 2003-2024

Vituozzo Hybrid Infrastructure

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0	Didukung **Perangkat** > **Tambah** > **Host virtualisasi** > **infrastruktur Virtuozzo Hybrid**	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

Pembatasan

- **Cadangan VM tanpa agen dengan disk pada penyimpanan iSCSI eksternal**
  Anda tidak dapat mencadangkan VM dari Virtuozzo Hybrid Infrastructure, jika disk VM diletakkan pada volume iSCSI eksternal (terpasang ke klaster VHI).
- **Operasi yang didukung untuk mesin dengan volume logis**
  Pencadangan dan pemulihan beban kerja dengan volume logis, seperti LDM di Windows (disk dinamis) dan LVM di Linux, didukung dengan beberapa keterbatasan. Untuk informasi lebih lanjut tentang keterbatasan, lihat "Operasi yang didukung dengan volume logis" (hlm. 56).

Amazon

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Instans Amazon EC2	Tidak didukung	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

Microsoft Azure

Platform	Pencadangan tanpa agen (Cadangkan di tingkat hypervisor)	Pencadangan berbasis agen (Pencadangan dari dalam OS tamu)
Mesin virtual Azure	Tidak didukung	Didukung **Perangkat** > **Tambah** > **Stasiun Kerja** atau **Server** > **Windows** atau **Linux**

© Acronis International GmbH, 2003-2024

Kompatibilitas dengan perangkat lunak enkripsi

Tidak ada batasan pada pencadangan dan pemulihan data yang dienkripsi oleh perangkat lunak enkripsi *tingkat file*.

Perangkat lunak enkripsi *tingkat disk* mengenkripsi data yang sedang diproses. Inilah sebabnya data yang ada di dalam cadangan tidak terenkripsi. Perangkat lunak enkripsi tingkat disk sering memodifikasi area sistem: catatan boot, tabel partisi, atau tabel sistem file. Faktor ini memengaruhi pencadangan dan pemulihan tingkat disk, kemampuan sistem yang dipulihkan untuk melakukan boot dan akses ke Secure Zone.

Anda dapat mencadangkan data yang dienkripsi oleh perangkat lunak enkripsi tingkat disk berikut:

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

Untuk memastikan pemulihan tingkat disk yang dapat diandalkan, ikuti aturan umum dan rekomendasi spesifik perangkat lunak.

Aturan instalasi umum

Kami sangat menyarankan agar Anda menginstal perangkat lunak enkripsi sebelum Anda menginstal agen perlindungan.

Cara menggunakan Secure Zone

Secure Zone tidak boleh dienkripsi dengan enkripsi tingkat disk. Ini adalah satu-satunya cara menggunakan Secure Zone:

1. Instal perangkat lunak enkripsi; lalu instal agen.
2. Buat Secure Zone.
3. Jangan sertakan Secure Zone saat mengenkripsi disk atau volumenya.

Aturan pencadangan umum

Anda dapat melakukan pencadangan tingkat disk pada sistem operasi.

Prosedur pemulihan spesifik perangkat lunak

Microsoft BitLocker Drive Encryption

Untuk memulihkan sistem yang dienkripsi oleh BitLocker:

1. Lakukan boot dari media yang dapat di-boot.
2. Pulihkan sistem. Data yang dipulihkan tidak akan dienkripsi.

© Acronis International GmbH, 2003-2024

3. Boot ulang sistem yang dipulihkan.
4. Aktifkan BitLocker.

Jika Anda hanya perlu memulihkan satu partisi dari disk multi-partisi, lakukan pemulihan pada sistem operasi. Pemulihan pada media yang dapat di-boot mungkin dapat menyebabkan partisi yang dipulihkan tidak terdeteksi oleh Windows.

McAfee Endpoint Encryption dan PGP Whole Disk Encryption

Anda hanya dapat memulihkan partisi sistem yang terenkripsi menggunakan media yang dapat di-boot.

Jika sistem yang dipulihkan gagal melakukan boot, buat ulang Master Boot Record seperti yang dijelaskan pada artikel basis pengetahuan Microsoft berikut:
https://support.microsoft.com/kb/2622803

Kompatibilitas dengan penyimpanan Dell EMC Data Domain

Anda dapat menggunakan perangkat Dell EMC Data Domain sebagai penyimpanan cadangan.

Dengan penyimpanan ini, kami merekomendasikan Anda untuk menggunakan skema pencadangan yang secara rutin membuat cadangan penuh, misalnya **Selalu penuh**. Untuk mempelajari lebih lanjut tentang skema pencadangan yang tersedia, lihat "Skema cadangan" (hlm. 417).

Kunci retensi (mode Tata Kelola) didukung. Jika kunci retensi diaktifkan, Anda perlu menambahkan variabel lingkungan `AR_RETENTION_LOCK_SUPPORT` ke mesin dengan agen perlindungan yang menggunakan penyimpanan ini sebagai tujuan cadangan.

Catatan
Penyimpanan Dell EMC Data Domain dengan kunci retensi yang diaktifkan tidak didukung oleh Agen untuk Mac.

Untuk menambahkan variabel lingkungan `AR_RETENTION_LOCK_SUPPORT`

Di Windows

1. Masuk sebagai administrator ke mesin dengan agen perlindungan.
2. Di **Panel Kontrol**, buka **Sistem dan Keamanan** > **Sistem** > **Pengaturan sistem tingkat lanjut**.
3. Di **tab Tingkat Lanjut**, klik **Variabel Lingkungan**.
4. Di panel **Variabel sistem**, klik **Baru**.
5. Di jendela **Variabel Sistem Baru**, tambahkan variabel baru sebagai berikut:
   - Nama variabel: `AR_RETENTION_LOCK_SUPPORT`
   - Nilai variabel: `1`
6. Klik **OK**.

© Acronis International GmbH, 2003-2024

7. Di jendela **Variabel Lingkungan**, klik **OK**.
8. Mulai ulang mesin.

Di Linux

1. Masuk sebagai administrator ke mesin dengan agen perlindungan.
2. Buka direktori `/sbin`, lalu buka file `acronis_mms` untuk mengedit.
3. Di atas baris `export LD_LIBRARY_PATH`, tambahkan baris berikut:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Simpan file `acronis_mms`.
5. Mulai ulang mesin.

Dalam alat virtual

1. Masuk sebagai administrator ke alat virtual.
2. Buka direktori `/bin`, lalu buka file `autostart` untuk mengedit.
3. Di bawah baris `export LD_LIBRARY_PATH`, tambahkan baris berikut:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Simpan file `autostart`.
5. Mulai ulang mesin alat virtual.

Fitur perlindungan yang didukung oleh sistem operasi

Topik ini berisi informasi tentang fitur perlindungan dari Cyber Protect Cloud. Itu tidak mencantumkan fitur pencadangan dan pemulihan.

Fitur perlindungan hanya didukung pada mesin yang dipasang agen perlindungan. Mereka tidak tersedia untuk mesin virtual yang dicadangkan dalam mode tanpa agen, misalnya, oleh Agen untuk Hyper-V, Agen untuk VMware, Agen untuk Virtuozzo Hybrid Infrastructure, Agen untuk Scale Computing, atau Agen untuk oVirt.

Beberapa fitur mungkin memerlukan pelisensian tambahan sesuai model pelisensian yang diterapkan.

Sistem operasi dan versi yang didukung

Windows

Kecuali dinyatakan lain untuk rangkaian fitur tertentu, versi Windows berikut ini didukung:

- Windows 7 Service Pack 1 dan versi setelahnya
- Windows Server 2008 R2 Paket Layanan 1 dan yang lebih baru

© Acronis International GmbH, 2003-2024

Catatan
Untuk Windows 7, Anda harus menginstal pemutakhiran berikut dari Microsoft sebelum menginstal agen perlindungan.

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

Untuk informasi lebih lanjut mengenai pembaruan yang diperlukan, lihat artikel basis pengetahuan ini.

Linux

Distribusi Linux yang didukung dan versinya bergantung pada kumpulan fitur, dan ditampilkan di bagian bawah setiap tabel.

macOS

Versi macOS yang didukung bergantung pada kumpulan fitur, dan ditampilkan di bagian bawah setiap tabel.

Set fitur	Windows	Linux	macOS
Rencana proteksi default			
Pekerja Jarak Jauh	Iya	Tidak	Tidak
Pekerja kantor (antivirus pihak ketiga)	Iya	Tidak	Tidak
Pekerja kantor (antivirus Cyber Protect)	Iya	Tidak	Tidak
Cyber Protect Essentials (hanya untuk Cyber Protect edisi Essentials)	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

Set fitur	Windows	Linux	macOS
Cadangan forensik			
Mengumpulkan timbunan memori mentah	Iya	Tidak	Tidak
Snapshot proses yang sedang berjalan	Iya	Tidak	Tidak
Notarisasi cadangan forensik citra lokal	Iya	Tidak	Tidak
Notarisasi cadangan forensik citra awan	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

© Acronis International GmbH, 2003-2024

Fitur	Windows	Linux	macOS
Perlindungan data berkelanjutan (CDP)			
CDP untuk file dan folder	Iya	Tidak	Tidak
CDP untuk file yang diubah melalui jalur aplikasi	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

Set fitur	Windows	Linux	macOS
Penemuan otomatis dan instalasi jarak jauh			
Penemuan berbasis jaringan	Iya	Tidak	Tidak
Penemuan berbasis Active Directory	Iya	Tidak	Tidak
Penemuan berbasis templat (mengimpor mesin dari file)	Iya	Tidak	Tidak
Penambahan perangkat manual	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

Set fitur	Windows	Linux	macOS
Active Protection			
Deteksi injeksi proses	Iya	Tidak	Tidak
Pemulihan otomatis file yang terpengaruh dari cache lokal	Iya	Iya	Iya
Pertahanan diri untuk file cadangan Acronis	Iya	Tidak	Tidak
Pertahanan diri untuk perangkat lunak Acronis	Iya	Tidak	Iya (Hanya Active Protection dan komponen antimalware)
Manajemen proses tepercaya/terblokir	Iya	Tidak	Iya
Pengecualian proses/folder	Iya	Iya	Iya
Deteksi ransomware berdasarkan perilaku proses (berbasis AI)	Iya	Iya	Iya
Deteksi proses cryptomining berdasarkan perilaku proses	Iya	Tidak	Tidak

© Acronis International GmbH, 2003-2024

Set fitur	Windows	Linux	macOS
Active Protection			
Proteksi drive eksternal (HDD, flash drive, kartu SD)	Iya	Tidak	Iya
Perlindungan folder jaringan	Iya	Iya	Iya
Perlindungan sisi server	Iya	Tidak	Tidak
Perlindungan untuk Zoom, Cisco Webex, Citrix Workspace, dan Microsoft Teams	Iya	Tidak	Tidak
Untuk informasi selengkapnya tentang sistem operasi yang didukung dan versinya, lihat "Platform yang didukung" (hlm. 814).			

Set fitur	Windows	Linux	macOS
Perlindungan Antivirus and Antimalware			
Fungsionalitas Active Protection yang terintegrasi penuh	Iya	Tidak	Tidak
Proteksi antimalware waktu nyata	Iya	Ya, dengan paket Advanced Antimalware	Ya, dengan paket Advanced Antimalware
Perlindungan antimalware waktu nyata tingkat lanjut dengan deteksi berbasis tanda tangan lokal	Iya	Iya	Iya
Analisis statik untuk file portable yang dapat dieksekusi	Iya	Tidak	Iya*
Pemindaian antimalware sesuai permintaan	Iya	Iya**	Iya
Perlindungan folder jaringan	Iya	Iya	Tidak
Perlindungan sisi server	Iya	Tidak	Tidak
Pindai file arsip	Iya	Tidak	Iya
Pindai drive yang dapat dilepas	Iya	Tidak	Iya
Pindai file baru dan yang diubah saja	Iya	Tidak	Iya
Pengecualian file/folder	Iya	Iya	Iya***
Pengecualian proses	Iya	Tidak	Iya
Mesin analisis perilaku	Iya	Tidak	Iya

© Acronis International GmbH, 2003-2024

Set fitur	Windows	Linux	macOS
Perlindungan Antivirus and Antimalware			
Pencegahan eksploit	Iya	Tidak	Tidak
Karantina	Iya	Iya	Iya
Pembersihan otomatis karantina	Iya	Iya	Iya
Pemfilteran URL (http/https)	Iya	Tidak	Tidak
Daftar putih seluruh perusahaan	Iya	Tidak	Iya
Manajemen firewall****	Iya	Tidak	Tidak
Manajemen Microsoft Defender Antivirus*****	Iya	Tidak	Tidak
Manajemen Microsoft Security Essentials	Iya	Tidak	Tidak
Mendaftarkan dan mengelola perlindungan Antivirus dan Antimalware melalui Windows Security Center	Iya	Tidak	Tidak
Untuk informasi selengkapnya tentang sistem operasi yang didukung dan versinya, lihat "Platform yang didukung" (hlm. 814).			

* Analisis statis untuk file portabel yang dapat dieksekusi hanya didukung untuk pemindaian terjadwal pada macOS.

** Persyaratan mulai tidak didukung untuk pemindaian sesuai permintaan di Linux.

*** Pengecualian file/folder hanya didukung jika Anda menentukan file dan folder yang tidak akan dipindai oleh perlindungan waktu nyata atau pemindaian terjadwal pada macOS.

**** Manajemen firewall didukung di Windows 8 dan yang lebih baru. Windows Server tidak didukung.

***** Manajemen Microsoft Defender Antivirus didukung di Windows 8.1 dan yang lebih baru.

Set fitur	Windows	Linux	macOS
Penilaian kerentanan			
Penilaian kerentanan sistem operasi dan aplikasi aslinya	Iya	Iya******	Iya
Penilaian kerentanan untuk aplikasi pihak ketiga	Iya	Tidak	Iya
Untuk informasi selengkapnya tentang sistem operasi yang didukung dan versinya, lihat "Produk Microsoft dan produk pihak ketiga yang didukung" (hlm. 951), "Produk Linux yang didukung" (hlm. 953), dan "Produk Apple dan pihak ketiga yang didukung" (hlm. 952).			

© Acronis International GmbH, 2003-2024

****** Penilaian kerentanan bergantung pada ketersediaan penasehat keamanan resmi untuk distribusi tertentu, misalnya https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce, dan lainnya.

Set fitur	Windows	Linux	macOS
Manajemen patch			
Persetujuan otomatis patch	Iya	Tidak	Tidak
Instalasi otomatis patch	Iya	Tidak	Tidak
Pengujian patch	Iya	Tidak	Tidak
Instalasi patch manual	Iya	Tidak	Tidak
Penjadwalan patch	Iya	Tidak	Tidak
Patch aman yang gagal: cadangan mesin sebelum menginstal patch sebagai bagian dari rencana proteksi	Iya	Tidak	Tidak
Pembatalan boot ulang mesin jika pencadangan sedang berjalan	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

Fitur	Windows	Linux	macOS
Peta perlindungan data			
Definisi file penting yang dapat disesuaikan	Iya	Tidak	Tidak
Memindai mesin untuk menemukan file yang tidak terlindungi	Iya	Tidak	Tidak
Gambaran umum lokasi yang tidak terlindungi	Iya	Tidak	Tidak
Kemampuan untuk memulai tindakan perlindungan dari widget peta perlindungan Data (tindakan **Lindungi semua file**)	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

Set fitur	Windows	Linux	macOS
Kesehatan disk			
Kontrol kesehatan HDD dan SSD berbasis AI	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

© Acronis International GmbH, 2003-2024

Fitur	Windows	Linux	macOS
Rencana proteksi pintar berdasarkan peringatan Pusat Operasi Perlindungan Cyber Acronis (CPOC)			
Umpan ancaman	Iya	Tidak	Tidak
Wizard perbaikan	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

Set fitur	Windows	Linux	macOS
Pemindaian cadangan			
Pemindaian antimalware cadangan profil sebagai bagian dari rencana pencadangan	Iya	Tidak	Tidak
Pemindaian cadangan profil untuk malware di awan	Iya	Tidak	Tidak
Pemindaian malware terhadap cadangan terenkripsi	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

Set fitur	Windows	Linux	macOS
Pemulihan aman			
Pemindaian Antimalware dengan perlindungan Antivirus dan Antimalware selama proses pemulihan	Iya	Tidak	Tidak
Pemulihan aman untuk cadangan terenkripsi	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

Set fitur	Windows	Linux	macOS
Koneksi desktop jarak jauh			
Koneksi melalui NEAR	Iya	Iya	Iya
Koneksi melalui RDP	Iya	Tidak	Tidak
Koneksi melalui Berbagi Layar Apple	Tidak	Tidak	Iya
Koneksi melalui klien web	Iya	Tidak	Tidak
Koneksi melalui Bantuan Cepat	Iya	Iya	Iya
Bantuan jarak jauh	Iya	Iya	Iya

© Acronis International GmbH, 2003-2024

Set fitur	Windows	Linux	macOS
Koneksi desktop jarak jauh			
Transfer file	Iya	Iya	Iya
Transmisi tangkapan layar	Iya	Iya	Iya
Untuk informasi selengkapnya tentang sistem operasi yang didukung dan versinya, lihat "Platform yang didukung" (hlm. 988).			

Set fitur	Windows	Linux	macOS
Skor #CyberFit			
Status Skor #CyberFit	Iya	Tidak	Tidak
Alat bantu mandiri Skor #CyberFit	Iya	Tidak	Tidak
Rekomendasi Skor #CyberFit	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

Set fitur	Windows	Linux	macOS
Pencegah kehilangan data			
Kontrol perangkat	Iya	Tidak	Didukung pada Macs dengan prosesor Intel yang menjalankan macOS 10.15 dan lebih baru atau macOS 11.2.3 atau lebih baru. Tidak didukung pada prosesor Apple silicon berbasis ARM, seperti Apple M1 / M2.
Advanced Data Loss Prevention	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44).			

© Acronis International GmbH, 2003-2024

Set fitur	Windows	Linux	macOS
Opsi manajemen			
Skenario penjualan lebih tinggi untuk mempromosikan edisi Cyber Protect	Iya	Iya	Iya
Konsol manajemen jarak jauh dan terpusat berbasis web	Iya	Iya	Iya
Sistem operasi dan versi yang didukung: Platform independen.			

Set fitur	Windows	Linux	macOS
Opsi perlindungan			
Penghapusan jarak jauh	Iya	Tidak	Tidak
Didukung untuk Windows 10 dan versi lebih baru.			

Set fitur	Windows	Linux	macOS
Monitor			
Aplikasi Cyber Protect	Iya	Tidak	Iya
Status proteksi untuk Zoom	Iya	Tidak	Tidak
Status proteksi untuk Cisco Webex	Iya	Tidak	Tidak
Status proteksi untuk Citrix Workspace	Iya	Tidak	Tidak
Status proteksi untuk Microsoft Teams	Iya	Tidak	Tidak
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44). Di macOS, Cyber Protect Monitor didukung untuk semua versi tempat Anda dapat menginstal Agen untuk Mac. Untuk informasi lebih lanjut, lihat "Agen untuk Mac" (hlm. 28).			

Set fitur	Windows	Linux	macOS
Inventaris perangkat lunak			
Pemindaian inventaris perangkat lunak	Iya	Tidak	Iya
Pemantauan inventaris perangkat lunak	Iya	Tidak	Iya
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44). Di macOS, Inventaris perangkat keras didukung untuk versi 10.13.x − 13.x.			

© Acronis International GmbH, 2003-2024

Set fitur	Windows	Linux	macOS
Inventaris perangkat keras			
Pemindaian inventaris perangkat keras	Iya	Tidak	Iya
Pemantauan inventaris perangkat keras	Iya	Tidak	Iya
Lihat versi Windows yang didukung di "Sistem operasi dan versi yang didukung" (hlm. 44). Di macOS, Inventaris perangkat keras didukung untuk versi 10.13.x − 13.x.			

Sistem file yang didukung

Agen perlindungan dapat mencadangkan sistem file apa pun yang dapat diakses dari sistem operasi tempat agen diinstal. Misalnya, Agen untuk Windows dapat mencadangkan dan memulihkan sistem file ext4 jika driver yang sesuai diinstal di Windows.

Tabel berikut merangkum sistem file yang dapat dicadangkan dan dipulihkan (media yang dapat di-boot hanya mendukung pemulihan). Pembatasan berlaku untuk agen dan media yang dapat di-boot.

Sistem file	Didukung oleh			Pembatasan
	Agen	Media yang dapat di-boot untuk Windows dan Linux	Media yang dapat di-boot untuk Mac	
FAT16/32	Semua agen	+	+	Tidak ada pembatasan
NTFS	Semua agen	+	+	
ext2/ext3/ext4	Semua agen	+	-	
HFS+	Agen untuk Mac	-	+	
APFS	Agen untuk Mac	-	+	• Didukung mulai dengan macOS High Sierra 10.13 • Konfigurasi disk harus dibuat ulang secara manual ketika memulihkan ke mesin non-asli atau bare metal.

© Acronis International GmbH, 2003-2024

Sistem file	Didukung oleh			Pembatasan
	Agen	Media yang dapat di-boot untuk Windows dan Linux	Media yang dapat di-boot untuk Mac	
JFS	Agen untuk Linux	+	-	• Filter file (Penyertaan/Pengecualian) tidak didukung • Pencadangan inkremental/diferensial cepat tidak dapat diaktifkan
ReiserFS3	Agen untuk Linux	+	-	
ReiserFS4	Agen untuk Linux	+	-	• Filter file (Penyertaan/Pengecualian) tidak didukung • Pencadangan inkremental/diferensial cepat tidak dapat diaktifkan • Volume tidak dapat diubah ukurannya selama pemulihan
ReFS	Semua agen	+	+	• Filter file (Penyertaan/Pengecualian) tidak didukung • Pencadangan inkremental/diferensial cepat tidak dapat diaktifkan • Volume tidak dapat diubah ukurannya selama pemulihan • Selama pemulihan file dari cadangan ReFS, hanya isi yang dipulihkan. Daftar kontrol akses (ACL) dan aliran alternatif tidak dipulihkan. File jarang dipulihkan sebagai file biasa.
XFS	Semua agen	+	+	• Filter file (Penyertaan/Pengecualian) tidak didukung • Pencadangan inkremental/diferensial cepat tidak dapat diaktifkan

© Acronis International GmbH, 2003-2024

Sistem file	Didukung oleh			Pembatasan
	Agen	**Media yang dapat di-boot untuk Windows dan Linux**	**Media yang dapat di-boot untuk Mac**	
				• Volume tidak dapat diubah ukurannya selama pemulihan • Mode cadangan bertahap cepat tidak didukung untuk sistem file XFS. Cadangan bertahap dan diferensial volume XFS ke awan mungkin secara signifikan lebih lambat dibandingkan cadangan ext4 yang menggunakan mode cadangan bertahap cepat.
Linux swap	Agen untuk Linux	+	-	Tidak ada pembatasan
exFAT	Semua agen	+ Media yang dapat di-boot tidak dapat digunakan untuk pemulihan jika cadangan *disimpan di* exFAT	+	• Hanya cadangan disk/volume yang didukung • Filter file (Penyertaan/Pengecualian) tidak didukung • File individual tidak dapat dipulihkan dari cadangan

Perangkat lunak secara otomatis beralih ke mode sektor per sektor ketika mencadangkan drive dengan sistem file yang tidak dikenal atau tidak didukung (misalnya, Btrfs). Pencadangan sektor per sektor dimungkinkan untuk sistem file apa pun yang:

- berbasis blok
- menjangkau disk tunggal
- memiliki skema partisi MBR/GPT standar

Jika sistem file tidak memenuhi persyaratan tersebut, pencadangan akan gagal.

© Acronis International GmbH, 2003-2024

Deduplikasi Data

Di Windows Server 2012 dan yang lebih baru, Anda dapat mengaktifkan fitur Deduplikasi Data untuk volume NTFS. Deduplikasi Data mengurangi ruang yang digunakan pada volume dengan menyimpan fragmen duplikat hanya dari file volume.

Anda dapat mencadangkan dan memulihkan volume yang dideduplikasi–yang diaktifkan pada tingkat disk, tanpa pembatasan. Cadangan tingkat file didukung, kecuali saat menggunakan Acronis VSS Provider. Untuk memulihkan file dari cadangan disk, jalankan mesin virtual dari cadangan Anda, atau pasang cadangan pada mesin yang menjalankan Windows Server 2012 atau lebih baru, dan kemudian salin file dari volume terpasang.

Fitur Deduplikasi Data Windows Server tidak terkait dengan fitur Deduplikasi Cadangan Acronis.

Operasi yang didukung dengan volume logis

Pencadangan dan pemulihan beban kerja dengan volume logis, seperti LDM di Windows (disk dinamis) dan LVM di Linux, didukung dengan batasan-batasan berikut.

Cadangan

Backup berbasis agen adalah backup yang dibuat oleh agen perlindungan yang diinstal pada beban kerja atau oleh media yang dapat di-boot.

Cadangan tanpa agen hanya tersedia untuk mesin virtual. Cadangan tanpa agen dilakukan pada level hypervisor oleh agen yang dapat mencadangkan dan memulihkan semua mesin virtual di lingkungan tersebut. Tidak ada agen individu yang diinstal pada mesin virtual yang dilindungi.

Untuk informasi selengkapnya tentang perbedaan antara cadangan berbasis agen dan tanpa agen, lihat "Pencadangan berbasis agen dan tanpa agen" (hlm. 65).

Cadangan berbasis agen	Cadangan tanpa agen
• Volume logis didukung pada basis per volume. • Filter file (Penyertaan/Pengecualian) didukung.	• Ketika volume logis terdeteksi pada disk, disk tersebut dicadangkan dalam mode sektor demi sektor (RAW). Struktur partisi dari disk tidak dianalisis dan tidak ada citra volume yang disimpan secara terpisah. • Volume LDM atau LVM individu tidak dapat dipilih sebagai sumber cadangan - baik dengan seleksi langsung maupun dengan menggunakan aturan kebijakan. Hanya **Mesin keseluruhan** yang tersedia di bagian **Apa yang harus dicadangkan** dari rencana proteksi. • Filter file (Inklusi/Eksklusi) tidak didukung. Setiap inklusi atau eksklusi yang dikonfigurasi akan diabaikan.

© Acronis International GmbH, 2003-2024

Pemulihan

Pemulihan berbasis agen adalah pemulihan yang dilakukan oleh agen yang diinstal pada beban kerja atau oleh media yang dapat di-boot.

Pemulihan tanpa agen hanya mendukung mesin virtual sebagai target. Pemulihan tanpa agen dilakukan pada level hypervisor oleh agen yang dapat mencadangkan dan memulihkan semua mesin virtual dalam lingkungan tersebut. Anda tidak perlu secara manual membuat mesin target tempat cadangan dipulihkan.

	Dari cadangan berbasis agen	**Dari cadangan tanpa agen**
Pemulihan berbasis agen	• Pemulihan per-volume tersedia. • Pemulihan file dan folder tersedia.	• Pemulihan per-volume tidak tersedia. • Pemulihan file dan folder tersedia.
Pemulihan tanpa agen	• Migrasi mesin (P2V, V2P, dan V2V) tidak didukung. Untuk memulihkan data dari cadangan berbasis agen, gunakan media yang dapat di-boot. • Operasi **Jalankan sebagai VM** tidak mendapatkan dukungan. • Pemulihan file dan folder tersedia.	• Pemulihan per-volume tidak tersedia. • Pemulihan mesin secara keseluruhan tersedia. • Pemulihan file dan folder tersedia. • Operasi **Jalankan sebagai VM** didukung. Untuk membuat mesin virtual dapat di-boot, Anda mungkin perlu mengubah urutan boot. Untuk informasi lebih lanjut, lihat artikel Basis Pengetahuan ini. • Konversi ke jenis-jenis mesin virtual berikut ini didukung: ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ Scale Computing HC3

© Acronis International GmbH, 2003-2024

Menginstal dan menyebarkan agen Cyber Protection

Persiapan

Langkah 1

Pilih agen, tergantung pada apa yang akan Anda cadangkan. Untuk informasi lebih lanjut tentang kemungkinan pilihan, lihat Agen mana yang saya perlukan?

Langkah 2

Pastikan bahwa ada cukup ruang bebas di hard drive Anda untuk menginstal agen. Untuk informasi mendetail tentang ruang yang diperlukan, lihat "Persyaratan sistem untuk agen" (hlm. 65).

Langkah 3

Unduh program penyiapan. Untuk menemukan tautan unduhan, klik **Semua perangkat** > **Tambah**.

Halaman **Tambah peranti** menyediakan penginstal web untuk setiap agen yang diinstal di Windows. Penginstal web adalah file kecil yang dapat dieksekusi untuk mengunduh program penyiapan utama dari Internet dan menyimpannya sebagai file sementara. File ini akan langsung dihapus setelah instalasi.

Jika Anda ingin menyimpan program penyiapan secara lokal, unduh paket yang berisi semua agen untuk instalasi di Windows menggunakan tautan di bagian bawah halaman **Tambah peranti**. Tersedia paket 32-bit dan 64-bit. Paket tersebut memungkinkan Anda untuk menyesuaikan daftar komponen yang akan diinstal. Paket tersebut juga memungkinkan instalasi tanpa pengawasan, misalnya, melalui Kebijakan Grup. Skenario lanjutan ini dijelaskan di bagian "Menyebarkan agen melalui Kebijakan Grup" (hlm. 167).

Untuk mengunduh program penyiapan Agen untuk Microsoft 365, klik ikon akun di sudut kanan atas, lalu klik **Unduhan** > **Agen untuk Microsoft 365**.

Instalasi di Linux dan macOS dilakukan dari program penyiapan biasa.

Semua program penyiapan memerlukan koneksi Internet untuk mendaftarkan mesin di layanan Cyber Protection. Jika tidak ada koneksi Internet, instalasi akan gagal.

Langkah 4

Fitur Cyber Protect memerlukan Microsoft Visual C++ 2017 Redistributable. Harap pastikan bahwa ini sudah diinstal di mesin Anda atau installah sebelum menginstal agen. Setelah instalasi Microsoft Visual C++, mulai ulang mungkin perlu dilakukan. Anda dapat menemukan paket Microsoft Visual

© Acronis International GmbH, 2003-2024

C++ Redistributable di sini https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Langkah 5

Verifikasi bahwa firewall dan komponen lain dari sistem keamanan jaringan Anda (seperti server proksi) memungkinkan koneksi masuk dan keluar melalui port TCP berikut.

- Port **443** dan **8443**

  Port ini digunakan untuk mengakses konsol Cyber Protect, mendaftarkan agen, mengunduh sertifikat, otorisasi pengguna, dan mengunduh file dari penyimpanan awan.
- Port dalam rentang **7770** – **7800**

  Agen menggunakan port ini untuk berkomunikasi dengan server manajemen.
- Port **44445** dan **55556**

  Agen menggunakan port ini untuk transfer data selama pencadangan dan pemulihan.

Jika server proxy diaktifkan di jaringan Anda, lihat "Mengonfigurasi pengaturan server proxy" (hlm. 71) untuk memahami apakah Anda perlu mengonfigurasi pengaturan ini di setiap mesin yang menjalankan agen proteksi.

Kecepatan koneksi internet minimum yang diperlukan untuk mengelola agen dari awan adalah 1 Mbit/s (jangan bingung dengan kecepatan transfer data yang dapat diterima untuk mencadangkan ke awan). Pertimbangkan hal ini jika Anda menggunakan teknologi koneksi bandwidth rendah seperti ADSL.

Port TCP yang diperlukan untuk pencadangan dan replikasi mesin virtual VMware

- Port **443**

  Agen untuk VMware (Windows dan Alat Virtual) menghubungkan ke port ini pada host ESXi/server vCenter untuk melakukan operasi manajemen VM, seperti membuat, memperbarui, dan menghapus VM pada vSphere selama operasi pencadangan, pemulihan, dan replikasi VM.
- Port **902**

  Agen untuk VMware (Windows dan Alat Virtual) menghubungkan ke port ini pada host ESXi untuk membuat sambungan NFC guna membaca/menulis data pada disk VM selama operasi pencadangan, pemulihan, dan replikasi VM.
- Port **3333**

  Jika Agen untuk VMware (Alat Virtual) berjalan pada host/klaster ESXi yang merupakan target untuk replikasi VM, lalu lintas replikasi VM tidak bergerak secara langsung ke host ESXi pada port **902**. Lalu lintas justru bergerak dari sumber Agen untuk VMware ke port TCP **3333** pada Agen untuk VMware (Alat Virtual) yang terletak di host/klaster ESXi target.

  Agen untuk VMware sumber yang membaca data dari disk VM asli dapat berada di mana pun dan dapat dalam tipe apa pun: Peralatan Virtual atau Windows.

© Acronis International GmbH, 2003-2024

Layanan yang bertanggung jawab untuk menerima data replikasi VM pada Agen untuk VMware (Peralatan Virtual) target disebut “Server disk replika.” Layanan ini bertanggung jawab atas teknik optimalisasi WAN, seperti kompresi lalu lintas dan deduplikasi selama replikasi VM, termasuk seeding replika (lihat Seeding replika awal). Jika tidak ada Agent untuk VMware (Peralatan Virtual) yang berjalan di host ESXi target, layanan ini menjadi tidak tersedia, sehingga skenario seeding replika tidak didukung.

Port yang dibutuhkan oleh komponen Downloader

Komponen Downloader bertanggung jawab untuk mengirimkan pembaruan ke komputer dan mendistribusikannya ke instance Downloader lainnya. Ini dapat berjalan dalam mode agen yang mengubah komputer menjadi agen Downloader. Agen Downloader mengunduh pembaruan dari internet dan bertindak sebagai sumber distribusi pembaruan ke komputer lain. Downloader membutuhkan port berikut untuk beroperasi.

- Port TCP dan UDP (masuk) **6888**
  Digunakan oleh protokol BitTorrent untuk pembaruan antar-pasangan torrent.
- Port UDP **6771**
  Digunakan sebagai port penemuan pasangan lokal. Juga mengambil bagian dalam pembaruan antar-pasangan.
- Port TCP **18018**
  Digunakan untuk komunikasi antara updater yang bekerja dalam mode berbeda: Updater dan UpdaterAgent.
- Port TCP **18019**
  Port lokal, digunakan untuk komunikasi antara Updater dan agen proteksi.

Langkah 6

Pada mesin tempat Anda berencana untuk menginstal agen proteksi, verifikasi bahwa port lokal berikut tidak digunakan oleh proses lain.

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

Catatan
Anda tidak perlu membukanya di firewall.

Mengganti port yang digunakan oleh agen proteksi

Beberapa port yang diperlukan oleh agen proteksi mungkin digunakan oleh aplikasi lain dalam lingkungan Anda. Untuk menghindari konflik, Anda dapat mengubah port default yang digunakan oleh agen proteksi dengan memodifikasi file-file berikut ini.

© Acronis International GmbH, 2003-2024

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

Agen mana yang saya perlukan?

Memilih agen tergantung pada apa yang akan Anda cadangkan. Tabel di bawah ini meringkas informasi, untuk membantu Anda membuat keputusan.

Di Windows, Agen untuk Exchange, Agen untuk SQL, Agen untuk Active Directory, dan Agen untuk Oracle memerlukan bahwa Agen untuk Windows juga diinstal. Jadi, jika Anda menginstal, misalnya, Agen untuk SQL, Anda juga akan dapat mencadangkan seluruh mesin tempat agen diinstal.

Kami menyarankan Anda juga menginstal Agen untuk Windows ketika Anda menginstal Agen untuk VMware (Windows) dan Agen untuk Hyper-V.

Di Linux, Agen untuk Oracle, Agen untuk MySQL/MariaDB, dan Agen untuk Virtuozzo mengharuskan Agen untuk Linux (64-bit) juga diinstal. Agen-agen ini disatukan ke dalam file penyetelan Agen untuk Linux (64-bit).

Apa yang akan Anda cadangkan?	Agen mana yang akan diinstal?	Di mana akan menginstalnya?
Mesin fisik		
Mesin fisik yang menjalankan Windows	Agen untuk Windows	Di mesin yang akan dicadangkan.
Mesin fisik yang menjalankan Linux	Agen untuk Linux	
Mesin fisik yang menjalankan macOS	Agen untuk Mac	
Database		
Database SQL	Agen untuk SQL	Di mesin yang menjalankan Microsoft SQL Server.
Database MySQL	Agen untuk MySQL/MariaDB (Disatukan ke dalam file penyetelan Agen untuk Linux (64-bit))	Pada mesin yang menjalankan MySQL Server.
Database MariaDB	Agen untuk MySQL/MariaDB	Pada mesin yang menjalankan MariaDB Server.

© Acronis International GmbH, 2003-2024

	(Disatukan ke dalam file penyetelan Agen untuk Linux (64-bit))	
Basis data Exchange	Agen untuk Exchange	Pada mesin yang menjalankan peran Kotak surat Microsoft Exchange Server.*
Database Oracle	Agen untuk Oracle (Di Linux, disatukan ke dalam file penyetelan Agen untuk Linux (64-bit))	Pada mesin yang menjalankan Database Oracle.
Beban kerja awan-ke-awan		
Kotak surat Microsoft 365 (Agen cloud dan agen lokal)	Agen cloud (Instalasi tidak diperlukan)	Fungsi ini tersedia dengan agen cloud yang disebarkan dalam pusat data. Untuk informasi lebih lanjut, lihat "Menggunakan versi awan Agen untuk Microsoft 365" (hlm. 605).
	Agen untuk Office 365	Di mesin Windows yang terhubung ke Internet. Untuk informasi lebih lanjut, lihat "Menggunakan Agen untuk Office 365 yang diinstal secara lokal" (hlm. 601).
File Microsoft 365 OneDrive dan situs SharePoint Online	Agen cloud (Instalasi tidak diperlukan)	Fungsi ini tersedia dengan agen cloud yang disebarkan dalam pusat data. Untuk informasi lebih lanjut, lihat "Menggunakan versi

© Acronis International GmbH, 2003-2024

		awan Agen untuk Microsoft 365" (hlm. 605).
Kotak surat Gmail Google Workspace, file Google Drive, dan file drive Shared	Agen cloud (Instalasi tidak diperlukan)	Fungsi ini tersedia dengan agen cloud yang disebarkan dalam pusat data. Untuk informasi lebih lanjut, lihat "Melindungi data Google Workspace" (hlm. 638).
Active Directory		
Mesin yang menjalankan Active Directory Domain Services	Agen untuk Active Directory	Pada pengontrol domain.
Mesin virtual		
Mesin virtual VMware ESXi	Agen untuk VMware (Windows)	Pada mesin Windows yang memiliki akses jaringan ke vCenter Server dan ke penyimpanan mesin virtual.**
	Agen untuk VMware (Virtual Appliance)	Pada host ESXi.
Mesin virtual Hyper-V	Agen untuk Hyper-V	Pada host Hyper-V.
Mesin virtual Scale Computing HC3	Agen untuk Scale Computing HC3 (Alat Virtual)	Di host Scale Computing HC3.
Mesin virtual Red Hat Virtualization (dikelola oleh oVirt)	Agen untuk oVirt (Alat Virtual)	Di host Red Hat Virtualization.
Mesin virtual dan kontainer Virtuozzo***	Agen untuk Virtuozzo (Disatukan ke dalam file penyetelan Agen untuk Linux (64-bit))	Pada host Virtuozzo.

© Acronis International GmbH, 2003-2024

Mesin virtual Virtuozzo Hybrid Infrastructure	Agen untuk Virtuozzo Hybrid Infrastructure (Alat Virtual)	Di host Virtuozzo Hybrid Infrastructure.
Mesin virtual yang dihosting di Amazon EC2	Sama halnya untuk mesin fisik****	Di mesin yang akan dicadangkan.
Mesin virtual yang dihosting di Windows Azure		
Mesin virtual Citrix XenServer		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
Mesin Virtual berbasis kernel (KVM), tidak dikelola oleh oVirt		
Mesin virtual Oracle, tidak dikelola oleh oVirt		
Mesin virtual Nutanix AHV		
Red Hat Virtualization (RHV/RHEV), dikelola oleh oVirt	Agen untuk oVirt (Alat Virtual)	Di host virtualisasi.
Mesin Virtual berbasis kernel (KVM), dikelola oleh oVirt		
Mesin virtual Oracle, dikelola oleh oVirt		
Perangkat seluler		
Perangkat seluler yang menjalankan Android	Aplikasi seluler untuk Android	Di perangkat seluler yang akan dicadangkan.
Perangkat seluler yang menjalankan iOS	Aplikasi seluler untuk iOS	

*Selama instalasi, Agen untuk Exchange memeriksa ruang kosong yang memadai di mesin yang akan menjalankannya. Ruang kosong yang setara dengan 15% dari Database Exchange terbesar diperlukan untuk sementara waktu selama pemulihan granular.

**Jika ESXi Anda menggunakan penyimpanan yang terpasang SAN, instal agen pada mesin yang terhubung ke SAN yang sama. Agen akan mencadangkan mesin virtual langsung dari penyimpanan, bukan melalui host ESXi dan LAN. Untuk petunjuk terperinci, lihat "Agen untuk VMware - pencadangan tanpa LAN" (hlm. 686).

***Untuk Virtuozzo 7, hanya kontainer ploop yang didukung. Mesin virtual tidak didukung.

****Mesin virtual dianggap virtual jika dicadangkan oleh agen eksternal. Jika agen diinstal di sistem tamu, operasi pencadangan dan pemulihan akan sama dengan mesin fisik. Akan tetapi, jika Cyber Protection dapat mengidentifikasi suatu mesin virtual menggunakan instruksi CPUID, kuota layanan mesin virtual akan ditetapkan padanya. Jika Anda menggunakan passthrough langsung atau opsi lain yang menerapkan mask pada ID pabrik CPU, hanya kuota layanan untuk mesin fisik yang dapat ditetapkan.

© Acronis International GmbH, 2003-2024

Pencadangan berbasis agen dan tanpa agen

Backup berbasis agen membutuhkan agen perlindungan yang diinstal pada setiap mesin yang dilindungi. Backup berbasis agen didukung pada semua mesin fisik dan mesin virtual. Untuk informasi lebih lanjut tentang agen apa yang Anda butuhkan dan di mana menginstalnya, lihat "Agen mana yang saya perlukan?" (hlm. 61)

Backup tanpa agen didukung oleh beberapa platform virtualisasi dan tidak tersedia untuk mesin fisik. Backup tanpa agen hanya memerlukan satu agen perlindungan, yang diinstal pada mesin khusus di lingkungan virtual. Agen ini mencadangkan semua mesin virtual lainnya di lingkungan ini. Untuk informasi lebih lanjut tentang jenis backup yang didukung per platform virtualisasi, lihat "Platform virtualisasi yang didukung" (hlm. 32).

Untuk beberapa platform virtualisasi, peralatan virtual tersedia. Alat virtual (Virtual Appliance/VA) adalah mesin virtual siap pakai yang berisi agen perlindungan. Alat virtual tersedia dalam format khusus hypervisor, seperti .ovf, .ova, atau .qcow.

Jenis cadangan apa yang saya perlukan?

Kami merekomendasikan cadangan berbasis agen jika Anda membutuhkan hal berikut:

- Fungsi perlindungan tambahan, seperti antivirus dan antimalware, manajemen patch, atau koneksi desktop jarak jauh. Untuk informasi lebih lanjut tentang fitur-fitur ini, lihat "Fitur perlindungan yang didukung oleh sistem operasi" (hlm. 44).
- Pisahkan mesin virtual pada level penyewa. Misalnya, karena Anda ingin memberikan akses kepada pengguna di penyewa, yang hanya bisa digunakan ke cadangan mereka sendiri.
- Cadangan tingkat file yang dapat Anda pulihkan ke sistem operasi tamu.

Kami merekomendasikan cadangan tanpa agen jika Anda membutuhkan hal berikut:

- Hanya cadangan, tanpa fitur perlindungan tambahan.
- Pengelolaan yang disederhanakan—Anda dapat mencadangkan beberapa mesin virtual, cukup dengan menginstal dan mengkonfigurasi satu agen.
- Penggunaan sumber daya minimal—satu agen khusus menggunakan lebih sedikit CPU dan RAM dibandingkan dengan beberapa agen yang diinstal pada setiap mesin virtual di lingkungan Anda.
- Pengaturan cadangan spesifik, seperti cadangan LAN-free. Untuk informasi lebih lanjut tentang fitur ini, lihat "Agen untuk VMware - pencadangan tanpa LAN" (hlm. 686).
- Lebih sedikit overhead konfigurasi. Agen khusus mencadangkan mesin virtual pada level hypervisor, tanpa mempertimbangkan sistem operasi tamu.

Persyaratan sistem untuk agen

Agen	Ruang disk diperlukan untuk instalasi

© Acronis International GmbH, 2003-2024

Agen untuk Windows	1,2 GB
Agen untuk Linux	2 GB
Agen untuk Mac	1 GB
Agen untuk SQL dan Agen untuk Windows	1,2 GB
Agen untuk Exchange dan Agen untuk Windows	1,3 GB
Agen untuk Pencegahan Kebocoran Data	500 MB
Agen untuk Microsoft 365	500 MB
Agen untuk Active Directory dan Agen untuk Windows	2 GB
Agen untuk VMware dan Agen untuk Windows	1,5 GB
Agen untuk Hyper-V dan Agen untuk Windows	1,5 GB
Agen untuk Virtuozzo dan Agen untuk Linux	1 GB
Agen untuk Virtuozzo Hybrid Infrastructure	700 MB
Agen untuk Oracle dan Agen untuk Windows	2,2 GB
Agen untuk Oracle dan Agen untuk Linux	2 GB
Agen untuk MySQL/MariaDB dan Agen untuk Linux	2 GB

Operasi pencadangan, termasuk menghapus cadangan, membutuhkan sekitar 1 GB RAM per 1 TB ukuran cadangan. Konsumsi memori dapat bervariasi, tergantung jumlah dan jenis data yang diproses oleh agen.

Catatan
Penggunaan RAM dapat meningkat saat mencadangkan ke set cadangan ekstra besar (4 TB dan lebih banyak lagi).

Pada sistem x64, operasi dengan media yang dapat di-boot atau pemulihan disk dengan mulai ulang membutuhkan setidaknya 2 GB memori.

Di beban kerja dengan prosesor modern, seperti Intel Core Gen ke-11 atau AMD Ryzen 7, yang mendukung teknologi CET, sebagian fitur Agen untuk Pencegahan Kebocoran Data dinonaktifkan demi mencegah terjadinya konflik. Tabel berikut mencantumkan ketersediaan fitur Kontrol Perangkat dan Advanced DLP pada sistem yang memiliki CPU tersebut.

Fitur	Kontrol Perangkat	Advanced DLP

© Acronis International GmbH, 2003-2024

Saluran lokal		
Penyimpanan yang dapat dilepas	n/a	Iya
Penyimpanan yang dapat dilepas dan dienkripsi	Iya	n/a
Printer	n/a	Tidak
Drive yang dipetakan dan dialihkan	n/a	Iya
Papan klip yang dialihkan	n/a	Tidak
Komunikasi jaringan		
Email SMTP	n/a	Iya
Microsoft Outlook (MAPI)	n/a	Iya
Catatan IBM	n/a	Tidak
Webmails	n/a	Iya
Layanan pesan instan (ICQ)	n/a	Tidak
Layanan pesan instan (Viber)	n/a	Tidak
Layanan pesan instan (IRC, Jabber, Skype, Viber)	n/a	Iya
Layanan berbagi file	n/a	Iya
Jejaring sosial	n/a	Iya
Berbagi file jaringan lokal (SMB)	n/a	Iya
Akses web (HTTP/HTTPS)	n/a	Iya
Transfer file (FTP/FTPS)	n/a	Iya
Pembuatan daftar izin transfer data		
Daftar izin untuk tipe perangkat	n/a	Iya
Daftar izin untuk komunikasi jaringan	n/a	Iya
Daftar izin untuk host jarak jauh	n/a	Iya
Daftar izin untuk aplikasi	n/a	Iya
Perangkat periferal		
Penyimpanan yang dapat dilepas	Iya	Iya
Penyimpanan yang dapat dilepas dan dienkripsi	Iya	Iya
Printer	Tidak	Tidak
Perangkat seluler terkoneksi MTP	Tidak	Tidak

© Acronis International GmbH, 2003-2024

Adaptor Bluetooth	Iya	Iya
Drive optik	Iya	Iya
Drive flopi	Iya	Iya
Papan klip Windows	Tidak	Tidak
Tangkapan layar	Tidak	Tidak
Drive yang dipetakan dan dialihkan	Iya	Iya
Papan klip yang dialihkan	Tidak	Tidak
Perlindungan diri Agen Perlindungan Cyber		
Perlindungan dari pengguna akhir reguler	Iya	Iya
Perlindungan dari administrator sistem lokal	Iya	Iya

Paket Linux

Untuk menambahkan modul yang diperlukan ke kernel Linux, program penyiapan membutuhkan paket Linux berikut:

- Paket dengan header atau sumber kernel. Versi paket harus cocok dengan versi kernel.
- Sistem kompilator GNU Compiler Collection (GCC). Versi GCC harus menjadi kompilator kernel.
- Alat Make.
- Interpreter Perl.
- Pustaka `libelf-dev`, `libelf-devel`, atau `elfutils-libelf-devel` untuk membuat kernel dimulai dengan 4.15 dan dikonfigurasi dengan CONFIG_UNWINDER_ORC = y. Untuk beberapa distribusi, seperti Fedora 28, diperlukan instalasi secara terpisah dari header kernel.

Nama paket tersebut bervariasi tergantung distribusi Linux Anda.

Di Red Hat Enterprise Linux, CentOS, dan Fedora, paket biasanya akan diinstal oleh program penyiapan. Di distribusi lain, Anda perlu menginstal paket tersebut jika belum diinstal atau belum memiliki versi yang diperlukan.

Apakah paket yang diperlukan sudah diinstal?

Untuk memeriksa apakah paket sudah diinstal, lakukan langkah berikut:

1. Jalankan perintah berikut untuk mengetahui versi kernel dan versi GCC yang diperlukan:

   ```
   cat /proc/version
   ```

   Perintah ini mengembalikan baris yang mirip dengan berikut: `Linux versi 2.6.35.6` dan `gcc versi 4.5.1`

© Acronis International GmbH, 2003-2024

2. Jalankan perintah berikut untuk memeriksa apakah alat Make dan kompilator GCC sudah diinstal:

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

   Untuk **gcc**, pastikan versi yang dikembalikan oleh perintah sama seperti di `versi gcc` pada langkah 1. Untuk **make**, cukup pastikan perintah sudah dijalankan.
3. Periksa apakah versi paket yang sesuai untuk membuat modul kernel sudah diinstal:
   - Di Red Hat Enterprise Linux, CentOS, dan Fedora, jalankan perintah berikut:

     ```
     daftar yum diinstal | grep kernel-devel
     ```

   - Di Ubuntu, jalankan perintah berikut:

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

   Pada kedua kasus tersebut, pastikan versi paketnya sama dengan `versi Linux` pada langkah 1.
4. Jalankan perintah berikut untuk memeriksa apakah interpreter Perl sudah diinstal:

   ```
   perl --version
   ```

   Jika Anda melihat informasi tentang versi Perl, artinya interpreter sudah diinstal.
5. Di Red Hat Enterprise Linux, CentOS, dan Fedora, jalankan perintah berikut untuk memeriksa apakah `elfutils-libelf-devel` sudah diinstal:

   ```
   daftar yum diinstal | grep elfutils-libelf-devel
   ```

   Jika Anda melihat informasi tentang versi pustaka, artinya pustaka sudah diinstal.

Menginstal paket dari repositori

Tabel berikut mencantumkan cara menginstal paket yang diperlukan dalam berbagai distribusi Linux.

Distribusi Linux	Nama paket	Cara menginstal
Red Hat Enterprise Linux	**kernel-devel gcc make elfutils-libelf-devel**	Program penyiapan akan mengunduh dan menginstal paket secara otomatis menggunakan langganan Red Hat Anda.
	perl	Jalankan perintah berikut:

© Acronis International GmbH, 2003-2024

		`yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Program penyiapan akan mengunduh dan menginstal paket secara otomatis.
	perl	Jalankan perintah berikut: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Jalankan perintah berikut:
		`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`

Paket akan diunduh dari repositori distribusi dan diinstal.

Untuk distribusi Linux lainnya, lihat dokumentasi distribusi tentang nama yang tepat dari paket yang diperlukan dan cara menginstalnya.

Menginstal paket secara manual

Anda mungkin perlu menginstal paket **secara manual** jika:

- Mesin tidak memiliki langganan Red Hat aktif atau koneksi Internet.
- Program pengaturan tidak dapat menemukan versi **kernel-devel** atau **gcc** yang sesuai dengan versi kernel. Jika tersedia **kernel-devel** yang lebih baru dibandingkan kernel Anda, perbarui kernel atau instal versi **kernel-devel** secara manual.
- Anda memiliki paket yang diperlukan di jaringan lokal dan tidak perlu menghabiskan waktu untuk melakukan pencarian dan pengunduhan otomatis.

Dapatkan paket dari jaringan lokal atau situs web pihak ketiga tepercaya, dan instal paket sebagai berikut:

© Acronis International GmbH, 2003-2024

- Di Red Hat Enterprise Linux, CentOS, dan Fedora, jalankan perintah berikut sebagai pengguna root:

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

- Di Ubuntu, jalankan perintah berikut:

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

Contoh: Menginstal paket secara manual di Fedora 14

Ikuti langkah berikut untuk menginstal paket yang diperlukan di Fedora 14 pada mesin 32-bit:

1. Jalankan perintah berikut untuk menentukan versi kernel dan versi GCC yang diperlukan:

   ```
   cat /proc/version
   ```

   Output perintah ini meliputi hal-hal berikut:

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

2. Dapatkan paket **kernel-devel** dan **gcc** yang sesuai dengan versi kernel ini:

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

3. Dapatkan paket **make** untuk Fedora 14:

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

4. Instal paket dengan menjalankan perintah berikut sebagai pengguna 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
   ```

   Anda dapat menentukan semua paket ini dalam satu perintah `rpm`. Instalasi salah satu paket ini mungkin memerlukan instalasi paket tambahan untuk menyelesaikan dependensi.

Mengonfigurasi pengaturan server proxy

Agen perlindungan dapat mentransfer data melalui server proksi HTTP/HTTPS. Server harus beroperasi melalui tunnel HTTP tanpa memindai atau mengganggu lalu lintas HTTP. Proksi man-in-the-middle tidak didukung.

Karena agen mendaftarkan dirinya di cloud selama instalasi, Anda harus mengonfigurasi pengaturan server proxy selama instalasi agen atau terlebih dahulu.

Untuk Windows

© Acronis International GmbH, 2003-2024

Jika server proxy dikonfigurasikan di **Panel kontrol** > **Opsi Internet** > **Koneksi**, program penyiapan akan membaca pengaturan server proksi dari registri dan menggunakannya secara otomatis.

Gunakan prosedur ini jika Anda ingin melakukan tugas berikut.

- Konfigurasikan pengaturan proksi sebelum instalasi agen.
- Perbarui pengaturan proksi setelah instalasi agen.

Untuk mengonfigurasi pengaturan proxy selama instalasi agen, lihat "Menginstal agen proteksi di Windows" (hlm. 76).

Catatan
Prosedur ini hanya berlaku bila file `http-proxy.yaml` tidak ada di mesin. Jika file `http-proxy.yaml` ada di mesin, Anda harus memperbarui pengaturan proxy di file tersebut, karena ini akan menggantikan pengaturan di file `aakore.yaml`.

File `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml` dibuat saat Anda mengonfigurasi pengaturan server proksi dengan menggunakan Cyber Protection Monitor. Untuk informasi lebih lanjut, lihat "Mengonfigurasi pengaturan server proxy di Cyber Protect Monitor" (hlm. 311).

Untuk membuka file `http-proxy.yaml`, Anda harus menjadi anggota Grup administrator di Windows.

Untuk mengonfigurasi pengaturan proxy

1. Buat dokumen teks baru dan buka di editor teks, seperti Notepad.
2. Salin dan tempel baris berikut ke dalam file.

```
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. Ganti `proxy.company.com` dengan nama host server proksi/alamat IP Anda, dan `000001bb` dengan nilai heksadesimal nomor port. Misalnya, `000001bb` adalah port 443.
4. Jika server proksi Anda membutuhkan otentikasi, ganti `proxy_login` dan `proxy_password` dengan kredensial server proksi. Atau, hapus baris ini dari file.
5. Simpan dokumen sebagai `proxy.reg`.
6. Jalankan file sebagai administrator.
7. Konfirmasi bahwa Anda ingin mengedit registri Windows.
8. Jika agen belum diinstal pada beban kerja ini, instal sekarang. Jika agen sudah terinstal pada beban kerja, lanjutkan ke langkah berikutnya.
9. Buka file `%programdata%\Acronis\Agent\etc\aakore.yaml` di editor teks.
   Untuk membuka file ini, Anda harus menjadi anggota Grup administrator di Windows.

© Acronis International GmbH, 2003-2024

10. Temukan bagian **env** atau buat bagian tersebut, lalu tambahkan baris berikut.

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

11. Ganti `proxy_login` dan `proxy_password` dengan kredensial server proksi, dan `proxy_address:port` dengan alamat dan nomor port dari server proksi.
12. Dalam menu **Start**, klik **Run**, ketik: **cmd**, lalu klik **OK**.
13. Mulai ulang layanan aakore dengan menjalankan perintah berikut.

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

14. Mulai ulang agen dengan menjalankan perintah berikut.

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

Untuk macOS

Gunakan prosedur ini jika Anda ingin melakukan tugas berikut.

- Konfigurasikan pengaturan proksi sebelum instalasi agen.
- Perbarui pengaturan proksi setelah instalasi agen.

Untuk mengonfigurasi pengaturan proxy selama instalasi agen, lihat "Menginstal agen proteksi di macOS" (hlm. 81).

Untuk mengonfigurasi pengaturan proxy

1. Buat file `/Library/Application Support/Acronis/Registry/Global.config` dan buka di editor teks, seperti Text Edit.
2. Salin dan tempel baris berikut ke dalam file.

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

3. Ganti `proxy.company.com` dengan nama host server proksi/alamat IP Anda, dan `443` dengan nilai desimal nomor port.
4. Jika server proksi Anda membutuhkan otentikasi, ganti `proxy_login` dan `proxy_password` dengan kredensial server proksi. Atau, hapus baris ini dari file.

© Acronis International GmbH, 2003-2024

5. Simpan file.
6. Jika agen belum diinstal pada beban kerja ini, instal sekarang. Jika agen sudah terinstal pada beban kerja, lanjutkan ke langkah berikutnya.
7. Buka file `/Library/Application Support/Acronis/Agent/etc/aakore.yaml` di editor teks.
8. Temukan bagian **env** atau buat bagian tersebut lalu tambahkan baris berikut.

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

9. Ganti `proxy_login` dan `proxy_password` dengan kredensial server proksi, dan `proxy_address:port` dengan alamat dan nomor port dari server proksi.
10. Buka **Aplikasi** > **Utilitas** > **Terminal**.
11. Mulai ulang layanan aakore dengan menjalankan perintah berikut.

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

12. Mulai ulang agen dengan menjalankan perintah berikut.

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

Untuk Linux

Jalankan file instalasi dengan parameter `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`. Gunakan prosedur berikut untuk memperbarui pengaturan proxy setelah instalasi agen perlindungan.

Untuk mengonfigurasi pengaturan proxy

1. Buka file `/etc/Acronis/Global.config` di editor teks.
2. Lakukan salah satu langkah berikut:
   - Jika pengaturan proxy ditentukan selama instalasi agen, temukan bagian berikut.

```
<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>
```

   - Jika pengaturan proxy tidak ditentukan selama instalasi agen, salin baris berikut dan tempelkan ke dalam file di antara tag `<registry name="Global">...</registry>`.

```
<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>
```

3. Ganti `ADDRESS` dengan nama host server proksi/alamat IP yang baru, dan `PORT` dengan nilai desimal nomor port.
4. Jika server proksi Anda membutuhkan otentikasi, ganti `LOGIN` dan `PASSWORD` dengan kredensial server proksi. Atau, hapus baris ini dari file.
5. Simpan file.
6. Buka file `/opt/acronis/etc/aakore.yaml` dalam editor teks.
7. Temukan bagian **env** atau buat bagian tersebut dan tambahkan baris berikut:

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

8. Ganti `proxy_login` dan `proxy_password` dengan kredensial server proksi, dan `proxy_address:port` dengan alamat dan nomor port dari server proksi.
9. Mulai ulang layanan aakore dengan menjalankan perintah berikut.

```
sudo service aakore restart
```

10. Mulai ulang agen dengan menjalankan perintah yang berjalan di direktori mana pun.

```
sudo service acronis_mms restart
```

Untuk media yang dapat di-boot

Saat bekerja menggunakan media yang dapat di-boot, Anda mungkin perlu mengakses penyimpanan cloud melalui server proxy. Untuk mengonfigurasi pengaturan server proksi, klik **Alat** > **Server proksi**, lalu konfigurasikan nama host/alamat IP server proksi, port, dan kredensial.

Menginstal agen proteksi

Anda dapat menginstal agen pada mesin yang menjalankan sistem operasi yang tercantum dalam "Sistem dan lingkungan operasi yang didukung". Sistem operasi yang mendukung fitur Cyber Protect tercantum dalam "Fitur Cyber Protect yang didukung oleh sistem operasi".

Mengunduh agen proteksi

Sebelum Anda menginstal agen, Anda harus mengunduh file instalasinya dari konsol Cyber Protect.

Untuk mengunduh agen sekaligus menambahkan beban kerja untuk melindungi

1. Pada konsol Cyber Protect, navigasi ke **Perangkat** > **Semua perangkat**.
2. Di kanan atas, klik **Tambah peranti**.

© Acronis International GmbH, 2003-2024

3. Pada panel **Tambah perangkat**, dari menu drop-down **Saluran rilis**, pilih versi agen.
   - **Rilis sebelumnya** - unduh versi agen dari rilis sebelumnya.
   - **Terbaru** - unduh versi agen terbaru yang tersedia.
4. Pilih agen yang sesuai dengan sistem operasi beban kerja yang Anda tambahkan.
   Dialog **Simpan sebagai** terbuka.
5. [Hanya untuk Macs dengan prosesor silikon Apple (seperti Apple M1)] Klik **Batalkan**. Dalam panel **Tambahkan Mac** yang terbuka, klik tautan **Unduh penginstal ARM**.
6. Pilih lokasi untuk menyimpan file instalasi agen dan klik **Simpan**.

Untuk mengunduh agen untuk penggunaan kemudian

1. Pada sudut kanan atas konsol Cyber Protect, klik ikon **Pengguna**.
2. Klik **Unduh**.
3. Pada dialog **Unduhan**, dari menu drop-down **Saluran rilis**, pilih versi agen.
   - **Rilis sebelumnya** - unduh versi agen dari rilis sebelumnya.
   - **Terbaru** - unduh versi agen terbaru yang tersedia.
4. Gulir daftar penginstal yang tersedia untuk menemukan penginstal agen yang Anda butuhkan dan klik ikon unduh pada akhir barisnya.
   Dialog **Simpan sebagai** terbuka.
5. Pilih lokasi untuk menyimpan file instalasi agen dan klik **Simpan**.

Menginstal agen proteksi di Windows

Prasyarat

Unduh agen yang Anda perlukan pada beban kerja yang ingin Anda lindungi. Lihat "Mengunduh agen proteksi" (hlm. 75).

Untuk menginstal Agen untuk Windows

1. Pastikan mesin terhubung ke Internet.
2. Masuk sebagai administrator dan mulai penginstal.
3. [Opsional] Klik **Sesuaikan pengaturan instalasi** dan buat perubahan sesuai keinginan Anda:
   - Untuk mengubah komponen yang akan diinstal (misalnya, untuk menonaktifkan instalasi Monitor Cyber Protection atau Alat Baris Perintah, atau untuk menginstal Agen untuk Proteksi Antimalware atau Agen untuk penyaringan URL).

     Catatan
     Pada mesin Windows, fitur Proteksi Antimalware memerlukan instalasi Agen untuk Proteksi Antimalware, dan fitur penyaringan URL memerlukan instalasi Agen untuk penyaringan URL. Agen-agen ini diinstal secara otomatis untuk beban kerja yang dilindungi jika modul **Antivirus & Proteksi Antimalware** dan/atau **Penyaringan URL** diaktifkan dalam rencana proteksi mereka.

© Acronis International GmbH, 2003-2024

- Untuk mengubah metode pendaftaran beban kerja di layanan Cyber Protection. Anda dapat beralih dari **Gunakan konsol layanan** (default) ke **Gunakan kredensial** atau **Gunakan token pendaftaran**.
- Untuk mengubah jalur instalasi.
- Untuk mengubah akun pengguna yang di bawahnya layanan agen akan berjalan. Untuk perincian, lihat "Mengubah akun masuk pada mesin Windows" (hlm. 84).
- Untuk memverifikasi atau mengubah nama host server proksi/alamat IP, port, dan kredensial. Jika server proksi diaktifkan di Windows, maka akan dideteksi dan digunakan secara otomatis.

4. Klik **Instal**.
5. [Hanya saat menginstal Agen untuk VMware] Tentukan alamat dan kredensial akses untuk Server vCenter atau host ESXi yang berdiri sendiri tempat Anda ingin mencadangkan dan memulihkan mesin virtual, lalu klik **Selesai**.

   Kami menyarankan Anda menggunakan akun khusus untuk mengakses Server vCenter atau host ESXi, daripada menggunakan akun yang sudah ada dengan peran Administrator. Untuk mempelajari lebih lanjut tentang hak istimewa yang diperlukan untuk akun khusus, lihat "Agen untuk VMware – hak istimewa yang diperlukan" (hlm. 696).
6. [Hanya ketika menginstal pada pengontrol domain] Tentukan akun pengguna yang layanan agennya akan dijalankan, lalu klik **Selesai**. Untuk alasan keamanan, program penyiapan tidak membuat akun baru secara otomatis di pengontrol domain.

   Catatan
   Akun pengguna yang Anda tentukan harus diberi hak `Log sebagai layanan`. Akun ini harus telah digunakan di pengontrol domain, agar folder profilnya dibuat di mesin tersebut.

   Untuk informasi lebih lanjut tentang menginstal agen pada pengontrol domain hanya baca, lihat artikel basis pengetahuan ini.
7. Jika Anda mempertahankan metode pendaftaran default **Gunakan konsol layanan** di langkah 3, tunggu hingga layar pendaftaran muncul, lalu lanjutkan ke langkah berikutnya. Jika tidak, tidak diperlukan tindakan lainnya.
8. Lakukan salah satu langkah berikut:
   - Jika Anda masuk dengan akun administrator perusahaan, daftarkan beban kerja untuk perusahaan Anda:
     a. Klik **Daftarkan beban kerja**.
     b. Di jendela browser yang terbuka, masuk ke konsol Cyber Protect dan tinjau detail registrasi.
     c. Di daftar **Mendaftar untuk akun**, pilih akun pengguna pelanggan Anda di mana Anda ingin mendaftarkan beban kerja.
     d. Klik **Periksa kode**, lalu klik **Konfirmasi pendaftaran**.
   - Jika Anda masuk dengan akun administrator mitra, daftarkan beban kerja untuk pelanggan Anda:

© Acronis International GmbH, 2003-2024

a. Klik **Daftarkan beban kerja**.

b. Di jendela browser yang terbuka, masuk ke konsol Cyber Protect dan tinjau detail registrasi.

c. Di daftar **Mendaftar untuk akun**, pilih akun pengguna pelanggan Anda di mana Anda ingin mendaftarkan beban kerja.

d. Klik **Periksa kode**, lalu klik **Konfirmasi pendaftaran**.

- Klik **Tampilkan info pendaftaran**. Program penyiapan menampilkan tautan pendaftaran dan kode pendaftaran. Jika Anda tidak dapat menyelesaikan registrasi beban kerja di mesin saat ini, salin tautan dan kode pendaftaran, lalu ikuti langkah-langkah pendaftaran di mesin lain. Dalam hal ini, Anda harus memasukkan kode pendaftaran pada formulir pendaftaran. Kode pendaftaran valid selama satu jam.

  Selain itu, Anda juga dapat mengakses formulir pendaftaran dengan mengklik **Semua perangkat** > **Tambah**, gulir ke bawah ke **Pendaftaran via kode**, lalu klik **Daftar**.

  Catatan
  Jangan keluar dari program penyiapan sampai Anda mengonfirmasi pendaftaran. Untuk memulai kembali pendaftaran, Anda harus memulai ulang program penyiapan dan mengulangi prosedur instalasi.

  Akibatnya, beban kerja akan diberikan ke akun yang digunakan untuk masuk ke konsol Cyber Protect.

- Daftarkan beban kerja secara manual menggunakan baris perintah. Untuk informasi lebih lanjut tentang cara melakukan ini, lihat "Mendaftarkan dan membatalkan pendaftaran beban kerja secara manual" (hlm. 119).

9. [Jika agen terdaftar di bawah akun yang penyewanya berada dalam mode Kepatuhan] Atur kata sandi enkripsi.

Menginstal agen proteksi di Linux

Persiapan

- Unduh agen yang Anda butuhkan pada mesin yang akan Anda lindungi. Lihat "Mengunduh agen proteksi" (hlm. 75).
- Pastikan bahwa paket Linux yang diperlukan sudah diinstal pada mesin.
- Saat menginstal agen di SUSE Linux, pastikan bahwa Anda memakai `su -`, bukan `sudo`. Jika tidak, kesalahan berikut akan terjadi saat Anda mencoba mendaftarkan agen melalui konsol Cyber Protect: `Gagal meluncurkan browser web. Tidak ada tampilan yang tersedia.`

  Beberapa distribusi Linux, seperti SUSE, tidak meneruskan variabel DISPLAY saat menggunakan sudo, dan penginstal tidak dapat membuka browser di antarmuka pengguna grafis (GUI).

Instalasi

Untuk menginstal Agen untuk Linux, Anda memerlukan sedikitnya 2 GB ruang disk yang tersedia.

© Acronis International GmbH, 2003-2024

Untuk menginstal Agen untuk Linux

1. Pastikan mesin terhubung ke Internet.
2. Sebagai pengguna root, navigasi ke direktori dengan file instalasi, buat file yang dapat dieksekusi, lalu jalankan.

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

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

   Jika server proxy diaktifkan di jaringan Anda, ketika menjalankan file instalasi, tentukan nama host server/alamat IP dan port dalam format berikut: `--http-proxy-host=ADDRESS` `--http-proxy-port=PORT` `--http-proxy-login=LOGIN` `--http-proxy-password=PASSWORD`.

   Jika Anda ingin mengubah metode default pendaftaran mesin pada layanan Cyber Protection, jalankan file instalasi dengan salah satu dari parameter berikut:

   - `--register-with-credentials` – untuk meminta nama pengguna dan kata sandi selama instalasi
   - `--token=STRING` – untuk menggunakan token pendaftaran
   - `--skip-registration` – untuk melewati pendaftaran
3. Pilih kotak centang untuk agen yang ingin Anda instal. Agen berikut tersedia:
   - Agen untuk Linux
   - Agen untuk Virtuozzo
   - Agen untuk Oracle
   - Agen untuk MySQL/MariaDB

   Agen untuk Virtuozzo, Agen untuk Oracle, dan Agen untuk MySQL/MariaDB memerlukan Agen untuk Linux (64-bit) agar diinstal juga.
4. Jika Anda mempertahankan metode pendaftaran default di langkah 2, lanjutkan ke langkah berikutnya. Jika tidak, masukkan nama pengguna dan kata sandi untuk layanan Cyber Protection, atau tunggu hingga mesin akan didaftarkan menggunakan token.
5. Lakukan salah satu langkah berikut:
   - Jika Anda masuk dengan akun administrator perusahaan, daftarkan beban kerja untuk perusahaan Anda:
     a. Klik **Daftarkan beban kerja**.
     b. Di jendela browser yang terbuka, masuk ke konsol Cyber Protect dan tinjau detail registrasi.
     c. Di daftar **Mendaftar untuk akun**, pilih akun pengguna pelanggan Anda di mana Anda ingin mendaftarkan beban kerja.
     d. Klik **Periksa kode**, lalu klik **Konfirmasi pendaftaran**.
   - Jika Anda masuk dengan akun administrator mitra, daftarkan beban kerja untuk pelanggan Anda:

© Acronis International GmbH, 2003-2024

a. Klik **Daftarkan beban kerja**.

b. Di jendela browser yang terbuka, masuk ke konsol Cyber Protect dan tinjau detail registrasi.

c. Di daftar **Mendaftar untuk akun**, pilih akun pengguna pelanggan Anda di mana Anda ingin mendaftarkan beban kerja.

d. Klik **Periksa kode**, lalu klik **Konfirmasi pendaftaran**.

- Klik **Tampilkan info pendaftaran**. Program penyiapan menampilkan tautan pendaftaran dan kode pendaftaran. Jika Anda tidak dapat menyelesaikan registrasi beban kerja di mesin saat ini, salin tautan dan kode pendaftaran, lalu ikuti langkah-langkah pendaftaran di mesin lain. Dalam hal ini, Anda harus memasukkan kode pendaftaran pada formulir pendaftaran. Kode pendaftaran valid selama satu jam.

  Selain itu, Anda juga dapat mengakses formulir pendaftaran dengan mengklik **Semua perangkat** > **Tambah**, gulir ke bawah ke **Pendaftaran via kode**, lalu klik **Daftar**.

  Catatan
  Jangan keluar dari program penyiapan sampai Anda mengonfirmasi pendaftaran. Untuk memulai kembali pendaftaran, Anda harus memulai ulang program penyiapan dan mengulangi prosedur instalasi.

  Akibatnya, beban kerja akan diberikan ke akun yang digunakan untuk masuk ke konsol Cyber Protect.
- Daftarkan beban kerja secara manual menggunakan baris perintah. Untuk informasi lebih lanjut tentang cara melakukan ini, lihat "Mendaftarkan dan membatalkan pendaftaran beban kerja secara manual" (hlm. 119).

6. [Jika agen terdaftar di bawah akun yang penyewanya berada dalam mode Kepatuhan] Atur kata sandi enkripsi.
7. Jika UEFI Secure Boot diaktifkan pada mesin, akan diinformasikan bahwa Anda harus memulai ulang sistem setelah penginstalan. Pastikan untuk mengingat kata sandi apa (kata sandi dari pengguna akar atau "acronis") yang harus digunakan.

   Catatan
   Penginstalan akan menghasilkan kunci baru yang digunakan untuk menandatangani modul kernel. Anda harus mendaftarkan kunci baru ini ke daftar Machine Owner Key (MOK) dengan memulai ulang mesinnya. Tanpa mendaftarkan kunci baru, agen Anda tidak akan operasional. Jika Anda mengaktifkan UEFI Secure Boot setelah penginstalan agen, Anda perlu menginstal ulang agen.

8. Setelah instalasi selesai, lakukan salah satu langkah berikut:
   - Klik **Mulai Kembali**, jika Anda disarankan untuk memulai kembali sistem di langkah sebelumnya.

© Acronis International GmbH, 2003-2024

Selama memulai ulang sistem, pilih untuk manajemen MOK (Machine Owner Key), pilih **Daftarkan MOK**, lalu daftarkan kunci dengan menggunakan kata sandi yang disarankan di langkah sebelumnya.

- Jika tidak, klik **Keluar**.

Informasi penyelesaian masalah disediakan dalam file:
`/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

Menginstal agen proteksi di macOS

Prasyarat

Unduh agen yang Anda perlukan pada beban kerja yang ingin Anda lindungi. Lihat "Mengunduh agen proteksi" (hlm. 75).

Untuk menginstal Agen untuk Mac (x64 atau ARM64)

1. Pastikan mesin terhubung ke Internet.
2. Klik dua kali pada file instalasi (.dmg).
3. Tunggu saat sistem operasi melakukan mounting profil disk instalasi.
4. Klik dua kali pada **Instal**.
5. Jika server proksi diaktifkan di jaringan Anda, klik **Agen Perlindungan** di bar menu, klik **Pengaturan server proksi**, lalu tentukan nama host server proksi/alamat IP, port, dan kredensial.
6. Jika diminta, berikan kredensial administrator.
7. Klik **Lanjutkan**.
8. Tunggu hingga layar pendaftaran muncul.
9. Lakukan salah satu langkah berikut:
   - Jika Anda masuk dengan akun administrator perusahaan, daftarkan beban kerja untuk perusahaan Anda:
     a. Klik **Daftarkan beban kerja**.
     b. Di jendela browser yang terbuka, masuk ke konsol Cyber Protect dan tinjau detail registrasi.
     c. Di daftar **Mendaftar untuk akun**, pilih akun pengguna pelanggan Anda di mana Anda ingin mendaftarkan beban kerja.
     d. Klik **Periksa kode**, lalu klik **Konfirmasi pendaftaran**.
   - Jika Anda masuk dengan akun administrator mitra, daftarkan beban kerja untuk pelanggan Anda:
     a. Klik **Daftarkan beban kerja**.
     b. Di jendela browser yang terbuka, masuk ke konsol Cyber Protect dan tinjau detail registrasi.

© Acronis International GmbH, 2003-2024

c. Di daftar **Mendaftar untuk akun**, pilih akun pengguna pelanggan Anda di mana Anda ingin mendaftarkan beban kerja.

d. Klik **Periksa kode**, lalu klik **Konfirmasi pendaftaran**.

- Klik **Tampilkan info pendaftaran**. Program penyiapan menampilkan tautan pendaftaran dan kode pendaftaran. Jika Anda tidak dapat menyelesaikan registrasi beban kerja di mesin saat ini, salin tautan dan kode pendaftaran, lalu ikuti langkah-langkah pendaftaran di mesin lain. Dalam hal ini, Anda harus memasukkan kode pendaftaran pada formulir pendaftaran. Kode pendaftaran valid selama satu jam.

  Selain itu, Anda juga dapat mengakses formulir pendaftaran dengan mengklik **Semua perangkat** > **Tambah**, gulir ke bawah ke **Pendaftaran via kode**, lalu klik **Daftar**.

  Catatan
  Jangan keluar dari program penyiapan sampai Anda mengonfirmasi pendaftaran. Untuk memulai kembali pendaftaran, Anda harus memulai ulang program penyiapan dan mengulangi prosedur instalasi.

  Akibatnya, beban kerja akan diberikan ke akun yang digunakan untuk masuk ke konsol Cyber Protect.
- Daftarkan beban kerja secara manual menggunakan baris perintah. Untuk informasi lebih lanjut tentang cara melakukan ini, lihat "Mendaftarkan dan membatalkan pendaftaran beban kerja secara manual" (hlm. 119).

10. [Jika agen terdaftar di bawah akun yang penyewanya berada dalam mode Kepatuhan] Atur kata sandi enkripsi.
11. Jika versi macOS Anda adalah Mojave 10.14.x atau di atasnya, berikan akses disk penuh kepada agen perlindungan untuk memungkinkan operasi pencadangan.

    Untuk instruksi, lihat Berikan izin 'Akses Disk Penuh' untuk agen Perlindungan Cyber (64657).
12. Untuk menggunakan fungsionalitas desktop jarak jauh, berikan izin sistem yang diperlukan kepada Connect Agent. Untuk informasi lebih lanjut, lihat "Memberikan izin sistem yang diperlukan kepada Connect Agent" (hlm. 82).

Memberikan izin sistem yang diperlukan kepada Connect Agent

Untuk mengaktifkan semua fitur dari fungsionalitas desktop jarak jauh di beban kerja macOS, selain izin akses disk penuh, Anda juga perlu memberikan izin berikut kepada Connect Agent:

- Perekaman Layar - memungkinkan perekaman layar beban kerja macOS melalui NEAR. Sebelum izin ini diberikan, semua koneksi kontrol jarak jauh akan ditolak.
- Aksesibilitas - memungkinkan koneksi jarak jauh dalam mode kontrol melalui NEAR
- Mikrofon - memungkinkan pengalihan suara dari beban kerja macOS jarak jauh ke beban kerja lokal melalui NEAR. Untuk mengaktifkan fitur pengalihan suara, driver penangkap suara harus diinstal di beban kerja. Untuk informasi lebih lanjut, lihat "Pengalihan suara jarak jauh" (hlm. 990).
- Otomatisasi - memungkinkan tindakan pengosongan Keranjang sampah

© Acronis International GmbH, 2003-2024

Setelah memulai agen pada beban kerja macOS, beban kerja akan memeriksa apakah agen memiliki hal tersebut dan akan meminta Anda memberikan izin, jika diperlukan.

Cara memberikan izin Perekaman Layar

1. Pada dialog **Berikan izin sistem yang diperlukan** untuk Agen Cyber Protect, klik **Siapkan izin sistem**.
2. Pada dialog **Izin sistem**, klik **Minta izin Perekaman Layar**.
3. Klik **Buka Preferensi Sistem**.
4. Pilih **Connect Agent**.

Jika agen tidak memiliki izin ketika Anda mencoba mengakses beban kerja dari jarak jauh, dialog permintaan izin Perekaman Layar akan ditampilkan. Hanya pengguna lokal yang dapat menjawab dialog.

Cara memberikan izin Aksesibilitas

1. Pada dialog **Berikan izin sistem yang diperlukan** untuk Agen Cyber Protect, klik **Siapkan izin sistem**.
2. Pada dialog **Izin sistem**, klik **Minta izin Aksesibilitas**.
3. Klik **Buka Preferensi Sistem**.
4. Klik ikon gembok di sudut kiri bawah jendela agar berubah menjadi tidak terkunci. Sistem akan meminta Anda memberikan kata sandi administrator untuk membuat perubahan.
5. Pilih **Connect Agent**.

Cara memberikan izin Mikrofon

1. Pada dialog **Berikan izin sistem yang diperlukan** kepada Connect Agent, klik **Siapkan izin sistem**.
2. Pada dialog **Izin sistem**, klik **Minta izin Mikrofon**.
3. Klik **OK**.

Catatan
Anda juga harus menginstal driver penangkap suara pada beban kerja macOS untuk memungkinkan agen memanfaatkan izin yang diberikan dan mengalihkan suara beban kerja. Untuk informasi lebih lanjut, lihat "Pengalihan suara jarak jauh" (hlm. 990).

Cara memberikan izin Otomatisasi

1. Pada dialog **Berikan izin sistem yang diperlukan** kepada Connect Agent, klik **Siapkan izin sistem**.
2. Pada dialog **Izin sistem**, klik **Minta izin Otomatisasi**.

© Acronis International GmbH, 2003-2024

Mengubah akun masuk pada mesin Windows

Pada layar **Pilih komponen**, tentukan akun yang di dalamnya layanan akan berjalan dengan menetapkan **Akun masuk untuk layanan agen**. Anda dapat memilih salah satu dari tindakan berikut:

- **Gunakan Akun Pengguna Layanan** (default untuk layanan agen)

  Akun Pengguna Layanan adalah akun sistem Windows yang digunakan untuk menjalankan layanan. Keuntungan dari pengaturan ini adalah kebijakan keamanan domain yang tidak memengaruhi hak pengguna akun ini. Secara default, agen berjalan di bawah akun **Sistem Lokal**.
- **Buat akun baru**

  Nama akunnya adalah Agent User untuk agen.
- **Gunakan akun berikut**

  Jika Anda menginstal agen pada pengontrol domain, sistem akan meminta Anda menentukan akun yang ada (atau akun yang sama) untuk agen. Untuk alasan keamanan, sistem tidak membuat akun baru secara otomatis di pengontrol domain.

  Akun pengguna yang Anda tentukan ketika program penyiapan berjalan di pengontrol domain harus diberi hak `Masuk sebagai layanan`. Akun ini harus telah digunakan di pengontrol domain, agar folder profilnya dibuat di mesin tersebut.

  Untuk informasi lebih lanjut tentang menginstal agen pada pengontrol domain hanya baca, lihat artikel basis pengetahuan ini.

Jika Anda memilih opsi **Buat akun baru** atau **Gunakan akun berikut**, pastikan bahwa kebijakan keamanan domain tidak memengaruhi hak akun terkait. Jika akun kehilangan hak pengguna yang diberikan selama instalasi, komponen dapat bekerja dengan tidak semestinya atau tidak berfungsi.

Diperlukan hak istimewa untuk akun masuk

Agen perlindungan dijalankan sebagai Managed Machine Service (MMS) pada mesin Windows. Akun di mana agen akan menjalankan harus memiliki hak khusus untuk agen untuk bekerja dengan benar. Dengan demikian, pengguna MMS harus diberikan hak-hak berikut:

1. Termasuk dalam grup **Operator Pencadangan** dan **Administrator**. Pada Pengendali Domain, pengguna harus dimasukkan dalam grup **Admin Domain**.
2. Diberikan izin **Kontrol Penuh** pada folder `%PROGRAMDATA%\Acronis` (pada Windows XP dan Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) dan pada subfoldernya.
3. Diberikan izin **Kontrol Penuh** pada kunci registri tertentu dengan kunci berikut: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Menetapkan hak pengguna berikut:
   - Masuk sebagai layanan
   - Sesuaikan kuota memori untuk suatu proses

© Acronis International GmbH, 2003-2024

- Ganti token level proses
- Modifikasi nilai lingkungan firmware

Cara menetapkan hak pengguna

Ikuti petunjuk di bawah ini untuk menetapkan hak pengguna (contoh ini menggunakan hak pengguna **Masuk sebagai layanan**, langkah-langkahnya sama untuk hak pengguna lainnya):

1. Masuk ke komputer dengan menggunakan akun dengan hak administratif.
2. Buka **Alat Bantu Administratif** dari **Panel Kontrol** (atau klik Win+R, ketik **kontrol alat bantu admin**, dan tekan Enter) dan buka **Kebijakan Keamanan Lokal**.
3. Perluas **Kebijakan Lokal** dan klik **Penetapan Hak Pengguna.**
4. Di panel kanan, klik kanan **Masuk sebagai layanan** dan pilih **Properti**.
5. Klik pada tombol **Tambahkan Pengguna atau Grup...** untuk menambahkan pengguna baru.
6. Di jendela **Pilih Pengguna, Komputer, Akun Layanan, atau Grup**, temukan pengguna yang ingin Anda masukkan dan klik **OK**.
7. Klik **OK** di **Masuk sebagai Properti layanan** untuk menyimpan perubahan.

Penting
Pastikan bahwa pengguna yang telah Anda tambahkan ke hak pengguna **Masuk sebagai layanan** tidak tercantum dalam kebijakan **Tolak masuk sebagai layanan** di **Kebijakan Keamanan Lokal**.

Perhatikan bahwa kami menyarankan Anda untuk tidak mengubah akun masuk secara manual setelah instalasi selesai.

Instalasi dinamis dan penghapusan instalasi komponen

Untuk beban kerja Windows yang dilindungi oleh agen versi 15.0.26986 (dirilis pada Mei 2021) atau lebih baru, komponen berikut diinstal secara dinamis—yaitu, hanya jika diperlukan oleh rencana proteksi:

- Agen untuk penyaringan URL—diperlukan untuk operasi fitur penyaringan URL.
- Agen untuk Proteksi Antimalware—wajib untuk pengoperasian fitur proteksi antimalware.
- Agen untuk Pencegahan Kehilangan Data—diperlukan untuk pengoperasian fitur kontrol perangkat.

Secara default, komponen-komponen ini tidak diinstal. Komponen masing-masing secara otomatis diinstal jika beban kerja menjadi terlindungi oleh rencana yang modul berikut ini diaktifkan:

- Perlindungan Antivirus & Antimalware
- Pemfilteran URL
- Kontrol perangkat

© Acronis International GmbH, 2003-2024

Demikian pula, jika tidak ada rencana proteksi yang memerlukan perlindungan antimalware, pemfilteran URL, atau fitur kontrol perangkat lagi, komponen yang bersangkutan akan dihapus secara otomatis.

Instalasi dinamis atau penghapusan instalasi komponen memerlukan waktu hingga 10 menit setelah Anda mengubah rencana proteksi. Namun, jika salah satu dari operasi berikut ini berjalan, penginstalan dinamis atau penghapusan instalasi akan dimulai setelah operasi ini selesai:

- Cadangan
- Pemulihan
- Replikasi cadangan
- Replikasi mesin virtual
- Menguji replika
- Menjalankan mesin virtual dari cadangan (termasuk finalisasi)
- Failover pemulihan bencana
- Failback pemulihan bencana
- Menjalankan skrip (untuk fungsionalitas Pembuatan Skrip Cyber)
- Instalasi patch
- Pencadangan konfigurasi ESXi

Instalasi atau penghapusan instalasi tanpa pengawasan

Instalasi atau penghapusan instalasi tanpa pengawasan di Windows

Di Windows, Anda dapat melakukan instalasi atau penghapusan instalasi tanpa pengawasan dengan cara berikut:

- Dengan menggunakan file EXE dari program penyiapan dan menentukan parameter instalasi pada baris perintah.
- Dengan menggunakan file MSI yang Anda ekstrak dari program penyiapan, dan menentukan parameter instalasi dengan salah satu cara berikut:
  - Dalam file MST
  - Langsung di baris perintah

Instalasi dan penghapusan instalasi tanpa pengawasan dengan file EXE

Untuk jenis instalasi tanpa pengawasan ini, unduh program pengaturan, lalu mulai dari baris perintah dengan parameter instalasi yang diperlukan. Untuk melihat parameter yang dapat Anda gunakan, lihat "Parameter untuk instalasi tanpa pengawasan (EXE)" (hlm. 89).

Anda tidak perlu mengekstrak paket instalasi, file MSI, dan MST terlebih dahulu.

© Acronis International GmbH, 2003-2024

Menginstal dan mencopot agen and komponen (EXE)

Untuk melakukan instalasi tanpa pengawasan dengan file EXE, jalankan program penyiapan dan tentukan parameter instalasi pada baris perintah.

Untuk mengunduh program penyiapan, di konsol Cyber Protect, klik ikon akun di pojok kanan atas, lalu klik **Unduhan**. Tautan unduhan juga tersedia di panel **Tambahkan perangkat**.

Untuk menginstal agen dan komponen

1. Mulai antarmuka baris perintah sebagai admin, lalu navigasikan ke file EXE dari program pengaturan.
2. Untuk memulai program penyiapan dan menentukan parameter instalasi, jalankan perintah berikut:

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

   Gunakan spasi untuk memisahkan parameter, dan koma tanpa spasi untuk memisahkan nilai parameter. Misalnya:

   ```
   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
   ```

   Untuk memeriksa parameter yang tersedia dan nilainya, lihat "Parameter untuk instalasi tanpa pengawasan (EXE)" (hlm. 89).

Contoh

- Menginstal Agen untuk Windows, Agen untuk Antimalware, Agen untuk penyaringan URL, Alat Baris Perintah, dan Cyber Protect Monitor. Mendaftarkan beban kerja di layanan Cyber Protection dengan menggunakan nama pengguna dan kata sandi.

  ```
  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
  ```

- Menginstal Agen untuk Windows, Alat Baris Perintah, dan Cyber Protect Monitor. Membuat akun masuk baru untuk layanan agen di Windows. Mendaftarkan beban kerja di layanan Cyber Protection dengan menggunakan 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
  ```


© Acronis International GmbH, 2003-2024

- Menginstal Agen untuk Windows, Alat Baris Perintah, Agen untuk Oracle dan Cyber Protect Monitor. Mendaftarkan mesin di layanan Cyber Protection dengan menggunakan nama pengguna dan kata sandi.

```
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
```

- Menginstal Agen untuk Windows, Alat Baris Perintah, dan Cyber Protect Monitor. Mengatur bahasa antarmuka pengguna ke Jerman. Mendaftarkan mesin di layanan Cyber Protection dengan menggunakan token. Mengatur proksi 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
```

Untuk mencopot komponen yang sudah diinstal

1. Mulai antarmuka jalur perintah sebagai administrator, kemudian buka `%ProgramFiles%\BackupClient\RemoteInstall`.
2. Jalankan perintah berikut:

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

   Untuk memeriksa parameter yang tersedia dan nilainya, lihat "Parameter untuk instalasi tanpa pengawasan (EXE)" (hlm. 89).

Contoh

- Menghapus instalasi Cyber Protect Monitor.

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

Untuk menghapus instalasi agen

1. Mulai antarmuka jalur perintah sebagai administrator, kemudian buka `%Program Files%\Common Files\Acronis\BackupAndRecovery`.
2. Jalankan perintah berikut:

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

   Untuk memeriksa parameter yang tersedia dan nilainya, lihat "Parameter untuk instalasi tanpa pengawasan (EXE)" (hlm. 89).

© Acronis International GmbH, 2003-2024

Contoh

- Menghapus instalasi Agen untuk Windows dan semua komponennya. Menghapus semua log, tugas, dan pengaturan konfigurasi.

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

- Menghapus instalasi Agen untuk Windows yang dilindungi kata sandi dan semua komponennya. Menghapus semua log, tugas, dan pengaturan konfigurasi.

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

Parameter untuk instalasi tanpa pengawasan (EXE)

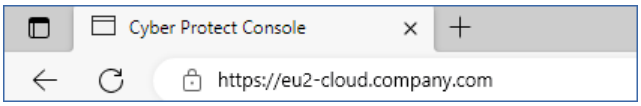
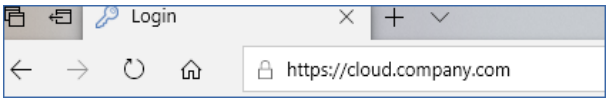
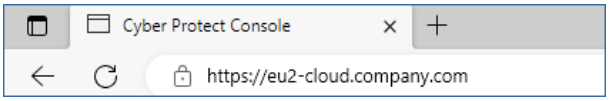
Tabel berikut merangkum parameter untuk instalasi tanpa pengawasan dengan file EXE.

Parameter	Deskripsi
Parameter umum	
`--add-components=`<component1,component2,...,componentN>	Komponen yang akan diinstal. Lihat daftar lengkap komponen yang tersedia di "Komponen untuk instalasi tanpa pengawasan (EXE)" (hlm. 94). Saat Anda menentukan beberapa komponen, pisahkan dengan koma. Jangan menambahkan spasi sebelum atau sesudah koma. Jika Anda menentukan komponen yang sudah terinstal, komponen ini akan diperbaiki atau diperbarui, tergantung pada versi program penyiapan dan versi komponen yang diinstal. Jika Anda tidak menentukan parameter ini, serangkaian komponen default akan diinstal, bergantung pada mesin tempat Anda melakukan instalasi. Misalnya, Agen untuk SQL hanya diinstal pada mesin yang menjalankan MS SQL Server.
`--install-dir=`<path>	Folder tempat komponen yang dipilih akan diinstal. Jika folder yang ditentukan tidak ada, maka folder tersebut akan dibuat. Jika Anda tidak menentukan parameter ini, folder default akan digunakan: `C:\Program Files\BackupClient`.
`--log-dir=`<path>	Folder tempat log instalasi akan disimpan. Jika Anda tidak menentukan parameter ini, folder default

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
	akan digunakan: `%ProgramData%\Acronis\InstallationLogs`.
`--language=`<code>	Bahasa produk. Nilai-nilai berikut tersedia: 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. Jika Anda tidak menentukan parameter ini, dan bahasa sistem mesin tempat Anda melakukan instalasi tercantum di atas, maka bahasa sistem akan digunakan. Dalam semua kasus lainnya, nilainya ditetapkan ke en.
`--quiet`	Gunakan parameter ini untuk menjalankan program pengaturan tanpa menampilkan antarmuka pengguna grafis. Jangan menggunakannya bersamaan dengan parameter `--register-only`.
`--help`	Gunakan parameter ini untuk melihat daftar semua parameter yang tersedia yang dapat Anda gunakan pada baris perintah dan deskripsinya.
`--fss-onboarding-auto-start`	Gunakan parameter ini bersama dengan parameter `--quiet` untuk menampilkan File Sync & Share wizard on-boarding setelah instalasi tanpa pengawasan.
Parameter pendaftaran	
`--registration=`{skip | by-credentials | by-token | device-flow}	Gunakan parameter ini untuk memilih cara mendaftarkan agen setelah instalasi. Untuk melewati pendaftaran, tentukan `skip`. Anda bisa mendaftarkan agennya nanti, dengan menggunakan parameter `--register-only`. Untuk mendaftarkan agen dengan menggunakan kredensial, tentukan `by-credentials`, lalu gunakan parameter `--reg-login` dan `--reg-password`. Selain itu, Anda hanya dapat menggunakan parameter `--reg-login` dan `--reg-password`, sehingga penentuan `--registration=by-credentials` bersifat opsional. Untuk mendaftarkan agen dengan token pendaftaran, tentukan `by-token`, lalu gunakan parameter `--reg-token`. Selain itu, Anda hanya dapat menggunakan parameter `--reg-token`, yang menjadikan penentuan `--registration=by-token` bersifat opsional.

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
	Untuk mendaftarkan agen dengan menggunakan protokol OAuth 2.0, tentukan `device-flow`. Setelah instalasi selesai, halaman registrasi terbuka secara otomatis. Saat Anda menggunakan `--registration=device-flow`, tentukan alamat pusat data yang tepat sebagai nilai untuk parameter `--reg-address`. Ini adalah URL yang Anda lihat **setelah masuk** ke layanan Cyber Protection. Misalnya, `https://eu2-cloud.company.com`.  Jangan gunakan `--registration=device-flow` dengan parameter `--quiet`.
`--reg-address=`<url>	URL layanan Cyber Protection. Anda dapat menggunakan parameter ini dengan parameter `--reg-login` and `--reg-password`, atau parameter `--reg-token`. • Saat Anda menggunakannya dengan `--reg-login` dan parameter `--reg-password`, tentukan alamat yang Anda gunakan **untuk log in** ke layanan Cyber Protection. Misalnya, `https://cloud.company.com`:  • Saat Anda menggunakannya dengan parameter `--reg-token`, tentukan alamat pusat data yang tepat. Ini adalah URL yang Anda lihat **setelah masuk** ke layanan Cyber Protection. Misalnya, `https://eu2-cloud.company.com`.  Jangan gunakan `https://cloud.company.com` dengan parameter `--reg-token`.
`--reg-login=`<login> `--reg-password=`<password>	Kredensial untuk akun tempat agen akan didaftarkan di layanan Cyber Protection. Ini bukan akun administrator mitra. Saat Anda menggunakan parameter ini, menentukan parameter `--registration` bersifat opsional. Jangan gunakan parameter ini dengan parameter `--reg-token`.

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
`--reg-token=`<token>	Token pendaftaran. Token pendaftaran adalah rangkaian 12 karakter, dipisahkan menjadi tiga segmen dengan tanda hubung. Untuk informasi lebih lanjut tentang cara membuatnya, lihat "Membuat token pendaftaran" (hlm. 167). Saat Anda menggunakan parameter ini, menentukan parameter `--registration` bersifat opsional. Jangan gunakan parameter ini dengan parameter `--reg-login` dan `--reg-password`.
`--register-only`	Gunakan parameter ini untuk melewati instalasi dan mendaftarkan agen dengan menggunakan protokol OAuth 2.0 (alur perangkat). Setelah instalasi selesai, halaman registrasi terbuka secara otomatis. Jangan gunakan `--register-only` dengan parameter `--quiet`.
Akun masuk untuk layanan agen	
`--agent-account=`{system | new | custom} atau `--agent-account-login=`<login> `--agent-account-password=`<password>	Gunakan parameter ini untuk menentukan akun masuk yang akan menjalankan layanan agen. Untuk informasi lebih lanjut tentang akun masuk, lihat "Mengubah akun masuk pada mesin Windows" (hlm. 84). Untuk menggunakan akun **Sistem Lokal**, tentukan `--agent-account=system` atau jangan gunakan parameter `--agent-account` dalam perintah Anda. Untuk membuat layanan agen berjalan di bawah akun masuk baru, **Acronis Agent User**, yang dibuat secara otomatis, tentukan `baru`. Untuk membuat layanan agen berjalan pada akun yang sudah ada, tentukan kredensial akun dengan menggunakan parameter `--agent-account-login` dan `--agent-account-password`. Dalam hal ini, menentukan parameter `--agent-account=custom` bersifat opsional.
Parameter vCenter/ESXi	
`--esxi-address=`<host>	Nama host atau alamat IP vCenter Server atau host ESXi. Gunakan parameter ini saat Anda menginstal Agen untuk VMware.
`--esxi-login=`<login>	Kredensial akses ke vCenter Server atau host ESXi.

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
`--esxi-password=`<password>	Gunakan parameter ini saat Anda menginstal Agen untuk VMware.
Parameter proxy	
`--http-proxy=`{none | system | custom}	Gunakan parameter ini untuk menentukan server proxy HTTP yang ingin Anda gunakan untuk pencadangan dan pemulihan dari penyimpanan cloud. Jika menonaktifkan koneksi server proxy, tentukan `--http-proxy=none`. Untuk menggunakan server proxy seluruh sistem, tentukan `--http-proxy=system` atau jangan gunakan parameter `--http-proxy` dalam perintah Anda. Untuk menggunakan server proxy lain, tentukan alamat dan kredensial server proxy dengan menggunakan parameter `--http-proxy-address`, `--http-proxy-login`, dan `--http-proxy-password`. Dalam hal ini, menentukan parameter `--http-proxy=custom` bersifat opsional.
`--http-proxy-address=`<host>:<port>	Nama host atau alamat IP, dan port server proxy HTTP kustom.
`--http-proxy-login=`<login>	Masuk untuk server proksi HTTP kustom.
`--http-proxy-password=`<password>	Kata sandi untuk server proksi HTTP kustom.
Parameter penghapusan instalasi	
`--remove-components=`<component1,component2,...,componentN>	Komponen yang akan dihapus instalasinya. Lihat daftar lengkap komponen yang tersedia di "Komponen untuk instalasi tanpa pengawasan (EXE)" (hlm. 94). Saat Anda menentukan beberapa komponen, pisahkan dengan koma. Jangan menambahkan spasi sebelum atau sesudah koma. **Penting** Dengan menggunakan parameter ini, Anda hanya dapat menghapus instalasi komponen saja. Untuk menghapus instalasi produk sepenuhnya, buka Panel Kontrol Windows > Program dan Fitur, pilih produk, lalu klik **Uninstall**.
`--delete-all-settings`	Gunakan parameter opsional ini saat Anda menggunakan parameter `--remove-components` untuk menghapus semua log produk, tugas, dan pengaturan konfigurasi.

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
`--anti-tamper-password=<password>`	Kata sandi diperlukan untuk membatalkan instalasi Agen untuk Windows yang diproteksi kata sandi atau memodifikasi komponennya.

Komponen untuk instalasi tanpa pengawasan (EXE)

Tabel di bawah ini merangkum komponen yang dapat Anda gunakan untuk instalasi tanpa pengawasan melalui file EXE. Gunakan nama nilai untuk menentukan nilai parameter `--add-components`.

Untuk informasi lebih lanjut, lihat "Parameter untuk instalasi tanpa pengawasan (EXE)" (hlm. 89)"Parameter untuk instalasi tanpa pengawasan (MSI)" (hlm. 98)

Nama nilai	Deskripsi komponen
`agentForWindows`	Agen untuk Windows
`agentForSas`	Agen untuk Files Sync & Share
`agentForAd`	Agen untuk Active Directory
`agentForAmp`	Agen untuk Proteksi Antimalware dan Agen untuk penyaringan URL
`agentForDlp`	Agen untuk Pencegahan Kebocoran Data
`agentForEsx`	Agen untuk VMware (Windows)
`agentForExchange`	Agen untuk Exchange
`agentForHyperV`	Agen untuk Hyper-V
`agentForOffice365`	Agen untuk Office 365
`agentForOracle`	Agen untuk Oracle
`agentForSql`	Agen untuk SQL
`commandLine`	Command-Line Tool
`mediaBuilder`	Pembangun Media Yang Dapat Di-Boot
`trayMonitor`	Monitor Cyber Protect
`all`	Nilai ini menggabungkan semua komponen.
`allAgents`	Nilai ini menyatukan semua agen.

Instalasi dan penghapusan instalasi tanpa pengawasan dengan file MSI

Untuk jenis instalasi tanpa pengawasan ini, gunakan Windows Installer (program `Msiexec`). Ekstrak paket instalasi dan file MSI terlebih dahulu, dengan menggunakan antarmuka pengguna grafis dari

© Acronis International GmbH, 2003-2024

program pengaturan.

Saat Anda menginstal komponen dengan file MSI, Anda dapat menggunakan file transformasi MST untuk menyesuaikan parameter instalasi. Untuk informasi lebih lanjut tentang cara menggunakan kombinasi file MSI dan MST, lihat "Menginstal agen and komponen (kombinasi MSI dan MST)" (hlm. 96). Anda dapat menggunakan metode instalasi ini di domain Active Directory untuk menginstal agen perlindungan dengan menggunakan Kebijakan Grup Windows. Untuk informasi lebih lanjut, lihat "Menyebarkan agen melalui Kebijakan Grup" (hlm. 167).

Alternatifnya, Anda dapat menentukan parameter instalasi secara manual pada baris perintah. Dalam hal ini, Anda tidak memerlukan file MST. Untuk informasi lebih lanjut, lihat "Contoh" (hlm. 97).

Mengekstrak file MSI, MST, dan CAB

Ekstrak file MSI, MST, dan CAB dengan paket instalasi dengan menjalankan antarmuka pengguna grafis dari program penyiapan.

Untuk mengekstrak file MSI, MST, dan CAB

1. Jalankan antarmuka pengguna grafis dari program penyiapan, lalu klik **Buat file .mst dan .msi untuk instalasi tanpa pengawasan**.
2. Di **Apa yang diinstal**, pilih komponen yang ingin Anda instal, lalu klik **Selesai**.
   Paket instalasi untuk komponen ini akan diekstraksi dari program penyiapan sebagai file CAB.
3. Dalam **Pengaturan registrasi**, pilih **Gunakan kredensial** atau **Gunakan token pendaftaran**. Bergantung pada pilihan Anda, tentukan kredensial atau token pendaftaran, lalu klik **Selesai**.
   Untuk informasi lebih lanjut tentang cara membuat token pendaftaran, lihat "Membuat token pendaftaran" (hlm. 167).
4. [Hanya saat melakukan instalasi di pengontrol domain] di **Akun masuk untuk layanan agen**, pilih **Gunakan akun berikut**. Tentukan akun pengguna yang layanan agennya akan dijalankan, lalu klik **Selesai**. Untuk alasan keamanan, program penyiapan tidak membuat akun baru secara otomatis di pengontrol domain.

   Catatan
   Akun pengguna yang Anda tentukan harus diberi hak `Log sebagai layanan`. Akun ini harus telah digunakan di pengontrol domain, agar folder profilnya dibuat di mesin tersebut.

   Untuk informasi lebih lanjut tentang menginstal agen pada pengontrol domain hanya baca, lihat artikel basis pengetahuan ini.
5. Tinjau atau ubah pengaturan instalasi lain yang akan ditambahkan ke file MST, lalu klik **Lanjutkan**.
6. Pilih folder tempat file MSI, MST, dan CAB akan diekstraksi, lalu klik **Hasilkan**.

© Acronis International GmbH, 2003-2024

Menginstal agen and komponen (kombinasi MSI dan MST)

Gunakan file MST untuk menyesuaikan pengaturan instalasi untuk file MSI. Gunakan kombinasi MSI dan MST saat Anda menginstal agen di beberapa mesin melalui Kebijakan Grup Windows. Untuk informasi lebih lanjut, lihat "Menyebarkan agen melalui Kebijakan Grup" (hlm. 167).

Untuk menginstal komponen dengan file MSI dan MST

1. Ekstrak file MSI dan MST seperti yang dijelaskan di "Mengekstrak file MSI, MST, dan CAB" (hlm. 95).
2. Pada antarmuka baris perintah mesin tempat Anda ingin menginstal komponen, jalankan perintah berikut:

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

   Misalnya:

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

Menginstal dan mencopot agen and komponen (MSI dan pemilihan langsung)

Jalankan file MSI, pilih secara manual komponen yang akan diinstal, dan tentukan parameter instalasinya pada baris perintah. Dalam hal ini, Anda tidak memerlukan file MST.

Untuk menginstal agen dan komponen

1. Ekstrak file MSI dan paket instalasi (file CAB) seperti yang dijelaskan di "Mengekstrak file MSI, MST, dan CAB" (hlm. 95).

   Untuk metode instalasi ini, Anda hanya memerlukan file MSI dan CAB saja. Anda tidak memerlukan file MST.
2. Pada antarmuka baris perintah mesin, jalankan perintah berikut:

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

   Gunakan spasi untuk memisahkan parameter, dan koma tanpa spasi untuk memisahkan nilai parameter. Misalnya:

   ```
   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
   ```

   Untuk memeriksa parameter yang tersedia dan nilainya, lihat "Parameter untuk instalasi tanpa pengawasan (MSI)" (hlm. 98).

© Acronis International GmbH, 2003-2024

Contoh

- Menginstal Agen untuk Windows, Agen untuk Antimalware, Agen untuk penyaringan URL, Alat Baris Perintah, dan Cyber Protect Monitor. Mendaftarkan beban kerja di layanan Cyber Protection dengan menggunakan nama pengguna dan kata sandi.

```
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
```

- Menginstal Agen untuk Windows, Alat Baris Perintah, dan Cyber Protect Monitor. Membuat akun masuk baru untuk layanan agen di Windows. Mendaftarkan beban kerja di layanan Cyber Protection dengan menggunakan 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
```

- Menginstal Agen untuk Windows, Alat Baris Perintah, Agen untuk Oracle dan Cyber Protect Monitor. Mendaftarkan mesin di layanan Cyber Protection dengan menggunakan nama pengguna dan dikodekan dalam kata sandi base64. Anda mungkin perlu menyandikan kata sandi Anda jika berisi karakter khusus atau spasi kosong. Untuk informasi lebih lanjut tentang cara menyandikan kata sandi, lihat "Kata sandi dengan karakter spesial atau spasi kosong" (hlm. 122).

```
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==
```

- Menginstal Agen untuk Windows, Alat Baris Perintah, dan Cyber Protect Monitor. Mendaftarkan mesin di layanan Cyber Protection dengan menggunakan token. Mengatur proksi 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
```

Untuk mencopot komponen yang sudah diinstal

1. Ekstrak file MSI dan paket instalasi (file CAB) seperti yang dijelaskan di "Mengekstrak file MSI, MST, dan CAB" (hlm. 95).

© Acronis International GmbH, 2003-2024

Untuk metode instalasi ini, Anda hanya memerlukan file MSI dan CAB saja. Anda tidak memerlukan file MST.

2. Pada antarmuka baris perintah mesin, jalankan perintah berikut:

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

Untuk memeriksa parameter yang tersedia dan nilainya, lihat "Parameter untuk instalasi tanpa pengawasan (MSI)" (hlm. 98).

Contoh

- Menghapus monitor Cyber Protect.

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

Untuk menghapus instalasi agen

1. Ekstrak file MSI dan paket instalasi (file CAB) seperti yang dijelaskan di "Mengekstrak file MSI, MST, dan CAB" (hlm. 95).

   Untuk metode instalasi ini, Anda hanya memerlukan file MSI dan CAB saja. Anda tidak memerlukan file MST.
2. Pada antarmuka baris perintah mesin, jalankan perintah berikut:

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

Untuk memeriksa parameter yang tersedia dan nilainya, lihat "Parameter untuk instalasi tanpa pengawasan (MSI)" (hlm. 98).

Contoh

- Menghapus instalasi Agen untuk Windows dan semua komponennya. Menghapus semua log, tugas, dan pengaturan konfigurasi.

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

- Menghapus instalasi Agen untuk Windows yang dilindungi kata sandi dan semua komponennya. Menghapus semua log, tugas, dan pengaturan konfigurasi.

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

Parameter untuk instalasi tanpa pengawasan (MSI)

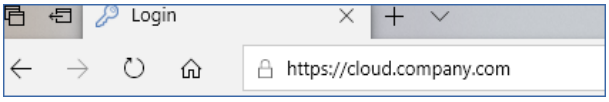
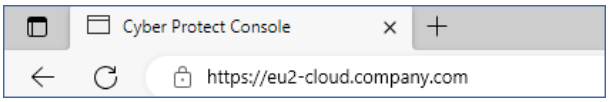
Tabel berikut merangkum parameter untuk instalasi tanpa pengawasan saat Anda menggunakan file MSI.

© Acronis International GmbH, 2003-2024

Anda dapat menggunakan parameter `msiexec` tambahan. Sebagai contoh, gunakan `/qn` untuk mencegah tampilnya elemen GUI apapun. Untuk mempelajari lebih lanjut tentang parameter `msiexec`, lihat dokumentasi Microsoft.

Parameter	Deskripsi
Parameter umum	
`ADDLOCAL=` <component1,component2,...,componentN>	Komponen yang akan diinstal. Lihat daftar lengkap komponen yang tersedia di "Komponen untuk instalasi tanpa pengawasan (MSI)" (hlm. 102). Saat Anda menentukan beberapa komponen, pisahkan dengan koma. Jangan menambahkan spasi sebelum atau sesudah koma. **Catatan** Anda harus mengekstrak file instalasi untuk semua komponen yang ingin Anda instal. Untuk informasi lebih lanjut tentang cara mengekstraknya, lihat "Mengekstrak file MSI, MST, dan CAB" (hlm. 95).
`TARGETDIR=`<path>	Folder tempat komponen yang dipilih akan diinstal. Jika folder yang ditentukan tidak ada, maka folder tersebut akan dibuat. Jika Anda tidak menentukan parameter ini, folder default akan digunakan: `C:\Program Files\BackupClient`.
`REBOOT=ReallySuppress`	Tentukan parameter ini jika Anda ingin memasang komponen tanpa menghidupkan ulang mesin.
`/l*v` <log file>	Tentukan parameter ini untuk menyimpan log verbose. Log ini diperlukan jika Anda hendak menginvestigasi masalah instalasi.
`CURRENT_LANGUAGE=`<language ID>	Bahasa produk. Nilai-nilai berikut tersedia: 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. Jika Anda tidak menentukan parameter ini, dan bahasa sistem mesin tempat Anda melakukan instalasi tercantum di atas, maka bahasa sistem akan digunakan. Dalam semua kasus lainnya, nilainya ditetapkan ke en.
`SKIP_SHA2_KB_CHECK={0,1}`	Gunakan parameter ini untuk memeriksa apakah pembaruan dukungan penandatanganan kode SHA2 dari Microsoft (KB4474419) diinstal pada mesin. Pemeriksaan hanya berjalan pada sistem operasi yang

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
	memerlukan pembaruan ini. Untuk mengetahui apakah ini diperlukan untuk sistem operasi Anda, lihat "Sistem operasi dan lingkungan yang Didukung" (hlm. 23). Gunakan parameter ini dengan nilai yang disetel ke `1` untuk melewatkan pemeriksaan. Jika Anda tidak menentukan parameter atau menetapkan nilainya `0`, dan pembaruan dukungan penandatanganan kode SHA2 tidak ditemukan pada mesin, instalasi gagal.
`FSS_ONBOARDING_AUTO_START={0,1}`	Gunakan parameter ini dengan nilai yang disetel ke `1` untuk menampilkan File Sync & Share wizard on-boarding setelah instalasi tanpa pengawasan. Jika Anda tidak menentukan parameter ini atau menetapkan nilainya menjadi `0`, wizard on-boarding tidak akan ditampilkan.
Parameter pendaftaran	
`REGISTRATION_ADDRESS`	URL layanan Cyber Protection. Anda dapat menggunakan parameter ini dengan parameter `REGISTRATION_LOGIN` dan `REGISTRATION_PASSWORD`, atau dengan `REGISTRATION_TOKEN`. • Saat Anda menggunakannya dengan parameter `REGISTRATION_LOGIN` and `REGISTRATION_PASSWORD`, tentukan alamat yang Anda gunakan **untuk login** ke layanan Cyber Protection. Misalnya, `https://cloud.company.com`:  • Saat Anda menggunakannya dengan parameter `REGISTRATION_TOKEN`, tentukan alamat pusat data yang tepat. Ini adalah URL yang Anda lihat **setelah masuk** ke layanan Cyber Protection. Misalnya, `https://eu2-cloud.company.com`.  Jangan gunakan `https://cloud.company.com` dengan parameter `REGISTRATION_TOKEN`.

`REGISTRATION_LOGIN`
 	
`REGISTRATION_PASSWORD`
	Kredensial untuk akun tempat agen akan didaftarkan di layanan Cyber Protection. Ini bukan akun administrator mitra.

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
	Jangan gunakan parameter ini dengan parameter `REGISTRATION_TOKEN`.
`REGISTRATION_PASSWORD_ENCODED`	Kata sandi untuk akun tempat agen akan didaftarkan di layanan Cyber Protection, dikodekan dalam base64. Untuk informasi lebih lanjut tentang cara menyandikan kata sandi Anda, lihat "Kata sandi dengan karakter spesial atau spasi kosong" (hlm. 122).
`REGISTRATION_TOKEN`	Token registrasi. Token registrasi adalah rangkaian 12 karakter, dipisahkan menjadi tiga segmen dengan tanda hubung. Untuk informasi lebih lanjut tentang cara membuatnya, lihat "Membuat token pendaftaran" (hlm. 167). Jangan gunakan parameter ini dengan parameter `REGISTRATION_LOGIN` dan `REGISTRATION_PASSWORD`.
`REGISTRATION_REQUIRED={0,1}`	Gunakan parameter ini untuk memilih apa yang terjadi jika registrasi gagal. Jika Anda menetapkan nilainya menjadi `1`, instalasinya juga gagal. Jika Anda menetapkan nilai ke `0` atau tidak menentukan parameter, instalasi berhasil diselesaikan meskipun registrasi gagal.
Akun masuk untuk layanan agen	
`MMS_USE_SYSTEM_ACCOUNT={0,1}`	Gunakan parameter ini dengan nilai `1`, untuk membuat layanan berjalan di bawah akun masuk **Sistem Lokal**. Untuk informasi lebih lanjut tentang akun masuk, lihat "Mengubah akun masuk pada mesin Windows" (hlm. 84).
`MMS_CREATE_NEW_ACCOUNT={0,1}`	Gunakan parameter ini dengan nilai `1`, untuk membuat layanan agen berjalan di bawah akun masuk baru, **Acronis Agent User**, yang tercipta secara otomatis.

`MMS_SERVICE_USERNAME=<user name>`
 	
`MMS_SERVICE_PASSWORD=<password>`
	Gunakan parameter ini untuk menentukan akun masuk yang sudah ada yang akan menjalankan layanan agen.

Parameter vCenter/ESXi	
`SET_ESX_SERVER={0,1}`	Gunakan parameter ini saat Anda menginstal Agen untuk VMware. Jika Anda menetapkan nilai ke `0`, Agen untuk VMware tidak akan terhubung ke vCenter Server atau host ESXi. Jika Anda menetapkan nilainya menjadi `1`, tentukan

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
	parameter berikut: `ESX_HOST`, `EXI_USER`, `ESX_PASSWORD`.
`ESX_HOST=`<nama host>	Nama host atau alamat IP vCenter Server atau host ESXi.
`ESX_USER=`<user name> `ESX_PASSWORD=`<password>	Kredensial akses ke vCenter Server atau host ESXi.
Parameter proxy	
`HTTP_PROXY_ADDRESS=`<IP address> `HTTP_PROXY_PORT=`<port>	Gunakan parameter ini untuk menentukan server proxy HTTP yang akan digunakan agen. Jika Anda tidak menggunakan server proxy, jangan tentukan parameter ini.
`HTTP_PROXY_LOGIN=`<login> `HTTP_PROXY_PASSWORD=`<password>	Kredensial untuk server proksi HTTP. Gunakan parameter ini jika server proxy memerlukan autentikasi.
Parameter penghapusan instalasi	
`REMOVE={<list of components>|ALL}`	Komponen yang akan dihapus instalasinya. Saat Anda menentukan beberapa komponen, pisahkan dengan koma. Jangan menambahkan spasi sebelum atau sesudah koma. Untuk menghapus semua komponen produk, tetapkan nilainya menjadi `ALL`.
`DELETE_ALL_SETTINGS={0, 1}`	Untuk menghapus semua log produk, tugas, dan pengaturan konfigurasi, atur nilainya menjadi `1`. Gunakan parameter opsional ini saat Anda menggunakan parameter `REMOVE`.
`ANTI_TAMPER_PASSWORD=<password>`	Kata sandi diperlukan untuk membatalkan instalasi Agen untuk Windows yang diproteksi kata sandi atau memodifikasi komponennya.

Komponen untuk instalasi tanpa pengawasan (MSI)

Tabel di bawah ini merangkum komponen yang dapat Anda gunakan untuk instalasi tanpa pengawasan melalui file MSI. Gunakan nama nilai untuk menentukan nilai untuk parameter `ADDLOCAL`. Untuk informasi lebih lanjut, lihat "Parameter untuk instalasi tanpa pengawasan (MSI)" (hlm. 98).

Nama nilai	Deskripsi komponen	Harus diinstal bersama	Bitness

© Acronis International GmbH, 2003-2024

AgentFeature	Komponen inti untuk agen		32-bit/64-bit
MmsMspComponents	Komponen inti untuk pencadangan	AgentFeature	32-bit/64-bit
BackupAndRecoveryAgent	Agen untuk 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	Agen untuk Pencegahan Kebocoran Data	BackupAndRecoveryAgent	32-bit/64-bit
SasAgentFeature	Agen untuk File Sync & Share	TrayMonitor	32-bit/64-bit
ArxAgentFeature	Agen untuk Exchange	MmsMspComponents	32-bit/64-bit
ArsAgentFeature	Agen untuk SQL	BackupAndRecoveryAgent	32-bit/64-bit
ARADAgentFeature	Agen untuk Active Directory	BackupAndRecoveryAgent	32-bit/64-bit
ArxOnlineAgentFeature	Agen untuk Microsoft 365	MmsMspComponents	32-bit/64-bit
OracleAgentFeature	Agen untuk Oracle	BackupAndRecoveryAgent	32-bit/64-bit
AcronisESXSupport	Agen untuk VMware ESX(i) (Windows)	BackupAndRecoveryAgent	64-bit
HyperVAgent	Agen untuk Hyper-V	BackupAndRecoveryAgent	32-bit/64-bit
CommandLineTool	Command-Line Tool		32-bit/64-bit
TrayMonitor	Cyber Protect Monitor	AgentFeature	32-bit/64-bit

© Acronis International GmbH, 2003-2024

BackupAndRecoveryBootableComponents	Pembangun Media Yang Dapat Di-Boot		32-bit/64-bit

Instalasi atau penghapusan tanpa pengawasan di Linux

Bagian ini menjelaskan cara menginstal atau menghapus agen perlindungan dalam mode tanpa pengawasan pada mesin yang menjalankan Linux, menggunakan baris perintah.

Untuk menginstal agen

1. Buka Terminal.

2. Lakukan salah satu langkah berikut:

- Untuk memulai instalasi dengan menentukan parameter pada baris perintah, jalankan perintah berikut:

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

  Di sini, <package name> adalah nama paket instalasi (file .i686 atau .x86_64). Semua parameter yang tersedia beserta nilainya dijelaskan dalam "Parameter pemasangan atau penghapusan instalasi tanpa pengawasan" (hlm. 105).
- Untuk memulai instalasi dengan parameter yang ditentukan dalam file teks yang terpisah, jalankan perintah berikut:

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

  Pendekatan ini mungkin berguna jika Anda tidak ingin memasukkan informasi sensitif pada baris perintah. Dalam hal ini, Anda dapat menentukan pengaturan konfigurasi dalam file teks yang terpisah dan memastikan bahwa hanya Anda yang dapat mengaksesnya. Letakkan setiap parameter di baris baru, diikuti dengan nilai parameter tersebut, misalnya:

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

  atau

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


© Acronis International GmbH, 2003-2024

Jika parameter yang sama ditentukan pada baris perintah dan dalam file teks, nilai baris perintah melebihi.

3. Jika UEFI Secure Boot diaktifkan pada mesin, akan diinformasikan bahwa Anda harus memulai ulang sistem setelah instalasi. Pastikan bahwa Anda mengingat kata sandi apa (yang dari pengguna akar atau "acronis") yang harus digunakan. Selama memulai ulang sistem, pilih untuk manajemen MOK (Machine Owner Key), pilih **Daftarkan MOK**, lalu daftarkan kunci dengan menggunakan kata sandi yang disarankan.

Jika Anda mengaktifkan UEFI Secure Boot setelah instalasi agen, ulangi instalasi, termasuk langkah 3. Jika tidak, pencadangan akan gagal.

Untuk menghapus instalasi agen

1. Buka Terminal.
2. Lakukan salah satu langkah berikut:
   - Untuk menghapus instalan Agen dan menghapus semua log, tugas, dan pengaturan konfigurasi, jalankan perintah berikut:

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

   - Untuk menghapus instalan agen tetapi mempertahan ID-nya (misalnya, jika Anda berencana untuk menginstal agen nantinya), jalankan perintah berikut:

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

   - Untuk menghapus instalan agen menggunakan file instalasi, jalankan perintah berikut:

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

     Di sini, `<package name>` adalah nama paket instalasi (file .i686 atau .x86_64). Semua parameter yang tersedia beserta nilainya dijelaskan dalam "Parameter pemasangan atau penghapusan instalasi tanpa pengawasan" (hlm. 105).

     Catatan
     Gunakan perintah ini hanya saat paket instalasi adalah versi yang sama dengan agen yang diinstal dan jika `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` korup atau tidak dapat diakses.

Parameter pemasangan atau penghapusan instalasi tanpa pengawasan

Bagian ini menjelaskan parameter yang digunakan selama instalasi atau penghapusan instalasi tanpa pengawasan di Linux.

Konfigurasi minimal untuk instalasi tanpa pengawasan termasuk parameter `-a` dan pendaftaran (misalnya, parameter `--login` dan `--password`; parameter `--rain` dan `--token`). Anda dapat menggunakan lebih banyak parameter untuk menyesuaikan instalasi Anda.

© Acronis International GmbH, 2003-2024

Parameter instalasi

Parameter dasar

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

Komponen yang akan diinstal, dipisahkan dengan koma dan tanpa karakter spasi. Komponen berikut ini tersedia dalam paket instalasi .x86_64:

Komponen	Deskripsi komponen
BackupAndRecoveryAgent	Agen untuk Linux
AgentForPCS	Agen untuk Virtuozzo
OracleAgentFeature	Agen untuk Oracle
MySQLAgentFeature	Agen untuk MySQL/MariaDB

Tanpa parameter ini, semua komponen di atas akan diinstal.

Agen untuk Virtuozzo, Agen untuk Oracle, dan Agen untuk MySQL/MariaDB memerlukan Agen untuk Linux agar diinstal juga.

Paket instalasi .i686 hanya berisi BackupAndRecoveryAgent.

`{-a|--auto}`

Proses instalasi dan pendaftaran akan selesai tanpa interaksi pengguna lebih lanjut. Saat menggunakan parameter ini, Anda harus menentukan akun tempat agen akan terdaftar di layanan Cyber Protection, baik dengan menggunakan parameter `--token`, atau dengan menggunakan parameter `--login` dan `--password`.

`{-t|--strict}`

Jika parameter ditentukan, setiap peringatan yang terjadi selama instalasi akan mengakibatkan kegagalan instalasi. Tanpa parameter ini, instalasi akan berhasil meskipun terdapat peringatan.

`{-n|--nodeps}`

Ketidakadaan paket Linux yang diperlukan akan diabaikan selama instalasi.

`{-d|--debug}`

Menulis log instalasi dalam mode verbose.

`--options-file=<lokasi>`

Parameter instalasi akan dibaca dari file teks, bukan dari baris perintah.

`--language=<ID bahasa>`

© Acronis International GmbH, 2003-2024

Bahasa produk. Nilai yang tersedia adalah sebagai berikut: `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`.
Jika parameter ini tidak ditentukan, bahasa produk akan ditentukan oleh bahasa sistem Anda dengan ketentuan bahwa ada dalam daftar di atas. Jika tidak, bahasa produk akan diatur ke bahasa Inggris (`en`).

Parameter pendaftaran

Tentukan salah satu parameter berikut:

- `{-g|--login=}<nama pengguna>` dan `{-w|--password=}<kata sandi>`

  Kredensial untuk akun yang akan menjadi tempat agen terdaftar di layanan Cyber Protection. Ini bukan akun administrator mitra.

- `--token=<token>`

  Token pendaftaran adalah rangkaian dari 12 karakter, yang dipisahkan oleh tanda hubung dalam tiga segmen. Anda dapat menghasilkan satu di konsol Cyber Protect, seperti yang dijelaskan di "Menyebarkan agen melalui Kebijakan Grup".

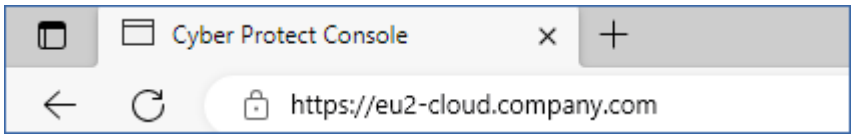
  Anda tidak dapat menggunakan parameter `--token` bersama dengan parameter `--login`, `--password`, dan `--register-with-credentials`.

  - `{-C|--rain=}<alamat layanan>`

    URL layanan Cyber Protection.

    Anda tidak perlu memasukkan parameter ini secara eksplisit ketika Anda menggunakan parameter `--login` dan `--password` untuk pendaftaran, karena penginstal secara default menggunakan alamat yang benar – ini akan menjadi alamat yang Anda gunakan **untuk masuk** ke layanan Cyber Protection. Misalnya:

    Namun, saat Anda menggunakan `{-C|--rain=}` dengan parameter `--token`, Anda harus menentukan alamat pusat data yang tepat. Ini adalah URL yang Anda lihat **setelah Anda masuk** ke layanan Cyber Protection. Misalnya:

- `--register-with-credentials`

  Jika parameter ini ditentukan, antarmuka grafis penginstal akan dimulai. Untuk menyelesaikan pendaftaran, masukkan nama pengguna dan kata sandi untuk akun tempat agen terdaftar di layanan Cyber Protection. Ini bukan akun administrator mitra.

- `--skip-registration`

© Acronis International GmbH, 2003-2024

Gunakan parameter ini jika Anda perlu menginstal agen tetapi Anda berencana untuk mendaftarkannya di layanan Cyber Protection nanti. Untuk informasi lebih lanjut tentang cara melakukan ini, lihat "Mendaftarkan mesin secara manual".

Parameter tambahan

`--http-proxy-host=<alamat IP>` dan `--http-proxy-port=<port>`

Server proksi HTTP yang akan digunakan agen untuk cadangan dan pemulihan dari awan, dan untuk koneksi ke server manajemen. Tanpa parameter ini, tidak ada server proksi yang akan digunakan.

`--http-proxy-login=<masuk>` dan `--http-proxy-password=<kata sandi>`

Kredensial untuk server proksi HTTP. Gunakan parameter ini jika server memerlukan autentikasi.

`--tmp-dir=<lokasi>`

Menetapkan folder tempat file sementara disimpan selama instalasi. Folder default adalah **/var/tmp**.

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

Pustaka yang dapat didistribusikan kembali akan digunakan selama instalasi, meskipun mungkin sudah ada pada sistem Anda.

`--skip-prereq-check`

Tidak akan ada pemeriksaan apakah paket yang diperlukan untuk menyusun modul snapapi sudah diinstal.

`--force-weak-snapapi`

Penginstal tidak akan menyusun modul snapapi. Sebagai gantinya, penginstal akan menggunakan modul yang sudah jadi yang mungkin tidak cocok dengan kernel Linux. Kami tidak menyarankan Anda menggunakan opsi ini.

`--skip-svc-start`

Layanan tidak akan mulai secara otomatis setelah instalasi. Paling sering, parameter ini digunakan dengan `--skip-registration`.

Parameter informasi

`{-?|--help}`

Menampilkan deskripsi parameter.

`--usage`

Menampilkan deskripsi singkat tentang penggunaan perintah.

`{-v|--version}`

© Acronis International GmbH, 2003-2024

Menampilkan versi paket instalasi.

`--product-info`

Menunjukkan nama produk dan versi paket instalasi.

`--snapapi-list`

Menampilkan modul snapapi siap pakai yang tersedia.

`--components-list`

Menampilkan komponen penginstal.

Parameter untuk fitur lama

Parameter ini terkait dengan komponen lama, agent.exe.

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

Menetapkan jalur ke file sertifikat kustom untuk komunikasi SSL.

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

Menetapkan port di mana agent.exe mendengarkan koneksi. Port defaultnya adalah 9876.

Parameter penghapusan instalasi

`{-u|--uninstall}`

Menghapus instalasi produk.

`--purge`

Menghapus instalasi produk dan menghapus log, tugas, dan pengaturan konfigurasinya. Anda tidak perlu menentukan parameter `--uninstall` secara eksplisit ketika Anda menggunakan yang `--purge`.

Contoh

- Menginstal Agen untuk Linux tanpa mendaftarkannya.

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

- Menginstal Agen untuk Linux, Agen untuk Virtuozzo, dan Agen untuk Oracle, dan mendaftarkannya dengan menggunakan kredensial.

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

- Menginstal Agen untuk Oracle dan Agen untuk Linux, dan mendaftarkannya dengan menggunakan token pendaftaran.

© 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
```

- Menginstal Agen untuk Linux, Agen untuk Virtuozzo, dan Agen untuk Oracle dengan pengaturan konfigurasi dalam file teks yang terpisah.

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

- Menghapus instalasi Agen untuk Linux, Agen untuk Virtuozzo, dan Agen untuk Oracle, serta menghapus semua log, tugas, dan pengaturan konfigurasinya.

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

Instalasi dan penghapusan instalasi tanpa pengawasan di macOS

Bagian ini menjelaskan cara menginstal, mendaftar, dan menghapus instalan agen proteksi dalam mode tanpa pengawasan pada mesin yang menjalankan macOS menggunakan baris perintah.

Izin yang diperlukan

Sebelum Anda memulai instalasi tanpa pengawasan pada beban kerja Mac, Anda harus mengubah Kontrol Kebijakan Preferensi Privasi untuk mengizinkan akses Aplikasi serta ekstensi kernel dan sistem di macOS beban kerja untuk memungkinkan instalasi agen Cyber Protection. Lihat "Izin yang diperlukan untuk instalasi tanpa pengawasan di macOS" (hlm. 112).

Setelah menyebarkan payload PPPC, Anda dapat melanjutkan dengan prosedur di bawah.

Untuk mengunduh file instalasi (.dmg)

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Klik **Tambah**, lalu klik **Mac**.

Untuk menginstal agen

1. Buka Terminal.
2. Buat direktori sementara tempat Anda akan memasang file instalasi (dmg).

   ```
   mkdir <dmg_root>
   ```

   Di sini, `<dmg_root>` adalah nama pilihan Anda.
3. Pasang file .dmg.

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

   Di sini, `<dmg_file>` adalah nama file instalasi. Misalnya, **Cyber_Protection_Agent_for_MAC_x64.dmg**.
4. Jalankan penginstal.

© Acronis International GmbH, 2003-2024

- Jika Anda menggunakan penginstal penuh untuk Mac, seperti `CyberProtect_AgentForMac_x64.dmg` atau `CyberProtect_AgentForMac_arm64.dmg`, jalankan perintah berikut.

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

  Catatan
  Jika Anda ingin mengaktifkan onboarding otomatis untuk File Sync & Share, jalankan perintah berikut. Opsi ini akan meminta kata sandi administrator.

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

- Jika Anda menggunakan penginstal universal untuk Mac, seperti `CyberProtect_AgentForMac_web.dmg`, jalankan perintah berikut.

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

5. Lepaskan file instalasi (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Contoh

```
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
```

Untuk menghapus instalasi agen

1. Buka Terminal.
2. Lakukan salah satu langkah berikut:
   - Untuk menghapus instalan agen, jalankan perintah berikut:

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

   - Untuk menghapus instalan Agen dan menghapus semua log, tugas, dan pengaturan konfigurasi, jalankan perintah berikut:

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


© Acronis International GmbH, 2003-2024

Izin yang diperlukan untuk instalasi tanpa pengawasan di macOS

Sebelum Anda memulai instalasi tanpa pengawasan pada beban kerja Mac, Anda harus mengubah Kontrol Kebijakan Preferensi Privasi untuk mengizinkan akses Aplikasi serta ekstensi kernel dan sistem di macOS beban kerja untuk memungkinkan instalasi agen Cyber Protection. Anda dapat melakukan hal ini dengan menyebarkan payload PPPC khusus atau dengan mengonfigurasi preferensi di antarmuka pengguna grafis beban kerja. Izin berikut diperlukan.

Persyaratan untuk macOS 11 (Big Sur) atau yang lebih baru

Tab	Bagian	Bidang	Nilai

© Acronis International GmbH, 2003-2024

Kontrol Kebijakan Preferensi Privasi	Akses Aplikasi	Pengidentifikasi	com.acronis.backup

© Acronis International GmbH, 2003-2024

		Jenis Pengidentifikasi	ID Bundel
		Persyaratan Kode	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
		APLIKASI ATAU LAYANAN	SystemPolicyAllFiles
		AKSES	Izinkan
	Akses Aplikasi	Pengidentifikasi	com.acronis.backup.aakore
		Jenis Pengidentifikasi	ID Bundel
		Persyaratan Kode	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
		APLIKASI ATAU LAYANAN	SystemPolicyAllFiles
		AKSES	Izinkan
	Akses Aplikasi	Diidentifikasi	com.acronis.backup.activeprotection
		Jenis Pengidentifikasi	ID Bundel
		Persyaratan Kode	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
		APLIKASI ATAU LAYANAN	SystemPolicyAllFiles
		AKSES	Izinkan

© Acronis International GmbH, 2003-2024

	Akses Aplikasi	Pengidentifikasi	cyber-protect-service
		Jenis Pengidentifikasi	ID Bundel
		Persyaratan Kode	`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`
		APLIKASI ATAU LAYANAN	SystemPolicyAllFiles
		AKSES	Izinkan
Ekstensi Sistem		Izinkan pengguna menyetujui ekstensi sistem	Diaktifkan
	Tim ID dan Ekstensi Sistem yang Diizinkan	Nama Tampilan	Ekstensi Sistem Agen Acronis Cyber Protection
		Jenis Ekstensi Sistem	Pengidentifikasi Tim yang Diizinkan
		Pengidentifikasi Tim	ZU2TV78AA6

Persyaratan untuk versi macOS sebelum versi 11

Tab	Bagian	Bidang	Nilai

© Acronis International GmbH, 2003-2024

Kontrol Kebijakan Preferensi Privasi	Akses Aplikasi	Pengidentifikasi	com.acronis.backup

© Acronis International GmbH, 2003-2024

		Jenis Pengidentifikasi	ID Bundel
		Persyaratan Kode	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
		APLIKASI ATAU LAYANAN	SystemPolicyAllFiles
		AKSES	Izinkan
	Akses Aplikasi	Pengidentifikasi	com.acronis.backup.aakore
		Jenis Pengidentifikasi	ID Bundel
		Persyaratan Kode	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
		APLIKASI ATAU LAYANAN	SystemPolicyAllFiles
		AKSES	Izinkan
	Akses Aplikasi	Diidentifikasi	com.acronis.backup.activeprotection
		Jenis Pengidentifikasi	ID Bundel
		Persyaratan Kode	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
		APLIKASI ATAU LAYANAN	SystemPolicyAllFiles
		AKSES	Izinkan

© Acronis International GmbH, 2003-2024

	Akses Aplikasi	Pengidentifikasi	cyber-protect-service
		Jenis Pengidentifikasi	ID Bundel
		Persyaratan Kode	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
		APLIKASI ATAU LAYANAN	SystemPolicyAllFiles
		AKSES	Izinkan
Ekstensi Kernel yang Disetujui		Izinkan pengguna menyetujui ekstensi kernel	Diaktifkan
		Izinkan pengguna standar menyetujui ekstensi kernel lama (macOS 11 atau yang lebih baru)	Diaktifkan
	ID Tim dan Ekstensi Kernel yang Disetujui	ID Tim yang Disetujui - Nama Tampilan	Ekstensi Kernel Agen Acronis Cyber Protection
		ID Tim	ZU2TV78AA6
		ID Bundel Ekstensi Kernel	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
Ekstensi Sistem		Izinkan pengguna menyetujui ekstensi sistem	Diaktifkan
	Tim ID dan Ekstensi Sistem yang Diizinkan	Nama Tampilan	Ekstensi Sistem Agen Acronis Cyber Protection
		Jenis Ekstensi Sistem	Pengidentifikasi Tim yang Diizinkan
		Pengidentifikasi Tim	ZU2TV78AA6

© Acronis International GmbH, 2003-2024

Mendaftarkan dan membatalkan pendaftaran beban kerja secara manual

Beban kerja secara otomatis terdaftar di layanan Cyber Protection saat Anda menginstal agen proteksi. Saat Anda membatalkan pendaftaran agen proteksi, beban kerja secara otomatis dibatalkan pendaftarannya dan menghilang dari konsol Cyber Protect.

Anda juga dapat mendaftarkan beban kerja secara manual, dengan menggunakan antarmuka baris perintah. Anda mungkin perlu menggunakan registrasi manual, misalnya, jika registrasi otomatis gagal atau jika Anda ingin memindahkan beban kerja ke penyewa baru atau akun pengguna baru.

Untuk mendaftarkan beban kerja menggunakan nama pengguna dan kata sandi

Di Windows

Di baris perintah, jalankan perintah berikut:

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

Misalnya:

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

Di Linux

Di baris perintah, jalankan perintah berikut:

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

Misalnya:

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

Di macOS

Di baris perintah, jalankan perintah berikut:

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

Misalnya:

© 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
```

Catatan
Gunakan nama pengguna dan kata sandi untuk akun yang dipakai untuk mendaftar beban kerja. Ini bukan akun administrator mitra.

Alamat layanan adalah URL yang Anda gunakan **untuk masuk** ke layanan Cyber Protection. Misalnya, `https://cloud.company.com`.

Penting
Jika kata sandi Anda berisi karakter spesial atau spasi kosong, lihat "Kata sandi dengan karakter spesial atau spasi kosong" (hlm. 122).

Penting
Jika Anda menggunakan macOS 10.14 atau yang lebih baru, berikan akses disk penuh kepada agen perlindungan. Untuk melakukannya, tuju **Aplikasi** >**Utilitas**, dan lalu jalankan **Asisten Agen Cyber Protect**. Selanjutnya, ikuti petunjuk dalam jendela aplikasi.

Untuk mendaftarkan beban kerja dengan menggunakan token registrasi

Di Windows

Di baris perintah, jalankan perintah berikut:

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

Misalnya:

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

Di Linux

Di baris perintah, jalankan perintah berikut:

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

Misalnya:

© 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
```

Di macOS

Di baris perintah, jalankan perintah berikut:

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

Misalnya:

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

Penting
Jika Anda menggunakan macOS 10.14 atau yang lebih baru, berikan akses disk penuh kepada agen perlindungan. Untuk melakukannya, tuju **Aplikasi** >**Utilitas**, dan lalu jalankan **Asisten Agen Cyber Protect**. Selanjutnya, ikuti petunjuk dalam jendela aplikasi.

Alat virtual

1. Di konsol alat virtual, tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.
2. Pada saran perintah, jalankan perintah berikut:

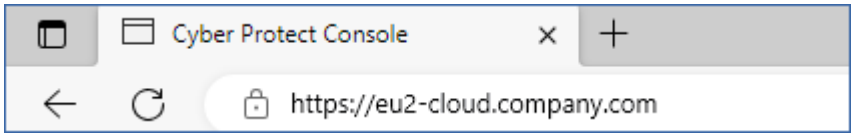
   ```
   register_agent -o register -t cloud -a <service address> --token <registration token>
   ```

   Misalnya:

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

3. Untuk kembali ke antarmuka grafis alat, tekan ALT+F1.

Catatan
Saat Anda menggunakan token registrasi, Anda harus menentukan alamat pusat data yang tepat. Ini adalah URL yang Anda lihat **setelah masuk** ke layanan Cyber Protection. Misalnya, `https://eu2-cloud.company.com`.



Jangan gunakan `https://cloud.company.com` di sini.

Token pendaftaran adalah rangkaian dari 12 karakter, yang dipisahkan oleh tanda hubung dalam tiga segmen. Untuk informasi lebih lanjut tentang cara membuatnya, lihat "Membuat token pendaftaran" (hlm. 167).

© Acronis International GmbH, 2003-2024

Untuk membatalkan pendaftaran beban kerja

Di Windows

Di baris perintah, jalankan perintah berikut:

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

Misalnya:

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

Di Linux

Di baris perintah, jalankan perintah berikut:

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

Di macOS

Di baris perintah, jalankan perintah berikut:

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

Alat virtual

1. Di konsol alat virtual, tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.
2. Pada saran perintah, jalankan perintah berikut:

   ```
   register_agent -o unregister
   ```

3. Untuk kembali ke antarmuka grafis alat, tekan ALT+F1.

Memindahkan beban kerja ke penyewa lain

Memindahkan beban kerja ke penyewa lain tidak didukung secara asli. Sebagai solusinya, Anda dapat membatalkan pendaftaran beban kerja, lalu mendaftarkannya di penyewa lain. Semua rencana proteksi yang diterapkan akan dicabut dari beban kerja tersebut, dan rencana tersebut akan kehilangan akses ke cadangannya di penyimpanan cloud penyewa asli.

Untuk informasi lebih lanjut tentang cara mendaftarkan beban kerja di penyewa baru atau di bawah akun pengguna baru, lihat "Mengubah registrasi beban kerja" (hlm. 123).

Kata sandi dengan karakter spesial atau spasi kosong

Jika kata sandi Anda berisi karakter spesial atau spasi kosong, lampirkan dengan tanda kutip saat Anda mengetiknya pada baris perintah.

Misalnya, di Windows, jalankan perintah ini:

 © Acronis International GmbH, 2003-2024

Templat perintah:

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

Contoh perintah:

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

Jika perintah ini gagal, kodekan kata sandi Anda ke dalam format base64 di https://www.base64encode.org/. Lalu, pada baris perintah, tentukan kata sandi yang dikodekan dengan menggunakan parameter -b atau --base64.

Misalnya, di Windows, jalankan perintah ini:

Templat perintah:

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

Contoh perintah:

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

Mengubah registrasi beban kerja

Anda dapat mengubah registrasi beban kerja saat ini dengan mendaftarkannya ke penyewa baru atau akun pengguna baru.

Penting
Saat Anda mengubah registrasi beban kerja, semua rencana proteksi yang berlaku pada beban kerja tersebut akan dibatalkan. Untuk melanjutkan proteksi beban kerja, terapkan rencana proteksi yang baru.

Jika Anda mendaftar beban kerja di penyewa baru, beban kerja akan kehilangan akses ke cadangan di penyimpanan awan penyewa asli. Cadangan di penyimpanan non-awan akan tetap dapat diakses.

Anda dapat mengubah registrasi beban kerja dengan menggunakan baris perintah atau menggunakan penginstal GUI. Saat Anda menggunakan baris perintah, Anda tidak akan perlu menghapus instalasi agen.

Untuk mengubah registrasi beban kerja

Dengan menggunakan baris perintah

© Acronis International GmbH, 2003-2024

1. Batalkan pendaftaran agen proteksi, sebagaimana dijelaskan di "Untuk membatalkan pendaftaran beban kerja" (hlm. 122).
2. Daftarkan agen proteksi di penyewa baru atau akun pengguna baru, sebagaimana dijelaskan di "Untuk mendaftarkan beban kerja menggunakan nama pengguna dan kata sandi" (hlm. 119) atau di "Untuk mendaftarkan beban kerja dengan menggunakan token registrasi" (hlm. 120).

Dengan menggunakan penginstal GUI

1. Hapus instalasi agen proteksi.
2. Instal agen proteksi, lalu daftarkan di penyewa baru atau akun pengguna baru.

Untuk informasi lebih lanjut tentang cara menginstal dan mendaftarkan agen, lihat "Menginstal agen proteksi" (hlm. 75).

Penemuan manual mesin

Dengan penemuan otomatis, Anda dapat:

- Mengotomatiskan instalasi agen perlindungan dan registrasi mesin dengan mendeteksi mesin di domain Active Directory Anda atau jaringan lokal.
- Instal dan perbarui agen perlindungan pada beberapa mesin.
- Gunakan sinkronisasi dengan Active Directory, untuk mengurangi upaya penyediaan sumber daya dan mengelola mesin dalam domain Active Directory besar.

Prasyarat

Untuk melakukan autodiscovery, Anda membutuhkan setidaknya satu mesin dengan agen perlindungan terinstal di jaringan lokal atau domain Active Directory Anda. Agen ini digunakan sebagai agen penemuan.

Penting
Hanya agen yang diinstal di mesin Windows yang dapat menjadi agen penemuan. Jika tidak ada agen penemuan di lingkungan Anda, Anda tidak akan dapat menggunakan opsi **Beberapa perangkat** di panel **Tambah perangkat**.

Instalasi jarak jauh agen didukung hanya untuk mesin yang menjalankan Windows (Windows XP tidak didukung). Untuk instalasi jarak jauh pada mesin yang menjalankan Windows Server 2012 R2, Anda harus memiliki Windows update KB2999226 yang terinstal di mesin ini.

Cara kerja autodiscovery

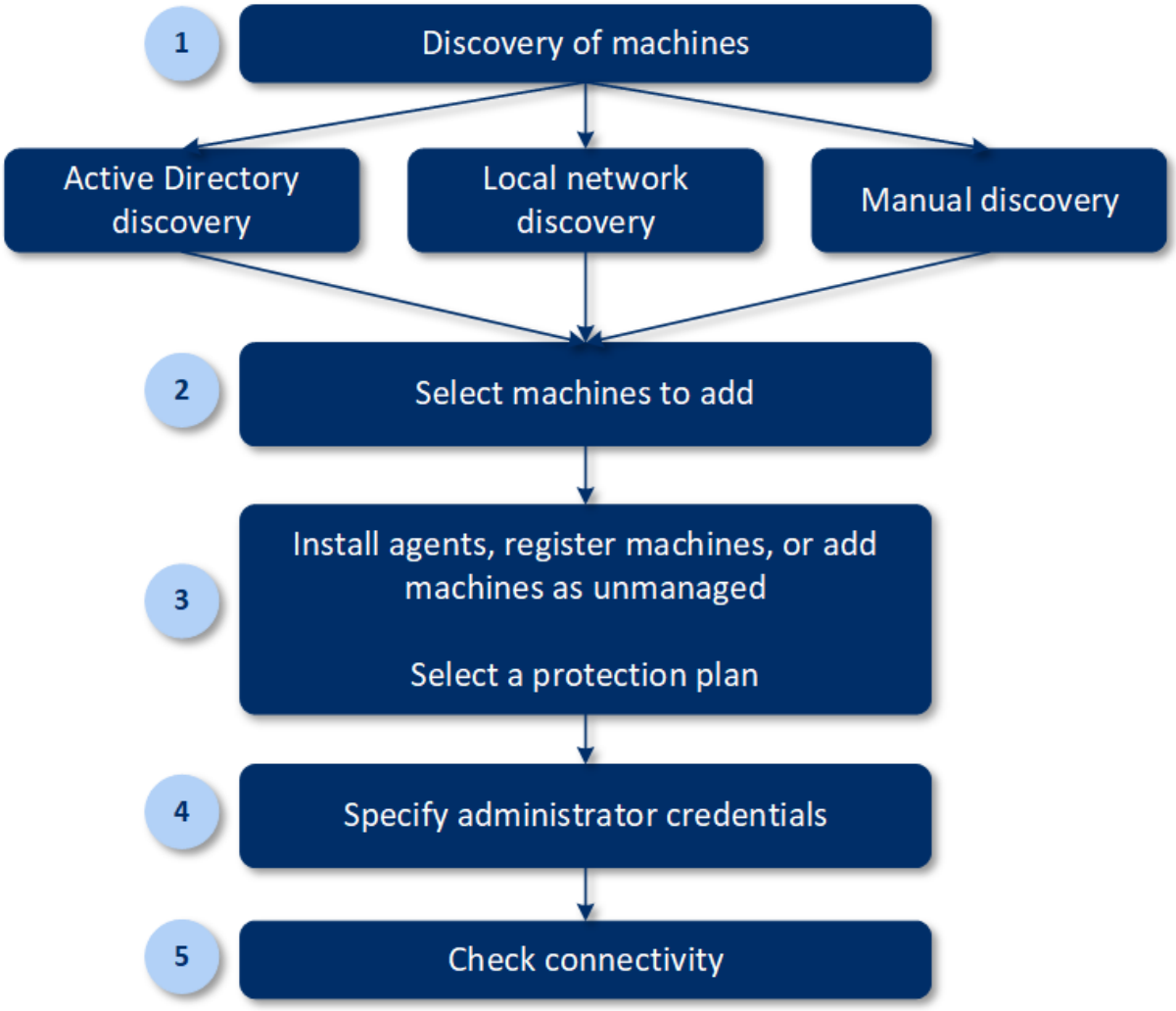
Selama penemuan jaringan lokal, agen penemuan mengumpulkan informasi berikut untuk setiap mesin di jaringan, menggunakan NetBIOS discovery, Web Service Discovery (WSD), dan tabel Address Resolution Protocol (ARP):

© Acronis International GmbH, 2003-2024

- Nama (pendek/nama host NetBIOS)
- Nama domain yang sepenuhnya memenuhi syarat (FQDN)
- Domain/kelompok kerja
- Alamat IPv4/IPv6
- Alamat MAC
- Sistem operasi (nama/versi/rangkaian)
- Kategori mesin (stasiun kerja/server/pengontrol domain)

Selama penemuan Active Directory, agen penemuan, selain daftar di atas, mengumpulkan informasi tentang Unit Organisasi (OU) mesin dan informasi terperinci tentang nama dan sistem operasi mesin. Akan tetapi, alamat IP dan MAC tidak dikumpulkan.

Diagram berikut meringkas proses autodiscovery.



1. Pilih metode penemuan:
   - Penemuan Active Directory
   - Penemuan jaringan lokal

© Acronis International GmbH, 2003-2024

- Penemuan manual – Menggunakan alamat IP atau nama host mesin, atau mengimpor daftar mesin dari file

  Hasil penemuan Active Directory atau jaringan lokal tidak termasuk mesin dengan agen perlindungan yang terinstal.

  Selama penemuan manual, agen perlindungan yang ada diperbarui dan didaftarkan ulang. Jika Anda melakukan autodiscovery menggunakan akun yang sama yang dengannya agen terdaftar, agen hanya akan diperbarui ke versi terbaru. Jika Anda melakukan autodiscovery menggunakan akun lain, agen akan diperbarui ke versi terbaru dan didaftarkan ulang menggunakan penyewa yang memiliki akun tersebut.

2. Pilih mesin yang ingin Anda tambahkan ke penyewa Anda.
3. Pilih cara untuk menambah mesin-mesin ini:
   - Instal agen perlindungan dan komponen tambahan pada mesin, dan daftarkan di konsol Cyber Protect.
   - Daftarkan mesin di konsol Cyber Protect (jika agen perlindungan sudah diinstal).
   - Tambahkan mesin ke konsol Cyber Protect sebagai **Mesin yang tidak dikelola**, tanpa menginstal agen perlindungan.

   Anda juga dapat menerapkan rencana perlindungan yang ada ke mesin tempat Anda menginstal agen perlindungan atau yang Anda daftarkan di konsol Cyber Protect.
4. Berikan kredensial administrator untuk mesin yang dipilih.
5. Verifikasi bahwa Anda dapat terhubung ke mesin menggunakan kredensial yang ditentukan.

Mesin-mesin yang ditampilkan di konsol Cyber Protect, termasuk dalam kategori berikut:

- **Ditemukan**– Mesin yang ditemukan, tetapi agen perlindungan tidak diinstal di mesin tersebut.
- **Dikelola** – Mesin dengan agen perlindungan yang sudah diinstal.
- **Tidak terlindungi** – Mesin di mana rencana proteksi tidak diterapkan. Mesin yang tidak terlindungi meliputi mesin yang ditemukan dan mesin yang dikelola tanpa ada rencana proteksi yang diterapkan.
- **Terlindungi** – Mesin di mana rencana proteksi diterapkan.

Cara kerja instalasi jarak jauh agen

1. Agen penemuan menghubungkan mesin target menggunakan nama host, alamat IP, dan kredensial administrator yang ditetapkan dalam wizard penemuan, lalu mengunggah file `web_installer.exe` ke mesin ini.
2. File `web_installer.exe` berjalan di mesin target dalam mode tanpa pengawasan.
3. Penginstal web mengambil paket instalasi tambahan dari awan, lalu menginstalnya ke mesin target melalui perintah `msiexec`.
4. Setelah instalasi selesai, komponen terdaftar di awan.

© Acronis International GmbH, 2003-2024

Catatan
Instalasi agen jarak jauh tidak didukung untuk Pengontrol Domain karena izin tambahan diperlukan agar layanan agen berjalan.

Melakukan autodiscovery dan manual discovery

Sebelum memulai penemuan, pastikan bahwa prasyarat sudah terpenuhi.

Catatan
Penemuan otomatis tidak didukung untuk menambahkan Pengontrol Domain karena izin tambahan diperlukan agar layanan agen berjalan.

Untuk menemukan mesin

1. Di konsol Cyber Protect, buka **Perangkat**> **Semua perangkat**.
2. Klik **Tambah**.
3. Dalam **Beberapa perangkat**, klik **hanya Windows**. Wizard penemuan terbuka.
4. [Jika terdapat unit dalam organisasi Anda] Pilih suatu unit. Lalu, dalam **Agen penemuan** Anda akan dapat memilih agen yang terkait dengan unit yang dipilih dan unit turunannya.
5. Pilih agen penemuan yang akan melakukan pemindaian untuk mendeteksi mesin.
6. Pilih metode penemuan:
   - **Cari Active Directory**. Pastikan bahwa mesin dengan agen penemuan adalah anggota domain Active Directory.
   - **Pindai jaringan lokal**. Jika agen penemuan yang dipilih tidak dapat menemukan mesin apa pun, pilih agen penemuan lainnya.
   - **Tentukan secara manual atau impor dari file**. Menentukan mesin secara manual untuk ditambahkan atau mengimpor mesin dari file teks.
7. [Jika metode penemuan Active Directory dipilih] Pilih cara mencari mesin:
   - **Dalam daftar unit organisasi**. Pilih grup mesin yang akan ditambahkan.
   - **Berdasarkan kueri dialek LDAP**. Gunakan kueri dialek LDAP untuk memilih mesin. **Basis pencarian** menetapkan tempat pencarian, sedangkan **Filter** memungkinkan Anda untuk menentukan kriteria pemilihan mesin.

© Acronis International GmbH, 2003-2024

8. Tergantung pada metode pencarian yang Anda pilih, lakukan salah satu dari tindakan berikut:

Metode penemuan	Tindakan
Cari Active Directory	Dalam daftar mesin yang ditemukan, pilih mesin-mesin yang ingin Anda tambahkan.
Pindai jaringan lokal	Dalam daftar mesin yang ditemukan, pilih mesin-mesin yang ingin Anda tambahkan.

Tentukan secara manual atau impor dari file	Tentukan alamat IP mesin atau nama host, atau impor daftar mesin dari file teks. File harus berisi alamat IP/nama host, satu per baris. Berikut adalah contoh file:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Setelah menambah alamat mesin secara manual atau mengimpornya dari file, agen berusaha untuk mengirim ping ke mesin yang ditambahkan dan menetapkan ketersediaannya.

9. Pilih tindakan yang harus dilakukan setelah penemuan:

Opsi	Deskripsi
Instal agen dan daftarkan mesin	Anda dapat memilih komponen apa saja yang akan diinstal pada mesin dengan mengeklik **Pilih komponen**. Untuk detail lebih lanjut, lihat "Memilih komponen untuk instalasi" (hlm. 131).
Masuk akun untuk layanan agen	Pengaturan ini tersedia di layar **Pilih komponen**. Pengaturan menentukan akun tempat layanan akan dijalankan. Anda dapat memilih salah satu dari opsi berikut: • **Gunakan Akun Pengguna Layanan** (default untuk layanan agen) Akun Pengguna Layanan adalah akun sistem Windows yang digunakan untuk menjalankan layanan. Keuntungan dari pengaturan ini adalah kebijakan keamanan domain yang tidak memengaruhi hak pengguna akun ini. Secara default, agen berjalan di bawah akun **Sistem Lokal**. • **Buat akun baru** Nama akunnya adalah Agent User untuk agen. • **Gunakan akun berikut** Jika Anda menginstal agen pada pengontrol domain, sistem akan meminta Anda menentukan akun yang ada (atau akun yang sama) untuk agen. Untuk alasan keamanan, sistem tidak membuat akun baru secara otomatis di pengontrol domain. Jika Anda memilih opsi **Buat akun baru** atau **Gunakan akun berikut**, pastikan bahwa kebijakan keamanan domain tidak memengaruhi hak akun terkait. Jika akun kehilangan hak pengguna yang ditetapkan selama instalasi, komponen

© Acronis International GmbH, 2003-2024

Opsi	Deskripsi
	mungkin bekerja secara tidak semestinya atau sama sekali tidak berfungsi.
Daftarkan mesin dengan agen yang terinstal	Gunakan opsi ini jika agen sudah terpasang pada mesin, dan Anda hanya perlu mendaftarkannya di Cyber Protection. Jika tidak ada agen yang ditemukan pada mesin, mesin akan ditambahkan sebagai **Tidak Dikelola**.
Tambahkan sebagai mesin yang tidak dikelola	Jika Anda memilih opsi ini, agen tidak akan diinstal pada mesin. Anda akan dapat melihatnya di konsol dan menginstal atau mendaftarkan agen nanti.
Mulai ulang mesin, jika diperlukan	Opsi ini muncul ketika **Menginstal agen dan mendaftarkan mesin** dipilih. Jika Anda memilih opsi ini, mesin akan di-restart sebanyak yang diperlukan untuk menyelesaikan instalasi. Memulai ulang mesin mungkin perlu dilakukan pada salah satu kasus berikut: • Instalasi prasyarat telah selesai, dan diperlukan restart untuk melanjutkan instalasi. • Instalasi selesai tetapi memulai ulang diperlukan karena beberapa file terkunci selama instalasi. • Instalasi selesai tetapi memulai ulang perlu dilakukan untuk perangkat lunak lain yang diinstal sebelumnya.
Jangan memulai ulang jika pengguna login	Opsi ini muncul ketika **Mulai ulang mesin jika diperlukan** dipilih. Jika Anda memilih opsi ini, mesin tidak akan memulai ulang secara otomatis jika pengguna masuk ke dalam sistem. Misalnya, jika pengguna sedang bekerja sementara instalasi harus dinyalakan ulang, sistem tidak akan memulai ulang secara otomatis. Jika prasyarat telah dipasang tetapi mesin tidak dimulai ulang karena ada pengguna yang sedang masuk, Anda harus memulai ulang mesin dan menjalankan instalasi hingga selesai. Jika agen telah diinstal tetapi kemudian mesin tidak dimulai ulang, Anda harus memulai ulang mesin tersebut.
Pengguna tempat mendaftarkan mesin	[Jika ada unit di organisasi Anda] Pilih akun pengguna unit atau unit bawahan tempat Anda ingin mendaftarkan mesin. [Ketika melakukan autodiscovery pada level penyewa mitra] Dalam daftar penyewa pelanggan yang Anda kelola, perluas struktur pohon, lalu pilih akun pengguna yang ingin Anda daftarkan mesinnya. [Ketika melakukan autodiscovery sebagai administrator pelanggan] Jika Anda memilih **Instal agen dan daftarkan mesin** atau **Daftarkan mesin dengan agen yang terinstal**, ada juga opsi untuk menerapkan rencana proteksi ke mesin. Jika Anda memiliki beberapa rencana proteksi, Anda dapat memilih mana yang akan digunakan.

10. Tentukan kredensial pengguna dengan hak Administrator untuk semua mesin.

© Acronis International GmbH, 2003-2024

Penting
Perhatikan bahwa instalasi agen secara jarak jauh dapat berfungsi tanpa persiapan apa pun hanya jika Anda menetapkan kredensial untuk akun administrator bawaan (akun pertama yang dibuat saat sistem operasi diinstal). Jika Anda ingin menentukan beberapa kredensial administrator khusus, Anda harus melakukan persiapan manual tambahan seperti yang dijelaskan di "Mempersiapkan mesin untuk instalasi jarak jauh" (hlm. 130).

11. Sistem memeriksa konektivitas ke semua mesin. Jika koneksi ke beberapa mesin gagal, Anda dapat mengubah kredensial untuk mesin tersebut.

Saat penemuan mesin dimulai, Anda akan menemukan tugas terkait dalam aktivitas **Pemantauan**> **Aktivitas** > **Penemuan mesin**.

Mempersiapkan mesin untuk instalasi jarak jauh

- Untuk instalasi yang berhasil pada mesin jarak jauh yang menjalankan Windows 7 atau yang lebih baru, opsi **Panel kontrol** > **Opsi folder** > **Lihat** > **Gunakan Wizard Berbagi** harus *dinonaktifkan* pada mesin tersebut.
- Untuk instalasi yang berhasil pada mesin jarak jauh yang *bukan* anggota Domain Active Directory, Kontrol Akun Pengguna (UAC) harus *dinonaktifkan* pada mesin tersebut. Untuk informasi lebih lanjut tentang cara menonaktifkannya, baca "Persyaratan Kontrol Akun Pengguna (UAC)" > Untuk menonaktifkan UAC.
- Secara default, kredensial akun administrator bawaan diperlukan untuk instalasi jarak jauh di mesin Windows apa pun. Untuk melakukan instalasi jarak jauh menggunakan kredensial akun administrator lain, pembatasan jarak jauh Kontrol Akun Pengguna (UAC) harus *dinonaktifkan*. Untuk informasi lebih lanjut tentang cara menonaktifkannya, baca "Persyaratan Kontrol Akun Pengguna (UAC)" > Untuk menonaktifkan batasan jarak jauh UAC.
- File dan Printer bersama harus *diaktifkan* pada mesin jarak jauh. Untuk mengakses opsi ini:
  - Pada mesin yang menjalankan Windows 2003 Server: buka **Panel Kontrol** > **Windows Firewall** > **Pengecualian** > **Berbagi File dan Printer**.
  - Pada mesin yang menjalankan Windows Server 2008, Windows 7, atau versi lebih baru: buka **Panel Kontrol** > **Windows Firewall** > **Pusat Jaringan dan Berbagi** > **Ubah pengaturan berbagi lanjutan**.
- Cyber Protection menggunakan port TCP 445, 25001, dan 43234 untuk instalasi jarak jauh.

  Port 445 dibuka secara otomatis ketika Anda mengaktifkan File dan Printer Bersama. Port 43234 dan 25001 dibuka secara otomatis melalui Windows Firewall. Jika Anda menggunakan firewall yang berbeda, pastikan ketiga port ini terbuka (ditambahkan ke pengecualian) untuk permintaan masuk dan keluar.

  Setelah instalasi jarak jauh selesai, port 25001 akan ditutup secara otomatis melalui Windows Firewall. Port 445 dan 43234 harus tetap terbuka jika Anda ingin memperbarui agen dari jarak jauh di waktu mendatang. Port 25001 secara otomatis dibuka dan ditutup melalui Windows Firewall selama setiap pembaruan. Jika Anda menggunakan firewall yang berbeda, biarkan ketiga port tetap terbuka.

© Acronis International GmbH, 2003-2024

Persyaratan tentang Kontrol Akun Pengguna (UAC)

Pada mesin yang menjalankan Windows 7 atau versi lebih baru dan bukan anggota domain Active Directory, operasi manajemen terpusat (termasuk instalasi jarak jauh) perlu menonaktifkan UAC dan batasan jarak jauh UAC.

Untuk menonaktifkan UAC

Lakukan salah satu dari langkah berikut sesuai dengan sistem operasinya:

- **Pada sistem operasi Windows sebelum Windows 8:**
  Buka **Panel Kontrol > Lihat berdasarkan: Ikon kecil > Akun Pengguna > Ubah Kontrol Akun Pengguna**, lalu geser slider ke **Jangan beri tahu**. Kemudian, mulai ulang mesin.
- **Di sistem operasi Windows apa pun**:
  1. Buka Registry Editor.
  2. Temukan kunci registri berikut: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. Untuk nilai **EnableLUA**, ubah pengaturan ke **0**.
  4. Mulai ulang mesin.

Untuk menonaktifkan batasan jarak jauh UAC

1. Buka Registry Editor.
2. Temukan kunci registri berikut: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Untuk nilai **LocalAccountTokenFilterPolicy**, ubah pengaturan ke **1**.
   Jika nilai **LocalAccountTokenFilterPolicy** tidak ada, buat sebagai DWORD (32-bit). Untuk informasi lebih lanjut tentang nilai ini, lihat dokumentasi Microsoft: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Catatan
Demi alasan keamanan, kami menyarankan setelah menyelesaikan operasi manajemen (misalnya, instalasi jarak jauh), Anda mengembalikan kedua pengaturan ke keadaan semula: **EnableLUA**=**1** dan **LocalAccountTokenFilterPolicy** = **0**

Memilih komponen untuk instalasi

Anda dapat menemukan deskripsi komponen wajib dan tambahan dalam tabel berikut:

Komponen	Deskripsi
Komponen wajib	
Agen untuk Windows	Agen ini mencadangkan disk, volume, dan file serta akan diinstal di mesin Windows. Agen ini akan selalu terinstal, tidak dapat dipilih.

© Acronis International GmbH, 2003-2024

Komponen tambahan	
Agen untuk Pencegahan Kebocoran Data	Agen ini memungkinkan Anda membatasi akses pengguna ke perangkat periferal, port, serta papan klip lokal dan yang dialihkan pada mesin dengan rencana proteksi. Agen ini akan diinstal jika dipilih.
Pemfilteran antimalware dan URL	Komponen ini mengaktifkan modul perlindungan Antivirus & Antimalware dan modul pemfilteran URL di rencana proteksi. Meskipun Anda memilih untuk tidak menginstalnya, itu akan diinstal secara otomatis nanti, jika salah satu modul ini diaktifkan dalam rencana proteksi untuk mesin.
Agen untuk Hyper-V	Agen ini mencadangkan mesin virtual Hyper-V dan akan diinstal pada host Hyper-V. Agen ini akan diinstal jika dipilih dan mendeteksi peran Hyper-V pada mesin.
Agen untuk SQL	Agen ini mencadangkan database SQL Server dan akan diinstal pada mesin yang menjalankan Microsoft SQL Server. Agen ini akan diinstal jika dipilih dan aplikasi terdeteksi pada mesin.
Agen untuk Exchange	Agen ini mencadangkan kotak surat dan database Exchange dan akan diinstal pada mesin yang menjalankan peran Kotak surat Microsoft Exchange Server. Agen ini akan diinstal jika dipilih dan aplikasi terdeteksi pada mesin.
Agen untuk Active Directory	Agen ini mencadangkan data Layanan Domain Active Directory dan akan diinstal pada pengontrol domain. Agen ini akan diinstal jika dipilih dan aplikasi terdeteksi pada mesin.
Agen untuk VMware (Windows)	Agen ini mencadangkan mesin virtual VMware dan akan diinstal pada mesin Windows yang memiliki akses jaringan ke vCenter Server. Agen ini akan diinstal jika dipilih.
Agen untuk Microsoft 365	Agen ini mencadangkan kotak surat Microsoft 365 ke tujuan lokal dan akan diinstal di mesin Windows. Agen ini akan diinstal jika dipilih.
Agen untuk Oracle	Agen ini mencadangkan database Oracle dan akan diinstal pada mesin yang menjalankan Database Oracle. Agen ini akan diinstal jika dipilih.
Monitor Cyber Protection	Komponen ini memungkinkan pengguna untuk memantau pelaksanaan tugas yang berjalan dalam area notifikasi dan akan diinstal di mesin Windows. Agen ini akan diinstal jika dipilih. Didukung di Windows 7 Service Pack 1 dan yang lebih baru, dan Windows Server 2008 R2 Service Pack 1 dan yang lebih baru.

Mengelola mesin yang ditemukan

Setelah proses penemuan dilakukan, Anda dapat menemukan seluruh mesin yang ditemukan di **Perangkat**> **Mesin yang tidak dikelola**.

© Acronis International GmbH, 2003-2024

Bagian ini dibagi menjadi subbagian berdasarkan metode penemuan yang digunakan. Daftar lengkap parameter mesin ditampilkan di bawah ini (daftar mungkin berbeda-beda bergantung pada metode penemuan):

Nama	Deskripsi
Nama	Nama mesin. Alamat IP akan ditampilkan jika nama mesin tidak dapat ditemukan.
Alamat IP	Alamat IP mesin.
Jenis penemuan	Metode penemuan yang digunakan untuk mendeteksi mesin.
Unit organisasi	Unit organisasi dalam Active Directory yang memiliki mesin. Kolom ini ditunjukkan jika kamu menampilkan daftar mesin dalam **Mesin yang tidak dikelola** > **Active Directory**.
Sistem operasi	Sistem operasi yang diinstal di mesin.

Terdapat bagian **Pengecualian**, di mana Anda dapat menambahkan mesin yang harus dilewati selama proses penemuan. Misalnya, jika tidak menghendaki ditemukannya mesin yang akurat, Anda dapat menambahkannya ke daftar ini.

Untuk menambahkan mesin ke **Pengecualian**, pilih mesin dalam daftar dan klik **Tambahkan ke pengecualian**. Untuk menghapus mesin dari **Pengecualian**, buka **Mesin yang tidak dikelola** > **Pengecualian**, pilih mesin, lalu klik **Hapus dari pengecualian**.

Anda dapat menginstal agen pelindung dan mendaftarkan sekumpulan mesin yang ditemukan dalam Cyber Protection dengan memilih mesin dalam daftar dan mengeklik **Instal dan daftarkan**. Wizard yang terbuka juga memungkinkan Anda untuk menetapkan rencana proteksi pada sekumpulan mesin.

Setelah agen perlindungan diinstal pada mesin, mesin tersebut akan ditampilkan di bagian **Perangkat**> **Mesin dengan agen**.

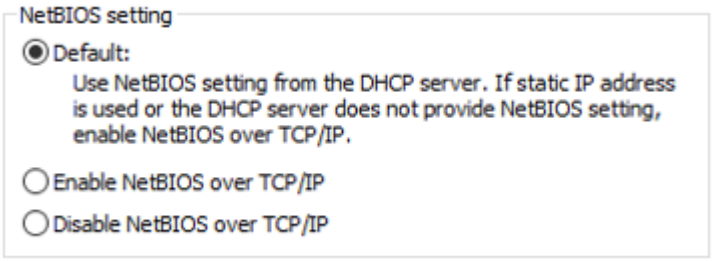
Untuk memeriksa status proteksi Anda, buka **Pemantauan**> **Ikhtisar** dan tambahkan widget **Status perlindungan** atau widget **Mesin penemuan**.

Penyelesaian masalah

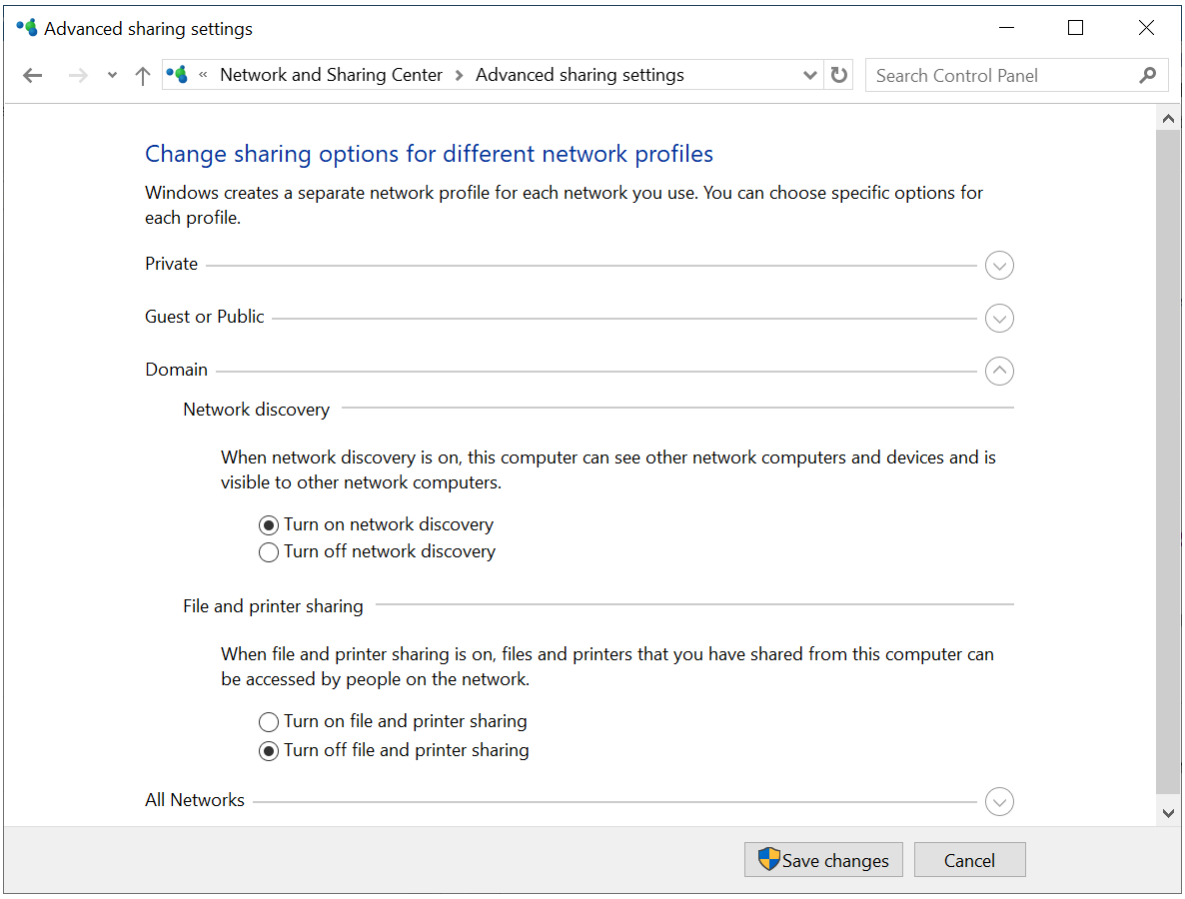
Jika Anda memiliki masalah apa pun dengan fungsi penemuan otomatis, cobalah periksa hal berikut:

© Acronis International GmbH, 2003-2024

- Periksa apakah NetBIOS pada TCP/IP diaktifkan atau diatur ke default.



- Dalam “Panel Kontrol\Jaringan dan Pusat Berbagi\Pengaturan berbagi lanjutan” aktifkan pencarian jaringan.



- Periksa apakah layanan Host Penyedia Fungsi Penemuan berjalan di mesin yang melakukan penemuan dan di mesin yang akan ditemukan.
- Periksa apakah layanan Publikasi Sumber daya Fungsi Penemuan berjalan di mesin yang akan ditemukan.

© Acronis International GmbH, 2003-2024

Menyebarkan Agen untuk VMware (Virtual Appliance)

Sebelum Anda memulai

Persyaratan sistem untuk agen

Secara default, alat virtual diberi 4 GB RAM dan 2 vCPU, yang telah optimal dan cukup untuk sebagian besar operasi.

Untuk meningkatkan kinerja pencadangan dan menghindari kegagalan terkait dengan kekurangan memori RAM, kami menyarankan Anda meningkatkan sumber daya ini menjadi 16 GB RAM dan 4 vCPU dalam kasus yang lebih berat. Misalnya, tingkatkan sumber daya yang ditetapkan jika Anda memperkirakan lalu lintas pencadangan melebihi 100 MB per detik (misalnya, dalam jaringan 10 Gigabit) atau jika Anda mencadangkan beberapa mesin virtual dengan hard drive besar (500 GB atau lebih) secara bersamaan.

Disk virtual milik alat memerlukan tidak lebih dari 6 GB. Format disk tebal atau tipis tidak masalah, karena tidak memengaruhi performa alat.

Berapa jumlah agen yang saya perlukan?

Meskipun satu alat virtual mampu melindungi keseluruhan lingkungan vSphere, sebaiknya sebarkan satu alat virtual per klaster vSphere (atau per host, jika tidak ada klaster). Tindakan ini akan mempercepat pencadangan karena alat dapat memasang disk yang dicadangkan menggunakan transpor HotAdd, sehingga lalu lintas pencadangan akan diarahkan dari satu disk lokal ke disk lainnya.

Penggunaan alat virtual dan Agen untuk VMware (Windows) pada saat yang bersamaan adalah sesuatu yang normal, selama keduanya terhubung pada vCenter Server yang sama *atau* terhubung ke host ESXi yang berbeda. Hindari kasus saat satu agen terhubung ke ESXi secara langsung dan agen lainnya terhubung ke vCenter Server yang mengelola ESXi ini.

Kami tidak menyarankan Anda menggunakan penyimpanan yang terpasang secara lokal (yaitu menyimpan cadangan pada disk virtual yang ditambahkan ke alat virtual) jika Anda memiliki lebih dari satu agen. Untuk pertimbangan lebih lanjut, lihat "Menggunakan penyimpanan yang terpasang secara lokal" (hlm. 689).

Nonaktifkan DRS otomatis untuk agen

Jika alat virtual disebarkan pada klaster vSphere, pastikan untuk menonaktifkan vMotion. Pada pengaturan DRS klaster, aktifkan tingkat otomasi mesin virtual, lalu atur **Tingkat otomasi** untuk alat virtual ke **Dinonaktifkan**.

© Acronis International GmbH, 2003-2024

Menyebarkan templat OVF

1. Klik **Semua perangkat** > **Tambah** > **VMware ESXi** > **Alat Virtual (OVF)**.
   Arsip .zip diunduh ke mesin Anda.
2. Ekstrak arsip .zip. Folder berisi satu file .ovf dan dua file .vmdk.
3. Pastikan file tersebut dapat diakses dari mesin yang menjalankan vSphere Client.
4. Mulai vSphere Client dan masuk ke vCenter Server.
5. Sebarkan templat OVF.
   - Ketika mengonfigurasi penyimpanan, pilih penyimpanan data bersama, jika ada. Format disk tebal atau tipis tidak masalah, karena tidak memengaruhi performa alat.
   - Ketika mengonfigurasi koneksi jaringan, pastikan untuk memilih jaringan yang memperbolehkan koneksi internet, agar agen dapat mendaftarkan dirinya dengan benar di awan.

Mengonfigurasi alat virtual

Setelah menerapkan alat virtual, Anda harus mengonfigurasinya agar dapat mengakses Server vCenter atau host ESXi dan layanan Cyber Protection.

Untuk mengonfigurasi alat virtual

1. Di Klien vSphere, buka konsol alat virtual.
2. Pastikan koneksi jaringan telah dikonfigurasi.
   Koneksi dikonfigurasi secara otomatis melalui Dynamic Host Configuration Protocol (DHCP).
   Untuk mengubah konfigurasi default, di bawah **Opsi agen**, di kolom **eth0**, klik **Ubah**, lalu tentukan pengaturan jaringan.
3. Hubungkan alat virtual ke vCenter Server atau host ESXi.
   a. Di bawah **Opsi agen**, di kolom **vCenter/ESX(i)**, pilih **Ubah**, lalu tentukan yang berikut ini.
      - [Jika Anda menggunakan vCenter Server] Nama atau alamat IP vCenter Server.
      - [Jika Anda tidak menggunakan vCenter Server] Nama atau alamat IP host ESXi tempat Anda ingin mencadangkan dan memulihkan mesin virtual. Untuk pencadangan yang lebih cepat, gunakan alat virtual di host yang sama.
      - Kredensial yang diperlukan alat untuk terhubung ke Server vCenter atau host ESXi.
        Kami menyarankan Anda menggunakan akun khusus untuk mengakses Server vCenter atau host ESXi, daripada menggunakan akun yang sudah ada dengan peran Administrator. Untuk mempelajari lebih lanjut tentang hak istimewa yang diperlukan untuk akun khusus, lihat "Agen untuk VMware – hak istimewa yang diperlukan" (hlm. 696).
   b. Klik **Periksa koneksi** untuk memverifikasi bahwa pengaturan sudah benar.
   c. Klik **OK**.
4. Daftarkan peralatan di layanan Cyber Protection dengan menggunakan salah satu cara berikut.

© Acronis International GmbH, 2003-2024

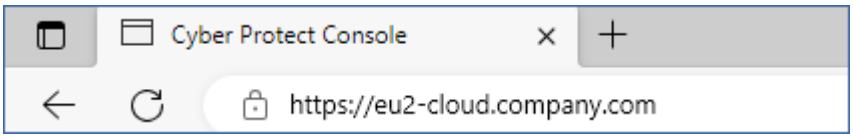
- [Hanya untuk penyewa tanpa autentikasi dua faktor] Daftarkan alat di antarmuka grafisnya.
  a. Di bawah **Opsi agen**, di bidang **Server Manajemen**, klik **Ubah**.
  b. Di bidang **Nama server/IP**, pilih **Awan**.
     Alamat layanan Cyber Protection muncul. Jangan ubah alamat ini kecuali diperintahkan.
  c. Di bidang **Nama pengguna** dan **Kata sandi**, tentukan kredensial untuk akun Anda di layanan Cyber Protection. Alat virtual dan mesin virtual yang dikelola alat terdaftar dengan akun ini.
  d. Klik **OK**.
- Daftarkan alat di antarmuka baris perintah.

  Catatan
  Dengan metode ini, Anda memerlukan token pendaftaran. Untuk informasi selengkapnya tentang cara membuatnya, lihat "Membuat token pendaftaran" (hlm. 167).

  a. Tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.
  b. Jalankan perintah berikut:

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

  Catatan
  Saat Anda menggunakan token registrasi, Anda harus menentukan alamat pusat data yang tepat. Ini adalah URL yang Anda lihat **setelah Anda masuk** ke konsol Cyber Protect. Misalnya, `https://eu2-cloud.company.com`.

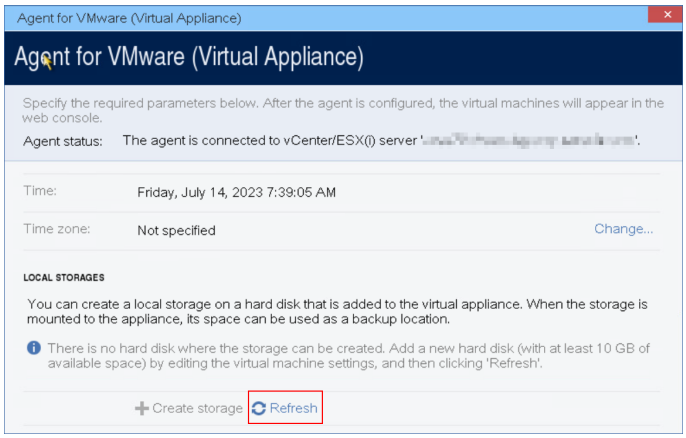
  

  Jangan gunakan `https://cloud.company.com` di sini.

  c. Untuk kembali ke antarmuka grafis alat, tekan ALT+F1.

5. [Opsional] Tambahkan penyimpanan lokal.
   a. Di Klien vSphere, pasang disk virtual ke alat virtual. Disk virtual harus memiliki setidaknya 10 GB ruang kosong.
   b. Di antarmuka pengguna grafis alat, klik **Menyegarkan**.

© Acronis International GmbH, 2003-2024



Tombol **Buat penyimpanan** menjadi aktif.

c. Klik **Buat penyimpanan.**

d. Tentukan label untuk penyimpanan, lalu klik **OK**.

e. Konfirmasi pilihan Anda dengan mengklik **Iya**.

6. [Jika server proksi diaktifkan pada jaringan Anda] Konfigurasikan server proxy.

   a. Tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.

   b. Buka file **/etc/Acronis/Global.config** dalam editor teks.

   c. Lakukan salah satu langkah berikut:

   - Jika pengaturan proksi ditentukan selama instalasi agen, temukan bagian berikut:

```
<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>
```

   - Jika tidak, salin baris di atas dan tempel ke file di antara tag `<registry name="Global">...</registry>`.

   d. Ganti `ADDRESS` dengan nama host server proksi/alamat IP yang baru, dan `PORT` dengan nilai desimal nomor port.

   e. Jika server proksi Anda membutuhkan otentikasi, ganti `LOGIN` dan `PASSWORD` dengan kredensial server proksi. Atau, hapus baris ini dari file.

   f. Simpan file.

   g. Buka file **/opt/acronis/etc/aakore.yaml** dalam editor teks.

   h. Temukan bagian **env** atau buat bagian tersebut dan tambahkan baris berikut:

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


© Acronis International GmbH, 2003-2024

i. Ganti `proxy_login` dan `proxy_password` dengan kredensial server proksi, dan `proxy_address:port` dengan alamat dan nomor port dari server proksi.
j. Jalankan perintah `reboot`.

Catatan
Untuk dapat memperbarui alat virtual yang diterapkan di belakang proxy, edit file `config.yaml` peralatan (`/opt/acronis/etc/va-updater/config.yaml`), dengan menambahkan baris berikut ke bagian bawah file tersebut, lalu memasukkan nilai khusus untuk lingkungan Anda:

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

Misalnya:

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

Menyebarkan Agen untuk Scale Computing HC3 (Alat Virtual)

Sebelum Anda memulai

Alat ini adalah mesin virtual yang diprakonfigurasi yang Anda sebarkan di Klaster Scale Computing HC3. Alat ini berisi agen proteksi yang memungkinkan Anda untuk mengelola perlindungan cyber untuk semua mesin virtual dalam klaster.

Persyaratan sistem untuk agen

Secara default, mesin virtual dengan agen menggunakan 2 vCPU dan RAM 4 GiB. Pengaturan ini cukup untuk sebagian besar operasi, tetapi Anda dapat mengubahnya dengan mengedit mesin virtual di antarmuka web Scale Computing HC3.

Untuk meningkatkan kinerja pencadangan dan menghindari kegagalan terkait dengan kekurangan memori RAM, kami menyarankan Anda meningkatkan sumber daya ini menjadi 4 vCPU dan 8 GiB RAM dalam kasus yang lebih berat. Contohnya, tingkatkan sumber daya yang ditetapkan jika Anda mengharapkan lalu lintas cadangan akan melebihi 100 MB per detik (misal, di jaringan 10-Gigabit) atau jika Anda mencadangkan banyak mesin virtual dengan hard drive besar (500 GB atau lebih) secara bersamaan.

Ukuran disk virtual alat sekitar 9 GB.

Berapa jumlah agen yang saya perlukan?

Satu agen dapat melindungi keseluruhan klaster. Namun, Anda dapat memiliki lebih dari satu agen dalam klaster jika Anda perlu mendistribusikan beban bandwidth lalu lintas cadangan.

© Acronis International GmbH, 2003-2024

Jika Anda memiliki lebih dari satu agen dalam klaster, mesin virtual akan otomatis didistribusikan secara merata di antara agen-agen tersebut sehingga setiap agen mengelola mesin dalam jumlah yang sama.

Distribusi ulang otomatis terjadi saat ketidakseimbangan beban di antara agen mencapai 20 persen. Hal ini dapat terjadi setelah Anda menambahkan atau menghapus mesin atau agen. Misalnya, Anda menyadari bahwa Anda membutuhkan lebih banyak agen untuk membantu dengan throughput dan Anda menyebarkan alat virtual tambahan ke klaster. Server manajemen akan menetapkan mesin yang paling tepat untuk agen baru. Beban agen lama akan berkurang. Ketika Anda menghapus agen dari server manajemen, mesin yang ditetapkan ke agen tersebut akan didistribusikan ulang di antara agen yang tersisa. Namun, hal ini tidak akan terjadi jika agen rusak atau dihapus secara manual dari klaster Scale Computing HC3. Redistribusi akan dimulai hanya setelah Anda menghapus agen tersebut dari konsol Cyber Protect.

Untuk memeriksa agen mana yang mengelola suatu mesin

1. Di konsol Cyber Protect, klik **Perangkat**, lalu pilih **Scale Computing**.
2. Klik ikon roda gigi di sudut kanan atas tabel, dan pada **Sistem**, pilih kotak centang **Agen**.
3. Periksa nama agen di kolom yang muncul.

Menyebarkan templat QCOW2

1. Masuk ke akun Cyber Protection Anda.
2. Klik **Perangkat** > **Semua perangkat** > **Tambahkan** > **Scale Computing HC3**.
   Arsip .zip diunduh ke mesin Anda.
3. Ekstrak arsip .zip, lalu simpan file .qcow2 dan file .xml ke folder bernama **ScaleAppliance**.
4. Unggah folder **ScaleAppliance** ke berbagi jaringan, dan pastikan klaster Scale Computing HC3 dapat mengaksesnya.
5. Masuk ke klaster Scale Computing HC3 sebagai administrator yang memiliki penetapan peran **Buat/Edit VM**. Untuk informasi lebih lanjut tentang peran yang diperlukan bagi operasi dengan mesin virtual Scale Computing HC3, lihat "Agen untuk Scale Computing HC3 – peran yang diperlukan" (hlm. 143).
6. Di antarmuka web Scale Computing HC3, impor templat mesin virtual dari folder **ScaleAppliance**.
   a. Klik ikon **Impor VM HC3**.
   b. Di jendela **Impor VM HC3**, tentukan hal berikut:
      - Nama untuk mesin virtual baru.
      - Berbagi jaringan tempat folder **ScaleAppliance** berada.
      - Nama pengguna dan kata sandi diperlukan untuk mengakses berbagi jaringan.
      - [Opsional] Tag domain untuk mesin virtual baru.
      - Jalur ke folder **ScaleAppliance** di berbagi jaringan.
   c. Klik **Impor**.

© Acronis International GmbH, 2003-2024

Setelah penyebaran selesai, Anda harus mengonfigurasikan alat virtual. Untuk informasi lebih lanjut tentang cara mengonfigurasinya, lihat "Mengonfigurasi alat virtual" (hlm. 141).

Catatan
Jika membutuhkan lebih dari satu alat virtual di klaster Anda, ulangi langkah-langkah di atas dan sebarkan alat virtual tambahan. Jangan membuat klona alat virtual yang sudah ada dengan opsi **Buat klona VM** di antarmuka web Scale Computing HC3.

Mengonfigurasi alat virtual

Setelah menyebarkan alat virtual, Anda harus mengonfigurasikannya agar dapat menjangkau klaster Scale Computing HC3 yang akan dilindungi dan layanan Cyber Protection.

Untuk mengonfigurasi alat virtual

1. Masuk ke akun Scale Computing HC3.
2. Pilih alat virtual yang ingin Anda konfigurasikan, lalu klik ikon **Konsol**.
3. Di bidang **eth0**, konfigurasi antarmuka jaringan alat.
   Pastikan alamat DHCP yang ditetapkan secara otomatis (jika ada) valid dalam jaringan yang digunakan mesin virtual Anda atau tetapkan secara manual. Tergantung pada jumlah jaringan yang digunakan alat, mungkin ada satu atau beberapa antarmuka yang perlu dikonfigurasikan.
4. Di bidang **Scale Computing**, klik **Ubah** untuk menentukan alamat klaster Scale Computing HC3 dan kredensial untuk mengaksesnya.
   a. Di bidang **Nama server/IP**, masukkan nama DNS atau alamat IP klaster.
   b. Di bidang **Nama pengguna** dan **Kata sandi**, masukkan kredensial untuk akun administrator Scale Computing HC3.
      Pastikan akun ini memiliki peran yang diperlukan untuk operasi dengan mesin virtual Scale Computing HC3. Untuk informasi lebih lanjut tentang peran ini, lihat "Agen untuk Scale Computing HC3 – peran yang diperlukan" (hlm. 143).
   c. Klik **Periksa koneksi** untuk memverifikasi bahwa pengaturan sudah benar.
   d. Klik **OK**.
5. Daftarkan peralatan di layanan Cyber Protection dengan menggunakan salah satu cara berikut.
   - [Hanya untuk penyewa tanpa autentikasi dua faktor] Daftarkan alat di antarmuka grafisnya.
     a. Di bawah **Opsi agen**, di bidang **Server Manajemen**, klik **Ubah**.
     b. Di bidang **Nama server/IP**, pilih **Awan**.
        Alamat layanan Cyber Protection muncul. Jangan ubah alamat ini kecuali diperintahkan.
     c. Di bidang **Nama pengguna** dan **Kata sandi**, tentukan kredensial untuk akun Anda di layanan Cyber Protection. Alat virtual dan mesin virtual yang dikelola alat terdaftar dengan akun ini.
     d. Klik **OK**.
   - Daftarkan alat di antarmuka baris perintah.

© Acronis International GmbH, 2003-2024

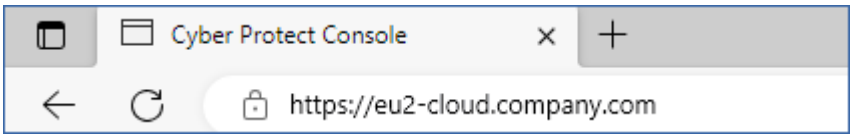
Catatan
Dengan metode ini, Anda memerlukan token pendaftaran. Untuk informasi selengkapnya tentang cara membuatnya, lihat "Membuat token pendaftaran" (hlm. 167).

a. Tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.

b. Jalankan perintah berikut:

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

Catatan
Saat Anda menggunakan token registrasi, Anda harus menentukan alamat pusat data yang tepat. Ini adalah URL yang Anda lihat **setelah Anda masuk** ke konsol Cyber Protect. Misalnya, `https://eu2-cloud.company.com`.



Jangan gunakan `https://cloud.company.com` di sini.

c. Untuk kembali ke antarmuka grafis alat, tekan ALT+F1.

6. [Opsional] Di bidang **Nama**, klik **Ubah** untuk mengedit nama default bagi alat virtual, yaitu **localhost**. Nama ini ditampilkan di konsol Cyber Protect.
7. [Opsional] Di bidang **Waktu**, klik **Ubah**, lalu pilih zona waktu lokasi Anda untuk memastikan operasi terjadwal berjalan pada waktu yang tepat.
8. [Jika server proksi diaktifkan pada jaringan Anda] Konfigurasikan server proxy.
   a. Tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.
   b. Buka file **/etc/Acronis/Global.config** dalam editor teks.
   c. Lakukan salah satu langkah berikut:
      - Jika pengaturan proksi ditentukan selama instalasi agen, temukan bagian berikut:

```
<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>
```

      - Jika tidak, salin baris di atas dan tempel ke file di antara tag `<registry name="Global">...</registry>`.
   d. Ganti `ADDRESS` dengan nama host server proksi/alamat IP yang baru, dan `PORT` dengan nilai desimal nomor port.

© Acronis International GmbH, 2003-2024

e. Jika server proksi Anda membutuhkan otentikasi, ganti `LOGIN` dan `PASSWORD` dengan kredensial server proksi. Atau, hapus baris ini dari file.

f. Simpan file.

g. Buka file **/opt/acronis/etc/aakore.yaml** dalam editor teks.

h. Temukan bagian **env** atau buat bagian tersebut dan tambahkan baris berikut:

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

i. Ganti `proxy_login` dan `proxy_password` dengan kredensial server proksi, dan `proxy_address:port` dengan alamat dan nomor port dari server proksi.

j. Jalankan perintah `reboot`.

Catatan

Untuk dapat memperbarui alat virtual yang diterapkan di belakang proxy, edit file `config.yaml` peralatan (`/opt/acronis/etc/va-updater/config.yaml`), dengan menambahkan baris berikut ke bagian bawah file tersebut, lalu memasukkan nilai khusus untuk lingkungan Anda:

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

Misalnya:

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

Untuk melindungi mesin virtual dalam klaster Scale Computing HC3

1. Masuk ke akun Cyber Protection Anda.
2. Navigasi ke **Perangkat** > **Scale Computing HC3**> <klaster Anda> atau temukan mesin Anda di **Perangkat** > **Semua perangkat**.
3. Pilih mesin dan terapkan rencana perlindungan pada mesin tersebut.

Agen untuk Scale Computing HC3 – peran yang diperlukan

Bagian ini menjelaskan peran yang diperlukan untuk operasi dengan mesin virtual Scale Computing HC3.

Operasi	Peran
Mencadangkan mesin virtual	Cadangan Buat/Edit VM Hapus VM
Memulihkan ke mesin virtual yang sudah ada	Cadangan

© Acronis International GmbH, 2003-2024

	Buat/Edit VM Kontrol Daya VM Hapus VM Pengaturan Klaster
Memulihkan ke mesin virtual baru	Cadangan Buat/Edit VM Kontrol Daya VM Hapus VM Pengaturan Klaster

Menyebarkan Agen untuk Virtuozzo Hybrid Infrastructure (Alat Virtual)

Sebelum Anda memulai

Alat ini adalah mesin virtual yang sudah dikonfigurasikan yang Anda sebarkan di Virtuozzo Hybrid Infrastructure. Alat ini memuat agen proteksi yang memungkinkan Anda mengelola perlindungan cyber untuk semua mesin virtual dalam klaster Virtuozzo Hybrid Infrastructure.

Catatan
Untuk memastikan bahwa cadangan dengan opsi cadangan **Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual** aktif berjalan dengan benar dan menangkap data dalam status aplikasi-konsisten, verifikasi bahwa Virtuozzo Guest Tool telah diinstal dan diperbarui pada mesin virtual yang dilindungi.

Persyaratan sistem untuk agen

Saat menyebarkan alat virtual, Anda dapat memilih antara berbagai kombinasi vCPU dan RAM (cara) yang sudah ditentukan sebelumnya. Anda juga dapat membuat cara Anda sendiri.

2 vCPU dan RAM 4 GB (cara medium) sudah optimal dan memadai untuk sebagian besar operasi. Untuk meningkatkan kinerja pencadangan dan menghindari kegagalan terkait dengan kekurangan memori RAM, kami menyarankan Anda meningkatkan sumber daya ini menjadi 4 vCPU dan 8 GB RAM dalam kasus yang lebih berat. Contohnya, tingkatkan sumber daya yang ditetapkan jika Anda mengharapkan lalu lintas cadangan akan melebihi 100 MB per detik (misal, di jaringan 10-Gigabit) atau jika Anda mencadangkan banyak mesin virtual dengan hard drive besar (500 GB atau lebih) secara bersamaan.

© Acronis International GmbH, 2003-2024

Berapa jumlah agen yang saya perlukan?

Satu agen dapat melindungi keseluruhan klaster. Namun, Anda dapat memiliki lebih dari satu agen dalam klaster jika Anda perlu mendistribusikan beban bandwidth lalu lintas cadangan.

Jika Anda memiliki lebih dari satu agen dalam klaster, mesin virtual akan otomatis didistribusikan secara merata di antara agen-agen tersebut sehingga setiap agen mengelola mesin dalam jumlah yang sama.

Distribusi ulang otomatis terjadi saat ketidakseimbangan beban di antara agen mencapai 20 persen. Hal ini dapat terjadi setelah Anda menambahkan atau menghapus mesin atau agen. Misalnya, Anda menyadari bahwa Anda membutuhkan lebih banyak agen untuk membantu dengan throughput dan Anda menyebarkan alat virtual tambahan ke klaster. Server manajemen akan menetapkan mesin yang paling tepat untuk agen baru. Beban agen lama akan berkurang. Ketika Anda menghapus agen dari server manajemen, mesin yang ditetapkan ke agen tersebut akan didistribusikan ulang di antara agen yang tersisa. Namun, hal ini tidak akan terjadi jika agen rusak atau dihapus secara manual dari simpul Virtuozzo Hybrid Infrastructure. Redistribusi hanya akan dimulai setelah Anda menghapus agen tersebut dari antarmuka web Cyber Protection.

Untuk memeriksa agen mana yang mengelola suatu mesin

1. Di konsol Cyber Protect, klik **Perangkat**, lalu pilih **Virtuozzo Hybrid Infrastructure**.
2. Klik ikon roda gigi di sudut kanan atas tabel, dan pada **Sistem**, pilih kotak centang **Agen**.
3. Periksa nama agen di kolom yang muncul.

Pembatasan

- Alat Virtuozzo Hybrid Infrastructure tidak dapat disebarkan dari jarak jauh.
- Pencadangan tanggap aplikasi mesin virtual tidak didukung.

Mengonfigurasi jaringan di Virtuozzo Hybrid Infrastructure

Sebelum menyebarkan dan mengonfigurasi alat virtual, jaringan Anda di Virtuozzo Hybrid Infrastructure harus sudah dikonfigurasikan.

Persyaratan jaringan untuk Agen Virtuozzo Hybrid Infrastructure (Alat Virtual)

- Alat virtual memerlukan 2 adaptor jaringan.
- Alat virtual harus dihubungkan ke jaringan Virtuozzo dengan jenis lalu lintas jaringan berikut:
  - API Komputasi
  - VM Cadangan
  - Publik ABGW
  - VM Publik

© Acronis International GmbH, 2003-2024

Untuk informasi lebih lanjut tentang mengonfigurasi jaringan, lihat Persyaratan klaster komputasi di dokumentasi Virtuozzo.

Mengonfigurasi akun pengguna di Virtuozzo Hybrid Infrastructure

Untuk mengonfigurasi alat virtual, Anda memerlukan akun pengguna Virtuozzo Hybrid Infrastructure. Akun ini harus memiliki peran **Administrator** di domain **Default**. Untuk informasi lebih lanjut tentang pengguna, lihat Panel admin pengelola pengguna di dokumentasi Virtuozzo Hybrid Infrastructure. Pastikan bahwa Anda memberikan akun ini akses ke semua proyek di domain **Default**.

Untuk memberikan akun ini akses ke semua proyek di domain Default

1. Buat file lingkungan untuk administrator sistem. Untuk melakukannya, jalankan skrip berikut di klaster Virtuozzo Hybrid Infrastructure melalui Antarmuka Baris Perintah OpenStack. Untuk informasi lebih lanjut tentang cara menghubungkan antarmuka ini, baca Menghubungkan antarmuka baris perintah OpenStack dalam dokumentasi Virtuozzo Hybrid Infrastructure.

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

2. Gunakan file lingkungan untuk mengotorisasi perintah OpenStack lebih lanjut:

   ```
   . /etc/kolla/admin-openrc.sh
   ```

3. Jalankan perintah berikut:

   ```
   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
   ```

   Di sini, <nama pengguna> adalah akun Virtuozzo Hybrid Infrastructure dengan peran **Administrator** di domain **Default**. Alat virtual akan menggunakan akun ini untuk mencadangkan dan memulihkan mesin virtual di segala project turunan di bawah domain **Default**.

Contoh

```
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
```


© Acronis International GmbH, 2003-2024

Untuk mengelola cadangan untuk mesin virtual di domain yang berbeda dari domain **Default**, jalankan perintah berikut juga.

Untuk memberikan akses ke semua proyek di domain yang berbeda

```
openstack --insecure role add --domain <domain name> --inherited --user <username> --
user-domain Default admin
```

Di sini, <domain name> adalah domain ke proyek tempat akun <username> nantinya memiliki akses.

Contoh

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-
domain Default admin
```

Setelah memberikan akses ke proyek, periksa peran apa yang ditetapkan ke akun tersebut.

Untuk memeriksa peran yang ditetapkan

```
openstack --insecure role assignment list --user <username> --names
```

Di sini, <username> adalah akun Virtuozzo Hybrid Infrastructure.

Contoh

```
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     |
+--------------+-----------------+---------+-------------+
```

Dalam contoh ini, opsi `-c Role`, `-c User`, `-c Project`, dan `-c Domain` digunakan untuk mempersingkat keluaran perintah agar pas dengan halaman.

Untuk memeriksa peran efektif apa yang ditetapkan ke akun di semua proyek, jalankan perintah berikut juga.

Untuk memeriksa peran efektif dalam semua proyek

```
openstack --insecure role assignment list --user <username> --names --effective
```

Di sini, <username> adalah akun Virtuozzo Hybrid Infrastructure.

© Acronis International GmbH, 2003-2024

Contoh

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

Dalam contoh ini, opsi `-c Role`, `-c User`, `-c Project`, dan `-c Domain` digunakan untuk mempersingkat keluaran perintah agar pas dengan halaman.

Menyebarkan templat QCOW2

1. Masuk ke akun Cyber Protection Anda.
2. Klik **Perangkat** > **Semua perangkat** > **Tambah** > **Virtuozzo Hybrid Infrastructure**.
   Arsip .zip diunduh ke mesin Anda.
3. Ekstrak arsip .zip. Arsip tersebut berisi file profil .qcow2.
4. Masuk ke akun Virtuozzo Hybrid Infrastructure Anda.
5. Tambahkan file profil .qcow2 ke klaster komputasi Virtuozzo Hybrid Infrastructure seperti berikut:
   - Pada tab **Komputasi** > **Mesin virtual** > **Gambar**, klik **Tambah gambar**.
   - Di jendela **Tambah gambar**, klik **Jelajahi**, lalu pilih file .qcow2.
   - Tentukan nama profil, pilih jenis **Generic Linux OS**, lalu klik **Tambahkan**.
6. Di tab **Komputasi** > **Mesin virtual** > **Mesin virtual**, klik **Buat mesin virtual**. Jendela akan terbuka, di sini Anda perlu menentukan parameter berikut:
   - Nama untuk mesin virtual baru.
   - Di bagian **Menyebarkan dari**, pilih **Gambar**.
   - Di jendela **Gambar**, pilih file gambar .qcow2 pada alat, lalu klik **Selesai**.

© Acronis International GmbH, 2003-2024

- Di jendela **Volume**, Anda tidak perlu menambah volume apa pun. Volume yang ditambahkan secara otomatis ke disk sistem sudah mencukupi.
- Di jendela **Cara**, pilih kombinasi vCPU dan RAM yang Anda inginkan, lalu klik **Selesai**. Biasanya, 2 vCPU dan RAM 4 GiB sudah cukup.
- Di jendela **Antarmuka jaringan**, klik **Tambah**, pilih jaringan virtual bertipe *publik*, lalu klik **Tambah**. Jaringan tersebut akan muncul dalam daftar **Antarmuka jaringan**.
  Jika Anda menggunakan pengaturan dengan lebih dari satu jaringan fisik (sehingga, lebih dari satu jaringan virtual bertipe publik), ulangi langkah ini dan pilih jaringan virtual yang Anda butuhkan.

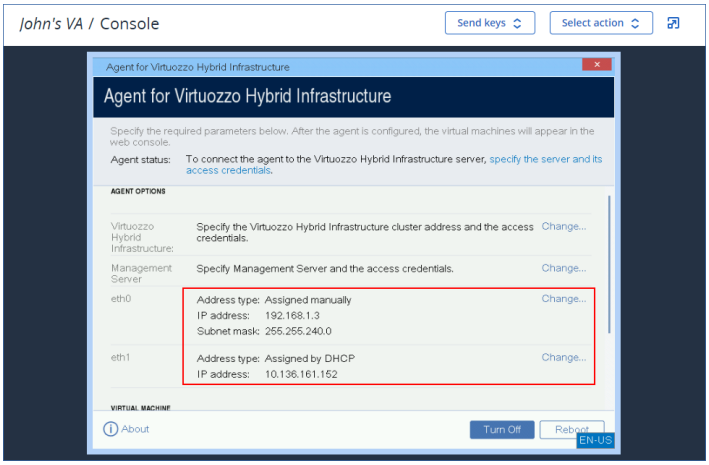
7. Klik **Selesai**.
8. Kembali ke jendela **Buat mesin virtual**, klik **Sebarkan** untuk membuat dan boot mesin virtual.

Mengonfigurasi alat virtual

Setelah menyebarkan Agen untuk Virtuozzo Hybrid Infrastructure (Alat Virtual), Anda harus mengonfigurasi alat virtual tersebut agar dapat menjangkau klaster Virtuozzo Hybrid Infrastructure yang akan dilindunginya, dan layanan awan Cyber Protection.

Untuk mengonfigurasi alat virtual

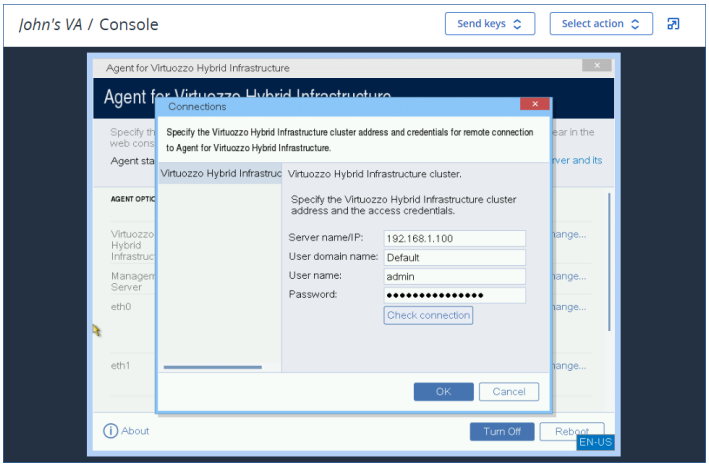
1. Masuk ke akun Virtuozzo Hybrid Infrastructure Anda.
2. Pada tab **Komputasi** > **Mesin virtual** > **Mesin Virtual**, pilih mesin virtual yang Anda buat. Lalu, klik **Konsol**.
3. Konfigurasi antarmuka jaringan pada alat. Mungkin ada satu atau beberapa antarmuka untuk dikonfigurasi – bergantung pada jumlah jaringan virtual yang digunakan alat. Pastikan alamat DHCP yang ditetapkan secara otomatis (jika ada) valid dalam jaringan yang digunakan mesin virtual Anda atau tetapkan secara manual.



4. Tentukan alamat klaster dan kredensial Virtuozzo:
   - Nama DNS atau alamat IP klaster Virtuozzo Hybrid Infrastructure – ini adalah alamat simpul manajemen klaster. Port default 5000 akan diatur secara otomatis. Jika menggunakan port yang berbeda, Anda perlu menetapkannya secara manual.

© Acronis International GmbH, 2003-2024

- Di bidang **Nama domain pengguna**, tentukan domain Anda di Virtuozzo Hybrid Infrastructure. Misalnya, **Default**.
  Nama domain peka huruf besar-kecil.
- Di bidang **Nama pengguna** dan **Kata sandi**, masukkan kredensial untuk akun pengguna Virtuozzo Hybrid Infrastructure dengan peran **Administrator** di domain yang ditentukan.
  Untuk informasi lebih lanjut tentang pengguna, peran, dan domain, baca Mengonfigurasi akun pengguna di Virtuozzo Hybrid Infrastructure.



5. Daftarkan peralatan di layanan Cyber Protection dengan menggunakan salah satu cara berikut.
   - [Hanya untuk penyewa tanpa autentikasi dua faktor] Daftarkan alat di antarmuka grafisnya.
     a. Di bawah **Opsi agen**, di bidang **Server Manajemen**, klik **Ubah**.
     b. Di bidang **Nama server/IP**, pilih **Awan**.
        Alamat layanan Cyber Protection muncul. Jangan ubah alamat ini kecuali diperintahkan.
     c. Di bidang **Nama pengguna** dan **Kata sandi**, tentukan kredensial untuk akun Anda di layanan Cyber Protection. Alat virtual dan mesin virtual yang dikelola alat terdaftar dengan akun ini.
     d. Klik **OK**.
   - Daftarkan alat di antarmuka baris perintah.

     Catatan
     Dengan metode ini, Anda memerlukan token pendaftaran. Untuk informasi selengkapnya tentang cara membuatnya, lihat "Membuat token pendaftaran" (hlm. 167).

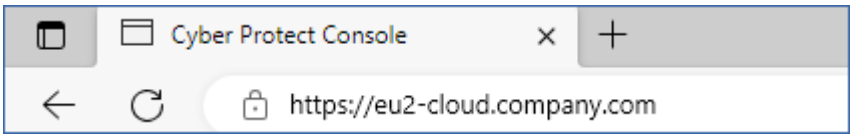
     a. Tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.
     b. Jalankan perintah berikut:

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


© Acronis International GmbH, 2003-2024

Catatan

Saat Anda menggunakan token registrasi, Anda harus menentukan alamat pusat data yang tepat. Ini adalah URL yang Anda lihat **setelah Anda masuk** ke konsol Cyber Protect. Misalnya, `https://eu2-cloud.company.com`.



Jangan gunakan `https://cloud.company.com` di sini.

c. Untuk kembali ke antarmuka grafis alat, tekan ALT+F1.

6. [Jika server proksi diaktifkan pada jaringan Anda] Konfigurasikan server proxy.
   a. Tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.
   b. Buka file **/etc/Acronis/Global.config** dalam editor teks.
   c. Lakukan salah satu langkah berikut:
      - Jika pengaturan proksi ditentukan selama instalasi agen, temukan bagian berikut:

```
<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>
```

      - Jika tidak, salin baris di atas dan tempel ke file di antara tag `<registry name="Global">...</registry>`.
   d. Ganti `ADDRESS` dengan nama host server proksi/alamat IP yang baru, dan `PORT` dengan nilai desimal nomor port.
   e. Jika server proksi Anda membutuhkan otentikasi, ganti `LOGIN` dan `PASSWORD` dengan kredensial server proksi. Atau, hapus baris ini dari file.
   f. Simpan file.
   g. Buka file **/opt/acronis/etc/aakore.yaml** dalam editor teks.
   h. Temukan bagian **env** atau buat bagian tersebut dan tambahkan baris berikut:

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

   i. Ganti `proxy_login` dan `proxy_password` dengan kredensial server proksi, dan `proxy_address:port` dengan alamat dan nomor port dari server proksi.
   j. Jalankan perintah `reboot`.

© Acronis International GmbH, 2003-2024

Catatan

Untuk dapat memperbarui alat virtual yang diterapkan di belakang proxy, edit file `config.yaml` peralatan (`/opt/acronis/etc/va-updater/config.yaml`), dengan menambahkan baris berikut ke bagian bawah file tersebut, lalu memasukkan nilai khusus untuk lingkungan Anda:

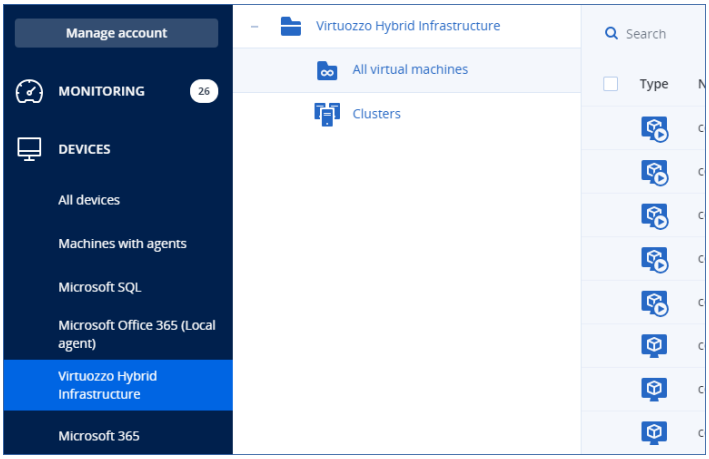
```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Misalnya:

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

Untuk melindungi mesin virtual dalam klaster Virtuozzo Hybrid Infrastructure

1. Masuk ke akun Cyber Protection Anda.
2. Buka **Perangkat** > **Virtuozzo Hybrid Infrastructure**> <klaster Anda> > **Proyek default** > **admin** atau temukan mesin Anda di **Perangkat** > **Semua perangkat**.
3. Pilih mesin dan terapkan rencana perlindungan pada mesin tersebut.



Menyebarkan Agen untuk oVirt (Alat Virtual)

Sebelum Anda memulai

Alat ini adalah mesin virtual yang sudah dikonfigurasi yang Anda sebarkan di pusat data Red Hat Virtualization/oVirt. Alat ini berisi agen proteksi yang memungkinkan Anda mengelola perlindungan cyber untuk semua mesin virtual di pusat data.

Persyaratan sistem untuk agen

Secara default, mesin virtual dengan agen menggunakan 2 vCPU dan RAM 4 GiB. Pengaturan ini cukup untuk sebagian besar operasi, tetapi Anda dapat mengeditnya di Portal Administrasi Red Hat Virtualization/oVirt.

© Acronis International GmbH, 2003-2024

Untuk meningkatkan kinerja pencadangan dan menghindari kegagalan terkait dengan kekurangan memori RAM, kami menyarankan Anda meningkatkan sumber daya ini menjadi 4 vCPU dan 8 GiB RAM dalam kasus yang lebih berat. Contohnya, tingkatkan sumber daya yang ditetapkan jika Anda mengharapkan lalu lintas cadangan akan melebihi 100 MB per detik (misal, di jaringan 10-Gigabit) atau jika Anda mencadangkan banyak mesin virtual dengan hard drive besar (500 GB atau lebih) secara bersamaan.

Ukuran disk virtual alat adalah 8 GiB.

Berapa jumlah agen yang saya perlukan?

Satu agen dapat melindungi seluruh pusat data. Namun, Anda dapat memiliki lebih dari satu agen di Pusat data jika perlu mendistribusikan beban bandwidth lalu lintas cadangan.

Jika Anda memiliki lebih dari satu agen di pusat data, mesin virtual akan otomatis didistribusikan di antara agen-agen tersebut sehingga setiap agen mengelola mesin dalam jumlah yang sama.

Distribusi ulang otomatis terjadi saat ketidakseimbangan beban di antara agen mencapai 20 persen. Hal ini dapat terjadi setelah Anda menambahkan atau menghapus mesin atau agen. Misalnya, Anda menyadari bahwa Anda membutuhkan lebih banyak agen untuk membantu throughput dan Anda menyebarkan alat virtual tambahan ke pusat data. Server manajemen akan menetapkan mesin yang paling tepat untuk agen baru. Beban agen lama akan berkurang. Ketika Anda menghapus agen, mesin yang ditetapkan ke agen tersebut akan didistribusikan ulang di antara agen yang tersisa. Namun, hal ini tidak akan terjadi jika agen rusak atau dihapus secara manual dari Portal Administrasi Red Hat Virtualization/oVirt. Redistribusi akan dimulai hanya setelah Anda menghapus agen tersebut dari konsol Cyber Protect.

Untuk memeriksa agen mana yang mengelola suatu mesin

1. Di konsol Cyber Protect, klik **Perangkat**, lalu pilih **oVirt**.
2. Klik ikon roda gigi di sudut kanan atas tabel, dan pada **Sistem**, pilih kotak centang **Agen**.
3. Periksa nama agen di kolom yang muncul.

Pembatasan

Operasi berikut tidak didukung untuk mesin virtual Red Hat Virtualization/oVirt:

- Cadangan keberadaan aplikasi
- Menjalankan mesin virtual dari cadangan
- Replikasi mesin virtual
- Mengubah pelacakan blok

Menyebarkan templat OVA

1. Masuk ke akun Cyber Protection Anda.
2. Klik **Perangkat** > **Semua perangkat** > **Tambahkan** > **Red Hat Virtualization (oVirt)**.

© Acronis International GmbH, 2003-2024

Arsip .zip diunduh ke mesin Anda.

3. Ekstrak arsip .zip. Arsip ini berisi satu file .ova.
4. Unggah file .ova ke host di pusat data Red Hat Virtualization/oVirt yang ingin Anda lindungi.
5. Masuk ke Portal Administrasi Red Hat Virtualization/oVirt sebagai administrator. Untuk informasi lebih lanjut tentang peran yang diperlukan bagi operasi dengan mesin virtual, lihat "Agen untuk oVirt - peran dan port yang diperlukan" (hlm. 157).
6. Dari menu navigasi, pilih **Komputasi** > **Mesin virtual**.
7. Klik ikon elipsis vertikal di atas tabel utama, lalu klik **Impor**.
8. Di jendela **Impor Mesin Virtual**, lakukan hal berikut:
   a. Di **Pusat data**, pilih pusat data yang ingin Anda lindungi.
   b. Di **Sumber**, pilih **Alat Virtual (OVA)**.
   c. Di **Host**, pilih host tempat Anda mengunggah file .ova.
   d. Di **Jalur File**, tentukan jalur ke direktori yang berisi file .ova.
   e. Klik **Muat**.
      Templat alat virtual oVirt dari file .ova muncul di panel **Mesin Virtual di Sumber**.
      Jika templat tidak muncul di panel ini, pastikan Anda sudah menentukan jalur yang benar ke file, file tidak rusak, dan host dapat dijangkau.
   f. Pada **Mesin Virtual di Sumber**, pilih templat alat virtual oVirt, lalu klik panah kanan.
      Template muncul di panel **Mesin virtual yang akan diimpor**.
   g. Klik **Berikutnya**.
9. Di jendela yang baru, klik nama alat, lalu konfigurasikan pengaturan berikut:
   - Pada tab **Antarmuka jaringan**, konfigurasi antarmuka jaringan.
   - [Opsional] Pada tab **Umum**, ubah nama default mesin virtual dengan agen.

Penyebaran selesai. Berikutnya, Anda harus mengonfigurasikan alat virtual. Untuk informasi lebih lanjut tentang cara mengonfigurasinya, lihat "Mengonfigurasi alat virtual" (hlm. 155).

Catatan
Jika membutuhkan lebih dari satu alat virtual di pusat data Anda, ulangi langkah-langkah di atas dan sebarkan alat virtual tambahan. Jangan membuat klona alat virtual yang sudah ada dengan opsi **Buat klona VM** di Portal Administrasi Red Hat Virtualization/oVirt.

Untuk mengecualikan alat virtual dari pencadangan grup dinamis, Anda juga harus mengecualikannya dari daftar mesin virtual di konsol Cyber Protect. Untuk mengecualikannya, di Portal Administrasi Red Hat Virtualization/oVirt, pilih mesin virtual dengan agen, lalu tetapkan tag `acronis_virtual_appliance` ke mesin virtual.

© Acronis International GmbH, 2003-2024

Mengonfigurasi alat virtual

Setelah menyebarkan alat virtual, Anda harus mengonfigurasinya agar dapat menjangkau mesin oVirt dan layanan Cyber Protection.

Untuk mengonfigurasi alat virtual

1. Masuk ke Portal Administrasi Red Hat Virtualization/oVirt.
2. Pilih alat virtual yang ingin Anda konfigurasikan, lalu klik ikon **Konsol**.
3. Di bidang **eth0**, konfigurasi antarmuka jaringan alat.
   Pastikan alamat DHCP yang ditetapkan secara otomatis (jika ada) valid dalam jaringan yang digunakan mesin virtual Anda atau tetapkan secara manual. Tergantung pada jumlah jaringan yang digunakan alat, mungkin ada satu atau beberapa antarmuka yang perlu dikonfigurasikan.
4. Di bidang **oVirt**, klik **Ubah** guna menentukan alamat mesin dan kredensial oVirt untuk mengaksesnya:
   a. Di bidang **Nama server/IP**, masukkan nama DNS atau alamat IP mesin.
   b. Di bidang **Nama pengguna** dan **Kata sandi**, masukkan kredensial administrator untuk mesin ini.
      Pastikan akun administrator ini memiliki peran yang diperlukan untuk operasi dengan mesin virtual Red Hat Virtualization/oVirt. Untuk informasi lebih lanjut tentang peran ini, lihat "Agen untuk oVirt - peran dan port yang diperlukan" (hlm. 157).
      Jika Keycloak adalah penyedia Single-Sign-On (SSO) untuk mesin oVirt (default di oVirt 4.5.1), gunakan format Keycloak saat menentukan nama pengguna. Contohnya, sebutkan akun administrator default sebagai `admin@ovirt@internalsso` bukan `admin@internal`.
   c. [Opsional] Klik **Periksa koneksi** untuk memastikan bahwa kredensial yang diberikan sudah benar.
   d. Klik **OK**.
5. Daftarkan peralatan di layanan Cyber Protection dengan menggunakan salah satu cara berikut.
   - [Hanya untuk penyewa tanpa autentikasi dua faktor] Daftarkan alat di antarmuka grafisnya.
     a. Di bawah **Opsi agen**, di bidang **Server Manajemen**, klik **Ubah**.
     b. Di bidang **Nama server/IP**, pilih **Awan**.
        Alamat layanan Cyber Protection muncul. Jangan ubah alamat ini kecuali diperintahkan.
     c. Di bidang **Nama pengguna** dan **Kata sandi**, tentukan kredensial untuk akun Anda di layanan Cyber Protection. Alat virtual dan mesin virtual yang dikelola alat terdaftar dengan akun ini.
     d. Klik **OK**.
   - Daftarkan alat di antarmuka baris perintah.

© Acronis International GmbH, 2003-2024

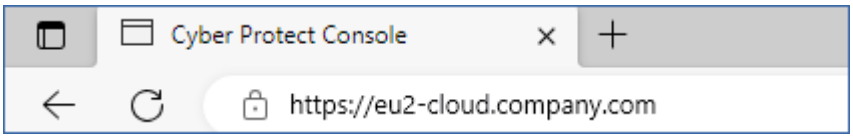
Catatan
Dengan metode ini, Anda memerlukan token pendaftaran. Untuk informasi selengkapnya tentang cara membuatnya, lihat "Membuat token pendaftaran" (hlm. 167).

a. Tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.

b. Jalankan perintah berikut:

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

Catatan
Saat Anda menggunakan token registrasi, Anda harus menentukan alamat pusat data yang tepat. Ini adalah URL yang Anda lihat **setelah Anda masuk** ke konsol Cyber Protect. Misalnya, `https://eu2-cloud.company.com`.



Jangan gunakan `https://cloud.company.com` di sini.

c. Untuk kembali ke antarmuka grafis alat, tekan ALT+F1.

6. [Opsional] Di bidang **Nama**, klik **Ubah** untuk mengedit nama default bagi alat virtual, yaitu **localhost**. Nama ini ditampilkan di konsol Cyber Protect.
7. [Opsional] Di bidang **Waktu**, klik **Ubah**, lalu pilih zona waktu lokasi Anda untuk memastikan operasi terjadwal berjalan pada waktu yang tepat.
8. [Opsional] [Jika server proksi diaktifkan pada jaringan Anda] Konfigurasikan server proxy.
   a. Tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.
   b. Buka file **/etc/Acronis/Global.config** dalam editor teks.
   c. Lakukan salah satu langkah berikut:
      - Jika pengaturan proksi ditentukan selama instalasi agen, temukan bagian berikut:

```
<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>
```

      - Jika tidak, salin baris di atas dan tempel ke file di antara tag `<registry name="Global">...</registry>`.
   d. Ganti `ADDRESS` dengan nama host server proksi/alamat IP yang baru, dan `PORT` dengan nilai desimal nomor port.

© Acronis International GmbH, 2003-2024

e. Jika server proksi Anda membutuhkan otentikasi, ganti `LOGIN` dan `PASSWORD` dengan kredensial server proksi. Atau, hapus baris ini dari file.

f. Simpan file.

g. Buka file **/opt/acronis/etc/aakore.yaml** dalam editor teks.

h. Temukan bagian **env** atau buat bagian tersebut dan tambahkan baris berikut:

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

i. Ganti `proxy_login` dan `proxy_password` dengan kredensial server proksi, dan `proxy_address:port` dengan alamat dan nomor port dari server proksi.

j. Jalankan perintah `reboot`.

Catatan

Untuk dapat memperbarui alat virtual yang diterapkan di belakang proxy, edit file `config.yaml` peralatan (`/opt/acronis/etc/va-updater/config.yaml`), dengan menambahkan baris berikut ke bagian bawah file tersebut, lalu memasukkan nilai khusus untuk lingkungan Anda:

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

Misalnya:

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

Untuk melindungi mesin virtual di pusat data Red Hat Virtualization/oVirt

1. Masuk ke akun Cyber Protection Anda.
2. Pilih **Perangkat** > **oVirt** > <klaster Anda> atau temukan mesin Anda di **Perangkat** > **Semua perangkat**.
3. Pilih mesin dan terapkan rencana perlindungan pada mesin tersebut.

Agen untuk oVirt - peran dan port yang diperlukan

Peran yang diperlukan

Untuk penyebaran dan operasinya, Agen untuk oVirt memerlukan akun administrator dengan peran yang ditetapkan berikut ini.

oVirt/Red Hat Virtualization 4.2 dan 4.3/Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager

© Acronis International GmbH, 2003-2024

- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4, 4.5

- SuperUser

Port yang diperlukan

Agen untuk oVirt terhubung ke mesin oVirt menggunakan URL yang Anda tentukan saat mengonfigurasi alat virtual. Biasanya, URL mesin memiliki format berikut: `https://ovirt.company.com`. Dalam kasus ini, protokol HTTPS dan port 443 digunakan.

Pengaturan oVirt non-default mungkin memerlukan port lain. Anda dapat menemukan port yang tepat dengan menganalisis format URL. Misalnya:

URL mesin oVirt	Port	Protokol
`https://ovirt.company.com/`	443	HTTPS
`http://ovirt.company.com/`	80	HTTP
`https://ovirt.company.com:1234/`	1234	HTTPS

Tidak ada port tambahan yang diperlukan untuk operasi Baca/Tulis disk, karena pencadangan dilakukan dalam mode HotAdd.

Menyebarkan Agen untuk Synology

Sebelum Anda memulai

Dengan Agen untuk Synology, Anda dapat mencadangkan file dan folder dari dan ke perangkat NAS Synology. Properti khusus NAS dan izin akses untuk berbagi, folder, dan file dilindungi.

Agen untuk Synology berjalan pada perangkat NAS. Oleh karena itu, Anda dapat menggunakan sumber daya perangkat untuk operasi pemrosesan data di luar host seperti replikasi cadangan, validasi, dan pembersihan. Untuk mempelajari lebih lanjut tentang operasi ini, lihat "Pemrosesan data off-host" (hlm. 197).

Catatan
Agen untuk Synology hanya mendukung perangkat NAS dengan prosesor x86_64. Prosesor ARM tidak didukung.

Anda dapat memulihkan cadangan ke lokasi asal atau lokasi baru di perangkat NAS, serta ke folder jaringan yang dapat diakses melalui perangkat tersebut. Cadangan di penyimpanan awan juga dapat dipulihkan ke perangkat NAS non-asli tempat Agen untuk Synology diinstal.

Tabel di bawah merangkum sumber dan tujuan cadangan yang tersedia.

© Acronis International GmbH, 2003-2024

Apa yang harus dicadangkan	Item untuk dicadangkan (Sumber cadangan)	Tempat menyimpan cadangan (Tujuan cadangan)
File/folder	Folder lokal*	Penyimpanan awan
		Folder lokal*
	Folder jaringan (SMB)**	Folder jaringan (SMB)**
		Folder NFS

* Mencakup drive USB yang terpasang ke perangkat NAS.

Catatan
Folder yang dienkripsi tidak didukung. Folder ini tidak ditampilkan di antarmuka pengguna grafis Cyber Protection.

** Menggunakan berbagi jaringan eksternal sebagai sumber cadangan atau tujuan cadangan melalui protokol SMB hanya tersedia untuk agen yang berjalan pada Synology DiskStation Manager 6.2.3 atau versi lebih baru. Data yang di-host pada NAS Synology itu sendiri, termasuk di berbagi jaringan yang di-host, dapat dicadangkan tanpa batasan.

Pembatasan

- Agen untuk Synology hanya mendukung perangkat NAS dengan prosesor x86_64. Prosesor ARM tidak didukung.
- Bagian terenkripsi yang dicadangkan dipulihkan menjadi tidak terenkripsi.
- Bagian cadangan yang mengaktifkan opsi **Kompresi file** dipulihkan dengan menonaktifkan opsi ini.
- Anda hanya dapat memulihkan cadangan yang dibuat oleh Agen untuk Synology ke perangkat NAS Synology.

Mengunduh program penyiapan

Program penyiapan untuk Agen untuk Synology tersedia dalam bentuk file SPK.

Agen untuk Synology 7.x

Untuk mengunduh program penyiapan

1. Pada konsol Cyber Protect, navigasi ke **Perangkat** > **Semua perangkat**.
2. Di pojok kanan atas, klik **Tambahkan**.
3. Di bagian **Network attached storage (NAS)**, klik **Synology**.
   Program penyiapan diunduh ke mesin Anda.

Agen untuk Synology 6.x

© Acronis International GmbH, 2003-2024

Untuk mengunduh program penyiapan

1. Pada konsol Cyber Protect, navigasi ke **Perangkat** > **Semua perangkat**.
2. Di pojok kanan atas, klik **Tambahkan**.
3. Di bagian **Network attached storage (NAS)**, klik **Synology**.
   Program penyiapan untuk Agen untuk Synology 7.x diunduh ke mesin Anda.
   Anda dapat menghentikan proses pengunduhan dengan aman atau mengabaikan file yang diunduh.
4. Klik **Unduh Agen untuk Synology 6.x**.
   Program penyiapan untuk Agen untuk Synology 6.x diunduh ke mesin Anda.

Menginstal Agen untuk Synology

Untuk menginstal Agen untuk Synology, jalankan file SPK di Synology DiskStation Manager.

Catatan
Agen untuk Synology hanya mendukung perangkat NAS dengan prosesor x86_64. Prosesor ARM tidak didukung.

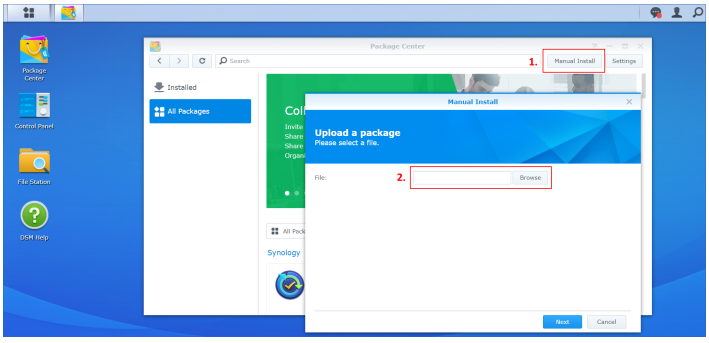
Agen untuk Synology 7.x

Prasyarat

- Perangkat NAS menjalankan versi DiskStation Manager 7.x.
- Anda adalah anggota grup **administrator** di perangkat NAS.
- Setidaknya ada 200 MB ruang bebas pada volume NAS tempat Anda ingin menginstal agen.
- Klien SSH tersedia di mesin Anda. Dokumen ini menggunakan Putty sebagai contoh.

Cara menginstal Agen untuk Synology

1. Masuk ke Synology DiskStation Manager.
2. Buka **Pusat Paket**.
3. Klik **Instal Manual**, lalu klik **Telusuri**.

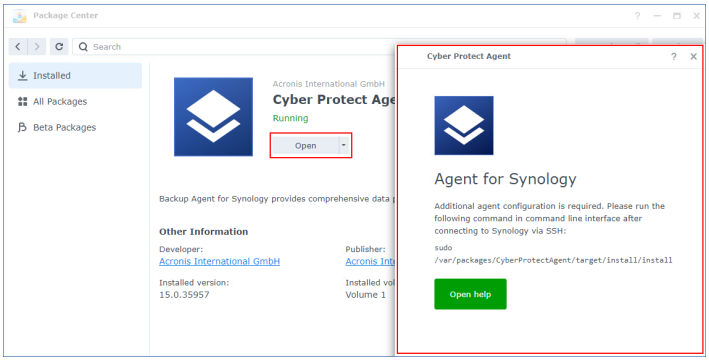


4. Pilih file SPK yang Anda unduh dari konsol Cyber Protect, lalu klik **Berikutnya**.

© Acronis International GmbH, 2003-2024

Peringatan bahwa Anda akan menginstal paket perangkat lunak pihak ketiga ditampilkan. Pesan ini adalah bagian dari prosedur instalasi standar.

5. Untuk mengonfirmasi bahwa Anda ingin memasang paket, klik **Setuju**.
6. Pilih volume tempat Anda ingin menginstal agen, lalu klik **Berikutnya**.
7. Periksa pengaturannya, lalu klik **Selesai**.
8. Di Synology DiskStation Manager **Pusat Paket**, buka Cyber Protect Agen untuk Synology, lalu verifikasi bahwa Anda melihat layar berikut.

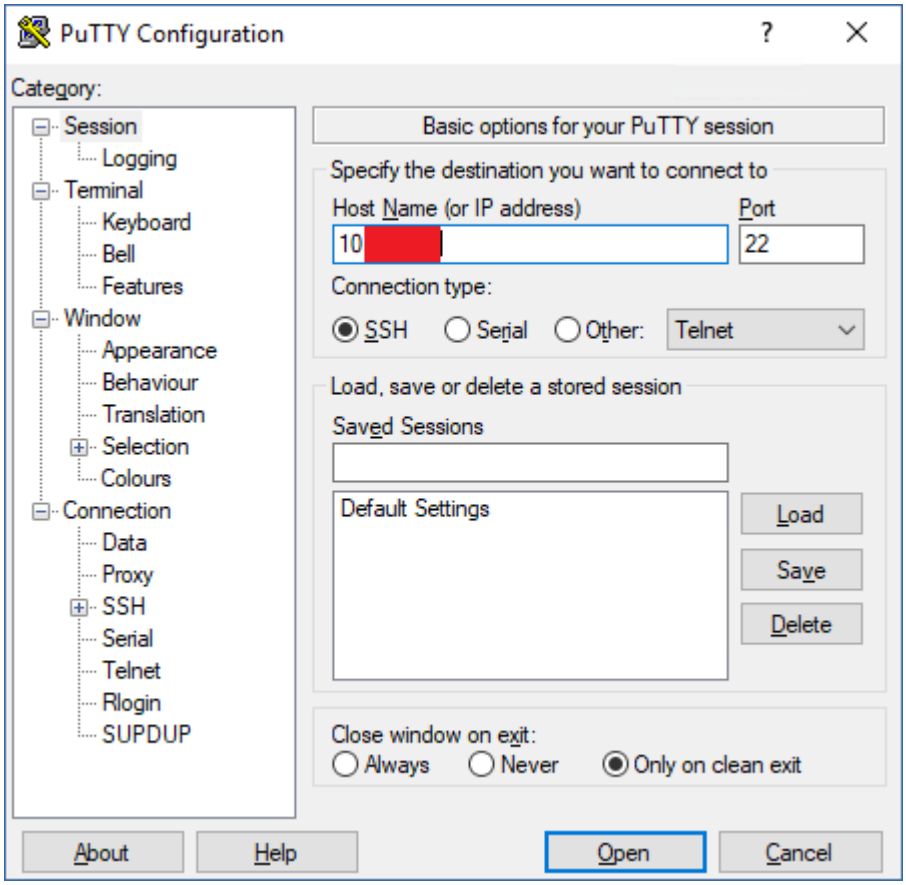


9. Di Synology DiskStation Manager **Panel Kontrol**, buka **Terminal & SNMP**, lalu aktifkan akses SSH ke perangkat NAS.
10. Jalankan skrip `instal` pada perangkat NAS dengan menggunakan klien SSH (dalam contoh ini, Putty).

    Skrip ini mengaktifkan akses root ke DSM 7.0 atau lebih baru, yang diperlukan untuk mengonfigurasi agen.

© Acronis International GmbH, 2003-2024

a. Mulai Putty, lalu tentukan alamat IP atau nama host perangkat NAS Synology Anda.



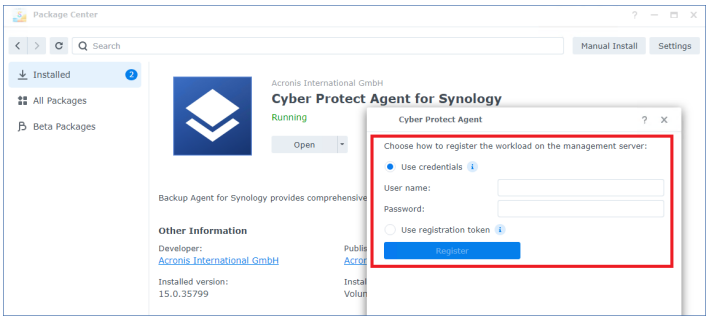
b. Klik **Buka**, lalu masuk sebagai administrator DSM Synology.

c. Jalankan perintah berikut.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

Setelah skrip dimulai, tunggu selama 15 detik selama layanan Cyber Protection diinisialisasi.

11. Di Synology DiskStation Manager **Panel Kontrol**, buka **Terminal & SNMP**, lalu nonaktifkan akses SSH ke perangkat NAS. Akses SSH tidak lagi diperlukan.
12. Di Synology DiskStation Manager **Pusat Paket**, buka Cyber Protect Agen untuk Synology.
13. Pilih metode registrasi.



© Acronis International GmbH, 2003-2024

- [Untuk mendaftarkan agen dengan menggunakan kredensial]
  - Dalam bidang **Nama pengguna** dan **Kata sandi**, tentukan kredensial untuk akun di tempat agen akan didaftarkan. Akun ini tidak bisa menjadi akun administrator mitra.
- [Untuk mendaftarkan agen dengan menggunakan token registrasi]
  - Di **Alamat registrasi**, tentukan alamat pusat data yang tepat. Alamat pusat data yang tepat adalah URL yang Anda lihat setelah Anda masuk ke konsol Cyber Protect. Sebagai contoh, `https://us5-cloud.acronis.com`.

    Catatan
    Jangan gunakan format URL tanpa alamat pusat data. Misalnya, jangan gunakan `https://cloud.acronis.com`.

  - Di kolom **Token**, tentukan token registrasi.
    Untuk informasi lebih lanjut tentang cara membuat token pendaftaran, lihat "Membuat token pendaftaran" (hlm. 167).

14. Klik **Daftar**.

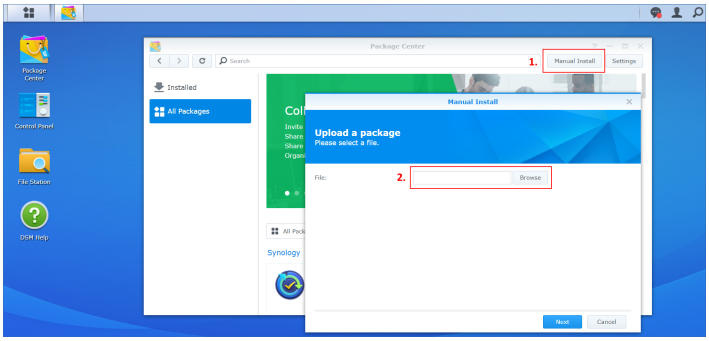
Agen untuk Synology 6.x

Prasyarat

- Perangkat NAS menjalankan versi DiskStation Manager 6.2.x.
- Anda adalah anggota grup **administrator** di perangkat NAS.
- Setidaknya ada 200 MB ruang bebas pada volume NAS tempat Anda ingin menginstal agen.

Cara menginstal Agen untuk Synology

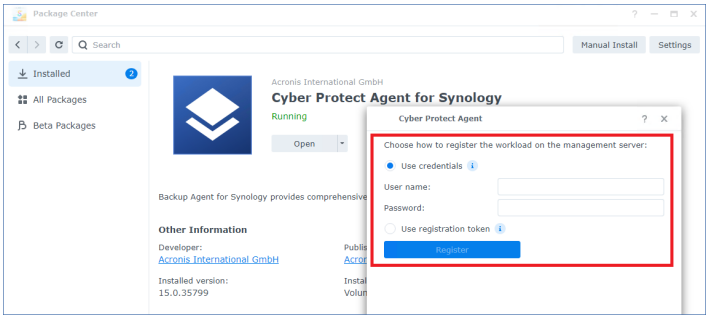
1. Masuk ke Synology DiskStation Manager.
2. Buka **Pusat Paket**.
3. Klik **Instal Manual**, lalu klik **Telusuri**.



4. Pilih file SPK yang Anda unduh dari konsol Cyber Protect, lalu klik **Berikutnya**.
   Peringatan bahwa Anda akan menginstal paket tanpa tanda tangan digital ditampilkan. Pesan ini adalah bagian dari prosedur instalasi standar.
5. Untuk mengonfirmasi bahwa Anda ingin memasang paket, klik **Ya**.
6. Pilih volume tempat Anda ingin menginstal agen, lalu klik **Berikutnya**.

© Acronis International GmbH, 2003-2024

7. Periksa pengaturannya, lalu klik **Terapkan**.
8. Di Synology DiskStation Manager **Pusat Paket**, buka Cyber Protect Agen untuk Synology.
9. Pilih metode registrasi.



- [Untuk mendaftarkan agen dengan menggunakan kredensial]
  - Dalam bidang **Nama pengguna** dan **Kata sandi**, tentukan kredensial untuk akun di tempat agen akan didaftarkan. Akun ini tidak bisa menjadi akun administrator mitra.
- [Untuk mendaftarkan agen dengan menggunakan token registrasi]
  - Di **Alamat registrasi**, tentukan alamat pusat data yang tepat. Alamat pusat data yang tepat adalah URL yang Anda lihat setelah Anda masuk ke konsol Cyber Protect. Sebagai contoh, `https://us5-cloud.acronis.com`.

    Catatan
    Jangan gunakan format URL tanpa alamat pusat data. Misalnya, jangan gunakan `https://cloud.acronis.com`.

  - Di kolom **Token**, tentukan token registrasi.

    Untuk informasi lebih lanjut tentang cara membuat token pendaftaran, lihat "Membuat token pendaftaran" (hlm. 167).
10. Klik **Daftar**.

Ketika registrasi selesai, perangkat NAS Synology muncul di konsol Cyber Protect, pada tab **Perangkat** > **Network Attached Storage**.

Untuk mencadangkan data di perangkat NAS, terapkan rencana proteksi.

Memperbarui Agen untuk Synology

Anda dapat memperbarui Agen untuk Synology 6.x ke versi Agen untuk Synology 6.x yang lebih baru. Demikian pula, Anda dapat memperbarui Agent untuk Synology 7.x ke versi Agen untuk Synology 7.x yang lebih baru.

Untuk memperbarui agen, jalankan versi terbaru program penyiapan di Synology DiskStation Manager. Registrasi orisinal agen, pengaturannya, dan rencana yang diterapkan ke beban kerja terlindungi akan dipertahankan.

Catatan
Anda tidak dapat memperbarui agen dari konsol Cyber Protect.

© Acronis International GmbH, 2003-2024

Memutakhirkan Agen untuk Synology 6.x ke Agen untuk Synology 7.x hanya didukung dengan menghapus instalasi agen lama dan menginstal agen yang lebih baru. Dalam kasus ini, semua rencana proteksi akan dibatalkan dan Anda harus menerapkannya kembali secara manual.

Agen untuk Synology 7.x

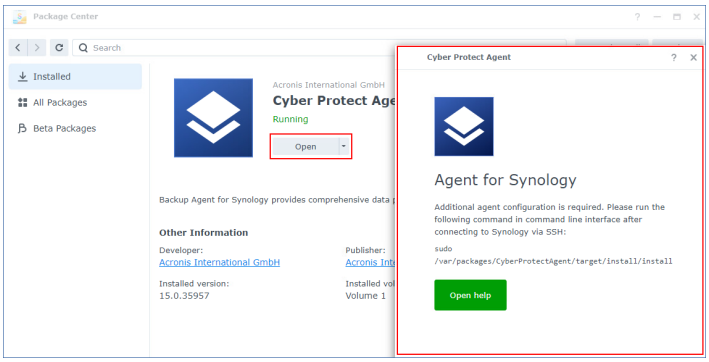
Prasyarat

- Anda adalah anggota grup **administrator** di perangkat NAS.
- Setidaknya ada 200 MB ruang bebas pada volume NAS tempat Anda ingin menginstal agen.
- Klien SSH tersedia di mesin Anda. Dokumen ini menggunakan Putty sebagai contoh.

Cara memperbarui Agen untuk Synology

1. Di DiskStation Manager, buka **Pusat Paket**.
2. Klik **Instal Manual**, lalu klik **Telusuri**.
3. Pilih file SPK terbaru untuk Agen untuk Synology 7.x yang Anda unduh dari konsol Cyber Protect, lalu klik **Berikutnya**.

   Peringatan bahwa Anda akan menginstal paket perangkat lunak pihak ketiga ditampilkan. Pesan ini adalah bagian dari prosedur instalasi standar.
4. Untuk mengonfirmasi bahwa Anda ingin memasang paket, klik **Setuju**.
5. Periksa pengaturannya, lalu klik **Selesai**.
6. Di Synology DiskStation Manager **Pusat Paket**, buka Cyber Protect Agen untuk Synology, lalu verifikasi bahwa Anda melihat layar berikut.

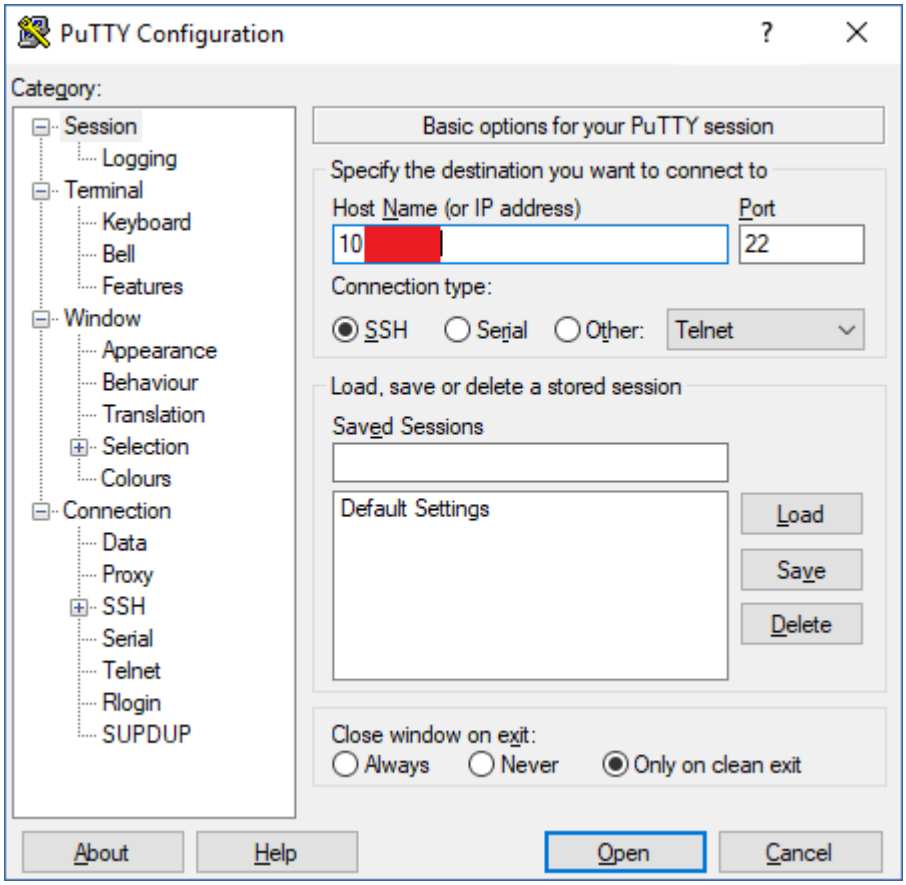


7. Di Synology DiskStation Manager **Panel Kontrol**, buka **Terminal & SNMP**, lalu aktifkan akses SSH ke perangkat NAS.
8. Jalankan skrip `instal` pada perangkat NAS dengan menggunakan klien SSH (dalam contoh ini, Putty).

   Skrip ini mengaktifkan akses root ke DSM 7.0 atau lebih baru, yang diperlukan untuk mengonfigurasi agen.

© Acronis International GmbH, 2003-2024

a. Mulai Putty, lalu tentukan alamat IP atau nama host perangkat NAS Synology Anda.



b. Klik **Buka**, lalu masuk sebagai administrator DSM Synology.

c. Jalankan perintah berikut.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

9. Di Synology DiskStation Manager **Panel Kontrol**, buka **Terminal & SNMP**, lalu nonaktifkan akses SSH ke perangkat NAS. Akses SSH tidak lagi diperlukan.

Agen untuk Synology 6.x

Prasyarat

- Anda adalah anggota grup **administrator** di perangkat NAS.
- Setidaknya ada 200 MB ruang bebas pada volume NAS tempat Anda ingin menginstal agen.

Cara memperbarui Agen untuk Synology

1. Di DiskStation Manager, buka **Pusat Paket**.
2. Klik **Instal Manual**, lalu klik **Telusuri**.
3. Pilih file SPK terbaru untuk Agen untuk Synology 6.x yang Anda unduh dari konsol Cyber Protect, lalu klik **Berikutnya**.

© Acronis International GmbH, 2003-2024

Peringatan bahwa Anda akan menginstal paket tanpa tanda tangan digital ditampilkan. Pesan ini adalah bagian dari prosedur instalasi standar.

4. Untuk mengonfirmasi bahwa Anda ingin memasang paket, klik **Ya**.
5. Periksa pengaturannya, lalu klik **Terapkan**.

Menyebarkan agen melalui Kebijakan Grup

Anda dapat menginstal (atau menyebarkan) Agen untuk Windows secara terpusat ke mesin yang menjadi anggota domain Active Directory menggunakan Kebijakan Grup Windows.

Di bagian ini, Anda akan mengetahui cara mengatur objek Kebijakan Grup untuk menyebarkan agen ke mesin di seluruh domain atau di unit organisasinya.

Setiap kali mesin masuk ke domain, objek Kebijakan Grup yang dihasilkan akan memastikan bahwa agen diinstal dan terdaftar.

Prasyarat

- Domain Active Directory dengan pengontrol domain yang menjalankan Microsoft Windows Server 2003 ke atas.
- Anda harus menjadi anggota grup **Admin Domain** di dalam domain ini.
- Anda telah mengunduh program penyiapan **Semua agen untuk Windows**.
  Untuk mengunduh program penyiapan, di konsol Cyber Protect, klik ikon akun di pojok kanan atas, lalu klik **Unduhan**. Tautan unduhan juga tersedia di panel **Tambah peranti**.

Cara menyebarkan agen melalui Kebijakan Grup

1. Buat token registrasi seperti yang dijelaskan di "Membuat token pendaftaran" (hlm. 167).
2. Buat file .mst, file .msi, dan file .cab, seperti yang dijelaskan di "Membuat file transformasi dan mengekstrak paket instalasi" (hlm. 170).
3. Siapkan objek Kebijakan Grup seperti yang dijelaskan di "Menyiapkan objek Kebijakan Grup" (hlm. 171).

Membuat token pendaftaran

Token registrasi mengirimkan identitas pengguna ke program penyiapan agen, tanpa menyimpan kredensial pengguna untuk konsol Cyber Protect. Ini memungkinkan pengguna untuk mendaftarkan sejumlah mesin di bawah akun mereka atau menerapkan rencana proteksi pada beban kerja mereka tanpa harus masuk ke Log.

Catatan
Rencana proteksi tidak diterapkan secara otomatis selama registrasi mesin. Menerapkan rencana proteksi adalah tugas yang terpisah.

© Acronis International GmbH, 2003-2024

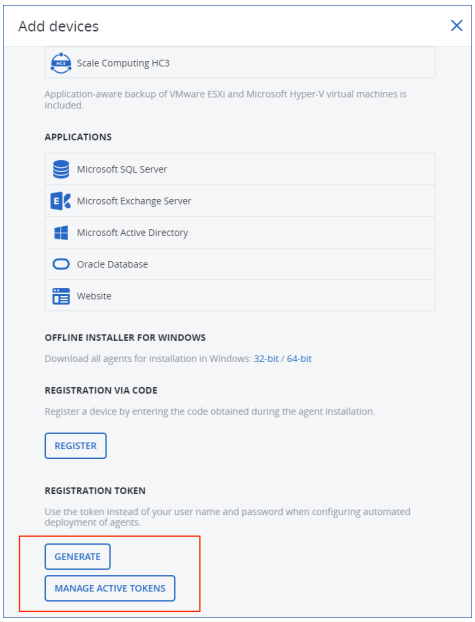
Untuk alasan keamanan, token memiliki masa pakai terbatas yang dapat Anda sesuaikan. Masa aktif default adalah 3 hari.

Pengguna dapat menghasilkan token registrasi hanya untuk akun mereka sendiri. Administrator dapat membuat token registrasi untuk semua akun pengguna di penyewa yang mereka kelola.

Untuk membuat token pendaftaran

Sebagai pengguna

1. Masuk ke konsol Cyber Protect.
2. Klik **Perangkat** > **Semua perangkat** > **Tambahkan**.
   Panel **Tambah peranti** terbuka di sebelah kanan.
3. Gulir ke bawah sampai **Token pendaftaran**, lalu klik **Hasilkan**.



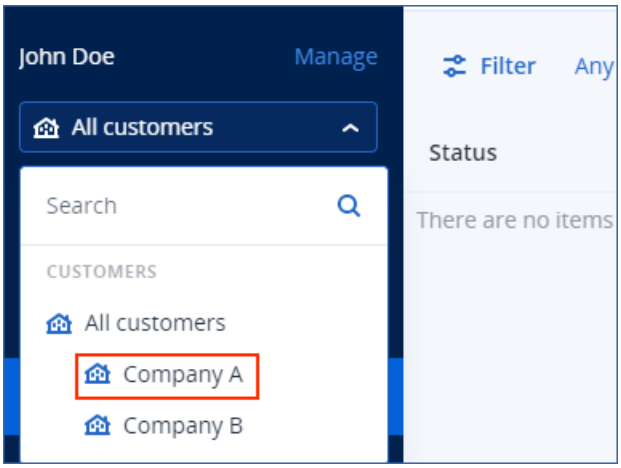
4. Tentukan masa pakai token.
5. Klik **Hasilkan token**.
6. Klik **Salin** untuk menyalin token ke papan klip perangkat Anda, atau menulis token secara manual.

Sebagai administrator

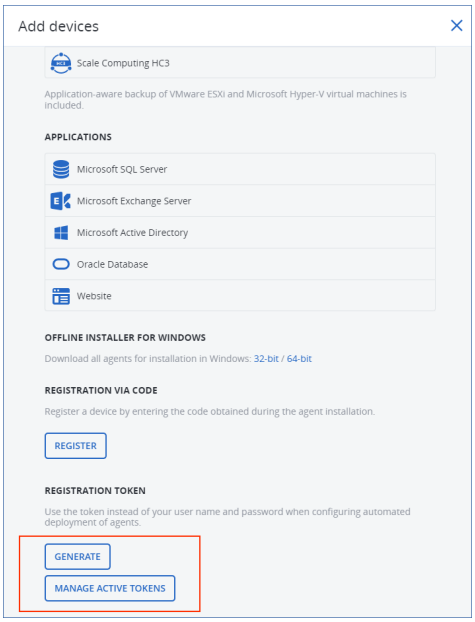
1. Masuk ke konsol Cyber Protect sebagai administrator.
   Jika Anda sudah masuk ke portal manajemen, Anda dapat membuka konsol Cyber Protect dengan menavigasi ke **Pemantauan** > **Penggunaan**, lalu di tab **Perlindungan**, klik **Kelola layanan**.

© Acronis International GmbH, 2003-2024

[Untuk administrator mitra yang mengelola penyewa pelanggan] Di konsol Cyber Protect, pilih penyewa dengan pengguna yang ingin Anda beri token. Anda tidak dapat menghasilkan token di level **Semua pelanggan**.



2. Di bawah **Perangkat**, klik **Semua perangkat** > **Tambahkan**.
   Panel **Tambah peranti** terbuka di sebelah kanan.
3. Gulir ke bawah sampai **Token pendaftaran**, lalu klik **Hasilkan**.



4. Tentukan masa pakai token.

© Acronis International GmbH, 2003-2024

5. Pilih pengguna yang tokennya ingin Anda buat.

   Catatan
   Saat Anda menggunakan token, beban kerja akan didaftarkan di bawah akun pengguna yang Anda pilih di sini.

6. [Opsional] Untuk mengaktifkan pengguna token guna menerapkan dan membatalkan rencana proteksi pada beban kerja yang ditambahkan, pilih rencana dari daftar drop-down.
   Perhatikan bahwa Anda perlu menjalankan skrip yang akan berlaku atau membatalkan rencana proteksi pada beban kerja yang ditambahkan. Lihat artikel basis pengetahuan ini untuk detail selengkapnya.
7. Klik **Hasilkan token**.
8. Klik **Salin** untuk menyalin token ke papan klip perangkat Anda, atau menulis token secara manual.

Cara melihat atau menghapus token registrasi

1. Masuk ke konsol Cyber Protect.
2. Klik **Perangkat** > **Semua perangkat** > **Tambahkan**.
3. Gulir ke bawah sampai **Token pendaftaran**, lalu klik **Kelola token aktif**.
   Daftar berisi token aktif yang dibuat untuk penyewa Anda akan terbuka di sebelah kanan.

   Catatan
   Untuk alasan keamanan, di kolom **Token**, hanya dua karakter pertama dari nilai token yang ditampilkan.

4. [Untuk menghapus token] Pilih ikon token, lalu klik **Hapus**.

Membuat file transformasi dan mengekstrak paket instalasi

Untuk menyebarkan agen perlindungan melalui Kebijakan Grup Windows, Anda memerlukan file transform (.mst) dan paket instalasi (file .msi dan .cab).

Catatan
Prosedur di bawah ini menggunakan opsi registrasi default, yaitu registrasi dengan token. Untuk mempelajari cara membuat token registrasi, lihat "Membuat token pendaftaran" (hlm. 167).

Cara membuat file .mst dan mengekstrak paket instalasi (file .msi dan .cab)

1. Masuk sebagai administrator pada mesin apa pun di dalam domain Active Directory.
2. Buat folder bersama yang akan berisi paket instalasi. Pastikan bahwa pengguna domain dapat mengakses folder bersama—misalnya, dengan membiarkan pengaturan berbagi default untuk **Semua Orang**.
3. Jalankan program penyiapan agen.

© Acronis International GmbH, 2003-2024

4. Klik **Buat file .mst dan .msi untuk instalasi tanpa pengawasan**.
5. Di **Apa yang diinstal**, pilih komponen yang ingin Anda sertakan dalam instalasi, lalu klik **Selesai**.
6. Di **Pengaturan registrasi**, klik **Tentukan**, masukkan token registrasi, lalu klik **Selesai**.
   Anda dapat mengubah metode registrasi dari **Gunakan token registrasi** (default) menjadi **Gunakan kredensial** atau **Lewati registrasi**. Opsi **Lewati registrasi** mengira bahwa Anda akan mendaftarkan beban kerja secara manual nanti.
7. Tinjau atau modifikasi pengaturan instalasi yang akan ditambahkan ke file .mst, lalu klik **Lanjutkan**.
8. Pada bagian **Simpan file ke**, tentukan jalur ke folder bersama yang Anda buat.
9. Klik **Hasilkan**.

Hasilnya, file .mst, file .msi, dan file .cab dibuat dan disalin ke folder bersama yang Anda tentukan.

Berikutnya, siapkan objek Kebijakan Grup Windows. Untuk mempelajari cara melakukannya, lihat "Menyiapkan objek Kebijakan Grup" (hlm. 171).

Menyiapkan objek Kebijakan Grup

Dalam prosedur ini Anda menggunakan paket instalasi yang Anda buat di "Membuat file transformasi dan mengekstrak paket instalasi" (hlm. 170) untuk menyiapkan objek Kebijakan Grup (GPO). GPO akan menyebarkan agen ke mesin dalam domain Anda.

Cara menyiapkan objek Kebijakan Grup

1. Masuk ke pengontrol domain sebagai administrator domain.
   Jika domain memiliki lebih dari satu pengontrol domain, masuk ke salah satunya sebagai administrator domain.
2. [Jika Anda menyebarkan agen di unit organisasi] Pastikan bahwa unit organisasi tempat Anda ingin menyebarkan agen ada di domain ini.
3. Pada menu **Start** Windows, arahkan ke **Administrative Tools**, lalu klik **Group Policy Management** (atau **Active Directory Users and Computers** untuk Windows Server 2003).
4. [Untuk Windows Server 2008 atau sebelumnya] Klik kanan nama domain atau unit organisasi, lalu klik **Buat GPO di domain ini, dan Tautkan di sini**.
5. [Untuk Windows Server 2003] Klik kanan nama domain atau unit organisasi, lalu klik **Properti**. Di kotak dialog, klik tab **Kebijakan Grup**, lalu klik **Baru**.
6. Beri nama objek Kebijakan Grup baru **Agen untuk Windows.**
7. Buka objek Kebijakan Grup **Agen untuk Windows** untuk mengedit:
   - [Di Windows Server 2008 ke atas] Pada **Objek Kebijakan Grup**, klik kanan objek Kebijakan Grup, lalu klik **Edit**.
   - [Di Windows Server 2003] Klik objek Kebijakan Grup, lalu klik **Edit**.
8. Pada snap-in editor objek Kebijakan Grup, perluas **Konfigurasi Komputer**.
9. [Untuk Windows Server 2012 atau sebelumnya] Perluas **Kebijakan** > **Pengaturan Perangkat Lunak**.

© Acronis International GmbH, 2003-2024

10. [Untuk Windows Server 2003 dan Windows Server 2008] Perluas **Pengaturan Perangkat Lunak**.
11. Klik kanan **Instalasi perangkat lunak**, arahkan ke **Baru**, lalu klik **Paket**.
12. Pilih paket instalasi .msi agen di folder bersama yang Anda buat, lalu klik **Buka**.
13. Di kotak dialog **Sebarkan Perangkat Lunak**, klik **Lanjutan**, lalu klik **OK**.
14. Di tab **Modifikasi**, klik **Tambah**, lalu pilih file .mst di folder bersama yang Anda buat.
15. Klik **OK** untuk menutup kotak dialog **Sebarkan Perangkat Lunak**.

Koneksi SSH ke alat virtual

Gunakan koneksi Secure Socket Shell (SSH) saat Anda mengakses alat virtual dari jarak jauh, untuk tujuan pemeliharaan.

Memulai Secure Shell daemon

Untuk mengizinkan koneksi SSH ke alat virtual, aktifkan Secure Shell daemon (sshd) pada alat tersebut.

Cara mengaktifkan Secure Shell daemon

1. Dalam perangkat lunak hypervisor, buka konsol alat virtual.
2. Dalam antarmuka pengguna grafik dari alat tersebut, tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.
3. Jalankan perintah berikut:

   ```
   /bin/sshd
   ```

4. [Hanya saat koneksi pertama ke alat] Atur kata sandi untuk pengguna `root`.
   Untuk memelajari cara mengatur kata sandi, lihat "Mengatur kata sandi root pada alat virtual" (hlm. 172).

Catatan
Kami merekomendasikan Anda untuk menghentikan Secure Shell daemon ketika Anda tidak menggunakan koneksi SSH.

Mengatur kata sandi root pada alat virtual

Sebelum membuat koneksi SSH ke alat virtual untuk pertama kalinya, Anda harus mengatur kata sandi root pada alat tersebut.

Cara mengatur kata sandi root

1. Dalam perangkat lunak hypervisor, buka konsol alat virtual.
2. Dalam antarmuka pengguna grafik dari alat tersebut, tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.

 © Acronis International GmbH, 2003-2024

3. Jalankan perintah berikut:

```
passwd
```

4. Tentukan kata sandi, lalu tekan Enter.

   Kata sandi harus berisi setidaknya sembilan karakter dan harus memiliki skor kompleksitas tiga atau lebih. Skor kompleksitas dihitung secara otomatis. Untuk mencapai skor yang lebih tinggi, gunakan kombinasi simbol khusus, simbol huruf besar dan kecil, dan angka.
5. Konfirmasi kata sandi, lalu tekan Enter.

Mengakses alat virtual melalui klien SSH

Prasyarat

- Klien SSH harus tersedia pada mesin jarak jauh. Prosedur di bawah ini menggunakan klien WinSCP sebagai contoh. Anda dapat menggunakan klien SSH apa pun, dengan menyesuaikan langkah-langkahnya sesuai kebutuhan.
- Secure Shell daemon (sshd) harus dijalankan pada alat virtual. Untuk informasi lebih lanjut, lihat "Memulai Secure Shell daemon" (hlm. 172).

Untuk mengakses alat virtual via WinSCP

1. Pada mesin jarak jauh, buka WinSCP.
2. Klik **Sesi** > **Sesi Baru**.
3. Pada **Protokol file**, pilih **SCP**.
4. Pada **Nama host**, tentukan alamat IP alat virtual Anda.
5. Dalam **Nama pengguna** dan **Kata sandi**, tentukan `root` dan kata sandi untuk pengguna `root`.
6. Klik **Masuk**.

Daftar semua direktori pada alat virtual ditampilkan.

Memperbarui agen

Anda dapat memperbarui semua agen secara manual dengan menggunakan konsol Cyber Protect atau dengan mengunduh dan menjalankan file instalasi.

Anda dapat mengonfigurasi pembaruan otomatis untuk beberap agen berikut:

- Agen untuk Windows
- Agen untuk Linux
- Agen untuk Mac
- Cyber Files Cloud Agen untuk File Sync & Share

© Acronis International GmbH, 2003-2024

Ruang kosong 4,2 GB di lokasi berikut diperlukan untuk memperbarui agen secara otomatis, atau secara manual menggunakan konsol Cyber Protect:

- Untuk Linux – direktori root
- Untuk Windows – volume tempat agen diinstal

Diperlukan ruang bebas 5 GB untuk memperbarui agen di macOS – di direktori root.

Catatan
[Untuk semua agen yang disediakan dalam bentuk alat virtual, termasuk Agen untuk VMware, Agen untuk Scale Computing, Agen untuk Virtuozzo Hybrid Infrastructure, Agen untuk RHV (oVirt)]

Untuk melakukan pembaruan alat virtual secara otomatis atau manual yang terletak di belakang proxy, server proxy harus dikonfigurasi pada setiap alat seperti berikut.

Dalam file `/opt/acronis/etc/va-updater/config.yaml`, tambahkan baris berikut di bagian bawah file dan masukkan nilai khusus untuk lingkungan Anda:

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

Memperbarui agen secara manual

Anda dapat memperbarui agen dengan menggunakan konsol Cyber Protect atau dengan mengunduh dan menjalankan file instalasi.

Peralatan virtual dengan versi berikut harus diperbarui hanya dengan menggunakan konsol Cyber Protect:

- Agen untuk VMware (Alat Virtual): versi 12.5.23094 dan yang lebih baru.
- Agen untuk Virtuozzo Hybrid Infrastructure (Alat Virtual): versi 12.5.23094 dan yang lebih baru.

Agen dengan versi berikut juga dapat diperbarui dengan menggunakan konsol Cyber Protect:

- Agen untuk Windows, Agen untuk VMware (Windows), Agen untuk Hyper-V: versi 12.5.21670, dan yang lebih baru.
- Agen untuk Linux: versi 12.5.23094 dan yang lebih baru.
- Agen lainnya: versi 12.5.23094 dan yang lebih baru.

Untuk menemukan versi agen, di konsol Cyber Protect, pilih mesin, lalu klik **Detail**.

Untuk memperbarui versi agen sebelumnya dari agen-agen tersebut, unduh dan instal versi terbaru secara manual. Untuk menemukan tautan unduhan, klik **Semua perangkat** > **Tambah**.

Prasyarat

Pada mesin Windows, fitur Cyber Protect memerlukan Microsoft Visual C++ 2017 Redistributable. Pastikan bahwa ini sudah diinstal di mesin Anda atau installah sebelum memperbarui agen. Setelah instalasi, mulai ulang mungkin perlu dilakukan. Anda dapat menemukan paket Microsoft Visual C++

© Acronis International GmbH, 2003-2024

Redistributable di situs web Microsoft https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Untuk memperbarui agen dengan menggunakan konsol Cyber Protect

1. Klik **Pengaturan** > **Agen-Agen**.
   Perangkat lunak menampilkan daftar mesin. Versi mesin agen yang kedaluwarsa ditandai dengan tanda seru berwarna oranye.
2. Pilih mesin yang ingin Anda perbarui agennya. Mesin harus online.
3. Klik **Perbarui agen**.

Catatan
Selama pembaruan, pencadangan apa pun yang sedang berjalan, akan gagal.

Untuk memperbarui Agen untuk VMware (Alat Virtual) yang versinya di bawah 12.5.23094

1. Klik **Pengaturan** > **Agen** > agen yang ingin Anda perbarui > **Detail**, lalu periksa bagian **Mesin virtual yang ditetapkan**. Anda harus memasukkan kembali pengaturan ini setelah pembaruan.
   a. Ingatlah posisi switch **Penetapan otomatis**.
   b. Untuk mengetahui mesin virtual apa yang ditetapkan secara manual pada agen, klik tautan **Ditetapkan:**. Perangkat lunak menampilkan daftar mesin virtual yang ditetapkan. Catat mesin yang memiliki `(M)` setelah nama agen di kolom **Agen**.
2. Hapus Agen untuk VMware (Alat Virtual), seperti yang dijelaskan pada "Menghapus instalasi agen". Pada langkah 5, hapus agen dari **Pengaturan** > **Agen-Agen**, meskipun Anda berencana menginstal agen kembali.
3. Menyebarkan Agen untuk VMware (Alat Virtual), seperti yang dijelaskan pada "Menyebarkan template OVF".
4. Mengonfigurasi Agen untuk VMware (Alat Virtual), seperti yang dijelaskan pada "Mengonfigurasi alat virtual".
   Jika Anda ingin memasang kembali penyimpanan yang terpasang secara lokal, pada langkah 7, lakukan hal berikut:
   a. Tambahkan disk yang berisi penyimpanan lokal ke alat virtual.
   b. Klik **Menyegarkan** > **Buat penyimpanan** > **Pasang**.
   c. Perangkat lunak menampilkan **Huruf** dan **Label** asli disk. Jangan mengubahnya.
   d. Klik **OK**.
5. Klik **Pengaturan** > **Agen** > agen yang ingin Anda perbarui > **Detail**, lalu rekonstruksikan pengaturan yang telah Anda catat di langkah 1. Jika beberapa mesin virtual ditetapkan secara manual pada agen, tetapkan lagi mesin virtual tersebut seperti dijelaskan dalam "Pengikatan mesin virtual".
   Saat konfigurasi agen selesai, rencana proteksi yang diterapkan pada agen lama akan diterapkan kembali secara otomatis pada agen baru.

© Acronis International GmbH, 2003-2024

6. Rencana pengaktifan pencadangan keberadaan aplikasi memerlukan kredensial OS tamu untuk dimasukkan kembali. Edit rencana ini dan masukkan kembali kredensial.
7. Rencana yang mencadangkan konfigurasi ESXi memerlukan kata sandi "root" untuk dimasukkan kembali. Edit rencana ini dan masukkan kembali kata sandi.

Untuk memperbarui definisi Perlindungan Cyber pada sebuah mesin

1. Klik **Pengaturan** > **Agen-Agen**.
2. Pilih mesin untuk Anda perbarui definisi Perlindungan Cyber-nya dan klik **Perbarui definisi**. Mesin harus online.

Untuk menetapkan peran Updater pada agen

1. Klik **Pengaturan** > **Agen-Agen**.
2. Pilih mesin yang ingin Anda beri peran Updater, klik **Detail**, lalu dalam bagian **definisi Perlindungan Cyber**, aktifkan **Gunakan agen ini untuk mengunduh dan mendistribusikan patch dan pembaruan**.

   Catatan
   Agen dengan peran Updater dapat mengunduh dan mendistribusikan patch hanya untuk produk pihak ketiga Windows. Untuk produk Microsoft, distribusi patch tidak didukung oleh agen Updater.

Untuk menghapus data yang di-cache pada agen

1. Klik **Pengaturan** > **Agen-Agen**.
2. Pilih mesin untuk Anda hapus data yang di-cache-nya (file pembaruan yang kedaluwarsa dan data manajemen patch) dan klik **Hapus cache**.

Memperbarui agen secara otomatis

Untuk memfasilitasi manajemen beberapa beban kerja, Anda dapat mengonfigurasi pembaruan otomatis untuk Agen untuk Windows, Agen untuk Linux, dan Agen untuk Mac. Pembaruan otomatis tersedia untuk agen versi 15.0.26986 (dirilis pada Maret 2021) atau yang lebih baru. Agen yang lebih lama harus diperbarui secara manual ke versi terbaru, terlebih dahulu.

Pembaruan otomatis didukung pada mesin yang menjalankan salah satu dari sistem operasi berikut:

- Windows XP SP 3 dan versi lebih baru
- Red Hat Enterprise Linux 6 dan yang lebih baru, CentOS 6, dan yang lebih baru
- OS X 10.9 Mavericks dan yang lebih baru

Pengaturan untuk pembaruan otomatis telah dikonfigurasikan sebelumnya di tingkat pusat data. Administrator perusahaan dapat menyesuaikan pengaturan ini - untuk semua mesin di perusahaan atau unit, atau untuk mesin individual. Jika tidak ada pengaturan khusus yang diterapkan, maka pengaturan dari tingkat atas digunakan, dalam urutan ini:

© Acronis International GmbH, 2003-2024

1. pusat data Cyber Protection
2. Perusahaan (penyewa pelanggan)
3. Unit
4. Mesin

Misalnya, administrator unit dapat mengonfigurasi pengaturan pembaruan otomatis khusus untuk semua mesin di unit, yang mungkin berbeda dari pengaturan yang diterapkan ke mesin di tingkat perusahaan. Administrator juga dapat mengonfigurasi pengaturan yang berbeda untuk satu atau lebih mesin individual di unit, yang tidak akan diterapkan pengaturan unit maupun pengaturan perusahaan.

Setelah mengaktifkan pembaruan otomatis, Anda dapat mengonfigurasi opsi berikut:

- **Perbarui saluran**
  Saluran pembaruan menentukan versi agen mana yang akan digunakan - yang paling mutakhir atau versi terbaru dari rilis sebelumnya.
- **Periode pemeliharaan**
  Periode pemeliharaan menentukan kapan pembaruan dapat diinstal. Jika periode pemeliharaan dinonaktifkan, pembaruan dapat dijalankan kapan saja.
  Bahkan dalam jendela pemeliharaan yang diaktifkan, pembaruan tidak akan diinstal saat agen menjalankan salah satu operasi berikut:
  - Cadangan
  - Pemulihan
  - Replikasi cadangan
  - Replikasi mesin virtual
  - Menguji replika
  - Menjalankan mesin virtual dari cadangan (termasuk finalisasi)
  - Failover pemulihan bencana
  - Failback pemulihan bencana
  - Menjalankan skrip (untuk fungsionalitas Pembuatan Skrip Cyber)
  - Instalasi patch
  - Pencadangan konfigurasi ESXi

Untuk menyesuaikan pengaturan pembaruan otomatis

1. Di konsol Cyber Protect, buka **Pengaturan** > **Agen**.
2. Pilih cakupan pengaturan:
   - Untuk mengubah pengaturan semua mesin, klik **Edit pengaturan pembaruan agen default**.
   - Untuk mengubah pengaturan untuk mesin tertentu, pilih mesin yang diinginkan, dan kemudian klik **Pengaturan pembaruan agen**.
3. Konfigurasikan pengaturan menurut kebutuhan Anda, lalu klik **Terapkan**.

© Acronis International GmbH, 2003-2024

Untuk menghapus pengaturan kustom pembaruan otomatis

1. Di konsol Cyber Protect, buka **Pengaturan** > **Agen**.
2. Pilih cakupan pengaturan:
   - Untuk menghapus pengaturan kustom semua mesin, klik **Edit pengaturan pembaruan agen default**.
   - Untuk menghapus pengaturan kustom untuk mesin tertentu, pilih mesin yang diinginkan, kemudian klik **Pengaturan pembaruan agen**.
3. Klik **Atur ulang ke pengaturan bawaan**, lalu klik **Terapkan**.

Untuk memeriksa status pembaruan otomatis

1. Di konsol Cyber Protect, buka **Pengaturan** > **Agen**.
2. Klik ikon roda gigi di sudut kanan atas tabel, lalu pastikan kotak centang **Pembaruan otomatis** dipilih.
3. Periksa status yang ditampilkan di kolom **Pembaruan otomatis**.

Memperbarui agen di beban kerja yang dilindungi BitLocker

Pembaruan agen yang mengenalkan perubahan pada Startup Recovery Manager mengintervensi BitLoker pada beban kerja tempat BitLocker dan Startup Recovery Manager diaktifkan. Jika terjadi hal demikian, setelah melakukan restart, kunci pemulihan BitLocker diperlukan. Untuk memitigasi masalah ini, tangguhkan atau matikan BitLocker sebelum Anda memperbarui agen.

Versi agen yang terpengaruh:

- 23.12.36943, dirilis pada Desember 2023

Anda juga dapat memeriksa apakah sebuah pembaruan memperkenalkan perubahan ke Startup Recovery Manager dalam catatan rilis dari agen proteksi.

Untuk memperbarui agen pada beban kerja dengan BitLocker dan Startup Recovery Manager diaktifkan

1. Pada beban kerja yang ingin Anda perbarui agennya, tangguhkan atau matikan BitLocker.
2. Perbarui agen.
3. Mulai ulang beban kerja.
4. Aktifkan BitLocker.

Mencegah penghapusan instalasi atau modifikasi agen yang tidak sah

Anda dapat melindungi Agen untuk Windows terhadap penghapusan instalasi atau modifikasi yang tidak sah, dengan mengaktifkan pengaturan **Proteksi kata sandi** pada rencana proteksi.

© Acronis International GmbH, 2003-2024

Pengaturan ini hanya tersedia saat **Perlindungan diri** diaktifkan.

Untuk mengaktifkan Proteksi kata sandi

1. Dalam rencana proteksi, perluas modul **Proteksi Antivirus & Antimalware** (modul **Active Protection** untuk edisi Pencadangan Cyber).
2. Klik **Perlindungan diri** dan pastikan bahwa switch **Perlindungan diri** diaktifkan.
3. Aktifkan switch **Proteksi kata sandi**.
4. Di jendela yang terbuka, salin kata sandi yang Anda perlukan untuk membatalkan instalasi atau memodifikasi komponen Agen untuk Windows.

   Kata sandi ini unik dan Anda tidak akan bisa memulihkannya setelah Anda menutup jendela ini. Jika Anda kehilangan atau lupa kata sandi, Anda dapat mengedit rencana proteksi dan membuat kata sandi yang baru.
5. Klik **Tutup**.
6. Dalam panel **Perlindungan diri**, klik **Selesai**.
7. Simpan rencana proteksi.

Proteksi kata sandi akan diaktifkan untuk mesin yang menjadi tujuan penerapan rencana proteksi. Proteksi kata sandi hanya tersedia untuk Agen untuk Windows versi *15.0.25851* atau lebih baru. Mesin harus online.

Anda dapat menerapkan rencana proteksi dengan Proteksi kata sandi yang diaktifkan ke mesin yang menjalankan macOS, namun tidak akan ada perlindungan yang diberikan. Anda tidak dapat menerapkan rencana ke mesin yang menjalankan Linux.

Anda juga tidak dapat menerapkan lebih dari satu rencana proteksi dengan proteksi kata sandi yang diaktifkan ke mesin Windows yang sama. Untuk mempelajari cara menyelesaikan pertentangan yang mungkin terjadi, lihat Menyelesaikan pertentangan rencana.

Untuk mengubah kata sandi dalam rencana proteksi yang sudah ada

1. Dalam rencana proteksi ini, perluas modul **Proteksi Antivirus & Antimalware** (modul **Active Protection** untuk edisi Pencadangan Cyber).
2. Klik **Perlindungan diri**.
3. Klik **Buat Kata sandi baru**.
4. Di jendela yang terbuka, salin kata sandi yang Anda perlukan untuk membatalkan instalasi atau memodifikasi komponen Agen untuk Windows.

   Kata sandi ini unik dan Anda tidak akan bisa memulihkannya setelah Anda menutup jendela ini. Jika Anda kehilangan atau lupa kata sandi, Anda dapat mengedit rencana proteksi dan membuat kata sandi yang baru.
5. Klik **Tutup**.
6. Dalam panel **Perlindungan diri**, klik **Selesai**.
7. Simpan rencana proteksi.

© Acronis International GmbH, 2003-2024

Menghapus instalasi agen

Saat Anda menghapus instalasi agen dari beban kerja, beban kerja secara otomatis dihapus dari konsol Cyber Protect. Jika beban kerja masih ditampilkan setelah Anda membongkar agen, misalnya, karena masalah jaringan, hapus beban kerja ini dari konsol secara manual. Untuk informasi lebih lanjut tentang cara melakukannya, lihat "Menghapus beban kerja dari konsol Cyber Protect" (hlm. 334).

Catatan
Menghapus agen tidak akan menghapus rencana atau cadangan apa pun.

Untuk menghapus instalasi agen

Windows

1. Masuk sebagai administrator ke mesin dengan agen.
2. Di **Panel kontrol**, buka **Program dan Fitur** (**Tambah atau Hapus Program** di Windows XP).
3. Klik kanan **Acronis Cyber Protect**, lalu pilih **Hapus instalasi**.
4. [Untuk agen yang dilindungi kata sandi] Tentukan kata sandi yang diperlukan untuk menghapus instalasi agen, lalu klik **Lanjut**.
5. [Opsional] Pilih kotak centang **Hapus log dan pengaturan konfigurasi**.
   Jika Anda berencana menginstal agen lagi, biarkan kotak centang ini kosong. Jika Anda mencentang kotak lalu menginstal agen lagi, beban kerja ini mungkin digandakan di konsol Cyber Protect dan cadangan lamanya mungkin tidak terkait dengannya.
6. Klik **Hapus instalasi**.

Linux

1. Di mesin dengan agen, jalankan `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` sebagai pengguna root.
2. [Opsional] Pilih kotak centang **Bersihkan semua jejak produk (Hapus log, tugas, kubah, dan pengaturan konfigurasi produk)**.
   Jika Anda berencana menginstal agen lagi, biarkan kotak centang ini kosong. Jika Anda mencentang kotak lalu menginstal agen lagi, beban kerja ini mungkin digandakan di konsol Cyber Protect dan cadangan lamanya mungkin tidak terkait dengannya.
3. Konfirmasi keputusan Anda.

macOS

1. Di mesin dengan agen, klik dua kali file .dmg instalasi.
2. Tunggu hingga sistem operasi memasang image disk instalasi.
3. Di dalam gambar, klik dua kali pada **Hapus instalasi**.

© Acronis International GmbH, 2003-2024

4. Jika diminta, berikan kredensial administrator.
5. Konfirmasi keputusan Anda.

Untuk menghapus instalasi komponen yang dibundel dengan Agen untuk Windows

Anda dapat menghapus instalasi komponen individual yang dibundel dengan Agen untuk Windows, seperti Cyber Protect Monitor, Agen untuk Pencegahan Kehilangan Data, atau Pembuat Media yang Dapat di-boot, tanpa menghapus instalasi Agen untuk Windows.

1. Masuk sebagai administrator ke mesin dengan agen.
2. Jalankan program penyiapan, lalu klik **Modifikasi komponen yang diinstal**.
3. Kosongkan kotak centang di sebelah komponen yang ingin Anda hapus instalasinya, lalu klik **Selesai**.

Untuk menghapus Agen untuk VMware (alat Virtual)

1. Dengan menggunakan vSphere Client, masuk ke vCenter Server.
2. [Jika alat virtual dinyalakan] Klik kanan alat virtual, lalu klik **Daya** > **Matikan**. Konfirmasi keputusan Anda.
3. [Jika alat virtual menggunakan penyimpanan terpasang secara lokal pada disk virtual dan Anda ingin menyimpan data pada disk tersebut] Hapus penyimpanan virtual dari alat virtual.
   a. Klik kanan VA, lalu klik **Edit Pengaturan**.
   b. Pilih disk dengan penyimpanan, lalu klik **Hapus**.
   c. Di **Opsi Penghapusan**, klik **Hapus dari mesin virtual**.
   d. Klik **OK**.

   Hasilnya, disk tetap di penyimpanan data. Anda dapat memasang disk ke VA lain.
4. Klik kanan VA, lalu klik **Hapus dari Disk**. Konfirmasi keputusan Anda.
5. [Opsional] [Jika Anda tidak berencana menggunakan alat ini lagi] Di konsol Cyber Protect, buka **Penyimpanan cadangan** > **Lokasi**, lalu hapus lokasi yang sesuai dengan penyimpanan yang terpasang secara lokal.

Pengaturan perlindungan

Untuk mengonfigurasi pengaturan perlindungan umum untuk Cyber Protection, di konsol Cyber Protect, buka **Pengaturan** > **Perlindungan**.

Pembaruan otomatis komponen

Secara default, semua agen dapat terhubung ke Internet dan mengunduh pembaruan.

Administrator dapat meminimalisasi lalu lintas bandwidth jaringan dengan memilih satu atau beberapa agen di lingkungan dan menetapkan peran Pembuat Pembaruan ke mereka. Maka, para agen khusus akan terhubung ke Internet dan mengunduh pembaruan. Agen lainnya akan

© Acronis International GmbH, 2003-2024

terhubung ke agen pembuat pembaruan khusus menggunakan teknologi rekan-ke-rekan, lalu mengunduh pembaruan dari mereka.

Agen tanpa peran Pembuat Pembaruan akan terhubung ke Internet jika tidak ada agen pembuat pembaruan khusus di lingkungan, atau jika koneksi ke agen pembuat pembaruan khusus tidak dapat dibust selama sekitar lima menit.

Agen pembaru mendistribusikan pembaruan dan patch untuk perlindungan Antivirus dan Antimalware, penilaian Kerentanan, dan manajemen Patch, tetapi tidak mencakup pembaruan versi agen.

Catatan
Agen dengan peran Updater dapat mengunduh dan mendistribusikan patch hanya untuk produk pihak ketiga Windows. Untuk produk Microsoft, distribusi patch tidak didukung oleh agen Updater.

Sebelum memberikan peran Pembuat Pembaruan ke agen, pastikan mesinnya cukup kuat dan memiliki koneksi Internet kecepat tinggi yang stabil, serta ada ruang disk yang cukup.

Untuk mempersiapkan mesin demi peran Pembuat Pembaruan

1. Di mesin agen tempat Anda berencana mengaktifkan peran Pembuat Pembaruan, terapkan aturan firewall berikut:
   - Masuk (masuk) "updater_incoming_tcp_ports": mengizinkan koneksi ke port TCP 18018 dan 6888 untuk semua profil firewall (publik, pribadi, dan domain).
   - Masuk (masuk) "updater_incoming_udp_ports": mengizinkan koneksi ke port UDP 6888 untuk semua profil firewall (publik, pribadi, dan domain).
2. Mulai ulang Acronis Agent Core Service.
3. Mulai ulang Layanan Firewall

Jika Anda tidak menerapkan aturan ini dan firewall diaktifkan, agen rekan akan mengunduh pembaruan dari Awan.

Untuk memberikan peran Updater pada agen perlindungan

1. Di konsol Cyber Protect, buka **Pengaturan** > **Agen**.
2. Pilih mesin dengan agen yang ingin Anda beri peran Updater.
3. Klik **Detail**, lalu aktifkan switch **Gunakan agen ini untuk mengunduh dan mendistribusikan patch dan pembaruan**.

Pembaruan rekan-ke-rekan bekerja sebagai berikut:

1. Sesuai jadwal, agen dengan peran Updater memeriksa file indeks yang diberikan oleh penyedia layanan untuk memperbarui komponen inti.
2. Agen dengan peran Updater mulai mengunduh dan mendistribusikan pembaruan ke semua agen.

© Acronis International GmbH, 2003-2024

Anda dapat menetapkan peran Pembuat Pembaruan ke banyak agen di lingkungan. Maka, jika satu agen dengan peran Pembuat Pembaruan sedang offline, agen lain dengan peran ini dapat menjadi sumber pembaruan definisi.

Memperbarui definisi Cyber Protection sesuai jadwal

Pada tab **Jadwal**, Anda dapat mengatur jadwal untuk pembaruan otomatis definisi Cyber Protection untuk setiap komponen berikut:

- Antimalware
- Penilaian kerentanan
- Manajemen patch

Untuk mengubah pengaturan pembaruan, navigasikan ke **Pengaturan** > **Perlindungan** > **Pembaruan definisi perlindungan** > **Jadwal**.

Jenis jadwal:

- **Harian** – tentukan pada hari apa pembaruan definisi dilakukan.
  Mulai pada – pilih jam berapa pembaruan definisi dilakukan.
- **Setiap jam** – tentukan jadwal jam spesifik untuk pembaruan.
  Jalankan setiap – tentukan pembaruan periodik.
  Dari ... **Hingga** – tentukan rentang waktu spesifik untuk pembaruan.

Memperbarui definisi Cyber Protection sesuai permintaan

Untuk memperbarui definisi Cyber Protection untuk mesin khusus sesuai permintaan

1. Di konsol Cyber Protect, buka **Pengaturan** > **Agen**.
2. Pilih mesin yang ingin Anda perbarui definisi perlindungannya, lalu klik **Perbarui definisi**.

Penyimpanan cache

Lokasi data cache adalah seperti berikut:

- Pada mesin Windows: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Pada mesin Linux: `/opt/acronis/var/atp-downloader/Cache`
- Pada mesin macOS: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Untuk mengubah pengaturan penyimpanan cache, navigasi ke **Pengaturan** > **Perlindungan** > **Pembaruan definisi perlindungan** > **Penyimpanan Cache**.

Dalam **File pembaruan dan data manajemen patch yang usang**, tentukan setelah berapa lama data cache akan dihapus.

Ukuran penyimpanan cache maksimum (GB) untuk agen:

© Acronis International GmbH, 2003-2024

- **Peran Updater** – tentukan ukuran penyimpanan untuk cache pada mesin dengan peran Updater.
- **Peran lain** – menetapkan ukuran penyimpanan untuk cache di mesin lainnya.

Catatan
Cyber Protection kumpulkan sampel malware yang terdeteksi untuk analisis tambahan agar kami dapat meningkatkan perangkat lunak kami. Anda dapat mengubah pengaturan ini kapan saja dalam tab **Proteksi**, dengan menonaktifkan pilihan **Kumpulkan dan unggah sampel malware ke CPOC**.

Mengubah kuota layanan mesin

Kuota layanan ditugaskan secara otomatis ketika rencana proteksi diterapkan ke mesin untuk pertama kalinya.

Kuota yang paling sesuai akan ditugaskan, bergantung kepada jenis mesin yang diproteksi, sistem operasinya, tingkat proteksi yang diperlukan, dan ketersedian kuota. Jika kuota yang paling sesuai tidak tersedia di organisasi Anda, kuota kedua terbaiklah yang akan ditugaskan. Misalnya, jika kuota yang paling sesuai adalah **Server Hosting Web** tapi kuota ini tidak tersedia, kuota **Server** yang akan ditugaskan.

Contoh penugasan kuota:

- Mesin fisik yang menjalankan Server Windows atau sistem operasi Linux (seperti Server Ubuntu) ditugasi kuota **Server**.
- Mesin fisik yang menjalankan Windows atau sistem operasi Linux (seperti Desktop Ubuntu) ditugasi kuota **Stasiun Kerja**.
- Mesin fisik yang menjalankan Windows 10 dengan mengaktifkan Hyper-V ditugaskan kuota **Stasiun Kerja**.
- Mesin desktop yang berjalan pada infrastruktur desktop virtual dan yang agen proteksinya diinstal di dalam sistem operasi tamu (misalnya, Agen untuk Windows), ditugaskan kuota **Mesin virtual**. Mesin jenis ini juga dapat menggunakan kuota **Stasiun Kerja** jika kuota **Mesin virtual** tidak tersedia.
- Mesin desktop yang berjalan pada infrastruktur desktop virtual dan yang agen proteksinya diinstal di dalam sistem operasi tamu (misalnya, Agen untuk VMware atau Agen untuk Hyper-V), ditugaskan kuota **Mesin virtual**.
- Server Hyper-V atau vSphere ditugaskan kuota **Server**.
- Server dengan cPanel atau Plesk ditugaskan kuota **Server Hosting Web**. Server jenis ini juga dapat menggunakan kuota **Mesin virtual** atau kuota **Server**, tergantung kepada jenis mesin lokasi server web berjalan, jika kuota **Server Hosting Web** tidak tersedia.
- Cadangan keberadaan aplikasi memerlukan kuota **Server**, bahkan untuk sebuah stasiun kerja.

Anda dapat secara manual mengubah tugas asli. Misalnya, untuk menerapkan rencana proteksi lanjutan ke mesin yang sama, Anda mungkin perlu meningkatkan kuota layanan mesin. Jika fitur

© Acronis International GmbH, 2003-2024

yang diperlukan oleh rencana proteksi ini tidak didukung dengan kuota layanan yang saat ini ditugaskan, rencana proteksi akan gagal.

Atau, Anda dapat mengubah kuota layanan jika Anda membeli kuota yang lebih sesuai setelah kuota asli ditetapkan. Misalnya, kuota **Stasiun Kerja** ditugaskan ke mesin virtual. Setelah membeli kuota **Mesin virtual**, Anda dapat menugaskan kuota ini secara manual ke mesin, daripada ke kuota **Stasiun Kerja** asli.

Anda juga dapat merilis kuota layanan yang saat ini ditetapkan, lalu menetapkannya ke mesin lain.

Anda dapat mengubah kuota layanan dari masing-masing mesin atau untuk sekelompok mesin.

Untuk mengubah kuota layanan dari masing-masing mesin

1. Di konsol Cyber Protect, buka **Perangkat**.
2. Pilih mesin yang diinginkan, lalu klik **Detail**.
3. Di bagian **Kuota layanan**, klik **Ubah**.
4. Di jendela **Ubah kuota**, pilih kuota layanan yang diinginkan atau **Tidak ada kuota**, lalu klik **Ubah**.

Untuk mengubah kuota layanan untuk sekelompok mesin

1. Di konsol Cyber Protect, buka **Perangkat**.
2. Pilih lebih dari satu mesin, lalu klik **Tetapkan kuota**.
3. Di jendela **Ubah kuota**, pilih kuota layanan yang diinginkan atau **Tidak ada kuota**, lalu klik **Ubah**.

Layanan Cyber Protection yang diinstal di lingkungan Anda

Cyber Protection menginstal beberapa atau semua layanan berikut, tergantung pada opsi Cyber Protection yang Anda gunakan.

Layanan yang diinstal di Windows

Nama layanan	Tujuan
Acronis Managed Machine Service	Menyediakan fungsi pencadangan, pemulihan, replikasi, retensi, validasi
Acronis Scheduler2 Service	Mengeksekusi tugas yang dijadwalkan pada kejadian tertentu
Acronis Active Protection Service	Menyediakan perlindungan terhadap ransomware
Acronis Cyber Protection Service	Menyediakan perlindungan antimalware

© Acronis International GmbH, 2003-2024

Layanan yang diinstal di macOS

Nama dan lokasi layanan	Tujuan
`/Library/LaunchDaemons/com.acronis.aakore.plist`	Membantu komunikasi antara Agen dan komponen manajemen
`/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist`	Menyediakan deteksi malware
`/Library/LaunchDaemons/com.acronis.mms.plist`	Menyediakan fungsi pencadangan dan pemulihan
`/Library/LaunchDaemons/com.acronis.schedule.plist`	Mengeksekusi tugas yang dijadwalkan

Menyimpan file log agen

Anda dapat menyimpan log agen ke file .zip. Jika pencadangan gagal karena alasan yang tidak diketahui, file ini akan membantu personel dukungan teknis untuk mengidentifikasi masalahnya.

Secara default, informasi dalam Log dioptimalkan untuk tiga hari terakhir, tetapi Anda dapat mengubah periode ini.

Untuk mengumpulkan log agen

1. Lakukan salah satu langkah berikut:
   - Di bawah **Perangkat**, pilih mesin yang Anda ingin kumpulkan log-nya, dan kemudian klik **Aktivitas**.
   - Di bawah **Pengaturan** > **Agen**, pilih mesin yang Anda ingin kumpulkan log-nya, dan kemudian klik **Detail**.
2. [Opsional] Untuk mengubah periode default di mana informasi sistem disertakan, klik panah di sebelah tombol **Kumpulkan informasi sistem**, dan kemudian pilih periode tersebut.
3. Klik **Kumpulkan informasi sistem**.
4. Jika diminta oleh browser web Anda, tentukan di mana file tersebut tersimpan.

VPN Terbuka Situs-ke-situs - Informasi tambahan

Saat membuat server pemulihan, Anda mengonfigurasi **Alamat IP di jaringan produksi**, dan **Alamat IP uji** server tersebut.

Setelah Anda melakukan failover (menjalankan mesin virtual di awan), dan masuk ke mesin virtual untuk memeriksa alamat IP server, Anda akan melihat **Alamat IP di jaringan produksi**.

Saat melakukan failover uji, Anda dapat menjangkau server uji hanya dengan menggunakan **Alamat IP uji**, yang hanya dapat dilihat di konfigurasi server pemulihan.

Untuk menjangkau server uji dari situs lokal Anda, Anda harus menggunakan **Alamat IP uji**.

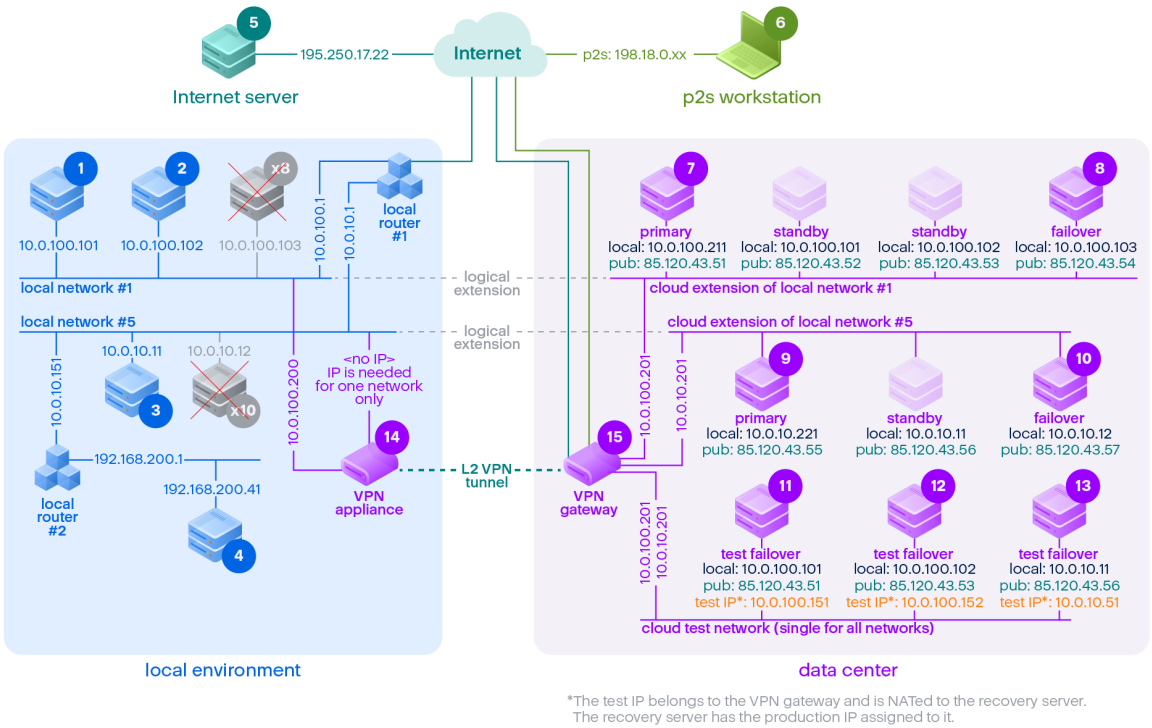
© Acronis International GmbH, 2003-2024

Catatan

Konfigurasi jaringan server selalu menunjukkan **Alamat IP di jaringan produksi** (karena server uji akan merefleksikan penampilan server produksi). Ini terjadi karena alamat IP uji tersebut tidak dimiliki oleh server uji, tetapi oleh gateway VPN, dan diterjemahkan ke alamat IP produksi menggunakan NAT.

Diagram di bawah ini menunjukkan contoh konfigurasi VPN Terbuka Situs-ke-situs. Beberapa server di lingkungan lokal dipulihkan ke awan menggunakan failover (sedangkan infrastruktur jaringannya tidak bermasalah).

1. Pelanggan mengaktifkan Pemulihan Bencana dengan:
   a. mengonfigurasi alat VPN (14), dan menyambungkannya ke server VPN awan khusus (15)
   b. melindungi beberapa server lokal dengan Pemulihan Bencana (1, 2, 3, x8, dan x10)
      Beberapa server di situs lokal (seperti 4) tersambung ke jaringan yang tidak tersambung ke alat VPN. Server tersebut tidak dilindungi dengan Pemulihan Bencana.
2. Bagian dari server (tersambung ke jaringan berbeda) yang berfungsi di situs lokal: (1, 2, 3, dan 4)
3. Server yang dilindungi (1, 2, dan 3) sedang diuji dengan failover uji (11, 12, dan 13)
4. Beberapa server di situs lokal tidak tersedia (x8, x10). Setelah melakukan failover, server menjadi tersedia di awan (8 dan 10)
5. Beberapa server utama (7 dan 9), yang tersambung ke jaringan berbeda, tersedia di lingkungan awan
6. (5) adalah server di Internet dengan alamat IP publik
7. (6) adalah stasiun kerja yang terkoneksi ke awan menggunakan koneksi VPN Titik-ke-situs (p2s)



© Acronis International GmbH, 2003-2024

Dalam contoh ini, pengaturan koneksi berikut tersedia (contohnya, "ping") dari server dalam baris **Dari:** ke server dalam kolom **Untuk:**.

	Hingga:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Dari:		lokal	lokal	lokal	lokal	internet	p2s	utama	failover	utama	failover	failover uji	failover uji	failover uji	alat VPN	server VPN
1	lokal		langsung	melalui router lokal 1	melalui router lokal 2	melalui router lokal 1 dan internet	tidak	melalui terowongan: lokal melalui router lokal 1 dan internet: pub	melalui terowongan: lokal melalui router lokal 1 dan internet: pub	melalui terowongan: lokal melalui router lokal 1 dan internet: pub	melalui terowongan: lokal melalui router lokal 1 dan internet: pub	melalui terowongan: NAT (server VPN) melalui router lokal 1 dan internet: pub	melalui terowongan: NAT (server VPN) melalui router lokal 1 dan internet: pub	melalui router lokal 1 dan terowongan: NAT (server VPN) melalui router lokal 1 dan internet: pub	langsung	tidak
2	lokal	langsung		melalui router lokal 1	melalui router lokal 2	melalui router lokal	tidak	melalui terowongan: lokal melalui rout	melalui terowongan: lokal melalui rout	melalui terowongan: lokal melalui rout	melalui terowongan: lokal melalui rout	melalui terowongan: NAT (server VPN)	melalui terowongan: NAT (server VPN)	melalui router lokal 1 dan terowongan:	langsung	tidak

© Acronis International GmbH, 2003-2024

	Hingga:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						1 dan internet		er lokal 1 dan internet: pub	er lokal 1 dan internet: pub	er lokal 1 dan internet: pub	er lokal 1 dan internet: pub	mel alui router lokal 1 dan internet: pub	mel alui router lokal 1 dan internet: pub	NAT (server VPN) mel alui router lokal 1 dan internet: pub		
3	lokal	mel alui router lokal 1	mel alui router lokal 1		mel alui router lokal 2	mel alui router lokal 1 dan internet	tidak	mel alui tero wongan: lokal mel alui router lokal 1 dan internet: pub	mel alui tero wongan: lokal mel alui router lokal 1 dan internet: pub	mel alui tero wongan: lokal mel alui router lokal 1 dan internet: pub	mel alui tero wongan: lokal mel alui router lokal 1 dan internet: pub	mel alui tero wongan: NAT (server VPN) mel alui router lokal 1 dan internet: pub	mel alui tero wongan: NAT (server VPN) mel alui router lokal 1 dan internet: pub	mel alui router lokal 1 dan tero wongan: NAT (server VPN) mel alui router lokal 1 dan internet: pub	mel alui router lokal	tidak
4	lokal	mel alui	mel alui	mel alui		m	tid	mel alui	mel alui	mel alui	mel alui	mel alui	mel alui	mel alui	mel al	tidak

© Acronis International GmbH, 2003-2024

	Hingga:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		router lokal 2 dan router 1	router lokal 2 dan router 1	router lokal 2		el alui router lokal 2, router 1, dan internet	ak	router lokal 2 dan tero wongan: lokal mel alui router lokal 2, router lokal 1, dan internet: pub	router lokal 2 dan tero wongan: lokal mel alui router lokal 2, router lokal 1, dan internet: pub	router lokal 2 dan tero wongan: lokal mel alui router lokal 2, router lokal 1, dan internet: pub	router lokal 2 dan tero wongan: lokal mel alui router lokal 2, router lokal 1, dan internet: pub	tero wongan: NAT (server VPN) mel alui router lokal 2, router 1, dan internet: pub	tero wongan: NAT (server VPN) mel alui router lokal 2, router 1, dan internet: pub	tero wongan: NAT (server VPN) mel alui router lokal 2, router 1, dan internet: pub	ui router lokal 2	
5	internet	tidak	tidak	tidak	tidak		n/a	mel alui Internet: pub	mel alui Internet: pub	mel alui Internet: pub	mel alui Internet: pub	mel alui Internet: pub	mel alui Internet: pub	mel alui Internet: pub	tidak	tidak
6	p2s	tidak	tidak	tidak	tidak	mel alui Internet		mel alui VPN p2s (server VPN): lokal mel alui Inter	mel alui VPN p2s (server VPN): lokal mel alui Inter	mel alui VPN p2s (server VPN): lokal mel alui Inter	mel alui VPN p2s (server VPN): lokal mel alui Inter	mel alui VPN p2s - NAT (server VPN) mel alui Internet:	mel alui VPN p2s - NAT (server VPN) mel alui Internet:	mel alui VPN p2s - NAT (server VPN) mel alui Internet:	tidak	tidak

© Acronis International GmbH, 2003-2024

	Hingga:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								net: pub	net: pub	net: pub	net: pub	pub	pub	pub		
7	utama	melalui terowongan	melalui terowongan	melalui terowongan dan router lokal 1	melalui terowongan dan router lokal 1 dan 2	melalui internet (melalui server VPN)	tidak		langsung di awan: lokal	melalui terowongan dan router lokal 1: lokal	melalui terowongan dan router lokal 1: lokal	melalui server VPN: NAT	melalui server VPN: NAT	melalui terowongan dan router lokal 1: NAT	tidak	Hanya protokol DHCP dan DNS
8	failover	melalui terowongan	melalui terowongan	melalui terowongan dan router lokal 1	melalui terowongan dan router lokal 1 dan 2	melalui internet (melalui server VPN)	tidak	langsung di awan: lokal		melalui terowongan dan router lokal 1: lokal	melalui terowongan dan router lokal 1: lokal	melalui server VPN: NAT	melalui server VPN: NAT	melalui terowongan dan router lokal 1: NAT	tidak	Hanya protokol DHCP dan DNS
9	utama	melalui terowon	melalui terowon	melalui terowon	melalui terowon	melalui	tidak	melalui terowon	melalui terowon		langsung di awa	melalui terowon	melalui terowon	melalui server	tidak	Hanya pr

© Acronis International GmbH, 2003-2024

	Hingga:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		gan dan router lokal 1	gan dan router lokal 1	gan	gan	internet (melalui server VPN)		gan dan router lokal 1: lokal	gan dan router lokal 1: lokal		n: lokal	gan dan router lokal 1: NAT	gan dan router lokal 1: NAT	VPN: NAT		otokol DHCP dan DNS
10	failover	melalui tero wongan dan router lokal 1	melalui tero wongan dan router lokal 1	melalui tero wongan	melalui tero wongan	melalui internet (melalui server VPN)	tidak	melalui tero wongan dan router lokal 1: lokal	melalui tero wongan dan router lokal 1: lokal	langsung di awan: lokal		melalui tero wongan dan router lokal 1: NAT	melalui tero wongan dan router lokal 1: NAT	melalui server VPN: NAT	tidak	Hanya protokol DHCP dan DNS
11	failover uji	tidak	tidak	tidak	tidak	melalui internet (melal	tidak	tidak	tidak	tidak	tidak		langsung di awan: lokal	melalui server VPN: lokal (per utean)	tidak	Hanya protokol DHCP dan

© Acronis International GmbH, 2003-2024

	Hingga:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						user server VPN)										DNS
12	failover uji	tidak	tidak	tidak	tidak	melalui internet (melalui user server VPN)	tidak	tidak	tidak	tidak	tidak	langsung di awan: lokal		melalui server VPN: lokal (per utean)	tidak	Hanya protokol DHCP dan DNS
13	failover uji	tidak	tidak	tidak	tidak	melalui internet (melalui user server VPN)	tidak	tidak	tidak	tidak	tidak	melalui server VPN: lokal (per utean)	melalui server VPN: lokal (per utean)		tidak	Hanya protokol DHCP dan DNS

© Acronis International GmbH, 2003-2024

	Hingga:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
14	alat VPN	langsung	langsung	melalui router lokal 1	melalui router lokal 2	melalui internet (router lokal 1)	tidak	tidak	tidak	tidak	tidak	tidak	tidak	tidak		tidak
15	server VPN	tidak	tidak	tidak	tidak	tidak	tidak	tidak	tidak	tidak	tidak	tidak	tidak	tidak	tidak	

Manajemen lisensi untuk server manajemen di lokasi

Untuk informasi terperinci tentang cara mengaktifkan server manajemen di lokasi atau mengalokasikan lisensi pada server tersebut, lihat Bagian pelisensian di Cyber Protect panduan pengguna.

© Acronis International GmbH, 2003-2024

Menentukan apa yang perlu dilindungi dan cara melindunginya

Tab manajemen

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Semua Rencana yang Anda buat tersedia di tab **Manajemen** dari konsol Cyber Protect .

Bagian berikut tersedia:

- **Rencana proteksi**
- **Rencana manajemen jarak jauh**
- **Rencana skrip**
- **Rencana pemantauan**
- **Repositori skrip**
- **Cadangan aplikasi awan**
- **Pemindaian cadangan**
- **Replikasi cadangan**
- **Validasi**
- **Pembersihan**
- **Konversi ke VM**
- **Replikasi VM**

Status rencana

Untuk rencana proteksi dan rencana replikasi VM, panel status menunjukkan status berkode warna berikut:

- OK (Hijau)
- Peringatan (Oranye)
- Kesalahan (Oranye gelap)
- Kritis (Merah)
- Rencana sedang berjalan (Biru)
- Rencana dinonaktifkan (Abu-abu)

Klik panel status untuk melihat detail tentang status rencana pada semua beban kerja tempat rencananya diterapkan.

© Acronis International GmbH, 2003-2024

Klik status tertentu untuk melihat daftar semua beban kerja dengan status ini.

Rencana proteksi

Pada tab **Manajemen** > **Rencana proteksi**, Anda dapat melihat informasi tentang rencana proteksi yang ada, melakukan tindakan dengan rencana proteksi tersebut, dan membuat rencana baru.

Untuk informasi lebih lanjut tentang rencana proteksi, lihat "Modul dan rencana proteksi" (hlm. 213).

Rencana pencadangan untuk aplikasi awan

Tab **Manajemen** > **Cadangan aplikasi awan** menampilkan rencana pencadangan awan-ke-awan. Rencana ini mencadangkan aplikasi yang berjalan di awan melalui agen yang berjalan di awan dan menggunakan penyimpanan awan sebagai lokasi pencadangan.

Di bagian ini, Anda dapat melakukan operasi berikut:

- Buat, lihat, jalankan, hentikan, edit, dan hapus rencana pencadangan
- Lihat aktivitas terkait setiap rencana pencadangan
- Lihat peringatan terkait setiap rencana pencadangan

Untuk informasi lebih lanjut tentang cadangan aplikasi awan, lihat:

- Melindungi data Microsoft 365
- Melindungi data Google Workspace

Menjalankan cadangan awan-ke-awan secara manual

Agar tidak mengganggu layanan Cyber Protection, jumlah operasi pencadangan awan-ke-awan manual dibatasi hingga 10 operasi per organisasi Microsoft 365 atau Google Workspace per jam. Setelah jumlah ini tercapai, jumlah operasi yang diperbolehkan diatur ulang menjadi satu per jam, lalu operasi tambahan akan tersedia setiap jam berikutnya (misalnya jam 1, 10 operasi; jam 2, 1 operasi; jam 3, 2 operasi) hingga total 10 operasi per jam tercapai.

Rencana pencadangan yang berlaku untuk grup perangkat (kotak surat, drive, situs) atau yang berisi lebih dari 10 perangkat tidak dapat dijalankan secara manual.

Rencana pemindaian cadangan

Untuk memindai cadangan dari malware (termasuk ransomware), buat rencana pemindaian cadangan.

Penting
Rencana pemindaian cadangan tidak didukung untuk semua beban kerja dan penyimpanan cadangan. Untuk perincian, lihat "Pembatasan" (hlm. 861).

Untuk membuat rencana pemindaian cadangan

 © Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Manajemen** > **Pemindaian cadangan**.
2. Klik **Buat rencana**.
3. Tentukan nama rencana dan parameter berikut:
   - **Jenis pemindaian**:
     - **Awan** – opsi ini tidak dapat diubah. Agen awan yang dipilih secara otomatis akan melakukan pemindaian cadangan.
   - **Cadangan yang akan dipindai**:
     - **Lokasi** – pilih lokasi dengan set cadangan yang ingin Anda pindai.
     - **Cadangan** – pilih set cadangan yang ingin Anda pindai.
   - **Pindai untuk**:
     - **Malware** – opsi ini tidak dapat diubah. Pemindaian memeriksa set cadangan terpilih dari malware (termasuk ransomware).
   - **Enkripsi** – untuk memindai set cadangan terenkripsi, menentukan kata sandi terenkripsi. Jika Anda memilih sebuah lokasi atau beberapa set cadangan dan kata sandi yang ditentukan tidak sesuai dengan set cadangan, sebuah peringatan akan muncul.
   - **Jadwal** – opsi ini tidak dapat diubah. Dalam penyimpanan awan, pemindaian dimulai secara otomatis.
4. Klik **Buat**.

Hasilnya, rencana pemindaian pencadangan dibuat dan agen awan akan memindai malware di lokasi atau set cadangan yang Anda tentukan.

Pemrosesan data off-host

Catatan
Fungsionalitas ini tersedia di penyewa pelanggan untuk yang **Cadangan Lanjutan - Server** atau **Cadangan Lanjutan - NAS** kuota diaktifkan sebagai bagian dari paket Cadangan Lanjutan.

Replikasi, validasi, dan pembersihan biasanya dilakukan oleh agen proteksi yang melakukan pencadangan. Ini memberikan beban tambahan pada mesin tempat agen berjalan, bahkan setelah proses pencadangan selesai. Untuk mengurangi beban mesin, Anda dapat membuat rencana perlindungan data off-host - yaitu, rencana terpisah untuk replikasi, validasi, pembersihan, dan konversi ke mesin virtual.

Dengan rencana proteksi Perlindungan Data di luar host, Anda dapat melakukan hal berikut:

- Pilih agen yang berbeda untuk operasi cadangan dan operasi perlindungan data di luar host
- Jadwalkan operasi pemrosesan data di luar host selama jam-jam di luar puncak untuk meminimalkan konsumsi bandwidth jaringan
- Jadwalkan operasi pemrosesan data di luar host selama jam non-bisnis, jika Anda tidak ingin memasang agen khusus untuk pemrosesan data di luar host

© Acronis International GmbH, 2003-2024

Catatan
Rencana pemrosesan data di luar host berjalan sesuai dengan pengaturan waktu (termasuk zona waktu) dari mesin tempat agen perlindungan diinstal. Untuk alat virtual (misalnya, Agen untuk VMware atau Agen untuk Scale Computing HC3), Anda dapat mengkonfigurasi zona waktu di antarmuka pengguna grafis dari agen tersebut.

Replikasi cadangan

Catatan
Fungsionalitas ini tersedia di penyewa pelanggan untuk yang **Cadangan Lanjutan - Server** atau **Cadangan Lanjutan - NAS** kuota diaktifkan sebagai bagian dari paket Cadangan Lanjutan.

Replikasi cadangan adalah menyalin cadangan ke lokasi lain. Sebagai operasi pemrosesan data di luar host, konfigurasi dilakukan di rencana replikasi cadangan.

Replikasi cadangan juga bisa menjadi bagian dari rencana proteksi. Untuk informasi lebih lanjut tentang opsi ini, lihat "Replikasi" (hlm. 439).

Membuat rencana replikasi cadangan

Untuk mereplikasi cadangan sebagai operasi pemrosesan data di luar host, Anda membuat rencana replikasi cadangan.

Untuk membuat rencana replikasi cadangan

1. Dalam konsol Cyber Protect, klik **Manajemen** > **Replikasi cadangan**.
2. Klik **Buat rencana**.
3. Dalam **Agen**, pilih agen yang akan melakukan replikasi.
   Anda dapat memilih agen apa pun yang memiliki akses baik menuju lokasi sumber dan lokasi replikasi.
4. Dalam **Item untuk direplikasi**, Pilih arsip atau lokasi cadangan yang akan dibersihkan.
   Untuk beralih antara arsip dan lokasi, gunakan fitur pengalih **Lokasi** / **Cadangan** di sudut kanan atas.
   Jika kamu memilih beberapa arsip terenkripsi, kata sandi enkripsinya harus sama. Untuk arsip yang menggunakan kata sandi enkripsi berbeda, buatlah rencana terpisah.
5. Dalam **Destinasi**, tentukan lokasi replikasi.
6. Dalam **Cara mereplikasi**, pilih cadangan (dikenal juga sebagai titik pemulihan) yang akan direplikasi.
   Opsi berikut tersedia:
   - **Semua cadangan**
   - **Hanya cadangan penuh**
   - **Hanya cadangan terakhir**

© Acronis International GmbH, 2003-2024

Untuk informasi lebih lanjut tentang opsi ini, lihat "Apa yang akan direplikasi" (hlm. 199).

7. Dalam **Jadwal**, konfigurasikan jadwal replikasi.

   Saat mengonfigurasi jadwal rencana replikasi cadangan, pastikan bahwa cadangan yang terakhir direplikasi akan tetap tersedia di lokasi aslinya saat replikasi cadangan dimulai. Jika cadangan ini tidak tersedia di lokasi asli, misalnya, karena dihapus oleh aturan retensi, seluruh arsip akan direplikasi sebagai cadangan penuh. Hal ini mungkin sangat memakan waktu dan akan menggunakan ruang penyimpanan tambahan.
8. Dalam **Aturan retensi**, tentukan aturan retensi untuk lokasi target.

   Opsi berikut tersedia:

   - **Berdasarkan jumlah cadangan**
   - **Berdasarkan usia pencadangan** (pengaturan terpisah untuk pencadangan bulanan, mingguan, harian, dan per jam)
   - **Berdasarkan ukuran total cadangan**
   - **Simpan cadangan tanpa batas**

     Catatan
     Memilih opsi ini akan membuat penggunaan penyimpanan meningkat. Anda harus menghapus cadangan yang tidak diperlukan secara manual.
9. [Jika kamu memilih arsip terenkripsi dalam **Item untuk direplikasi**] Aktifkan fitur pengalih **Kata sandi cadangan**, kemudian berikan kata sandi enkripsi.
10. [Opsional] Untuk mengubah opsi rencana, klik ikon roda gigi, kemudian konfigurasikan opsi sesuai kebutuhan.
11. Klik **Buat**.

Apa yang akan direplikasi

Catatan
Beberapa operasi replikasi, seperti replikasi seluruh lokasi atau replikasi semua cadangan di set cadangan, mungkin akan memakan banyak waktu.

Anda dapat mereplikasi set cadangan individu atau seluruh lokasi cadangan. Ketika mereplikasi lokasi cadangan, semua set cadangan di dalamnya akan direplikasi.

Set cadangan berisi cadangan (disebut juga sebagai titik pemulihan). Anda harus memilih cadangan yang akan direplikasi.

Opsi berikut tersedia:

- **Semua cadangan**
  Semua cadangan di set cadangan direplikasi setiap kali rencana replikasi berjalan.
- **Hanya cadangan penuh**
  Hanya cadangan penuh di set cadangan yang akan direplikasi.
- **Hanya cadangan terakhir**

© Acronis International GmbH, 2003-2024

Hanya cadangan terbaru di set cadangan yang akan direplikasi, terlepas dari jenisnya (penuh, diferensial, atau bertahap).

Pilih opsi sesuai kebutuhan Anda dan skema pencadangan yang Anda gunakan. Misalnya, jika Anda menggunakan skema pencadangan **Selalu inkremental (file tunggal)** dan hanya ingin mereplikasi cadangan bertahap terbaru, pilih **Hanya cadangan terakhir** di rencana replikasi cadangan.

Tabel berikut merangkum cadangan mana yang akan direplikasi dengan skema pencadangan yang berbeda.

	Selalu inkremental (file tunggal)	**Selalu penuh**	**Mingguan penuh, Kenaikan harian**	**Bulanan penuh, Mingguan diferensial, Harian inkremental (GFS)**
Semua cadangan	Semua cadangan di set cadangan	Semua cadangan di set cadangan	Semua cadangan di set cadangan	Semua cadangan di set cadangan
Hanya cadangan penuh	Hanya cadangan pertama, yaitu cadangan penuh	Semua cadangan	Satu cadangan setiap minggu*	Satu cadangan setiap bulan*
Hanya cadangan terakhir	Hanya cadangan terbaru di set cadangan*	Hanya cadangan terbaru di set cadangan*	Hanya cadangan terbaru di set cadangan, terlepas dari jenisnya*	Hanya cadangan terbaru di set cadangan, terlepas dari jenisnya*

*Saat mengonfigurasi jadwal rencana replikasi cadangan, pastikan bahwa cadangan yang terakhir direplikasi akan tetap tersedia di lokasi aslinya saat replikasi cadangan dimulai. Jika cadangan ini tidak tersedia di lokasi asli, misalnya, karena dihapus oleh aturan retensi, seluruh arsip akan direplikasi sebagai cadangan penuh. Hal ini mungkin sangat memakan waktu dan akan menggunakan ruang penyimpanan tambahan.

Lokasi yang didukung

Tabel berikut ini merangkum lokasi pencadangan yang didukung oleh rencana replikasi cadangan.

Lokasi cadangan	**Didukung sebagai sumber**	**Didukung sebagai target**
Penyimpanan awan	+	+
Folder lokal	+	+
Folder jaringan	+	+
Cloud publik	+	+
Folder NFS	–	–
Secure Zone	–	–

© Acronis International GmbH, 2003-2024

Validasi

Catatan
Fungsionalitas ini tersedia di penyewa pelanggan untuk yang **Cadangan Lanjutan - Server** atau **Cadangan Lanjutan - NAS** kuota diaktifkan sebagai bagian dari paket Cadangan Lanjutan.

Dengan memvalidasi cadangan, Anda memverifikasi bahwa Anda dapat memulihkan data darinya.

Untuk memvalidasi cadangan sebagai operasi pemrosesan data di luar host, Anda membuat rencana validasi. Untuk informasi lebih lanjut tentang cara membuatnya, lihat "Membuat rencana validasi" (hlm. 202).

Metode validasi berikut tersedia:

- Verifikasi checksum
- Jalankan sebagai mesin virtual
  - VM heartbeat
  - Validasi tangkapan layar

Anda dapat memilih satu atau lebih dari metode ini. Ketika lebih dari satu metode dipilih, operasi untuk setiap metode validasi dijalankan secara berurutan. Untuk informasi lebih lanjut tentang metode, lihat "VM heartbeat" (hlm. 205).

Anda dapat memvalidasi set cadangan atau lokasi cadangan. Validasi lokasi cadangan memvalidasi semua set cadangan di dalamnya.

Lokasi yang didukung

Tabel berikut menunjukkan lokasi cadangan yang didukung dan metode validasi.

Catatan
Opsi validasi tidak tersedia untuk pencadangan cloud publik karena mahalnya biaya membaca seluruh arsip dari cloud publik.

Lokasi cadangan	Verifikasi checksum	Jalankan sebagai mesin virtual	
		VM heartbeat	Validasi tangkapan layar
Penyimpanan awan	+	+	+
Folder lokal	+	+	+
Folder jaringan	+	+	+
Folder NFS	–	–	–
Secure Zone	–	–	–

© Acronis International GmbH, 2003-2024

Status validasi

Setelah validasi berhasil, cadangan ditandai dengan titik hijau dan label **Divalidasi**.

Jika validasi gagal, cadangan ditandai dengan titik merah. Validasi gagal meskipun hanya salah satu metode validasi yang digunakan yang gagal. Dalam beberapa kasus, ini mungkin akibat kesalahan konfigurasi rencana validasi – misalnya, menggunakan metode **VM heartbeat** untuk mesin virtual di host yang salah.

Status validasi cadangan diperbarui dengan setiap operasi validasi baru. Status untuk setiap metode validasi diperbarui secara terpisah. Itulah mengapa validasi cadangan yang mana satu metodenya gagal akan ditampilkan sebagai gagal hingga metode validasi yang sama berhasil, bahkan jika operasi validasi terbaru tidak menggunakan metode yang gagal dan berhasil diselesaikan.

Untuk informasi lebih lanjut tentang cara memeriksa status validasi, lihat "Memeriksa status validasi cadangan" (hlm. 207).

Membuat rencana validasi

Untuk memvalidasi set cadangan sebagai operasi pemrosesan data di luar host, Anda membuat rencana validasi.

Untuk membuat rencana validasi

1. Di konsol Cyber Protect, klik **Manajemen** > **Validasi**.
2. Klik **Buat rencana**.
   Templat untuk rencana validasi baru terbuka.
3. [Opsional] Untuk mengubah nama rencana, klik nama default.
4. Di **Agen**, pilih agen yang akan melakukan validasi, lalu klik **OK**.
   Jika Anda ingin melakukan validasi dengan menjalankan mesin virtual dari cadangan, pilih mesin dengan Agen untuk VMware atau Agen untuk Hyper-V. Jika tidak, pilih mesin yang memiliki akses ke lokasi pencadangan.
5. Di **Item untuk divalidasi**, pilih set cadangan yang ingin Anda validasi.
   a. Pilih cakupan untuk rencana – kumpulan cadangan individu atau seluruh lokasi, dengan mengeklik **Lokasi** atau **Cadangan** di sudut kanan atas.
      Jika cadangan yang dipilih dienkripsi, semuanya harus menggunakan kata sandi enkripsi yang sama. Untuk cadangan yang menggunakan kata sandi enkripsi yang berbeda, buat rencana terpisah.
   b. Klik **Tambah**.
   c. Bergantung pada cakupan rencana validasi, pilih lokasi atau set lokasi dan cadangan, lalu klik **Selesai**.
   d. Klik **Selesai**.

© Acronis International GmbH, 2003-2024

6. Di **Apa yang akan divalidasi**, pilih cadangan mana (juga dikenal sebagai titik pemulihan) dalam kumpulan cadangan yang dipilih untuk divalidasi. Opsi berikut tersedia:
   - **Semua cadangan**
   - **Hanya cadangan terakhir**
7. Di **Cara memvalidasi**, pilih metode validasi.

   Anda dapat memilih salah satu atau kedua opsi berikut:
   - **Verifikasi checksum**
   - **Jalankan sebagai mesin virtual**

   Untuk informasi lebih lanjut tentang metode, lihat "VM heartbeat" (hlm. 205).
8. [Jika Anda memilih **Verifikasi checksum**] Klik **Selesai**.
9. [Jika Anda memilih **Jalankan sebagai mesin virtual**]. Konfigurasikan pengaturan untuk metode ini.
   a. Di **Mesin target**, pilih jenis mesin virtual (ESXi atau Hyper-V), host, dan templat nama mesin, lalu klik **OK**.

      Nama default adalah **[Nama Mesin]_validate**.
   b. Di **Penyimpanan data** (untuk ESXi) atau **Path** (untuk Hyper-V), pilih penyimpanan data untuk mesin virtual.
   c. Pilih salah satu atau kedua metode validasi tersebut yang disediakan oleh **Jalankan sebagai mesin virtual**:
      - **VM heartbeat**
      - **Validasi tangkapan layar**
   d. [Opsional] Klik **Pengaturan VM** untuk mengubah ukuran memori dan koneksi jaringan mesin virtual.

      Secara default, mesin virtual tidak terhubung ke jaringan dan ukuran memori mesin virtual sama dengan ukuran mesin aslinya.
   e. Klik **Selesai**.
10. [Opsional] Di templat rencana validasi, klik **Jadwal**, lalu konfigurasikan.
11. [Jika set cadangan yang dipilih di **Item untuk divalidasi** sudah terenkripsi] Aktifkan switch **Cadangkan kata sandi**, kemudian berikan kata sandi enkripsi.
12. [Opsional] Untuk mengubah opsi rencana, klik ikon roda gigi.
13. Klik **Buat**.

Hasilnya, rencana validasi Anda sudah siap dan akan berjalan sesuai dengan jadwal yang Anda konfigurasikan. Untuk segera menjalankan rencana, pilih di **Manajemen** > **Validasi**, lalu klik **Jalankan sekarang**.

Setelah rencana dimulai, Anda dapat memeriksa aktivitas yang sedang berjalan dan menelusuri detailnya di konsol Cyber Protect, di bawah **Pemantauan** > **Aktivitas**.

Rencana validasi mungkin menyertakan beberapa cadangan dan satu cadangan dapat divalidasi oleh beberapa rencana validasi.

© Acronis International GmbH, 2003-2024

Catatan
Semua cadangan diproses secara berurutan, satu per satu, oleh satu tugas validasi.

Hanya satu tugas validasi yang dapat berjalan pada satu waktu pada agen tertentu. Beberapa tugas validasi dapat berjalan secara paralel jika dijalankan oleh agen yang berbeda: dua tugas secara bersamaan memerlukan dua agen, tiga tugas - tiga agen, dan seterusnya.

Tabel berikut merangkum kemungkinan status aktivitas validasi.

Hasil aktivitas	Rencanakan dengan satu cadangan	Rencanakan dengan banyak cadangan
Berhasil	Semua metode validasi berhasil	Semua metode validasi berhasil di semua cadangan
Berhasil dengan peringatan	N/A	Setidaknya satu metode validasi gagal di setidaknya satu cadangan
Gagal	Setidaknya satu metode validasi gagal	Setidaknya satu metode validasi gagal di semua cadangan

Metode validasi

Dalam rencana validasi, metode validasi berikut tersedia:

- Verifikasi checksum
- Jalankan sebagai mesin virtual
  - VM heartbeat
  - Validasi tangkapan layar

Verifikasi checksum

Validasi melalui verifikasi checksum menghitung checksum untuk setiap blok data yang dapat dipulihkan dari cadangan, lalu membandingkannya dengan checksum asli untuk blok data tersebut, yang ditulis selama proses pencadangan. Satu-satunya pengecualian adalah validasi cadangan tingkat file yang terletak di penyimpanan awan. Cadangan ini divalidasi dengan memeriksa konsistensi metadata yang disimpan dalam cadangan.

Validasi melalui verifikasi checksum adalah proses yang memakan waktu, bahkan untuk cadangan inkremental atau diferensial, yang berukuran kecil. Alasannya adalah operasi validasi tidak hanya memeriksa data yang secara fisik terdapat dalam cadangan tertentu, tetapi semua data yang perlu dipulihkan – yaitu, cadangan sebelumnya mungkin juga perlu divalidasi.

Validasi yang berhasil melalui verifikasi checksum berarti kemungkinan pemulihan data yang tinggi. Namun, validasi melalui metode ini tidak memeriksa semua faktor yang memengaruhi proses pemulihan.

© Acronis International GmbH, 2003-2024

Jika Anda mencadangkan sistem operasi, kami menyarankan agar Anda menggunakan beberapa operasi tambahan berikut:

- Uji pemulihan di bawah media yang dapat di-boot ke hard drive cadangan.
- Menjalankan mesin virtual dari cadangan di lingkungan ESXi atau Hyper-V.
- Menjalankan rencana validasi di mana metode validasi **Jalankan sebagai mesin virtual** diaktifkan.

Jalankan sebagai mesin virtual

Metode ini hanya berfungsi untuk pencadangan level disk yang berisi sistem operasi. Untuk menggunakannya, Anda memerlukan host ESXi atau Hyper-V dan agen perlindungan (Agen untuk VMware atau Agen untuk Hyper-V) yang mengelola host ini.

Metode validasi **Jalankan sebagai mesin virtual** tersedia dalam varian berikut:

- VM heartbeat
- Validasi tangkapan layar

Anda harus memilih setidaknya satu dari mereka.

VM heartbeat

Dengan metode validasi ini, agen menjalankan mesin virtual dari cadangan, menghubungkan ke VMware Tools atau Hyper-V Integration Services, lalu memeriksa respons heartbeat untuk memastikan bahwa sistem operasi berhasil dimulai. Jika koneksi gagal, agen akan berusaha menghubungkan setiap dua menit, hingga total lima kali. Jika tidak ada upaya yang berhasil, validasi akan gagal.

Terlepas dari jumlah rencana validasi dan cadangan yang divalidasi, agen yang melakukan validasi akan menjalankan satu mesin virtual secara bersamaan. Segera setelah hasil validasi menjadi jelas, agen akan menghapus mesin virtual dan menjalankan validasi berikutnya.

Catatan
Gunakan metode ini hanya saat Anda memvalidasi cadangan mesin virtual VMware dengan menjalankan pencadangan ini sebagai mesin virtual di host ESXi, dan mencadangkan mesin virtual Hyper-V dengan menjalankannya sebagai mesin virtual di host Hyper-V.

Validasi tangkapan layar

Dengan metode validasi ini, agen menjalankan mesin virtual dari cadangan, dan saat mesin virtual melakukan booting, tangkapan layar dibuat. Modul kecerdasan mesin (MI) memeriksa tangkapan layar dan jika ada layar masuk di layar tersebut, itu menandai cadangan sebagai tervalidasi.

Tangkapan layar dilampirkan ke titik pemulihan dan Anda dapat mengunduhnya di konsol Cyber Protect dalam waktu satu tahun setelah validasi. Untuk informasi lebih lanjut tentang cara memeriksa tangkapan layar, lihat "Memeriksa status validasi cadangan" (hlm. 207).

© Acronis International GmbH, 2003-2024

Jika notifikasi diaktifkan untuk akun pengguna Anda, Anda akan menerima email tentang status validasi cadangan, dengan tangkapan layar dilampirkan. Untuk informasi lebih lanjut tentang notifikasi, lihat Mengubah setelan notifikasi untuk pengguna.

Validasi tangkapan layar didukung oleh agen versi 15.0.30971 (dirilis pada November 2022) dan yang lebih baru.

Catatan
Validasi tangkapan layar berfungsi paling baik dengan cadangan sistem Windows dan Linux dengan layar masuk berbasis GUI. Metode ini tidak dioptimalkan untuk sistem Linux dengan layar masuk konsol.

Mengubah batas waktu untuk heartbeat VM dan validasi tangkapan layar

Ketika memvalidasi cadangan dengan menjalankannya sebagai mesin virtual, Anda dapat mengonfigurasi batas waktu antara booting mesin virtual dan mengirimkan permintaan heartbeat atau mengambil tangkapan layar.

Periode default-nya adalah sebagai berikut:

- Satu menit – Untuk cadangan yang disimpan di folder lokal atau di berbagi jaringan
- Lima menit – untuk cadangan yang disimpan di awan

Anda dapat mengubahnya dengan mengedit file konfigurasi untuk Agen untuk VMware atau Agen untuk Hyper-V.

Cara mengubah batas waktu

1. Buka file konfigurasi untuk mengedit. Anda dapat menemukan file ini di lokasi berikut:
   - Bagi Agen untuk VMware atau Agen untuk Hyper-V yang berjalan di Windows: `C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - Bagi Agen untuk VMware (Alat virtual): `/bin/mms_settings.config`
     Untuk informasi lebih lanjut tentang cara mengakses file konfigurasi pada alat virtual, lihat "Koneksi SSH ke alat virtual" (hlm. 172).
2. Buka `<validation>`, lalu ubah nilai untuk cadangan lokal dan cadangan awan sesuai kebutuhan:

```
<validation>
<run_vm>
<initial_timeout_minutes>
<local_backups>1</local_backups>
<cloud_backups>5</cloud_backups>
</initial_timeout_minutes>
</run_vm>
</validation>
```

3. Simpan file konfigurasi.

© Acronis International GmbH, 2003-2024

4. Mulai ulang agen.
   - [Bagi Agen untuk VMware atau Agen untuk Hyper-V yang berjalan di Windows] Jalankan perintah berikut di saran perintah:

     ```
     net stop mms
     ```

     ```
     net start mms
     ```

   - [Bagi Agen untuk VMware (Alat virtual)] Mulai ulang mesin virtual dengan agen.

Mengonfigurasi jumlah percobaan ulang jika terjadi kesalahan

Untuk memaksimalkan jumlah validasi yang berhasil, Anda dapat mengonfigurasi percobaan ulang otomatis untuk operasi validasi yang diakhiri dengan kesalahan.

Untuk mengonfigurasi percobaan ulang otomatis

1. Saat membuat rencana validasi, klik ikon roda gigi.
2. Pada panel **Opsi**, pilih **Penanganan kesalahan**.
3. Di bawah **Percobaan ulang, jika kesalahan terjadi**, klik **Iya**.
4. Dalam **Jumlah percobaan**, konfigurasikan jumlah percobaan ulang maksimum jika terjadi kesalahan.
   Operasi validasi akan berjalan lagi hingga selesai atau hingga jumlah percobaan ulang maksimum tercapai.
5. Dalam **Interval antara percobaan**, konfigurasikan batas waktu antara dua percobaan ulang berturut-turut.
6. Klik **Selesai**.

Memeriksa status validasi cadangan

Anda dapat memeriksa status validasi cadangan di tab **Perangkat** atau di tab **Penyimpanan cadangan**.

Anda juga dapat melihat status untuk setiap metode validasi dan mengunduh tangkapan layar yang diambil oleh metode validasi tangkapan layar.

Untuk informasi selengkapnya tentang cara kerja status, lihat "Status validasi" (hlm. 202).

Untuk memeriksa status validasi cadangan

Perangkat

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih beban kerja yang status validasi cadangannya ingin Anda periksa, lalu klik **Pemulihan**.
3. [Jika tersedia lebih dari satu lokasi cadangan] Pilih lokasi cadangan.
4. Pilih cadangan yang statusnya ingin Anda periksa.

© Acronis International GmbH, 2003-2024

Penyimpanan cadangan

1. Di konsol Cyber Protect, buka **Penyimpanan cadangan**.
2. Pilih lokasi penyimpanan set cadangan Anda.
3. Pilih kumpulan cadangan, lalu klik **Tampilkan cadangan**.
4. Pilih cadangan yang status validasinya ingin Anda periksa.

Pembersihan

Pembersihan adalah operasi yang menghapus cadangan usang sesuai dengan aturan retensi. Operasi ini hanya berlaku untuk agen dan beban kerja, dan bukan untuk cloud hingga cadangan cloud (yang mana hanya dapat dihapus secara manual).

Catatan
Fungsionalitas ini tersedia di penyewa pelanggan untuk yang **Cadangan Lanjutan - Server** atau **Cadangan Lanjutan - NAS** kuota diaktifkan sebagai bagian dari paket Cadangan Lanjutan.

Lokasi yang didukung

Rencana pembersihan mendukung semua lokasi pencadangan, kecuali untuk folder NFS dan Secure Zone.

Untuk membuat rencana pembersihan

1. Dalam konsol Cyber Protect, klik **Manajemen** > **Pembersihan**.
2. Klik **Buat rencana**.
3. Dalam **Agen**, pilih agen yang akan melakukan pembersihan.
   Anda dapat memilih agen apa pun yang memiliki akses ke lokasi pencadangan.
4. Dalam **Item untuk dibersihkan**, Pilih arsip atau lokasi cadangan yang akan dibersihkan.
   Untuk beralih antara arsip dan lokasi, gunakan fitur pengalih **Lokasi** / **Cadangan** di sudut kanan atas.
   Jika kamu memilih beberapa arsip terenkripsi, kata sandi enkripsinya harus sama. Untuk arsip yang menggunakan kata sandi enkripsi berbeda, buatlah rencana terpisah.
5. Dalam **Jadwal**, konfigurasikan jadwal pembersihan.
6. Dalam **Aturan retensi**, tentukan aturan retensi.
   Opsi berikut tersedia:
   - **Berdasarkan jumlah cadangan**
   - **Berdasarkan usia pencadangan** (pengaturan terpisah untuk pencadangan bulanan, mingguan, harian, dan per jam)
   - **Berdasarkan ukuran total cadangan**
7. [Jika kamu memilih arsip terenkripsi dalam **Item untuk direplikasi**] Aktifkan fitur pengalih **Kata sandi cadangan**, kemudian berikan kata sandi enkripsi.

© Acronis International GmbH, 2003-2024

8. [Opsional] Untuk mengubah opsi rencana, klik ikon roda gigi, kemudian konfigurasikan opsi sesuai kebutuhan.
9. Klik **Buat**.

Konversi ke mesin virtual

Konversi ke mesin virtual hanya tersedia untuk pencadangan level disk. Jika cadangan mencakup volume sistem dan berisi semua informasi yang diperlukan untuk memulai sistem operasi, mesin virtual yang dihasilkan dapat memulai sendiri. Jika tidak, Anda dapat menambahkan disk virtualnya ke mesin virtual lain.

Catatan
VM yang direplikasi melalui fungsi replikasi VM asli Scale Computing tidak dapat dicadangkan.

Anda dapat membuat rencana terpisah untuk konversi ke mesin virtual dan menjalankan rencana ini secara manual atau sesuai jadwal.

Untuk informasi tentang prasyarat dan batasan, lihat "Apa yang perlu Anda ketahui tentang konversi" (hlm. 210).

Catatan
Fungsionalitas ini tersedia di penyewa pelanggan untuk yang **Cadangan Lanjutan - Server** atau **Cadangan Lanjutan - NAS** kuota diaktifkan sebagai bagian dari paket Cadangan Lanjutan.

Untuk membuat rencana konversi ke mesin virtual

1. Klik **Manajemen** > **Konversi ke VM**.
2. Klik **Buat rencana**.
   Perangkat lunak menampilkan templat rencana baru.
3. [Opsional] Untuk mengubah nama rencana, klik nama default.
4. Di **Konversi ke**, pilih jenis mesin virtual target. **Anda dapat memilih salah satu dari hal berikut**:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **File VHDX**

     Catatan
     Untuk menghemat ruang penyimpanan, setiap konversi ke file VHDX atau beban kerja VMware menimpa file VHDX/VMDK di lokasi target yang dibuat selama konversi sebelumnya.
5. Lakukan salah satu langkah berikut:

© Acronis International GmbH, 2003-2024

- [Untuk VMware ESXi, Hyper-V, dan Scale Computing HC3] Klik **Host**, pilih host target, lalu tentukan templat nama mesin baru.
- [Untuk jenis mesin virtual lainnya] Di **Jalur**, tentukan tempat untuk menyimpan file mesin virtual dan templat nama file.

Nama default adalah **[Nama Mesin]_converted**.

6. Klik **Agen**, lalu pilih agen yang akan melakukan konversi.
7. Klik **Item untuk dikonversi**, lalu pilih cadangan yang akan dikonversi oleh mesin virtual ini.

   Anda dapat beralih antara memilih cadangan dan memilih seluruh lokasi dengan menggunakan switch **Lokasi** / **Cadangan** di sudut kanan atas.

   Jika cadangan yang dipilih dienkripsi, semuanya harus menggunakan kata sandi enkripsi yang sama. Untuk cadangan yang menggunakan kata sandi enkripsi yang berbeda, buat rencana terpisah.
8. [Khusus untuk VMware ESXi dan Hyper-V] Klik **Penyimpanan data** untuk ESXi atau **Jalur** untuk Hyper-V, lalu pilih penyimpanan data (penyimpanan) untuk mesin virtual.
9. [Hanya untuk VMware ESXi dan Hyper-V] Pilih mode provisi disk. Pengaturan default adalah **Tipis** untuk VMware ESXi dan **Memperluas secara dinamis** untuk Hyper-V.
10. [Opsional] [Untuk VMware ESXi, Hyper-V, dan Scale Computing HC3] Klik **Pengaturan VM** untuk memodifikasi ukuran memori, jumlah prosesor, atau koneksi jaringan mesin virtual.
11. [Opsional] Klik **Jadwal**, lalu ubah jadwal.
12. Jika cadangan yang dipilih dalam **Item untuk dikonversi** dienkripsi, aktifkan switch **Kata sandi cadangan**, lalu berikan kata sandi enkripsi. Jika tidak, lewati langkah ini.
13. [Opsional] Untuk mengubah opsi rencana, klik ikon roda gigi.
14. Klik **Buat**.

Apa yang perlu Anda ketahui tentang konversi

Jenis mesin virtual yang didukung

Konversi cadangan ke mesin virtual dapat dilakukan oleh agen yang sama yang melakukan pencadangan atau oleh agen lain.

Untuk melakukan konversi ke VMware ESXi, Hyper-V, atau Scale Computing HC3, Anda memerlukan masing-masing host ESXi, Hyper-V, atau Scale Computing HC3 dan agen perlindungan (Agen untuk VMware, Agen untuk Hyper-V, atau Agen untuk Scale Computing HC3) yang mengelola host ini.

Konversi ke file VHDX menganggap bahwa file akan terhubung sebagai disk virtual ke mesin virtual Hyper-V.

Tabel berikut meringkas tipe mesin virtual yang dapat Anda buat dengan operasi **Konversikan ke VM**. Baris dalam tabel menunjukkan tipe mesin virtual yang dikonversikan. Kolom menampilkan agen yang melakukan konversi.

Tipe	Agen	Age	Agen	Age	Age	Agen	Age	Agen	Agen

© Acronis International GmbH, 2003-2024

VM	untuk VMware	untuk Hyper-V	untuk Windows	untuk Linux	untuk Mac	untuk Scale Computing HC3	untuk oVirt (KVM)	untuk Virtuozzo Hybrid Infrastructure	untuk Virtuozzo
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–
VMware Workstation	+	+	+	+	–	–	–	–	–
File VHDX	+	+	+	+	–	–	–	–	–
Scale Computing HC3	–	–	–	–	–	+	–	–	–

Pembatasan

- Cadangan yang disimpan di NFS tidak dapat dikonversi.
- Cadangan yang disimpan di Secure Zone hanya dapat dikonversi oleh agen yang berjalan di mesin yang sama.
- Cadangan yang berisi Linux logical volume (LVM) hanya dapat dikonversi jika dibuat oleh Agen untuk VMware, Agen untuk Hyper-V, dan Agen untuk Scale Computing HC3 diarahkan ke hypervisor yang sama. Konversi lintas-hypervisor tidak didukung.
- Ketika cadangan mesin Windows dikonversi ke file VMware Workstation atau VHDX, mesin virtual yang dihasilkan akan mewarisi jenis CPU dari mesin yang melakukan konversi. Hasilnya, driver CPU yang sesuai akan diinstal di sistem operasi tamu. Jika dimulai pada host dengan jenis CPU yang berbeda, sistem tamu akan menampilkan eror driver. Perbarui driver ini secara manual.

Konversi reguler ke mesin virtual vs. menjalankan mesin virtual dari cadangan

Kedua operasi tersebut memberi Anda mesin virtual yang dapat dimulai dalam beberapa detik jika mesin asli mengalami kegagalan.

Konversi reguler ke mesin virtual membutuhkan sumber daya CPU dan memori. File dari mesin virtual akan secara konstan mengisi ruang di penyimpanan data (penyimpanan). Metode ini

© Acronis International GmbH, 2003-2024

mungkin tidak praktis jika host produksi digunakan untuk konversi. Namun, kinerja mesin virtual hanya dibatasi oleh sumber daya host.

Menjalankan mesin virtual dari cadangan akan memakai sumber daya hanya ketika mesin virtual sedang berjalan. Ruang penyimpanan data (penyimpanan) hanya diperlukan untuk menyimpan perubahan pada disk virtual. Namun, mesin virtual dapat berjalan lebih lambat, dikarenakan host tidak mengakses disk virtual secara langsung, tetapi berkomunikasi dengan agen yang membaca data dari cadangan. Selain itu, mesin virtual juga bersifat sementara.

Cara kerja konversi reguler ke mesin virtual

Cara kerja konversi reguler tergantung pada tempat Anda memilih untuk membuat mesin virtual.

- **Jika Anda memilih untuk menyimpan mesin virtual sebagai set file:** setiap konversi akan membuat kembali mesin virtual dari awal.
- **Jika Anda memilih untuk membuat mesin virtual di server virtualisasi** saat mengonversi cadangan inkremental atau diferensial, perangkat lunak secara bertahap memperbarui mesin virtual yang ada alih-alih membuatnya ulang. Konversi semacam itu biasanya berjalan lebih cepat. Cara tersebut akan menghemat lalu lintas jaringan dan sumber daya CPU dari host yang melakukan konversi. Jika memperbarui mesin virtual tidak dimungkinkan, perangkat lunak akan membuatnya kembali dari awal.

Berikut ini adalah deskripsi terperinci dari kedua kasus tersebut.

Jika Anda memilih untuk menyimpan mesin virtual sebagai set file

Sebagai hasil dari konversi pertama, mesin virtual baru akan dibuat. Setiap konversi berikutnya akan membuat ulang mesin ini dari awal. Pertama, mesin lama sementara akan diganti nama. Kemudian, mesin virtual baru dibuat dengan nama mesin lama sebelumnya. Jika operasi ini berhasil, mesin lama akan dihapus. Jika operasi ini gagal, mesin baru akan dihapus dan mesin lama diberi nama sebelumnya. Dengan cara ini, konversi akan selalu berakhir dengan satu mesin. Namun, diperlukan ruang penyimpanan tambahan selama konversi untuk menyimpan mesin yang lama.

Jika Anda memilih untuk membuat mesin virtual di server virtualisasi

Konversi pertama akan membuat mesin virtual baru. Konversi selanjutnya akan bekerja sebagai berikut:

- Jika sudah ada *cadangan penuh* sejak konversi terakhir, mesin virtual akan dibuat kembali dari awal, seperti yang dijelaskan sebelumnya di bagian ini.
- Jika tidak, mesin virtual yang ada akan diperbarui untuk menunjukkan perubahan sejak konversi terakhir. Jika pembaruan tidak dimungkinkan (misalnya, jika Anda menghapus snapshot intermediet, lihat di bawah), mesin virtual akan dibuat ulang dari awal.

© Acronis International GmbH, 2003-2024

Snapshot intermediet

Agar dapat memperbarui dengan aman mesin virtual yang dikonversi, perangkat lunak akan menyimpan snapshot hypervisor menengah dari mesin ini. Snapshot dinamai **Replika...** dan harus disimpan.

Snapshot **Replika...** akan sesuai dengan hasil konversi terbaru. Anda dapat menuju ke snapshot ini jika ingin mengembalikan mesin ke status tersebut; misalnya, jika Anda bekerja dengan mesin dan sekarang ingin membuang perubahan yang dibuat untuknya.

Untuk mesin virtual Scale Computing HC3 yang dikonversi, **Utility Snapshot** tambahan dibuat. Hanya layanan Cyber Protection yang menggunakannya.

Modul dan rencana proteksi

Untuk melindungi data, Anda harus membuat rencana proteksi, dan kemudian menerapkannya pada beban kerja Anda.

Rencana proteksi terdiri dari berbagai modul proteksi. Aktifkan modul yang Anda perlukan dan konfigurasikan pengaturan untuk membuat rencana proteksi yang memenuhi kebutuhan spesifik Anda.

Modul berikut tersedia:

- Cadangan. Mencadangkan sumber data Anda ke penyimpanan lokal atau awan.
- "Menerapkan pemulihan bencana" (hlm. 730). Meluncurkan salinan mesin Anda yang akurat di situs awan dan mengalihkan beban kerja dari mesin asli yang rusak ke server pemulihan di awan.
- Perlindungan Antivirus and Antimalware. Periksa beban kerja Anda menggunakan solusi antimalware bawaan.
- Deteksi dan Tanggapan Titik Akhir (EDR). Mendeteksi aktivitas yang mencurigakan di beban kerja, termasuk serangan yang tidak terdeteksi, dan membuat insiden untuk membantu Anda memahami cara serangan terjadi dan cara mencegahnya agak tidak terjadi lagi.
- Filtering URL. Melindungi mesin Anda dari ancaman yang berasal dari Internet, dengan memblokir akses ke URL berbahaya dan isi yang dapat diunduh.
- Windows Defender Antivirus. Mengelola pengaturan Windows Defender Antivirus untuk melindungi lingkungan Anda.
- Microsoft Security Essentials. Mengelola pengaturan Microsoft Security Essentials untuk melindungi lingkungan Anda.
- Penilaian kerentanan. Memeriksa Windows, Linux, macOS, produk pihak ketiga Microsoft, dan produk pihak ketiga macOS yang diinstal pada mesin Anda dan memberi tahu Anda tentang kerentanan.
- Manajemen patch. Menginstal patch dan pembaruan untuk Windows, Linux, macOS, produk pihak ketiga Microsoft, dan produk pihak ketiga macOS pada mesin Anda, untuk menyelesaikan kerentanan yang terdeteksi.

© Acronis International GmbH, 2003-2024

- Peta perlindungan data. Meenemukan data guna memantau status proteksi file-file penting.
- Kontrol perangkat. Menentukan perangkat yang diizinkan atau dilarang untuk digunakan oleh pengguna pada mesin Anda.
- Advanced Data Loss Prevention. Mencegah kebocoran data sensitif melalui perangkat periferal (seperti printer atau penyimpanan yang dapat dilepas) atau melalui transfer jaringan internal dan eksternal, berdasarkan kebijakan alur data.

Membuat rencana proteksi

Anda dapat membuat rencana proteksi dengan cara berikut:

- Pada tab **Perangkat**. Pilih satu atau beberapa beban kerja yang ingin Anda lindungi, lalu buat rencana proteksi untuk beban kerja tersebut.
- Pada tab **Manajemen** > **Rencana proteksi**. Buat rencana proteksi, lalu pilih satu atau beberapa beban kerja tempat rencana tersebut akan diterapkan.

Ketika membuat rencana proteksi, hanya modul yang berlaku untuk jenis beban kerja Anda yang akan ditampilkan.

Anda dapat menerapkan rencana proteksi ke lebih dari satu beban kerja. Anda juga dapat menerapkan beberapa rencana proteksi ke beban kerja yang sama. Untuk mempelajari lebih lanjut tentang konflik yang mungkin terjadi, lihat "Menyelesaikan pertentangan rencana" (hlm. 220).

Untuk membuat rencana proteksi

Perangkat

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih beban kerja yang ingin Anda lindungi, kemudian klik **Lindungi**.
3. [Jika sudah ada rencana yang diterapkan] Klik **Tambahkan rencana**.
4. Klik **Buat rencana** > **Perlindungan**.
   Panel rencana proteksi terbuka.
5. [Opsional] Untuk mengubah nama rencana proteksi, klik ikon pensil, lalu masukkan nama baru.
6. [Opsional] Untuk mengaktifkan atau menonaktifkan modul dalam rencana, alihkan tombol di sebelah nama modul.
7. [Opsional] Untuk mengonfigurasi modul, klik untuk membukanya, lalu ubah pengaturan sesuai kebutuhan Anda.
8. Ketika sudah siap, klik **Buat**.

> **Catatan**
> Untuk membuat rencana proteksi dengan enkripsi, tentukan kata sandi enkripsi. Untuk informasi lebih lanjut, lihat "Enkripsi" (hlm. 441).

Manajemen > Rencana proteksi

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana proteksi**.
2. Klik **Buat rencana**.
   Templat untuk rencana proteksi terbuka.
3. [Opsional] Untuk mengubah nama rencana proteksi, klik ikon pensil, lalu masukkan nama baru.
4. [Opsional] Untuk mengaktifkan atau menonaktifkan modul dalam rencana, alihkan tombol di sebelah nama modul.
5. [Opsional] Untuk mengonfigurasi modul, klik untuk membukanya, lalu ubah pengaturan sesuai kebutuhan Anda.
6. [Opsional] Untuk memilih beban kerja tempat Anda ingin menerapkan rencana, klik **Tambah peranti**.

   Catatan
   Anda dapat membuat rencana tanpa menerapkannya pada beban kerja apa pun. Anda dapat menambahkan beban kerja nanti, dengan mengedit rencana tersebut. Untuk informasi lebih lanjut tentang cara menambahkan beban kerja ke rencana, lihat "Menerapkan rencana proteksi pada beban kerja" (hlm. 216).

7. Ketika sudah siap, klik **Buat**.

   Catatan
   Untuk membuat rencana proteksi dengan enkripsi, tentukan kata sandi enkripsi. Untuk informasi lebih lanjut, lihat "Enkripsi" (hlm. 441).

Untuk menjalankan modul sesuai permintaan (seperti **Pencadangan**, **Perlindungan Antivirus dan Antimalware**, **Penilaian kerentanan**, **Manajemen Patch**, atau **Peta perlindungan data**), klik **Jalankan sekarang**.

Tonton video panduan Pembuatan rencana proteksi pertama.

Untuk informasi lebih lanjut tentang modul Pemulihan bencana, lihat "Membuat rencana proteksi pemulihan bencana" (hlm. 736).

Untuk informasi lebih lanjut tentang modul kontrol Perangkat, lihat "Bekerja dengan modul kontrol Perangkat" (hlm. 362).

Tindakan dengan rencana proteksi

Setelah membuat rencana proteksi, Anda dapat melakukan tindakan berikut dengan rencana proteksi:

- Terapkan rencana ke beban kerja atau sekelompok perangkat.
- Ganti nama rencana.
- Edit rencana.
  Anda dapat mengaktifkan dan menonaktifkan modul dalam rencana, dan mengubah pengaturannnya.

© Acronis International GmbH, 2003-2024

- Aktifkan atau nonaktifkan rencana.

  Rencana yang dinonaktifkan tidak akan berjalan pada beban kerja di tempatnya diterapkan.

  Tindakan ini memudahkan administrator yang nantinya ingin melindungi beban kerja yang sama dengan rencana yang sama. Rencananya tidak dibatalkan dari beban kerja dan Anda dapat memulihkan perlindungan secara cepat dengan mengaktifkan kembali rencana.
- Batalkan rencana dari beban kerja.

  Rencana yang dibatalkan tidak lagi diterapkan ke beban kerja.

  Tindakan ini memudahkan administrator yang tidak perlu perlindungan cepat untuk beban kerja yang sama dengan rencana yang sama lagi. Untuk memulihkan perlindungan yang diberikan oleh rencana yang dibatalkan, Anda harus mengetahui nama rencana ini, memilihnya dari daftar rencana yang tersedia, lalu menerapkannya kembali ke beban kerja yang sesuai.
- Menghentikan rencana.

  Tindakan ini menghentikan semua operasi pencadangan yang berjalan di seluruh beban kerja tempat rencana diterapkan. Pencadangan akan dimulai lagi sesuai jadwal rencana.

  Pemindaian antimalware tidak terpengaruh oleh tindakan ini dan akan diproses sesuai konfigurasi dalam jadwal.
- Klona rencana.

  Anda dapat membuat salinan rencana yang ada. Rencana baru ini tidak diterapkan ke beban kerja apa pun.
- Ekspor dan impor rencana.

  Anda dapat mengekspor rencana sebagai file JSON, yang dapat Anda impor kembali nanti. Oleh karena itu, Anda tidak perlu membuat rencana baru secara manual dan mengonfigurasi pengaturannya.

  Catatan
  Anda dapat mengimpor rencana proteksi yang dibuat di Cyber Protection 9.0 (dirilis pada Maret 2020) dan yang lebih baru. Rencana yang dibuat di versi yang lebih lama tidak kompatibel dengan Cyber Protection 9.0 dan yang lebih baru.

- Periksa detail rencana.
- Periksa aktivitas dan peringatan terkait rencana.
- Hapus rencana.

Menerapkan rencana proteksi pada beban kerja

Untuk melindungi beban kerja, Anda harus menerapkan rencana proteksi pada beban kerja.

Anda dapat menerapkan rencana dari tab **Perangkat** dan dari tab **Manajemen** > **Rencana Proteksi**.

Perangkat

1. Pilih satu atau beberapa beban kerja yang ingin Anda lindungi.
2. Klik **Lindungi**.

© Acronis International GmbH, 2003-2024

3. [Jika rencana proteksi lain sudah diterapkan pada beban kerja yang dipilih] Klik **Tambahkan rencana**.
4. Daftar rencana proteksi yang tersedia ditampilkan.
5. Pilih rencana proteksi yang ingin Anda terapkan, lalu klik **Terapkan**.

Manajemen > Rencana proteksi

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana proteksi**.
2. Pilih rencana proteksi yang ingin Anda terapkan.
3. Klik **Edit**.
4. Klik **Kelola perangkat**.
5. Di jendela **Perangkat**, klik **Tambahkan**.
6. Pilih beban kerja tempat Anda ingin menerapkan rencana, lalu klik **Tambahkan**.
7. Di jendela **Perangkat**, klik **Selesai**.
8. Di panel rencana proteksi, klik **Simpan**.

Untuk belajar cara menerapkan rencana proteksi ke grup perangkat, lihat "Menerapkan rencana ke grup" (hlm. 361).

Mengedit rencana proteksi

Ketika mengedit rencana, Anda dapat mengaktifkan dan menonaktifkan modul di dalamnya, dan mengubah pengaturannya.

Anda dapat mengubah rencana proteksi untuk semua beban kerja tempatnya diterapkan atau hanya beban kerja terpilih.

Anda dapat mengedit rencana dari tab **Perangkat** dan dari tab **Manajemen** > **Rencana Proteksi**.

Perangkat

1. Pilih satu atau beberapa beban kerja tempat rencana diterapkan.
2. Klik **Lindungi**.
3. Pilih rencana proteksi yang ingin Anda edit.
4. Klik ikon elipsis (...) di samping nama rencana, lalu klik **Edit**.
5. Klik modul yang ingin diedit, lalu konfigurasikan pengaturannya sesuai kebutuhan.
6. Klik **Simpan**.
7. [Jika Anda tidak memilih semua beban kerja tempat rencana diterapkan] Pilih cakupan pengeditan:
   - Untuk mengedit rencana di semua beban kerja tempatnya diterapkan, klik **Terapkan perubahan ke rencana proteksi ini (tindakan ini akan memengaruhi perangkat lainnya)**.

© Acronis International GmbH, 2003-2024

- Guna mengubah rencana hanya untuk beban kerja terpilih, klik **Buat rencana proteksi tambahan untuk mesin perangkat**.
  Hasilnya, rencana yang ada akan dicabut dari beban kerja terpilih. Rencana proteksi baru dengan pengaturan yang Anda konfigurasikan akan dibuat dan diaplikasikan pada beban kerja tersebut.

Manajemen > Rencana proteksi

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana proteksi**.
2. Pilih rencana proteksi yang ingin Anda edit.
3. Klik **Edit**.
4. Klik modul yang ingin diedit, lalu konfigurasikan pengaturannya sesuai kebutuhan.
5. Klik **Simpan**.

Catatan
Mengedit rencana dari tab **Manajemen** > **Rencana Proteksi** memengaruhi semua beban kerja yang menerapkan rencana tersebut.

Mencabut rencana proteksi

Ketika mencabut rencana, Anda menghapusnya dari satu atau beberapa beban kerja. Rencana masih melindungi beban kerja lain tempatnya diterapkan.

Anda dapat membatalkan rencana dari tab **Perangkat** dan tab **Manajemen** > **Rencana Proteksi**.

Perangkat

1. Pilih beban kerja tempat Anda ingin mencabut rencana.
2. Klik **Lindungi**.
3. Pilih rencana proteksi yang ingin Anda cabut.
4. Klik ikon elipsis (...) di samping nama rencana, lalu klik **Cabut**.

Manajemen > Rencana proteksi

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana proteksi**.
2. Pilih rencana proteksi yang ingin Anda cabut.
3. Klik **Edit**.
4. Klik **Kelola perangkat**.
5. Di jendela **Perangkat**, pilih beban kerja tempat Anda ingin mencabut rencana.
6. Klik **Hapus**.
7. Di jendela **Perangkat**, klik **Selesai**.
8. Dalam templat rencana proteksi, klik **Simpan**.

© Acronis International GmbH, 2003-2024

Mengaktifkan atau menonaktifkan rencana proteksi

Rencana yang diaktifkan akan aktif dan berjalan pada beban kerja tempatnya diterapkan. Rencana yang dinonaktifkan tidak aktif – rencana masih diterapkan ke beban kerja tetapi tidak berjalan pada beban kerja.

Ketika Anda mengaktifkan atau menonaktifkan rencana proteksi dari tab **Perangkat**, tindakan Anda hanya akan memengaruhi beban kerja yang dipilih.

Ketika Anda mengaktifkan atau menonaktifkan rencana proteksi dari tab **Manajemen** > **Rencana proteksi**, tindakan Anda memengaruhi semua beban kerja tempat rencana ini diterapkan. Selain itu, Anda dapat mengaktifkan atau menonaktifkan rencana proteksi.

Perangkat

1. Pilih beban kerja yang rencananya ingin Anda nonaktifkan.
2. Klik **Lindungi**.
3. Pilih rencana proteksi yang ingin Anda nonaktifkan.
4. Klik ikon elipsis (...) di samping nama rencana, lalu klik **Aktifkan** atau **Nonaktifkan**.

Manajemen > Rencana proteksi

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana proteksi**.
2. Pilih satu atau beberapa rencana proteksi yang ingin Anda aktifkan atau nonaktifkan.
3. Klik **Edit**.
4. Klik **Aktifkan** atau **Nonaktifkan** secara berurutan.

Catatan
Tindakan ini tidak memengaruhi rencana proteksi yang sudah dalam status target. Misalnya, jika pilihan Anda mencakup rencana yang diaktifkan dan dinonaktifkan, lalu Anda mengeklik **Aktifkan**, semua rencana yang dipilih akan diaktifkan.

Menghapus rencana proteksi

Ketika dihapus, rencana akan dicabut dari semua beban kerja dan dihapus dari konsol Cyber Protect.

Anda dapat menghapus rencana dari tab **Perangkat** dan tab **Manajemen** > **Rencana Proteksi**.

Perangkat

1. Pilih beban kerja mana pun yang menerapkan rencana proteksi yang ingin Anda hapus.
2. Klik **Lindungi**.
3. Pilih rencana proteksi yang ingin Anda hapus.
4. Klik ikon elipsis (...) di samping nama rencana, lalu klik **Hapus**.

© Acronis International GmbH, 2003-2024

Manajemen > Rencana proteksi

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana proteksi**.
2. Pilih rencana proteksi yang ingin Anda hapus.
3. Klik **Hapus**.
4. Konfirmasi pilihan Anda dengan memilih kotak centang **Saya mengonfirmasi penghapusan rencana**, lalu klik **Hapus**.

Menyelesaikan pertentangan rencana

Anda dapat menerapkan beberapa rencana proteksi ke beban kerja yang sama. Misalnya, Anda dapat menerapkan satu rencana proteksi yang hanya mengaktifkan dan mengonfigurasi modul **Antivirus dan Antimalware**, dan rencana proteksi lain yang hanya mengonfigurasi modul **Cadangan**.

Anda dapat menggabungkan rencana proteksi yang mengaktifkan modul yang berbeda. Anda juga dapat menggabungkan beberapa rencana proteksi yang hanya mengaktifkan modul **Cadangan**. Namun, jika ada modul lain yang diaktifkan di lebih dari satu rencana, akan terjadi konflik. Untuk menerapkan rencana, Anda harus menyelesaikan konflik terlebih dahulu.

Konflik antara rencana baru dan yang ada

Jika rencana baru mengalami konflik dengan rencana yang ada, Anda dapat menyelesaikan konflik dengan salah satu cara berikut:

- Buat rencana baru, terapkan, lalu nonaktifkan rencana sebelumnya yang mengalami konflik dengan rencana baru.
- Buat rencana baru, lalu nonaktifkan.

Konflik antara rencana individu dan grup

Jika rencana proteksi individu mengalami konflik dengan rencana grup yang diterapkan ke grup perangkat, Anda dapat menyelesaikan konflik dengan salah satu cara berikut:

- Hapus beban kerja dari grup perangkat, lalu terapkan rencana proteksi individu ke beban kerja tersebut.
- Edit rencana grup yang ada atau terapkan rencana grup baru ke grup perangkat.

Masalah lisensi

Modul rencana proteksi mungkin meminta kuota layanan tertentu ditetapkan ke beban kerja yang dilindungi. Jika kuota layanan yang ditetapkan tidak sesuai, Anda tidak akan dapat menjalankan, memperbarui, atau menerapkan rencana proteksi tempat modul terkait diaktifkan.

Untuk menyelesaikan masalah lisensi, lakukan salah satu hal berikut:

© Acronis International GmbH, 2003-2024

- Nonaktifkan modul yang tidak didukung oleh kuota layanan yang ditetapkan saat ini, dan lanjutkan menggunakan rencana proteksi.
- Ubah kuota layanan yang ditetapkan secara manual. Untuk mempelajari cara melakukannya, lihat "Mengubah kuota layanan mesin" (hlm. 184).

Rencana proteksi default

Rencana proteksi default adalah templat yang sudah dikonfigurasi sejak awal dan dapat diterapkan ke perangkat Anda, sehingga memastikan proteksi cepat. Dengan menggunakan rencana proteksi default, Anda tidak harus membuat rencana proteksi baru dari nol.

Saat menerapkan rencana proteksi default untuk pertama kali, templat disalin ke penyewa dan Anda dapat mengedit modul dalam rencana dan pengaturan.

Rencana default berikut tersedia:

- Cyber Protect Essentials

  Rencana ini menyediakan fungsionalitas proteksi dasar dan cadangan tingkat file.
- Pekerja jarak jauh

  Rencana ini dioptimalkan bagi pengguna yang bekerja dari jarak jauh. Rencana ini memberikan lebih banyak tugas berulang (seperti pencadangan, proteksi antimalware, dan penilaian kerentanan), aksi perlindungan yang lebih ketat, serta performa dan opsi daya yang dioptimalkan.
- Pekerja kantor (Antivirus pihak ketiga)

  Rencana ini dioptimalkan bagi pengguna yang bekerja di kantor dan lebih suka menggunakan perangkat lunak antivirus pihak ketiga. Dalam rencana ini, modul **Proteksi Antivirus and Antimalware** dinonaktifkan.
- Pekerja kantor (Antivirus Acronis)

  Rencana ini dioptimalkan bagi pengguna yang bekerja di kantor dan lebih suka menggunakan perangkat lunak antivirus Acronis.

Perbandingan rencana proteksi default

Modul dan opsi	Rencana proteksi default			
	Cyber Protect Essentials	**Pekerja jarak jauh**	**Pekerja kantor (Antivirus pihak ketiga)**	**Pekerja kantor (Antivirus Acronis)**
Cadangan	Terseida	Terseida	Terseida	Terseida
Apa yang harus dicadangkan Item untuk dicadangkan	File/folder [Semua Folder Profil]	Seluruh mesin	Seluruh mesin	Seluruh mesin

© Acronis International GmbH, 2003-2024

Modul dan opsi	Rencana proteksi default			
	Cyber Protect Essentials	**Pekerja jarak jauh**	**Pekerja kantor (Antivirus pihak ketiga)**	**Pekerja kantor (Antivirus Acronis)**
Perlindungan data berkelanjutan (CDP)	Dinonaktifkan	Diaktifkan	Dinonaktifkan	Dinonaktifkan
Tempat menyimpan cadangan	Penyimpanan awan	Penyimpanan awan	Penyimpanan awan	Penyimpanan awan
Jadwal	Senin hingga Jumat pada pukul 11.00 siang	Senin sampai Jumat pukul 12:00 siang Opsi tambahan yang diaktifkan dan persyaratan untuk mulai: • Jika mesin dimatikan, jalankan tugas yang tertinggal pada saat mesin dinyalakan • Bangun dari mode tidur atau hibernasi untuk memulai pencadangan terjadwal • Hemat daya baterai: Jangan dimulai ketika memakai daya baterai • Jangan dimulai ketika memakai koneksi bermeter	Senin hingga Jumat pada pukul 11.00 siang	Senin hingga Jumat pada pukul 11.00 siang
Skema cadangan	Selalu inkremental	Selalu inkremental	Selalu inkremental	Selalu inkremental
Berapa lama akan disimpan	Simpan cadangan tanpa batas	Bulanan: 12 bulan Mingguan: 4 minggu Harian: 7 hari	Bulanan: 12 bulan Mingguan: 4 minggu Harian: 7 hari	Bulanan: 12 bulan Mingguan: 4 minggu Harian: 7 hari

© Acronis International GmbH, 2003-2024

Modul dan opsi	Rencana proteksi default			
	Cyber Protect Essentials	**Pekerja jarak jauh**	**Pekerja kantor (Antivirus pihak ketiga)**	**Pekerja kantor (Antivirus Acronis)**
Opsi cadangan	Opsi bawaan	Opsi default, plus: • Pengaturan kinerja dan cadangan jendela (set hijau): Prioritas CPU: Rendah Kecepatan output: 50%	Opsi bawaan	Opsi bawaan
Perlindungan Antivirus and Antimalware	Terseida	Terseida	Tidak tersedia	Terseida
Active Protection	Mati	Mati	–	Mati
Antimalware Tingkat Lanjut	Nyala	Nyala	–	Nyala
Perlindungan folder jaringan	Nyala	Nyala	–	Nyala
Perlindungan sisi server	Mati	Mati	–	Mati
Perlindungan diri	Nyala	Nyala	–	Nyala
Deteksi proses cryptomining	Nyala	Nyala	–	Nyala
Karantina	Hapus file yang dikarantina setelah 30 hari	Hapus file yang dikarantina setelah 30 hari	–	Hapus file yang dikarantina setelah 30 hari
Mesin perilaku	Karantina	Karantina	–	Karantina
Pencegahan eksploit	Beri tahukan dan hentikan proses	Beri tahukan dan hentikan proses	–	Beri tahukan dan hentikan proses
Perlindungan waktu nyata	Karantina	Karantina	–	Karantina
Jadwalkan pemindaian	Pindai cepat:Karantina	Pindai cepat: Mati Pindai penuh:	–	Pindai cepat: Karantina

© Acronis International GmbH, 2003-2024

Modul dan opsi	Rencana proteksi default			
	Cyber Protect Essentials	**Pekerja jarak jauh**	**Pekerja kantor (Antivirus pihak ketiga)**	**Pekerja kantor (Antivirus Acronis)**
	Pukul 14:20, Minggu hingga Sabtu Pindai penuh:Mati	Karantina Pukul 13:55, Minggu hingga Sabtu Opsi tambahan yang diaktifkan dan persyaratan untuk mulai: • Jika mesin dimatikan, jalankan tugas yang tertinggal pada saat mesin dinyalakan • Bangun dari mode tidur atau hibernasi untuk memulai pencadangan terjadwal • Hemat daya baterai: Jangan dimulai ketika memakai daya baterai		Pukul 14:20, Minggu hingga Sabtu Pindai penuh: Mati
Pengecualian	Tidak ada	Tidak ada	–	Tidak ada
Pemfilteran URL	Terseida	Terseida	Terseida	Terseida
Akses situs web berbahaya	Selalu tanya pengguna	Blokir	Selalu tanya pengguna	Selalu tanya pengguna
Kategori yang akan difilter	Opsi bawaan	Opsi bawaan	Opsi bawaan	Opsi bawaan
Pengecualian	Tidak ada	Tidak ada	Tidak ada	Tidak ada
Penilaian kerentanan	Terseida	Terseida	Terseida	Terseida
Cakupan penilaian	Produk Microsoft,	Produk Microsoft,	Produk Microsoft,	Produk Microsoft,

© Acronis International GmbH, 2003-2024

Modul dan opsi	Rencana proteksi default			
	Cyber Protect Essentials	**Pekerja jarak jauh**	**Pekerja kantor (Antivirus pihak ketiga)**	**Pekerja kantor (Antivirus Acronis)**
kerentanan	produk pihak ketiga Windows	produk pihak ketiga Windows	produk pihak ketiga Windows	produk pihak ketiga Windows
Jadwal	Pukul 13:15, hanya hari Senin	Pukul 14:20, hanya hari Senin	Pukul 13:15, hanya hari Senin	Pukul 13:15, hanya hari Senin
Manajemen patch	Terseida	Terseida	Terseida	Terseida
Produk Microsoft	Semua pembaruan	Semua pembaruan	Semua pembaruan	Semua pembaruan
Produk pihak ketiga Windows	Hanya pembaruan berat	Hanya pembaruan berat	Hanya pembaruan berat	Hanya pembaruan berat
Jadwal	Pukul 15:10, hanya hari Senin	Pukul 14:20 siang, Senin hingga Jumat	Pukul 15:10, hanya hari Senin	Pukul 15:10, hanya hari Senin
Pencadangan prapembaruan	Mati	Nyala	Mati	Mati
Peta perlindungan data	Tidak tersedia	Terseida	Terseida	Terseida
Aturan pengecualian dan ekstensi	–	Opsi default dan ekstensi tambahan berikut: **Gambar** • .jpeg • .jpg • .png • .gif • .bmp • .ico • .wbmp • .xcf • .psd • .tiff • .dwg **Audio dan video**	Opsi bawaan (mendeteksi 66 ekstensi)	Opsi bawaan (mendeteksi 66 ekstensi)

© Acronis International GmbH, 2003-2024

Modul dan opsi	Rencana proteksi default			
	Cyber Protect Essentials	**Pekerja jarak jauh**	**Pekerja kantor (Antivirus pihak ketiga)**	**Pekerja kantor (Antivirus Acronis)**
		• .avi, • .mov, • .mpeg, • .mpg, • .mkv • .wav • .aif • .aifc • .aiff • .au • .snd • .mid • .midi • .mpga • .mp3 • .oga • .flac • .opus • .spx • .ogg • .ogx • .mp4		
Jadwal	–	Pukul 15:35, Senin hingga Jumat	Pukul 15:40, Senin hingga Jumat	Pukul 15:40, Senin hingga Jumat

Catatan
Jumlah modul dalam rencana proteksi default dapat bervariasi bergantung pada lisensi Cyber Protection Anda.

Menerapkan rencana proteksi default

Rencana proteksi default awal adalah templat pengaturan yang tidak dapat Anda edit. Saat Anda menerapkan rencana default untuk pertama kali, templat disalin ke penyewa Anda sebagai rencana proteksi prakonfigurasi dan diaktifkan pada beban kerja terpilih.

Rencana proteksi muncul di tab **Manajemen** > **Rencana proteksi**, lalu Anda dapat mengelolanya di sana.

Untuk menerapkan rencana proteksi default pertama kali

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih beban kerja yang ingin Anda lindungi.
3. Klik **Lindungi**.
4. Pilih salah satu rencana default, lalu klik **Terapkan**.

Mengedit rencana proteksi default

Anda dapat mengedit rencana proteksi default setelah menerapkannya untuk pertama kali.

Untuk mengedit rencana proteksi default yang diterapkan

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana proteksi**.
2. Pilih rencana yang ingin Anda edit, lalu klik **Edit**.
3. Modifikasi modul yang termasuk dalam rencana ini, atau opsinya, lalu klik **Simpan**.

Penting
Beberapa opsi tidak dapat dimodifikasi.

Rencana proteksi individu untuk integrasi panel kontrol hosting

Saat mengaktifkan integrasi panel kontrol hosting di server hosting web Anda yang menggunakan DirectAdmin, cPanel, atau Plesk, layanan Cyber Protection secara otomatis akan membuat rencana proteksi individu di akun pengguna Anda untuk setiap beban kerja. Rencana proteksi ini dikaitkan dengan beban kerja tertentu yang memulai pembuatan rencana proteksi, dan tidak dapat dibatalkan atau ditetapkan ke beban kerja lainnya.

Untuk berhenti menggunakan rencana proteksi individu, Anda dapat menghapusnya dari konsol Cyber Protect. Anda dapat mengidentifikasi rencana proteksi individu dengan melihat tanda di samping namanya.

Jika Anda menginginkan rencana proteksi yang dapat melindungi beberapa server hosting web yang menggunakan integrasi panel kontrol hosting, Anda dapat membuat rencana proteksi di konsol Cyber Protect dan menetepkannya ke beban kerja. Namun, modifikasi pada rencana proteksi yang ikut diterapkan juga pada beberapa panel kontrol hosting web lain hanya dapat dilakukan di konsol Cyber Protect, dan tidak dapat dilakukan di dalam integrasinya.

Skor #CyberFit untuk mesin

Skor #CyberFit memberi penilaian keamanan dan mekanisme penilaian yang mengevaluasi postur keamanan mesin Anda. Skor tersebut mengidentifikasi kesenjangan keamanan di lingkungan IT dan vektor serangan terbuka ke titik akhir, dan memberi rekomendasi tindakan untuk perbaikan dalam bentuk laporan. Fitur ini tersedia di semua edisi Cyber Protect.

Fungsi Skor #CyberFit didukung pada:

© Acronis International GmbH, 2003-2024

- Windows 7 (versi pertama) dan versi yang lebih baru
- Windows Server 2008 R2 dan versi yang lebih baru

Cara kerjanya

Agen perlindungan yang diinstal pada mesin melakukan penilaian keamanan dan menghitung Skor #CyberFit untuk mesin tersebut. Skor #CyberFit suatu mesin dihitung ulang secara otomatis dan berkala.

Mekanisme penilaian #CyberFit

Skor #CyberFit untuk sebuah mesin dihitung berdasarkan metrik berikut ini:

- Perlindungan antimalware 0-275
- Perlindungan cadangan 0-175
- Firewall 0-175
- Jaringan privat virtual (VPN) 0-75
- Enkripsi disk penuh 0-125
- Keamanan jaringan 0-25

Skor #CyberFit maksimal untuk sebuah mesin adalah 850.

Metrik	Apa yang dinilai?	Rekomendasi pada pengguna	Penentuan skor
Antimalware	Agen memeriksa apakah perangkat lunak antimalware diinstal pada mesin.	Temuan: • Perlindungan antimalware Anda diaktifkan (+275 poin) • Anda tidak memiliki perlindungan antimalware, sistem Anda mungkin berisiko (0 poin) Rekomendasi yang diberikan oleh Skor #CyberFit: Anda harus menginstal dan mengaktifkan solusi antimalware pada mesin Anda untuk tetap terlindung dari risiko keamanan. Anda harus mengunjungi situs web seperti AV-Test atau AV-Comparatives untuk melihat daftar solusi antimalware yang direkomendasikan.	275 - perangkat lunak antimalware diinstal pada mesin 0 - tidak ada perangkat lunak antimalware yang diinstal pada mesin
Cadangan	Agen memeriksa apakah solusi pencadangan diinstal pada mesin.	Temuan: • Anda memiliki solusi cadangan yang melindungi data Anda (+175 poin) • Tidak ada solusi cadangan yang ditemukan, data Anda dapat berisiko (0 poin)	175 - solusi cadangan diinstal pada mesin 0 - tidak ada

© Acronis International GmbH, 2003-2024

		Rekomendasi yang diberikan oleh Skor #CyberFit: Sebaiknya cadangkan data secara teratur untuk mencegah kehilangan data atau serangan ransomware. Berikut adalah beberapa solusi cadangan yang harus Anda pertimbangkan untuk digunakan: • Acronis Cyber Protect / Cyber Backup / True Image • Cadangan Windows Server (Windows Server 2008 R2 dan versi lebih baru)	solusi cadangan diinstal pada mesin
Firewall	Agen memeriksa apakah firewall tersedia dan diaktifkan dalam lingkungan Anda. Agen melakukan hal berikut: 1. Memeriksa apakah firewall publik dinyalakan di Windows Firewall and Network Protection. 2. Memeriksa apakah firewall pribadi dinyalakan di Windows Firewall and Network Protection. 3. Memeriksa solusi/agen firewall pihak ke-3 jika firewall publik dan pribadi	Temuan: • Anda memiliki firewall yang diaktifkan untuk jaringan publik dan pribadi, atau ditemukan solusi firewall pihak ke-3 (+175 poin) • Anda memiliki firewall yang diaktifkan hanya untuk jaringan publik (+100 poin) • Anda memiliki firewall yang diaktifkan hanya untuk jaringan pribadi (+75 poin) • Anda tidak memiliki firewall yang diaktifkan, koneksi jaringan Anda tidak aman (+0 poin) Rekomendasi yang diberikan oleh Skor #CyberFit: Kami menyarankan Anda mengaktifkan firewall untuk jaringan publik dan pribadi Anda guna meningkatkan perlindungan keamanan terhadap serangan jahat pada sistem Anda. Di bawah ini, panduan terperinci disediakan tentang pengaturan firewall Windows Anda, tergantung pada kebutuhan keamanan dan arsitektur jaringan Anda: Panduan untuk pengguna akhir/karyawan: Cara mengatur Windows Defender Firewall di PC Anda Cara mengatur Windows Firewall di PC Anda Panduan untuk administrator dan teknisi sistem: Cara menyebarkan Windows Defender Firewall dengan Keamanan Tingkat Lanjut Cara membuat Aturan Tingkat Lanjut dalam Windows Firewall	100 - Firewall publik Windows diaktifkan 75 - Firewall pribadi Windows diaktifkan 175 - Firewall publik dan pribadi Windows diaktifkan ATAU solusi firewall dari pihak ketiga diaktifkan 0 - firewall Windows, atau solusi firewall pihak ketiga tidak diaktifkan

© Acronis International GmbH, 2003-2024

	Windows dinonaktifkan.		
Jaringan Privat Virtual (VPN)	Agen memeriksa apakah solusi VPN diinstal pada mesin serta apakah VPN diaktifkan dan berfungsi.	Temuan: • Anda memiliki solusi VPN dan dapat dengan aman menerima dan mengirim data pada jaringan publik dan bersama (+75 poin) • Tidak ada solusi VPN yang ditemukan, sambungan Anda ke jaringan publik dan bersama tidak aman (0 poin) Rekomendasi yang diberikan oleh Skor #CyberFit: Kami menyarankan Anda menggunakan VPN untuk mengakses jaringan perusahaan dan data rahasia Anda. Penggunaan VPN sangat penting untuk menjaga keamanan dan privasi komunikasi Anda, terutama jika Anda menggunakan akses Internet gratis dari kafe, perpustakaan, bandara, atau tempat apa pun. Berikut adalah beberapa solusi VPN yang harus Anda pertimbangkan untuk digunakan: • VPN Bisnis Acronis • 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 aktif dan berfungsi 0 - VPN tidak aktif
Enkripsi disk	Agen memeriksa apakah mesin memiliki enkripsi disk yang aktif. Agen	Temuan: • Anda memiliki enkripsi disk penuh yang aktif, mesin Anda terlindungi dari kerusakan fisik (+125 poin) • Hanya beberapa hard drive yang dienkripsi, mesin Anda dapat berisiko mengalami kerusakan fisik (+75 poin)	125 - semua disk terenkripsi 75 - setidaknya salah satu disk Anda

© Acronis International GmbH, 2003-2024

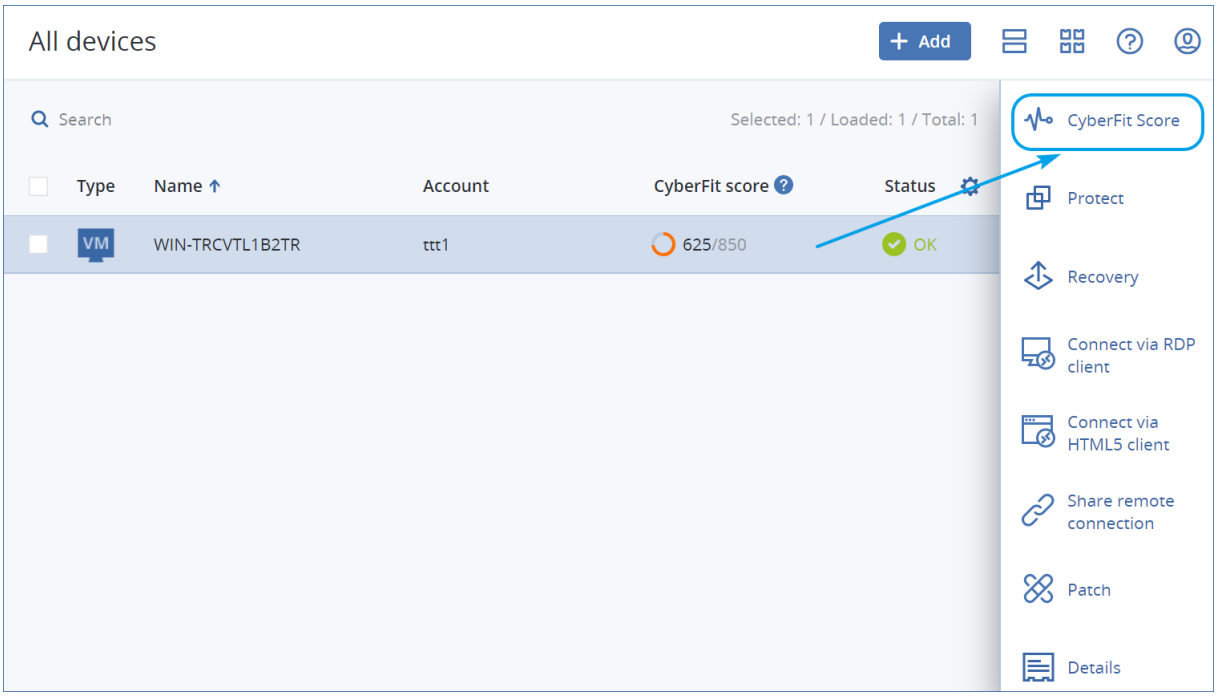
	memeriksa apakah Windows BitLocker diaktifkan.	• Tidak ada enkripsi disk yang ditemukan, mesin Anda berisiko mengalami kerusakan fisik (0 poin) Rekomendasi yang diberikan oleh Skor #CyberFit: Kami menyarankan Anda mengaktifkan Windows BitLocker untuk meningkatkan perlindungan data dan file Anda. Panduan: Cara mengaktifkan enkripsi perangkat di Windows	terenkripsi, tetapi ada juga disk yang tidak terenkripsi 0 - tidak ada disk yang terenkripsi
Keamanan jaringan (NTLM traffic keluar ke server jarak jauh)	Agen memeriksa apakah mesin memiliki lalu lintas NTLM ke luar yang terbatas ke server jarak jauh.	Temuan: • Lalu lintas NTLM keluar ke server jarak jauh ditolak, kredensial Anda terlindungi (+25 poin) • Lalu lintas NTLM keluar ke server jarak jauh tidak ditolak, kredensial Anda mungkin rentan terhadap paparan (0 poin) Rekomendasi yang diberikan oleh Skor #CyberFit: Untuk perlindungan keamanan yang lebih baik, kami menyarankan Anda menolak semua lalu lintas NTLM keluar ke server jarak jauh. Anda dapat menemukan informasi tentang cara mengubah pengaturan NTLM dan menambahkan pengecualian di sini dengan mengikuti tautan di bawah ini. Panduan: Batasi lalu lintas NTLM keluar ke server jarak jauh	25 - NTLM traffic keluar diatur ke TolakSemua 0 - NTLM traffic keluar diatur ke nilai lain

Berdasarkan nilai penjumlahan yang diberikan untuk setiap metrik, total Skor #CyberFit pada suatu mesin dapat sesuai untuk peringkat berikut yang mencerminkan tingkat proteksi titik akhir:

- 0 - 579 - Buruk
- 580 - 669 - Cukup
- 670 - 739 - Baik
- 740 - 799 - Sangat baik
- 800 - 850 - Luar biasa

Anda dapat melihat Skor #CyberFit untuk mesin Anda di konsol Cyber Protect: buka **Perangkat** > **Semua perangkat**. Pada daftar perangkat, Anda dapat melihat kolom **Skor #CyberFit**. Anda juga dapat menjalankan pemindaian Skor #CyberFit pada mesin untuk memeriksa postur keamanannya.

© Acronis International GmbH, 2003-2024



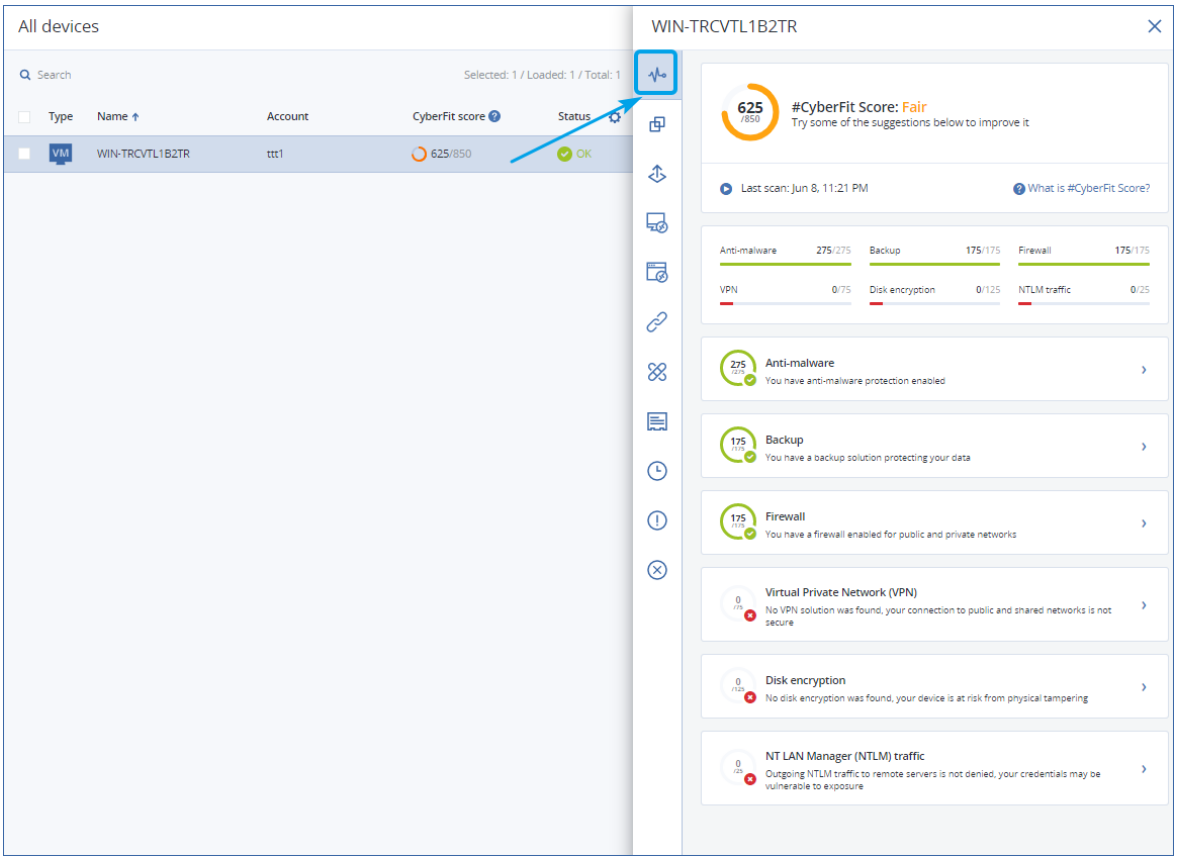
Anda juga dapat memperoleh informasi tentang Skor #CyberFit pada halaman widget dan laporan terkait.

Menjalankan pemindaian Skor #CyberFit

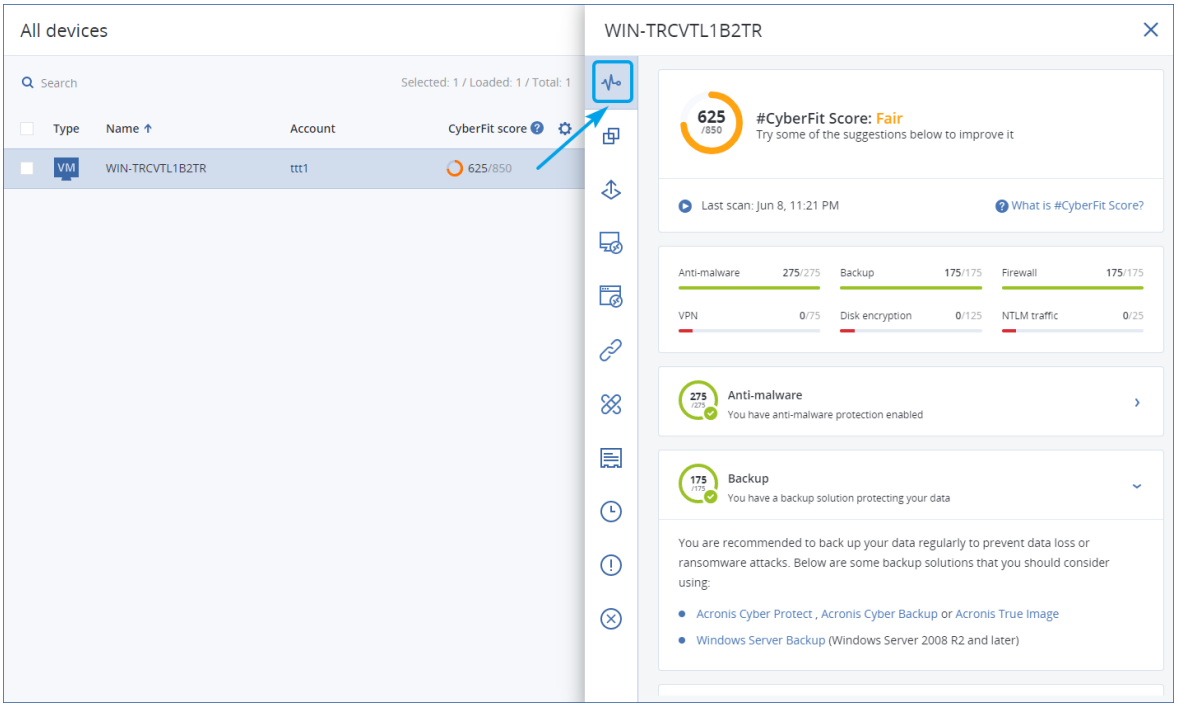
Untuk menjalankan pemindaian Skor #CyberFit

1. Di konsol Cyber Protect, buka **Perangkat**.
2. Pilih mesin dan klik **Skor #CyberFit**.
3. Jika mesin belum pernah dipindai sebelumnya, klik **Jalankan pemindaian pertama**.
4. Setelah pemindaian selesai, Anda akan melihat Skor #CyberFit total untuk mesin beserta skor keenam metrik yang dinilai untuk masing-masing - Antimalware, Cadangan, Firewall, Jaringan Privat Virtual (VPN), Enkripsi disk, dan lalu lintas Manajer LAN NT (NTLM).

© Acronis International GmbH, 2003-2024



5. Untuk memeriksa cara meningkatkan skor setiap metrik yang untuknya konfigurasi keamanan dapat ditingkatkan, perluas bagian terkait dan baca rekomendasinya.



6. Setelah membahas rekomendasi, Anda selalu dapat menghitung ulang Skor #CyberFit mesin dengan mengeklik tombol tanda panah tepat di bawah Skor #CyberFit total.

© Acronis International GmbH, 2003-2024

Pembuatan Skrip Cyber

Dengan Skrip Cyber, Anda dapat menggunakan skrip untuk mengotomatisasi operasi rutin pada mesin Windows dan macOS di lingkungan Anda, seperti menginstal perangkat lunak, memodifikasi konfigurasi, memulai atau menghentikan layanan, dan membuat akun. Dengan demikian, Anda dapat memangkas waktu untuk operasi semacam itu dan mengurangi risiko kesalahan saat melakukannya secara manual.

Skrip Cyber tersedia untuk administrator dan pengguna pada tingkat pelanggan, serta untuk administrator mitra (penyedia layanan). Untuk informasi lebih lanjut tentang berbagai tingkat administrasi, lihat "Dukungan beberapa penyewaan" (hlm. 327).

Skrip yang dapat Anda gunakan harus disetujui terlebih dahulu. Hanya administrator dengan peran **Administrator Cyber** yang dapat menyetujui dan menguji skrip baru. Untuk informasi lebih lanjut tentang mengubah status skrip, lihat "Mengubah status skrip" (hlm. 245).

Tergantung pada peran pengguna Anda, Anda dapat melakukan operasi yang berbeda dengan skrip dan rencana skrip. Untuk informasi lebih lanjut tentang peran, lihat "Peran pengguna dan hak Pembuatan Skrip Cyber" (hlm. 235).

Prasyarat

- Fungsi Skrip Cyber memerlukan paket Manajemen Lanjutan.
- Untuk menggunakan semua fitur Pembuatan Skrip Cyber seperti mengedit skrip, menjalankan skrip, membuat rencana skrip, dan sebagainya, Anda harus mengaktifkan autentikasi dua faktor untuk akun Anda.

Pembatasan

- Bahasa skrip berikut didukung:
  - PowerShell
  - Bash
- Operasi Pembuatan Skrip Cyber hanya dapat berjalan pada mesin target yang menginstal agen proteksi.

Platform yang didukung

Pembuatan Skrip Cyber tersedia untuk beban kerja Windows dan macOS.

Tabel berikut merangkum versi yang didukung.

© Acronis International GmbH, 2003-2024

Sistem operasi	Versi
Windows	Windows 7 SP1 dan lebih baru – semua edisi
	Windows 8/8.1 – semua edisi (x86, x64), kecuali untuk Windows RT edition
	Windows 10 – edisi Home, Pro, Education, Enterprise, dan IoT Enterprise
	Windows 11
	Windows Server 2008 R2 SP1 dan lebih baru – edisi Standard, Enterprise, Datacenter, Foundation, dan Web
	Windows Server 2012/2012 R2 – semua edisi
	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

Peran pengguna dan hak Pembuatan Skrip Cyber

Tindakan yang tersedia dengan skrip dan rencana skrip bergantung pada status skrip dan peran pengguna Anda.

Administrator dapat mengelola objek di penyewa mereka sendiri dan di penyewa anak. Mereka tidak dapat melihat atau mengakses objek pada level administrasi atas, jika ada.

Administrator level bawah hanya memiliki akses hanya baca ke rencana skrip yang diterapkan pada beban kerja mereka oleh administrator level atas.

Peran berikut memberikan hak terkait dengan Pembuatan Skrip Cyber:

- **Administrator perusahaan**

  Peran ini memberikan hak administrator penuh di semua layanan. Terkait dengan Pembuatan Skrip Cyber, peran ini memberikan hak yang sama dengan peran administrator Cyber.

- **Administrator cyber**

  Peran ini memberikan izin penuh, termasuk persetujuan skrip yang dapat digunakan di penyewa, dan kemampuan untuk menjalankan skrip dengan status **Pengujian**.
- **Administrator**

© Acronis International GmbH, 2003-2024

Peran ini memberikan izin sebagian, dengan kemampuan untuk menjalankan skrip yang disetujui serta membuat dan menjalankan rencana skrip yang menggunakan skrip yang disetujui.

- **Administrator hanya-baca**

  Peran ini memberikan izin terbatas, dengan kemampuan untuk melihat skrip dan rencana proteksi yang digunakan di penyewa.
- **Pengguna**

  Peran ini memberikan izin sebagian, dengan kemampuan untuk menjalankan skrip yang disetujui serta membuat dan menjalankan rencana skrip yang menggunakan skrip yang disetujui, tetapi hanya pada mesin milik pengguna.

Tabel berikut merangkum semua tindakan yang tersedia, bergantung pada status skrip dan peran pengguna.

Peran	Objek	Status skrip		
		Draf	Pengujian	Disetujui
Administrator Cyber **Administrator perusahaan**	Rencana skrip	Edit (Hapus draf skrip dari rencana) Hapus Mencabut Nonaktifkan Hentikan	Buat Edit Terapkan Aktifkan Jalankan Hapus Mencabut Nonaktifkan Hentikan	Buat Edit Terapkan Aktifkan Jalankan Hapus Mencabut Nonaktifkan Hentikan
	Skrip	Buat Edit Ubah status Klona Hapus Batalkan yang sedang berjalan	Buat Edit Ubah status Jalankan Klona Hapus Batalkan yang sedang berjalan	Buat Edit Ubah status Jalankan Klona Hapus Batalkan yang sedang berjalan
Administrator **Pengguna** (untuk beban kerja mereka sendiri)	Rencana skrip	Tampilan Mencabut Nonaktifkan	Tampilan Batalkan jalankan	Buat Edit Terapkan

© Acronis International GmbH, 2003-2024

		Hentikan		Aktifkan Jalankan Hapus Mencabut Nonaktifkan Hentikan
	Skrip	Buat Edit Klona Hapus Batalkan yang sedang berjalan	Tampilan Klona Batalkan yang sedang berjalan	Jalankan Klona Batalkan yang sedang berjalan
Administrator hanya-baca	Rencana skrip	Tampilan	Tampilan	Tampilan
	Skrip	Tampilan	Tampilan	Tampilan

Skrip

Sebuah skrip adalah serangkaian instruksi yang ditafsirkan pada saat runtime dan dieksekusi pada mesin target. Skrip menyediakan solusi yang nyaman untuk mengotomatisasi tugas yang berulang atau kompleks.

Dengan Skrip Cyber, Anda dapat menjalankan skrip yang telah ditentukan sebelumnya atau membuat skrip kustom. Anda dapat melihat semua skrip yang tersedia untuk Anda di **Manajemen** > **Repositori skrip**. Skrip yang telah ditentukan sebelumnya berada di bagian **Perpustakaan**. Skrip yang Anda buat atau klona ke penyewa Anda berada di bagian **Skrip Saya**.

Anda dapat menggunakan skrip dengan memasukkannya dalam rencana skrip atau dengan melakukan operasi **Penerapan skrip cepat**.

Catatan
Anda hanya dapat menggunakan skrip yang disetujui yang dibuat di penyewa Anda atau telah diklonakan ke dalamnya. Jika skrip dihapus dari repositori skrip atau berada dalam status **Draf**, skrip tersebut tidak akan berjalan. Anda dapat memeriksa detail operasi skrip atau membatalkannya di **Pemantauan** > **Aktivitas**.

Tabel berikut menyediakan informasi lebih lanjut tentang tindakan yang dapat dilakukan dengan skrip, tergantung pada statusnya.

© Acronis International GmbH, 2003-2024

Status	Tindakan yang mungkin dilakukan
Draf	Skrip baru yang Anda buat dan skrip yang Anda klona ke repositori Anda berada dalam status **Draf**. Anda tidak diizinkan untuk menjalankan skrip ini atau memasukkannya dalam rencana skrip.
Pengujian	Administrator dengan peran **Administrator Cyber** dapat menjalankan skrip ini dan memasukkannya dalam rencana skrip.
Disetujui	Anda dapat menjalankan skrip-skrip ini dan memasukkannya dalam rencana skrip.

Hanya administrator dengan peran **Administrator Cyber** yang dapat mengubah status skrip atau menghapus skrip yang telah disetujui. Untuk informasi lebih lanjut, lihat "Mengubah status skrip" (hlm. 245).

Membuat skrip

Anda dapat membuat skrip dengan menulis kode secara manual.

Untuk membuat skrip

1. Di konsol Cyber Protect, buka **Manajemen** > **Repositori skrip**.
2. Di **Skrip Saya**, klik **Buat skrip dengan menggunakan AI**.
3. Di panel utama, tulis isi skrip.

Penting
Saat Anda membuat skrip, sertakan pemeriksaan kode keluar untuk setiap operasi. Jika tidak, operasi yang gagal mungkin diabaikan dan status aktivitas skrip di **Pemantauan** > **Aktivitas** mungkin salah ditampilkan sebagai **Berhasil**.

4. Tentukan pengaturan skrip.

Pengaturan	Deskripsi
Nama skrip	Nama skrip. Bidang ini diisi secara otomatis, tetapi Anda dapat mengubah nilai tersebut.
Deskripsi	Deskripsi skrip. Pengaturan ini opsional. [Untuk skrip yang dihasilkan oleh AI] Bidang ini akan diisi secara otomatis saat pembuatan skrip. Anda dapat mengedit deskripsi yang disediakan oleh AI.
Bahasa	Bahasa skrip. Nilai yang tersedia adalah: • **PowerShell**. Ini adalah nilai default. • **Bash** [Pada skrip yang dihasilkan oleh AI] Pengaturan ini dikonfigurasi sebelum pembuatan skrip.
Sistem	Sistem operasi yang diinstal pada target beban kerja tempat skrip akan dijalankan.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
operasi	Nilai yang tersedia adalah: • **Windows**. Ini adalah nilai default. • **macOS** [Pada skrip yang dihasilkan oleh AI] Pengaturan ini dikonfigurasi sebelum pembuatan skrip.
Status	Status skrip. • **Draf**. Ini adalah nilai default. Skrip baru yang Anda buat dan skrip yang Anda klona ke repositori Anda berada dalam status **Draf**. Anda tidak diizinkan untuk menjalankan skrip **Draf** atau memasukkannya dalam rencana skrip. • **Pengujian**. Hanya administrator dengan peran **Administrator Cyber** yang dapat mengubah status skrip menjadi **Pengujian**, menjalankan skrip dalam status **Pengujian**, dan menjalankan rencana skrip dengan skrip tersebut. • **Disetujui**. Anda dapat menjalankan skrip **Disetujui** dan memasukkannya dalam rencana skrip. Hanya administrator dengan peran **Administrator Cyber** yang dapat mengubah status skrip atau menghapus skrip yang telah disetujui. Untuk informasi lebih lanjut, lihat "Mengubah status skrip" (hlm. 245).
Tag	Tag tidak peka terhadap huruf besar atau kecil dan dapat memiliki panjang hingga 32 karakter. Anda tidak dapat menggunakan tanda kurung bulat dan sudut, koma, atau spasi. Pengaturan ini bersifat opsional. [Untuk skrip yang dihasilkan oleh AI] Tag yang **dihasilkan-AI** akan ditambahkan secara otomatis setelah pembuatan skrip. Anda dapat menghapus tag ini secara manual atau menambahkan lebih banyak tag.

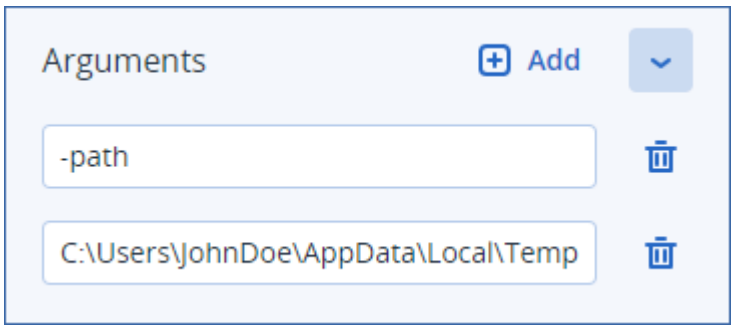
5. [Hanya untuk skrip yang memerlukan kredensial] Tentukan kredensial.

   Anda dapat menggunakan satu kredensial (misalnya, token) atau sepasang kredensial (misalnya, nama pengguna dan kata sandi).
6. [Hanya untuk skrip yang memerlukan argumen] Tentukan argumen dan nilainya, sebagai berikut:
   a. Klik **Tambah**.
   b. Di bidang **Tambah argumen**, tentukan argumennya.
   c. Klik **Tambah**.
   d. Di bidang kedua yang muncul, tentukan nilai argumen.

© Acronis International GmbH, 2003-2024

Catatan
Anda hanya dapat menentukan argumen yang telah Anda definisikan di isi skrip.

Misalnya:



e. Ulangi langkah di atas jika Anda perlu menambahkan lebih dari satu argumen.

7. Klik **Simpan**.

Skrip disimpan ke repositori Anda dalam status **Draf**.

Anda tidak dapat menggunakan skrip sampai administrator dengan peran **Administrator Cyber** mengubah statusnya menjadi **Disetujui**. Untuk informasi lebih lanjut, lihat "Mengubah status skrip" (hlm. 245).

Untuk menggunakan skrip di penyewa lain yang Anda kelola, Anda harus mengklona skrip ke penyewa tersebut. Untuk informasi lebih lanjut, lihat "Membuat kloning skrip" (hlm. 243).

Membuat skrip dengan menggunakan AI (ScriptPilot)

Catatan
ScriptPilot memerlukan paket Manajemen Lanjutan.

Dengan ScriptPilot, Anda dapat menggunakan AI untuk mengubah petunjuk menjadi skrip yang kuat, sehingga menghemat waktu dan usaha Anda. Anda dapat menggunakan fungsionalitas ini dengan cara berikut:

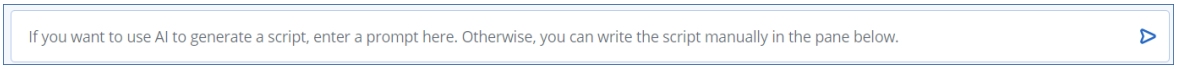
© Acronis International GmbH, 2003-2024

- Masukkan petunjuk untuk meminta AI membuat skrip dari awal.
- Masukkan petunjuk untuk meminta AI meninjau dan melengkapi kode yang telah Anda masukkan dalam badan skrip. Anda dapat menggunakan kemampuan ini ketika Anda mengalami kesulitan dengan kode yang lebih kompleks.

Dengan ScriptPilot yang menggunakan model GPT-4 dari OpenAI, Anda dapat membuat hingga 100 skrip untuk organisasi Anda setiap bulan, tanpa biaya tambahan.

Untuk membuat skrip dengan menggunakan AI

1. Di konsol Cyber Protect, buka **Manajemen** > **Repositori skrip**.
2. Di **Skrip Saya**, klik **Buat skrip dengan menggunakan AI**.
3. Dalam petunjuk, masukkan deskripsi tentang apa yang harus dilakukan skrip. Pastikan deskripsi yang Anda masukkan sejelas dan sedetail mungkin.

   Misalnya:

   ```
   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. Dalam petunjuk, klik tombol panah.
5. Di jendela konfirmasi, pilih Bahasa dan Sistem Operasi, lalu klik **Hasilkan**.

   Skrip yang dihasilkan oleh AI ditampilkan di panel utama. Nama dan deskripsi skrip secara otomatis dihasilkan oleh AI sehingga keduanya cocok dengan skrip tersebut. Tag yang **dibuat oleh AI** secara otomatis dimasukkan ke dalam skrip tersebut.
6. Tinjau skrip yang dihasilkan oleh AI dan jika perlu, edit secara manual.
7. Jika perlu, edit pengaturan skrip.

Pengaturan	Deskripsi
Nama skrip	Nama skrip. Bidang ini diisi secara otomatis, tetapi Anda dapat mengubah nilai tersebut.
Deskripsi	Deskripsi skrip. Pengaturan ini opsional. [Untuk skrip yang dihasilkan oleh AI] Bidang ini akan diisi secara otomatis saat pembuatan skrip. Anda dapat mengedit deskripsi yang disediakan oleh AI.
Bahasa	Bahasa skrip. Nilai yang tersedia adalah: • **PowerShell**. Ini adalah nilai default. • **Bash** [Pada skrip yang dihasilkan oleh AI] Pengaturan ini dikonfigurasi sebelum pembuatan skrip.
Sistem operasi	Sistem operasi yang diinstal pada target beban kerja tempat skrip akan dijalankan. Nilai yang tersedia adalah:

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	• **Windows**. Ini adalah nilai default. • **macOS** [Pada skrip yang dihasilkan oleh AI] Pengaturan ini dikonfigurasi sebelum pembuatan skrip.
Status	Status skrip. • **Draf**. Ini adalah nilai default. Skrip baru yang Anda buat dan skrip yang Anda klona ke repositori Anda berada dalam status **Draf**. Anda tidak diizinkan untuk menjalankan skrip **Draf** atau memasukkannya dalam rencana skrip. • **Pengujian**. Hanya administrator dengan peran **Administrator Cyber** yang dapat mengubah status skrip menjadi **Pengujian**, menjalankan skrip dalam status **Pengujian**, dan menjalankan rencana skrip dengan skrip tersebut. • **Disetujui**. Anda dapat menjalankan skrip **Disetujui** dan memasukkannya dalam rencana skrip. Hanya administrator dengan peran **Administrator Cyber** yang dapat mengubah status skrip atau menghapus skrip yang telah disetujui. Untuk informasi lebih lanjut, lihat "Mengubah status skrip" (hlm. 245).
Tag	Tag tidak peka terhadap huruf besar atau kecil dan dapat memiliki panjang hingga 32 karakter. Anda tidak dapat menggunakan tanda kurung bulat dan sudut, koma, atau spasi. Pengaturan ini bersifat opsional. [Untuk skrip yang dihasilkan oleh AI] Tag yang **dihasilkan-AI** akan ditambahkan secara otomatis setelah pembuatan skrip. Anda dapat menghapus tag ini secara manual atau menambahkan lebih banyak tag.

8. [Opsional] [Hanya untuk skrip yang memerlukan kredensial] Tentukan kredensial.

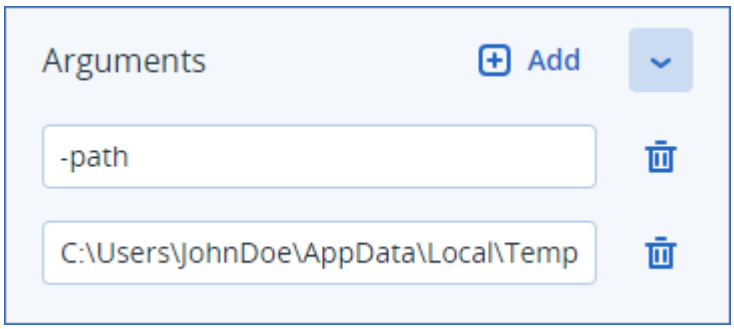
   Anda dapat menggunakan satu kredensial (misalnya, token) atau sepasang kredensial (misalnya, nama pengguna dan kata sandi).
9. [Hanya untuk skrip yang memerlukan argumen] Tentukan argumen dan nilainya, sebagai berikut:
   a. Klik **Tambah**.
   b. Di bidang **Tambah argumen**, tentukan argumennya.
   c. Klik **Tambah**.
   d. Di bidang kedua yang muncul, tentukan nilai argumen.

© Acronis International GmbH, 2003-2024

Catatan

Anda hanya dapat menentukan argumen yang telah Anda definisikan di isi skrip.

Misalnya:



e. Ulangi langkah di atas jika Anda perlu menambahkan lebih dari satu argumen.

10. Klik **Simpan**.

    Skrip disimpan ke repositori Anda dalam status **Draf**.

    Anda tidak dapat menggunakan skrip sampai administrator dengan peran **Administrator Cyber** mengubah statusnya menjadi **Disetujui**. Untuk informasi lebih lanjut, lihat "Mengubah status skrip" (hlm. 245).

    Untuk menggunakan skrip di penyewa lain yang Anda kelola, Anda harus mengklona skrip ke penyewa tersebut. Untuk informasi lebih lanjut, lihat "Membuat kloning skrip" (hlm. 243).

Membuat kloning skrip

Membuat kloning skrip diperlukan dalam kasus berikut:

- Sebelum menggunakan skrip dari **Perpustakaan**. Dalam hal ini, pertama-tama Anda harus mengklona skrip ke bagian **Skrip Saya**.
- Saat Anda ingin membuat klona skrip yang Anda buat di penyewa induk ke penyewa anak atau unitnya.

Untuk membuat klona skrip

1. Di **Repositori skrip**, cari skrip yang ingin Anda buat klonanya.
2. Lakukan salah satu langkah berikut:

© Acronis International GmbH, 2003-2024

- [Jika Anda membuat klona skrip dari **Skrip Saya**] Klik elipsis (...) di sebelah nama skrip, lalu klik **Buat klona**.
- [Jika Anda membuat klona skrip dari **Pustaka**] Klik **Buat klona** di samping nama skrip yang Anda pilih.

3. Pada pop-up **Klona skrip**, pilih salah satu status skrip berikut dari daftar drop-down **Status**:
   - **Draf** (secara default) — status ini tidak mengizinkan Anda langsung mengeksekusi skrip.
   - **Pengujian** — status ini mengizinkan Anda mengeksekusi skrip.
   - **Disetujui** — status ini mengizinkan Anda mengeksekusi skrip.
4. [Jika Anda mengelola lebih dari satu penyewa atau unit] Pilih tempat Anda ingin membuat klona skrip.

   Di kotak dialog **Klona skrip**, Anda hanya melihat penyewa yang dapat Anda kelola dan yang menerapkan paket Manajemen Tingkat Lanjut.

Akibatnya, skrip akan diklona ke bagian **Skrip Saya** dari penyewa atau unit yang Anda pilih. Jika Anda hanya mengelola satu penyewa tanpa unit di dalamnya, skrip secara otomatis disalin ke bagian **Skrip Saya**.

Penting
Kredensial yang digunakan skrip tidak disalin saat Anda membuat klona skrip ke penyewa non-asli.

Mengedit atau menghapus skrip

Catatan
Tergantung pada peran pengguna Anda, Anda dapat melakukan operasi yang berbeda dengan skrip dan rencana skrip. Untuk informasi lebih lanjut tentang peran, lihat "Peran pengguna dan hak Pembuatan Skrip Cyber" (hlm. 235).

Untuk mengedit skrip

1. Di **Repositori skrip**, buka **Skrip Saya**, lalu cari skrip yang ingin Anda edit.
2. Klik elipsis (...) di samping nama skrip, lalu klik **Edit**.
3. Edit skrip, lalu klik **Simpan**.
4. [Jika Anda mengedit skrip yang digunakan oleh rencana skrip] Konfirmasi pilihan Anda dengan mengeklik **Simpan skrip**.

   Catatan
   Versi terbaru skrip akan digunakan ketika waktu berikutnya rencana skrip berjalan.

Versi skrip

Versi baru skrip dibuat jika Anda mengedit salah satu atribut skrip berikut:

© Acronis International GmbH, 2003-2024

- isi skrip
- nama skrip
- deskripsi
- bahasa skrip
- kredensial
- argumen

Jika Anda mengubah atribut lain, hasil edit Anda akan ditambahkan ke versi skrip saat ini. Untuk mempelajari lebih lanjut tentang versi dan cara membandingkannya, lihat "Membandingkan versi skrip" (hlm. 246).

Catatan
Status skrip diperbarui hanya saat Anda mengubah nilai di bidang **Status**. Hanya administrator dengan peran administrator Cyber yang dapat mengubah status skrip.

Untuk menghapus skrip

1. Di **Repositori skrip**, buka **Skrip Saya**, lalu cari skrip yang ingin Anda hapus.
2. Klik elipsis (...) di samping nama skrip, lalu klik **Hapus**.
3. Klik **Hapus**.
4. [Jika Anda ingin menghapus skrip yang digunakan oleh rencana skrip] Konfirmasi pilihan Anda dengan mengeklik **Simpan skrip**.

   Catatan
   Rencana skrip yang menggunakan skrip yang dihapus akan gagal dijalankan.

Mengubah status skrip

Sebuah skrip baru yang dibuat dan berada dalam status **Draf** tidak dapat digunakan sampai statusnya diubah menjadi **Disetujui**. Tergantung pada kasus penggunaan, sebuah skrip mungkin berada dalam status **Pengujian** selama beberapa periode sebelum disetujui.

Catatan
Tergantung pada peran pengguna Anda, Anda dapat melakukan operasi yang berbeda dengan skrip dan rencana skrip. Untuk informasi lebih lanjut tentang peran, lihat "Peran pengguna dan hak Pembuatan Skrip Cyber" (hlm. 235).

Prasyarat

- Pengguna Anda adalah seorang administrator yang ditugaskan sebagai **Administrator Cyber**.
- Skrip dengan status yang sesuai tersedia.

Untuk mengubah status skrip

© Acronis International GmbH, 2003-2024

1. Di **Repositori Skrip**, buka **Skrip Saya**.
2. Klik elipsis (...) di samping nama skrip, lalu klik **Edit**.
3. Dalam daftar drop-down **Status**, pilih status.
4. Klik **Simpan**.
5. [Jika Anda mengubah status skrip yang sudah disetujui] Untuk mengkonfirmasi perubahan, klik **Simpan skrip**.

Catatan
Jika status skrip diturunkan versinya ke **Draf**, rencana skrip yang menggunakannya akan gagal dijalankan.
Hanya administrator dengan peran **Administrator Cyber** yang dapat menjalankan skrip dalam status **Pengujian** dan rencana skrip dengan skrip tersebut.

Membandingkan versi skrip

Anda dapat membandingkan dua versi skrip dan kembali ke versi sebelumnya. Anda juga dapat memeriksa siapa yang membuat versi tertentu, dan kapan.

Untuk membandingkan versi skrip

1. Di **Repositori skrip**, buka **Skrip Saya**, lalu cari skrip yang versinya ingin Anda bandingkan.
2. Klik elipsis (...) di samping nama skrip, lalu klik **Riwayat versi**.
3. Pilih dua versi yang ingin Anda bandingkan, lalu klik **Bandingkan versi**.
   Setiap perubahan dalam teks isi skrip, argumen, atau kredensialnya disorot.

Untuk kembali ke versi sebelumnya

1. Di jendela **Bandingkan versi skrip**, klik **Kembalikan ke versi ini**.
2. Dalam pop-up **Kembali ke versi sebelumnya**, dalam daftar drop-down **Status**, pilih status skrip.

Versi yang dipilih dipulihkan dan disimpan sebagai yang terbaru dalam riwayat versi.

Untuk memulihkan skrip, Anda juga dapat memilih versi dari jendela **Riwayat versi**, lalu klik tombol **Pulihkan**.

Penting
Anda hanya dapat menjalankan skrip dengan status **Pengujian** atau **Disetujui**. Untuk informasi lebih lanjut, lihat "Mengubah status skrip" (hlm. 245).

Mengunduh keluaran dari operasi skrip

Anda dapat mengunduh keluaran dari operasi skrip sebagai file .zip. Keluaran tersebut berisi dua file teks – `stdout` dan `stderr`. Dalam `stdout`, Anda dapat melihat hasil operasi skrip yang berhasil diselesaikan. File `stderr` berisi informasi tentang kesalahan yang terjadi selama operasi skrip.

Untuk mengunduh file keluaran

 © Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Pemantauan** > **Aktivitas**.
2. Klik aktivitas Pembuatan Skrip Cyber yang keluarannya ingin Anda unduh.
3. Pada layar **Detail aktivitas**, klik **Unduh keluaran**.

Repositori skrip

Anda dapat menemukan repositori skrip di bawah tab **Manajemen**. Di repositori, Anda dapat melakukan pencarian skrip berdasarkan nama dan deskripsinya. Anda juga dapat menggunakan filter, atau mengurutkan skrip berdasarkan nama atau statusnya.

Untuk mengelola skrip, klik elipsis (...) di samping namanya, lalu pilih tindakan yang diinginkan. Atau, klik skrip dan gunakan tombol di layar yang terbuka.

Repositori skrip berisi bagian berikut:

- **Skrip saya**

  Di sini, Anda dapat menemukan skrip yang dapat langsung Anda gunakan di lingkungan Anda. Ini adalah skrip yang Anda buat dari awal dan skrip yang Anda klona di sini.

  Anda dapat memfilter skrip di bagian ini dengan kriteria berikut:

  - Tag
  - Status
  - Bahasa
  - Sistem operasi
  - Pemilik skrip

- **Pustaka**

  Pustaka berisi skrip yang telah ditentukan sebelumnya yang dapat Anda gunakan di lingkungan setelah membuat kloning ke bagian **Skrip saya**. Anda hanya dapat memeriksa dan membuat klona skrip ini.

  Anda dapat memfilter skrip di bagian ini dengan kriteria berikut:

  - Tag
  - Bahasa
  - Sistem operasi

  Untuk informasi lebih lanjut, lihat Skrip yang Disetujui Vendor (70595).

Rencana skrip

Rencana skrip memungkinkan Anda menjalankan skrip pada banyak beban kerja, menjadwalkan menjalankan skrip, dan mengonfigurasi pengaturan tambahan.

Anda dapat menemukan rencana skrip yang Anda buat dan rencana yang diterapkan pada beban kerja Anda di **Manajemen** > **Rencana skrip**. Di sini, Anda dapat memeriksa lokasi, pemilik, atau status eksekusi rencana.

Bilah yang dapat diklik menunjukkan status berkode warna berikut untuk rencana skrip:

© Acronis International GmbH, 2003-2024

- Berjalan (Biru)
- Memeriksa kompatibilitas (Abu-abu gelap)
- Dinonaktifkan (Abu-abu terang)
- OK (Hijau)
- Peringatan kritis (Merah)
- Kesalahan (Oranye)
- Peringatan (Kuning)

Dengan mengeklik bilah, Anda dapat melihat status yang dimiliki suatu rencana dan berapa banyak beban kerja yang dimiliki. Setiap status juga dapat diklik.

Pada tab **Rencana skrip**, Anda dapat mengelola rencana dengan melakukan tindakan berikut:

- Jalankan
- Hentikan
- Edit
- Ganti nama
- Nonaktifkan
- Aktifkan
- Klona
- Ekspor. Konfigurasi rencana akan diekspor dalam format JSON ke mesin lokal.
- Hapus

Visibilitas rencana skrip dan tindakan yang tersedia dengannya bergantung pada pemilik rencana dan peran pengguna Anda. Misalnya, administrator perusahaan hanya dapat melihat rencana skrip milik mitra yang diterapkan pada beban kerja mereka, dan tidak dapat melakukan tindakan apa pun dengan rencana ini.

Untuk informasi lebih lanjut tentang siapa yang dapat membuat dan mengelola rencana skrip, lihat "Peran pengguna dan hak Pembuatan Skrip Cyber" (hlm. 235).

Untuk mengelola rencana skrip

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana skrip**.
2. Cari rencana yang ingin Anda kelola, lalu klik elipsis (...) di sebelahnya.
3. Pilih tindakan yang diinginkan, lalu ikuti petunjuk di layar.

Membuat rencana skrip

Anda dapat membuat rencana skrip dengan cara berikut:

- Pada tab **Perangkat**
  Pilih beban kerja, lalu buat rencana skrip untuk beban kerja tersebut.

© Acronis International GmbH, 2003-2024

- Pada tab **Manajemen** > **Rencana skrip**

  Buat rencana skrip, lalu pilih beban kerja tempat rencana tersebut akan diterapkan.

Untuk membuat rencana skrip pada tab Perangkat

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Pilih beban kerja atau grup perangkat tempat rencana tersebut akan diterapkan, lalu klik **Lindungi** atau **Lindungi grup**.
3. [Jika sudah ada rencana yang diterapkan] Klik **Tambahkan rencana**.
4. Klik **Buat rencana** > **Rencana skrip**.

   Sebuah templat untuk rencana skrip terbuka.
5. [Opsional] Untuk mengubah nama rencana skrip, klik ikon pensil.
6. Klik **Pilih skrip**, pilih skrip yang ingin Anda gunakan, lalu klik **Selesai**.

   Catatan
   Anda hanya dapat menggunakan skrip yang telah disetujui dari **Repositori Skrip** > **Skrip Saya**. Hanya administrator dengan peran **Administrator Cyber** yang dapat menggunakan skrip dalam status **Pengujian**. Untuk informasi lebih lanjut tentang peran, lihat "Peran pengguna dan hak Pembuatan Skrip Cyber" (hlm. 235).
7. Konfigurasikan jadwal dan syarat awal untuk rencana skrip.
8. Pilih di bawah akun mana skrip akan dijalankan pada beban kerja target. Opsi berikut tersedia:
   - Akun sistem (di macOS, ini adalah akun root)
   - Akun yang sedang log masuk
9. Tentukan berapa lama skrip dapat berjalan pada beban kerja target.

   Jika skrip tidak dapat selesai berjalan dalam jangka waktu yang ditentukan, operasi Pembuatan Skrip Cyber akan gagal.

   Nilai minimum yang dapat Anda tentukan adalah satu menit dan nilai maksimum adalah 1440 menit.
10. [Hanya untuk skrip PowerShell] Konfigurasikan kebijakan eksekusi PowerShell.

    Untuk informasi lebih lanjut tentang kebijakan ini, lihat dokumentasi Microsoft.
11. Klik **Buat**.

Untuk membuat rencana skrip pada tab Rencana skrip

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana skrip**.
2. Klik **Buat rencana**.

   Sebuah templat untuk rencana skrip terbuka.
3. [Opsional] Untuk memilih beban kerja atau grup perangkat tempat rencana baru akan diterapkan, klik **Tambahkan beban kerja**.
   a. Klik **Mesin dengan agen** untuk memperluas daftar, lalu pilih beban kerja atau grup perangkat yang diinginkan.

© Acronis International GmbH, 2003-2024

b. Klik **Tambah**.

Untuk informasi lebih lanjut tentang cara membuat grup perangkat di level mitra, lihat "Tab Perangkat" (hlm. 322).

Catatan
Anda juga dapat memilih beban kerja atau grup perangkat setelah Anda membuat rencana.

4. [Opsional] Untuk mengubah nama rencana skrip, klik ikon pensil.
5. Klik **Pilih skrip**, pilih skrip yang ingin Anda gunakan, lalu klik **Selesai**.

Catatan
Anda hanya dapat menggunakan skrip yang telah disetujui dari **Repositori Skrip** > **Skrip Saya**. Hanya administrator dengan peran **Administrator Cyber** yang dapat menggunakan skrip dalam status **Pengujian**. Untuk informasi lebih lanjut tentang peran, lihat "Peran pengguna dan hak Pembuatan Skrip Cyber" (hlm. 235).

6. Konfigurasikan jadwal dan syarat awal untuk rencana skrip.
7. Pilih di bawah akun mana skrip akan dijalankan pada beban kerja target. Opsi berikut tersedia:
   - Akun sistem (di macOS, ini adalah akun root)
   - Akun yang sedang log masuk
8. Tentukan berapa lama skrip dapat berjalan pada beban kerja target.
   Jika skrip tidak dapat selesai berjalan dalam jangka waktu yang ditentukan, operasi Pembuatan Skrip Cyber akan gagal.
   Nilai minimum yang dapat Anda tentukan adalah satu menit dan nilai maksimum adalah 1440 menit.
9. [Hanya untuk skrip PowerShell] Konfigurasikan kebijakan eksekusi PowerShell.
   Untuk informasi lebih lanjut tentang kebijakan ini, lihat dokumentasi Microsoft.
10. Klik **Buat**.

Jadwal dan syarat mulai

Jadwal

Anda dapat mengonfigurasi rencana skrip untuk dijalankan sekali atau berulang kali, dan untuk memulainya sesuai jadwal atau dipicu oleh peristiwa tertentu.

Opsi berikut tersedia:

- Jalankan sekali
  Untuk opsi ini, Anda harus mengonfigurasi tanggal dan waktu saat rencana akan berjalan.
- Jadwalkan berdasarkan waktu
  Dengan opsi ini, Anda dapat mengonfigurasi rencana skrip yang berjalan setiap jam, harian, atau bulanan.

© Acronis International GmbH, 2003-2024

Untuk membuat jadwal hanya efektif sementara, pilih kotak centang **Jalankan dalam rentang tanggal**, lalu konfigurasikan periode saat rencana terjadwal akan berjalan.

- Ketika pengguna masuk ke sistem

  Anda dapat memilih apakah pengguna tertentu atau pengguna mana pun yang masuk akan memicu rencana skrip.
- Ketika pengguna keluar dari sistem

  Anda dapat memilih apakah pengguna tertentu atau pengguna mana pun yang keluar akan memicu rencana skrip.
- Pada startup sistem
- Saat sistem dimatikan

  Catatan
  Opsi penjadwalan ini hanya berfungsi dengan skrip yang berjalan di bawah akun sistem.
- Saat sistem online

Persyaratan untuk memulai

Syarat mulai menambahkan lebih banyak fleksibilitas pada rencana terjadwal Anda. Jika Anda mengonfigurasi beberapa syarat, semuanya harus dipenuhi secara bersamaan agar rencana dapat dimulai.

Persyaratan untuk memulai menjadi tidak efektif jika Anda menjalankan rencana secara manual, dengan menggunakan opsi **Jalankan sekarang**.

Syarat	Deskripsi
Jalankan hanya jika beban kerja daring	Skrip akan berjalan ketika beban kerja target terhubung ke Internet.
Pengguna idle	Syarat ini terpenuhi ketika screen saver berjalan pada mesin atau mesin terkunci.
Pengguna telah keluar	Dengan syarat ini, Anda dapat menunda rencana skrip terjadwal hingga pengguna beban kerja target keluar.
Sesuai interval waktu	Dengan syarat ini, rencana skrip hanya dapat dimulai dalam interval waktu yang ditentukan. Misalnya, Anda dapat menggunakan syarat ini untuk membatasi syarat **Pengguna telah keluar**.
Hemat daya baterai	Dengan syarat ini, Anda dapat memastikan bahwa rencana skrip tidak akan terganggu karena baterai lemah. Opsi berikut tersedia: • Jangan dimulai ketika memakai daya baterai Rencana akan dimulai hanya jika mesin terhubung ke sumber listrik. • Mulai ketika memakai daya baterai jika level baterai lebih tinggi dari Rencana akan dimulai jika mesin terhubung ke sumber listrik atau jika tingkat baterai lebih tinggi dari nilai yang ditentukan.

© Acronis International GmbH, 2003-2024

Syarat	Deskripsi
Jangan memulai koneksi bermeter	Syarat ini mencegah rencana dimulai jika beban kerja target mengakses Internet melalui koneksi bermeter.
Jangan dimulai ketika terkoneksi ke jaringan Wi-Fi berikut	Syarat ini mencegah rencana dimulai jika beban kerja target terhubung ke salah satu jaringan nirkabel yang ditentukan. Untuk menggunakan syarat ini, Anda harus menentukan SSID jaringan terlarang. Pembatasan berlaku untuk semua jaringan yang berisi nama yang ditetapkan sebagai substring pada nama mereka, tidak sensitif huruf besar/kecil. Misalnya, jika Anda menentukan `phone` sebagai nama jaringan, rencana tidak akan dimulai saat perangkat terhubung ke salah satu jaringan berikut: `John's iPhone`, `phone_wifi`, atau `my_PHONE_wifi`.
Cek alamat IP perangkat	Syarat ini mencegah rencana dimulai jika salah satu alamat IP dari beban kerja target berada di dalam atau di luar rentang alamat IP yang ditentukan. Opsi berikut tersedia: • Mulai jika di luar rentang IP • Mulai jika di dalam rentang IP Hanya mendukung alamat IPv4.
Jika persyaratan untuk memulai tidak terpenuhi, tetap jalankan tugas	Opsi ini memungkinkan Anda untuk mengatur interval waktu setelah rencana akan berjalan, terlepas dari syarat lainnya. Rencana akan dimulai segera setelah syarat lain terpenuhi atau periode yang ditentukan berakhir, mana pun yang terlebih dahulu tercapai. Opsi ini tidak tersedia jika Anda mengonfigurasi rencana skrip untuk dijalankan hanya sekali.

Mengelola beban kerja target untuk rencana

Anda dapat memilih beban kerja atau grup perangkat yang akan menerapkan rencana skrip saat Anda membuat rencana, atau nanti.

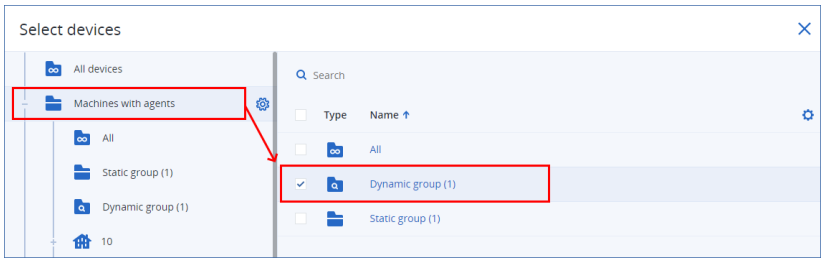
Administrator mitra dapat menerapkan rencana yang sama untuk beban kerja dari pelanggan yang berbeda, dan dapat membuat grup perangkat yang berisi beban kerja dari pelanggan yang berbeda. Untuk mempelajari cara membuat grup perangkat statis atau dinamis di level mitra, lihat "Tab Perangkat" (hlm. 322).

Untuk menambahkan beban kerja awal ke rencana

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana skrip**.
2. Klik nama rencana yang ingin Anda tentukan beban kerja targetnya.
3. Klik **Tambahkan beban kerja**.
4. Pilih beban kerja atau grup perangkat yang diinginkan, lalu klik **Tambahkan**.

© Acronis International GmbH, 2003-2024

Catatan
Untuk memilih grup perangkat, klik level induknya, lalu, di panel utama, pilih kotak centang di samping namanya.



5. Untuk menyimpan rencana yang telah diedit, klik **Simpan**.

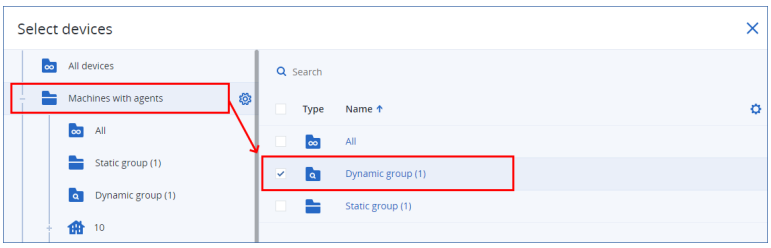
Untuk mengelola beban kerja yang ada untuk rencana

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana skrip**.
2. Klik nama rencana yang ingin Anda ubah target beban kerjanya.
3. Klik **Kelola beban kerja**.

   Layar **Perangkat** mencantumkan beban kerja yang saat ini diterapkan rencana skrip. Jika Anda mengelola lebih dari satu penyewa, beban kerja diurutkan berdasarkan penyewa.

   - Untuk menambahkan beban kerja atau grup perangkat baru, klik **Tambahkan**.
     a. Pilih beban kerja atau grup perangkat yang diinginkan. Anda dapat menambahkan beban kerja dari semua penyewa yang Anda kelola.

     Catatan
     Untuk memilih grup perangkat, klik level induknya, lalu, di panel utama, pilih kotak centang di samping namanya.

     b. Klik **Tambah**.
   - Untuk menghapus beban kerja atau grup perangkat, pilih yang akan dihapus, lalu klik **Hapus**.
4. Klik **Selesai**.
5. Untuk menyimpan rencana yang telah diedit, klik **Simpan**.

Rencana pada level administrasi yang berbeda

Tabel berikut merangkum rencana mana yang dapat dilihat dan dikelola oleh administrator dari berbagai level.

© Acronis International GmbH, 2003-2024

Administrator	Level administrasi	Rencana	Hak
Administrator mitra	Level mitra	Rencana sendiri	Akses penuh
		Rencana pelanggan (termasuk rencana dalam unit)	Akses penuh
		Rencana unit	Akses penuh
	Layanan pelanggan (untuk pelanggan yang dikelola oleh penyedia layanan)	Rencana mitra yang diterapkan pada beban kerja pelanggan ini	Hanya baca
		Rencana pelanggan (termasuk rencana dalam unit)	Akses penuh
		Rencana unit	Akses penuh
	Level unit (untuk pelanggan yang dikelola oleh penyedia layanan)	Rencana mitra yang diterapkan pada beban kerja unit ini	Hanya baca
		Rencana pelanggan yang diterapkan pada beban kerja unit ini	Hanya baca
		Rencana unit	Akses penuh
Administrator perusahaan	Layanan pelanggan	Rencana mitra yang diterapkan pada beban kerja pelanggan atau unit ini	Hanya baca
		Rencana pelanggan (termasuk rencana dalam unit)	Akses penuh
		Rencana unit	Akses penuh
	Level unit	Rencana mitra yang diterapkan pada beban kerja unit ini	Hanya baca
		Rencana pelanggan yang diterapkan pada beban kerja unit ini	Hanya baca
		Rencana unit	Akses penuh
Administrator unit	Level unit	Rencana mitra yang diterapkan pada beban kerja unit ini	Hanya baca
		Rencana pelanggan yang diterapkan pada beban kerja unit ini	Hanya baca

© Acronis International GmbH, 2003-2024

Administrator	Level administrasi	Rencana	Hak
		Rencana unit	Akses penuh

Penting
Pemilik rencana adalah penyewa tempat rencana itu dibuat. Jadi, jika administrator mitra membuat rencana di level penyewa pelanggan, penyewa pelanggan adalah pemilik rencana tersebut.

Masalah kompatibilitas dengan rencana skrip

Dalam beberapa kasus, menerapkan rencana skrip pada beban kerja dapat menyebabkan masalah kompatibilitas. Anda mungkin mengamati masalah kompatibilitas berikut:

- Sistem operasi tidak kompatibel – masalah ini muncul ketika sistem operasi beban kerja tidak didukung.
- Agen tidak didukung – masalah ini muncul ketika versi agen perlindungan pada beban kerja kedaluwarsa dan tidak mendukung fungsi Pembuatan Skrip Cyber.
- Kuota tidak memadai – masalah ini muncul ketika tidak ada kuota layanan yang cukup pada penyewa untuk ditetapkan ke beban kerja yang dipilih.

Jika rencana skrip diterapkan ke hingga 150 beban kerja yang dipilih secara terpisah, Anda akan diminta untuk menyelesaikan konflik yang ada sebelum menyimpan rencana tersebut. Untuk menyelesaikan konflik, hapus akar penyebabnya atau hapus beban kerja yang terdampak dari rencana. Untuk informasi lebih lanjut, lihat "Memecahkan masalah kompatibilitas dengan rencana skrip" (hlm. 255). Jika Anda menyimpan rencana tanpa menyelesaikan konflik, rencana akan otomatis dinonaktifkan untuk beban kerja yang tidak kompatibel dan peringatan akan ditampilkan.

Jika rencana skrip diterapkan ke lebih dari 150 beban kerja atau ke grup perangkat, rencana tersebut akan disimpan dan diperiksa kompatibilitasnya. Rencana akan otomatis dinonaktifkan untuk beban kerja yang tidak kompatibel, dan peringatan akan ditampilkan.

Memecahkan masalah kompatibilitas dengan rencana skrip

Bergantung pada penyebab masalah kompatibilitas, Anda dapat melakukan berbagai tindakan untuk menyelesaikan masalah sebagai bagian dari proses membuat rencana skrip baru.

Catatan
Saat memecahkan masalah kompatibilitas dengan menghapus beban kerja dari suatu rencana, Anda tidak dapat menghapus beban kerja yang menjadi bagian dari grup perangkat.

Cara menyelesaikan masalah kompatibilitas

1. Klik **Tinjau masalah**.
2. [Untuk menyelesaikan masalah kompatibilitas dengan sistem operasi yang tidak kompatibel]

© Acronis International GmbH, 2003-2024

a. Pada tab **Sistem operasi yang tidak kompatibel**, pilih beban kerja yang ingin Anda hapus.

b. Klik **Hapus beban kerja dari rencana**.

c. Klik **Hapus**, lalu klik **Tutup**.

3. [Untuk menyelesaikan masalah kompatibilitas agen yang tidak didukung dengan menghapus beban kerja dari rencana]

   a. Pada tab **Agen yang tidak didukung**, pilih beban kerja yang ingin Anda hapus.

   b. Klik **Hapus beban kerja dari rencana**.

   c. Klik **Hapus**, lalu klik **Tutup**.

4. [Untuk menyelesaikan masalah kompatibilitas agen yang tidak didukung dengan memperbarui versi agen] Klik **Buka daftar Agen**.

   Catatan
   Opsi ini hanya tersedia untuk administrator pelanggan.

5. [Untuk menyelesaikan masalah kompatibilitas kuota tidak memadai dengan menghapus beban kerja dari rencana]

   a. Pada tab **Kuota tidak memadai**, pilih beban kerja yang ingin Anda hapus.

   b. Klik **Hapus beban kerja dari rencana**.

   c. Klik **Hapus**, lalu klik **Tutup**.

6. [Untuk menyelesaikan masalah kompatibilitas kuota tidak memadai dengan meningkatkan kuota penyewa]

   Catatan
   Opsi ini hanya tersedia untuk administrator mitra.

   a. Pada tab **Kuota tidak memadai**, klik **Buka portal manajemen**.

   b. Tingkatkan layanan kuota untuk pelanggan.

Jalankan cepat skrip

Anda dapat langsung menjalankan skrip, tanpa mengikutsertakannya dalam rencana skrip. Anda tidak dapat menggunakan operasi ini pada lebih dari 150 beban kerja, pada beban kerja offline, atau pada grup perangkat.

Kuota layanan harus ditetapkan pada beban kerja target yang mendukung fungsionalitas menjalankan cepat skrip, dan paket Manajemen Tingkat Lanjut harus diaktifkan untuk penyewanya. Kuota layanan yang sesuai akan ditetapkan secara otomatis jika tersedia di penyewa.

© Acronis International GmbH, 2003-2024

Catatan
Anda hanya dapat menggunakan skrip yang telah disetujui dari **Repositori Skrip** > **Skrip Saya**. Hanya administrator dengan peran **Administrator Cyber** yang dapat menggunakan skrip dalam status **Pengujian**. Untuk informasi lebih lanjut tentang peran, lihat "Peran pengguna dan hak Pembuatan Skrip Cyber" (hlm. 235).

Anda dapat memulai jalankan cepat dengan cara berikut:

- Dari tab **Perangkat**
  Pilih satu atau beberapa beban kerja, lalu pilih skrip mana yang akan dijalankan.
- Dari tab **Manajemen** > **Repositori skrip**
  Pilih skrip, lalu pilih satu atau beberapa beban kerja target.

Untuk menjalankan skrip dari tab Perangkat

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih beban kerja tempat Anda ingin menjalankan skrip, lalu klik **Lindungi**.
3. Klik **Jalankan cepat skrip**.
4. Klik **Pilih skrip**, pilih skrip yang ingin Anda gunakan, lalu klik **Selesai**.
5. Pilih di bawah akun mana skrip akan dijalankan pada beban kerja target. Opsi berikut tersedia:
   - Akun sistem (di macOS, ini adalah akun root)
   - Akun yang sedang log masuk
6. Tentukan berapa lama skrip dapat berjalan pada beban kerja target.
   Jika skrip tidak dapat selesai berjalan dalam jangka waktu yang ditentukan, operasi Skrip Cyber akan gagal.
   Anda dapat menggunakan nilai antara 1 hingga 1440 menit.
7. [Hanya untuk skrip PowerShell] Konfigurasikan kebijakan eksekusi PowerShell.
   Untuk informasi lebih lanjut tentang kebijakan ini, lihat dokumen Microsoft.
8. Klik **Jalankan sekarang**.

Untuk menjalankan skrip dari tab repositori Skrip

1. Di konsol Cyber Protect, buka **Manajemen** > **Repositori skrip**.
2. Pilih skrip yang ingin Anda jalankan, lalu klik **Jalankan cepat skrip**.
3. Klik **Tambahkan beban kerja** untuk memilih beban kerja target, lalu klik **Tambahkan**.
4. Klik **Pilih skrip**, pilih skrip yang ingin Anda gunakan, lalu klik **Selesai**.
5. Pilih di bawah akun mana skrip akan dijalankan pada beban kerja target. Opsi berikut tersedia:
   - Akun sistem (di macOS, ini adalah akun root)
   - Akun yang sedang log masuk
6. Tentukan berapa lama skrip dapat berjalan pada beban kerja target.

© Acronis International GmbH, 2003-2024

Jika skrip tidak dapat selesai berjalan dalam jangka waktu yang ditentukan, operasi Skrip Cyber akan gagal.

Anda dapat menggunakan nilai antara 1 hingga 1440 menit.

7. [Hanya untuk skrip PowerShell] Konfigurasikan kebijakan eksekusi PowerShell.

   Untuk informasi lebih lanjut tentang kebijakan ini, lihat dokumen Microsoft.
8. Klik **Jalankan sekarang**.

Perlindungan aplikasi kolaborasi dan komunikasi

Zoom, Cisco Webex Meetings, Citrix Workspace, dan Microsoft Teams saat ini digunakan secara luas untuk konferensi video/web dan komunikasi. Layanan Cyber Protection memungkinkan Anda untuk melindungi alat bantu kolaborasi Anda.

Perlindungan untuk Zoom, Cisco Webex Meetings, Citrix Workspace, dan Microsoft Teams menggunakan konfigurasi yang sama. Pada contoh berikut ini, kami akan menunjukkan konfigurasi untuk Zoom.

Untuk mengatur perlindungan Zoom

1. Instal agen perlindungan pada mesin yang mana aplikasi kolaborasi diinstal.
2. Masuk ke konsol Cyber Protect dan terapkan paket perlindungan yang mengaktifkan salah satu modul berikut:
   - **Perlindungan Antivirus dan Antimalware** (dengan pengaturan **Perlindungan Diri** dan **Active Protection** diaktifkan) – jika Anda memiliki salah satu edisi Cyber Protect.
   - **Active Protection** (dengan pengaturan **Perlindungan Diri** diaktifkan) – jika Anda memiliki salah satu edisi Cyber Backup.
3. [Opsional] Untuk instalasi pembaruan otomatis, konfigurasikan modul **Manajemen patch** dalam rencana proteksi.

Hasilnya, aplikasi Zoom Anda akan terlindungi yang mencakup aktivitas berikut ini:

- Menginstal pembaruan klien Zoom secara otomatis
- Melindungi proses Zoom dari injeksi kode
- Mencegah operasi mencurigakan pada proses Zoom
- Melindungi file "host" dari menambahkan domain yang terkait dengan Zoom

© Acronis International GmbH, 2003-2024

Memahami tingkat proteksi Anda saat ini

Pemantauan

Tab **Pemantauan** tab memberikan informasi penting tentang tingkat perlindungan Anda saat ini, dan mencakup dasbor berikut:

- **Gambaran umum**
- **Aktivitas**
- **Peringatan**
- **Umpan ancaman** (untuk informasi lebih lanjut, lihat "Umpan ancaman" (hlm. 301))

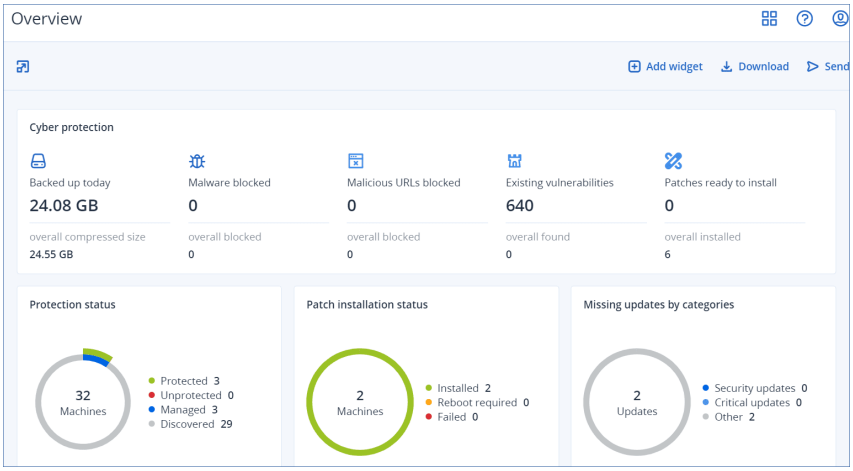
Dasbor Ikhtisar

Dasbor **Ikhtisar** menyediakan sejumlah widget kustom yang memberikan ikhtisar operasi terkait dengan layanan Cyber Protection. Widget untuk layanan lain akan tersedia di rilis mendatang.

Widget diperbarui setiap lima menit. Widget memiliki elemen yang dapat diklik sehingga memungkinkan Anda untuk menyelidiki dan menyelesaikan masalah. Anda dapat mengunduh status dasbor saat ini atau mengirimnya melalui email dalam format .pdf atau/dan .xlsx.

Anda dapat memilih dari berbagai macam widget, yang disajikan sebagai tabel, diagram lingkaran, diagram batang, daftar, dan peta pohon. Anda dapat menambahkan beberapa widget yang jenisnya sama dengan filter yang berbeda.

Tombol **Unduh** dan **Kirim** di **Pemantauan** > **Ikhtisar** tidak tersedia di edisi Standar layanan Cyber Protection.



Untuk mengatur ulang widget di dasbor

Seret dan lepaskan widget dengan mengklik namanya.

Untuk mengedit widget

© Acronis International GmbH, 2003-2024

Klik ikon pensil di sebelah nama widget. Pengeditan widget memungkinkan Anda untuk mengganti nama, mengubah rentang waktu, mengatur filter, dan mengelompokkan baris.

Untuk menambahkan widget

Klik **Tambah widget**, lalu lakukan salah satu cara berikut:

- Klik widget yang ingin Anda tambahkan. Widget akan ditambahkan dengan pengaturan default.
- Untuk mengedit widget sebelum menambahkannya, klik Sesuaikan saat widget dipilih. Setelah mengedit widget, klik **Selesai**.

Untuk menghapus widget

Klik ikon tanda X di sebelah nama widget.

Dasbor Aktivitas

Dasbor **Aktivitas** memberikan ikhtisar tentang aktivitas lampau dan saat ini. Secara default, periode retensi adalah 90 hari.

Untuk menyesuaikan tampilan dasbor **Aktivitas**, klik ikon roda gigi, lalu pilih kolom yang ingin Anda lihat.

Untuk melihat kemajuan aktivitas secara real time, pilih kotak centang **Refresh otomatis**. Namun, seringnya memperbarui beberapa aktivitas menurunkan kinerja server manajemen.

Anda dapat mencari aktivitas yang terdaftar dengan kriteria berikut:

- **Nama perangkat**
  Ini adalah mesin tempat aktivitas dilakukan.
- **Dimulai oleh**
  Ini adalah akun yang memulai aktivitas.

Anda juga dapat menyaring dengan properti berikut:

- **Status**
  Misalnya, berhasil, gagal, sedang berlangsung, dibatalkan.
- **Tipe**
  Misalnya, menerapkan rencana, menghapus cadangan, menginstal pembaruan perangkat lunak.
- **Waktu**
  Misalnya, aktivitas terbaru, aktivitas 24 jam terakhir, atau aktivitas selama periode tertentu dalam periode retensi default.

Untuk melihat detail lebih lanjut tentang suatu aktivitas, pilih aktivitas ini dari daftar, lalu dalam panel **Detail aktivitas**, klik **Semua properti**. Untuk informasi lebih lanjut tentang properti yang tersedia, lihat referensi API Aktivitas dan Tugas dalam Portal Jaringan Developer.

© Acronis International GmbH, 2003-2024

Dasbor Peringatan

Dasbor **Peringatan** menampilkan semua peringatan Anda saat ini. Peringatan yang tercantum adalah peringatan kritis atau kesalahan, dan biasanya terkait dengan tugas-tugas seperti pencadangan yang gagal karena beberapa alasan.

Untuk memfilter peringatan pada dasbor

1. Dari daftar drop-down **Tampilan**, pilih salah satu dari kriteria berikut:
   - **Keparahan peringatan**
   - **Kategori peringatan**
   - **Tipe peringatan**
   - **Tipe pemantauan**
   - **Rentang tanggal: dari ... ke ...**
   - **Beban kerja**
   - **Rencana**
   - **Pelanggan**
2. Jika Anda telah memilih **kategori Peringatan**, dari daftar drop-down **Kategori**, pilih kategori peringatan yang ingin Anda lihat.
3. Jika Anda ingin melihat semua peringatan tanpa filter, klik **Semua jenis peringatan**.

Di dalam setiap peringatan, Anda dapat melakukan hal berikut:

- Akses perangkat terkait yang berhubungan dengan peringatan dengan mengeklik tautan **Peralatan**.
- Baca dan coba ikuti beberapa saran di bagian **Penyelesaian Masalah** pada peringatan.
- Akses dokumentasi yang relevan dan artikel basis pengetahuan dengan mengeklik **Cari solusi**. Fungsionalitas **Cari solusi** akan mengisi permintaan Anda terlebih dahulu mengenai detail peringatan saat ini untuk membantu Anda secara efektif.

Untuk menyortir peringatan pada dasbor

Di tabel peringatan, klik tombol panah di samping salah satu nama kolom berikut:

- **Keparahan peringatan**
- **Tipe peringatan**
- **Dibuat**
- **Kategori peringatan**
- **Beban kerja**
- **Rencana**

© Acronis International GmbH, 2003-2024

Jenis peringatan

Peringatan akan dibuat untuk jenis peringatan berikut ini:

- Peringatan cadangan
- Peringatan pemulihan bencana
- Peringatan proteksi antimalware
- Peringatan pelisensian
- Peringatan pemfilteran URL
- Peringatan EDR
- Peringatan Kontrol Perangkat
- Peringatan sistem

Peringatan cadangan

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Pencadangan gagal	Peringatan dibuat ketika pencadangan gagal dengan kesalahan yang dapat diatasi ketika sedang berjalan atau terputus karena sistem dimatikan.	Periksa log operasi pencadangan yang salah: klik beban kerja untuk memilihnya, klik **Aktivitas**, lalu temukan peringatan dalam log. Pesan tersebut akan mengarahkan Anda ke akar masalah yang diberitahukan oleh perangkat lunak.
Pencadangan berhasil dengan peringatan	Peringatan dibuat ketika pencadangan berhasil dengan peringatan.	Periksa log konversi ke VM, replikasi, atau rencana validasi. Masalah selama operasi ini menghasilkan peringatan "Aktivitas gagal" atau "Aktivitas selesai dengan peringatan".
Pencadangan dibatalkan	Peringatan dibuat setiap kali aktivitas pencadangan dibatalkan secara manual oleh pengguna.	Anda dapat memulai pencadangan secara manual dengan mengeklik Jalankan sekarang atau menunggu hingga pencadangan berjalan pada waktu yang dijadwalkan berikutnya.
Operasi dibatalkan karena jendela pencadangan tertutup	Peringatan akan muncul ketika aktivitas pencadangan tidak dapat dilakukan karena tidak sesuai dengan jendela yang ditentukan dalam opsi pencadangan.	Konfigurasikan ulang jadwal atau edit opsi rencana pencadangan di jendela **Performa dan pencadangan**. Perluas bagian yang memuat produk Anda untuk mendapatkan petunjuk.

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Pencadangan sedang menunggu	Peringatan ini dibuat kapan pun Anda mengalami konflik penjadwalan dan dua tugas pencadangan dimulai pada saat yang bersamaan. Dalam kasus ini, tugas pencadangan kedua akan menunggu antrean sampai tugas pertama selesai atau dihentikan.	Pastikan bahwa cadangan Anda berjalan pada jendela waktu yang diharapkan dan sesuai dengan jadwalnya, dan hindari konflik penjadwalan jika memungkinkan.
Pencadangan tidak merespons	Peringatan akan muncul jika pencadangan yang sedang berjalan tidak menunjukkan kemajuan apa pun selama beberapa waktu, dan mungkin dibekukan.	Masalah ini mungkin disebabkan oleh penguncian. Ikuti artikel ini untuk mengumpulkan informasi pemecahan masalah yang diperlukan.
Pencadangan tidak dimulai	Peringatan dibuat ketika pencadangan terjadwal gagal dimulai karena alasan yang tidak diketahui.	Pastikan Anda menggunakan build terbaru dari produk Acronis Backup Anda. • Jika mesin agen tersedia selama waktu mulai pencadangan: 1. Edit waktu mulai tugas pencadangan. 2. Jika peringatan muncul lagi, buat ulang tugas pencadangan. 3. Jika tugas pencadangan yang baru dibuat juga memicu peringatan, hubungi Acronis Support untuk mendapatkan bantuan. • Jika agen sedang offline: 1. Jangan matikan mesin selama waktu pencadangan. 2. Jika mesin tidak dimatikan, pastikan Acronis Managed Machine Service berjalan: Mulai -> Cari -> services.msc -> cari Acronis Managed Machine Service. Hubungi Acronis Support, jika Anda membutuhkan bantuan.
Status pencadangan tidak diketahui	Peringatan dibuat ketika agen pencadangan offline pada	1. Periksa apakah agen diharapkan dalam keadaan offline (misalnya,

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
	waktu pencadangan yang dijadwalkan. Status cadangan sumber daya tidak akan diketahui hingga agen cadangan online.	notebook yang berada di luar jaringan Server Manajemen). 2. Jika agen tidak boleh offline, pastikan Acronis Managed Machine Service berjalan: Mulai -> Cari -> services.msc -> cari Acronis Managed Machine Service dan periksa statusnya. Mulai layanannya, jika masih berhenti.
Cadangan hilang	Peringatan dibuat ketika tidak ada pencadangan yang berhasil selama lebih dari [Hari dari pencadangan terakhir] hari.	
Pencadangan rusak	Peringatan akan muncul ketika aktivitas validasi berhasil dan menunjukkan bahwa cadangan rusak.	Ikuti langkah-langkah dari artikel Memecahkan Masalah dengan Cadangan yang Rusak. Jika Anda memerlukan bantuan untuk mengidentifikasi akar penyebab kerusakan arsip, hubungi Acronis Support.
Perlindungan Data Berkelanjutan gagal	Peringatan dibuat jika perlindungan pencadangan berkelanjutan gagal.	Perhatikan batasan berikut: 1. Perlindungan data berkelanjutan didukung hanya untuk sistem file NTFS dan sistem operasi berikut: • Desktop: Windows 7 dan versi lebih baru • Server: Windows Server 2008 R2 dan versi lebih baru 2. CDP tidak mendukung **Acronis Secure Zone** sebagai tujuan. 3. Folder NFS yang dipasang pada Windows tidak didukung. 4. Replikasi berkelanjutan tidak didukung: jika ada dua lokasi dalam rencana proteksi, irisan CDP dibuat hanya di tujuan pertama, dan kemudian perubahannya direplikasi ke lokasi kedua dengan cadangan berikutnya.

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
		5. Jika perubahan pada folder yang diproteksi lokal diterapkan dari sumber jaringan (misalnya saat pengguna mengakses folder dari jaringan), CDP tidak mendeteksinya. 6. Jika sebuah file sedang digunakan, misalnya beberapa perubahan sedang dilakukan pada file Excel, CDP tidak mendeteksi perubahan tersebut. Agar perubahan terdeteksi oleh CDP, simpan perubahan tersebut dan tutup file.
Konfigurasi host Hyper-V tidak valid	Peringatan dibuat ketika ada 2 atau lebih Agen untuk Hyper-V yang diinstal pada host Hyper-V dengan nama host yang sama, yang tidak didukung pada tingkat akun yang sama.	Anda harus mendaftarkan Agen ini untuk Hyper-V di bawah unit anak yang berbeda dari akun ini untuk menghindari konflik.
Validasi gagal	Peringatan akan muncul ketika proses validasi cadangan Anda tidak dapat diselesaikan.	Periksa log operasi yang salah: klik mesin untuk memilihnya, klik **Aktivitas**, lalu temukan peringatan dalam log. Pesan tersebut akan mengarahkan Anda ke akar masalah yang diberitahukan oleh perangkat lunak.
Gagal memigrasi cadangan di penyimpanan awan ke format baru	Peringatan akan muncul ketika gagal memigrasikan cadangan di penyimpanan awan ke format baru.	Migrasi arsip Acronis Cyber Backup Advanced dijelaskan di sini. Migrasi arsip Acronis Cyber Backup dijelaskan di sini. Sebelum menghubungi Acronis Support, silakan kumpulkan laporan berikut ini dengan menggunakan alat bantu migrate_archives: **migrate_archives.exe --account=<Acronis Account> --password=<password> --subaccounts=All > report1.txt** **migrate_archives.exe --cmd=finishUpgrade --**

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
		account=<Acronis Account> --password=<password> > report2.txt
Enkripsi kata sandi hilang	Peringatan akan muncul ketika kode enkripsi basis data salah, rusak, atau hilang.	Tidak ada cara untuk memulihkan cadangan terenkripsi jika Anda menghilangkan atau lupa kata sandi. Anda harus mengatur kata sandi enkripsi secara lokal pada perangkat yang dilindungi. Anda tidak dapat menetapkan kata sandi enkripsi di rencana proteksi Untuk informasi lebih lanjut, lihat Mengatur kata sandi enkripsi.
Pengunggahan tertunda	Peringatan dibuat jika pemeriksaan terjadwal menemukan bahwa Pengiriman Data Fisik ke arsip awan untuk rencana pencadangan ini tidak diunggah ke penyimpanan.	
Pemulihan cadangan gagal	Peringatan akan muncul bila operasi pemulihan gagal saat Anda mencoba memulihkan file atau cadangan sistem.	Tentukan tanggal pasti dari kegagalan pencadangan dan coba lakukan pemulihan dengan pencadangan terakhir yang berhasil.

Peringatan pemulihan bencana

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Kuota penyimpanan terlampaui	Peringatan dibuat ketika kuota lunak terlampaui untuk penyimpanan pemulihan bencana	Tambah kuota atau hapus beberapa arsip dari penyimpanan awan.
Kuota tercapai	Peringatan akan muncul ketika: • Kuota lunak terlampaui untuk server awan. • Kuota lunak terlampaui untuk titik komputasi. • Kuota lunak terlampaui untuk alamat IP publik.	
Kuota penyimpanan	Peringatan akan muncul ketika kuota	

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
terlampaui	keras terlampaui untuk penyimpanan pemulihan bencana. Penyimpanan ini digunakan oleh server utama dan server pemulihan. Jika kelebihan untuk kuota ini terlampaui, tidak dimungkinkan untuk membuat server utama dan pemulihan, atau menambah/memperluas disk server utama yang sudah ada. Jika kelebihan untuk kuota ini terlampaui, tidak dimungkinkan untuk memulai failover atau hanya memulai server yang terhenti. Server yang sedang berjalan akan tetap berjalan.	
Kuota terlampaui	Peringatan akan muncul ketika: • Kuota keras terlampaui untuk server awan. • Kuota keras terlampaui untuk titik komputasi. • Kuota keras terlampaui untuk alamat IP publik.	Pertimbangkan untuk membeli kuota perangkat tambahan atau menonaktifkan tugas pencadangan untuk perangkat yang tidak perlu Anda lindungi lagi.
Kesalahan failover	Peringatan dibuat ketika masalah sistem terjadi setelah tindakan fail-over dikirimkan.	1. Klik **Edit** pada server pemulihan. Untuk informasi lebih lanjut, lihat Membuat server pemulihan. 2. Kurangi CPU/RAM untuk server pemulihan. 3. Coba lakukan failover lagi.
Uji kesalahan failover	Peringatan akan muncul ketika masalah sistem terjadi setelah tindakan pengujian dikirimkan.	1. Klik **Edit** pada server pemulihan. Untuk informasi lebih lanjut, lihat Membuat server pemulihan. 2. Kurangi CPU/RAM untuk server pemulihan. 3. Coba lakukan failover lagi.

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
		Catatan Pastikan alamat IP dalam alamat IP di jaringan produksi sama dengan alamat IP yang dikonfigurasi di server DHCP.
Kesalahan failback	Peringatan dibuat ketika masalah sistem terjadi setelah fail-back dimulai.	Anda dapat melihat lokasi yang salah di daftar penyimpanan cadangan: lokasi tersebut memiliki nomor, bukan nama (biasanya, nama lokasi cocok dengan salah satu nama pengguna akhir yang ada) dan Anda belum membuat lokasi ini. Hapus lokasi yang salah: 1. Di konsol Cyber Protect, arahkan ke Penyimpanan Cadangan. 2. Temukan lokasinya dan klik ikon silang (x) untuk menghapusnya. 3. Konfirmasikan pilihan Anda dengan mengeklik Hapus. 4. Coba lagi failover.
Failback dibatalkan	Peringatan akan muncul ketika failback dibatalkan oleh pengguna.	Menutup peringatan secara manual dari konsol.
Kesalahan koneksi VPN	Peringatan dibuat ketika kegagalan koneksi VPN terjadi karena alasan yang tidak bergantung pada tindakan pengguna. Laporan status dari alat VPN sudah kedaluwarsa.	Jika Anda menghadapi masalah dalam menerapkan atau menghubungkan alat Acronis VPN, silakan hubungi Acronis Support. Mohon kirimkan informasi berikut ini melalui email Anda: • Tangkapan layar dari pesan kesalahan (jika ada) • Tangkapan layar antarmuka CLI Acronis VPN Appliance • Pusat data Acronis Backup Cloud dan nama grup Anda.
(Vpn Tidak Dapat Dijangkau)	Peringatan akan muncul ketika	Jika Anda menghadapi masalah

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Gateway konektivitas tidak dapat dijangkau	layanan DR tidak dapat mencapai gateway konektivitas. Laporan status dari gateway konektivitas sudah kedaluwarsa.	dalam menerapkan atau menghubungkan alat Acronis VPN, silakan hubungi Acronis Support. Mohon kirimkan informasi berikut ini melalui email Anda: • Tangkapan layar dari pesan kesalahan (jika ada) • Tangkapan layar antarmuka CLI Acronis VPN Appliance • Pusat data Acronis Backup Cloud dan nama grup Anda
Diperlukan penetapan ulang IP DR	Peringatan akan muncul jika alat VPN mendeteksi perubahan jaringan.	Tetapkan kembali alamat IP. Untuk informasi lebih lanjut, lihat Menetapkan ulang alamat IP.
Kegagalan gateway konektivitas	Peringatan akan muncul ketika gagal menggunakan server VPN di awan.	Gunakan Alat Verifikasi Koneksi dan periksa keluarannya dari kemungkinan kesalahan. Izinkan perangkat lunak Acronis melalui kontrol aplikasi pada firewall dan perangkat lunak antimalware Anda.
Kegagalan pembuatan server utama	Peringatan akan muncul ketika server utama tidak dibuat karena kesalahan.	
Kegagalan pembuatan server pemulihan	Peringatan akan muncul ketika server pemulihan tidak dibuat karena kesalahan.	Pastikan server pemulihan cocok dengan Persyaratan perangkat lunak.
Hapus Server Utama	Peringatan akan muncul ketika server utama dihapus.	
Kegagalan pemulihan server	Peringatan dibuat ketika server utama atau server pemulihan gagal pulih.	Temukan detailnya. Jika pesan kesalahan bersifat umum atau tidak jelas, misalnya "Kesalahan internal", buka **Pemulihan Bencana → Server**, klik untuk memilih mesin yang terpengaruh, lalu klik **Aktivitas**. Klik aktivitas, tahan ctrl dan klik kiri aktivitas tersebut. Sekarang Anda akan dapat melihat tanda

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
		elipsis (...) di dekat setiap aktivitas. Klik dan pilih **Info aktivitas tugas**.
Pencadangan gagal	Peringatan akan muncul ketika pencadangan server awan (server utama atau server dalam kondisi failover produksi) gagal.	1. Verifikasi koneksi lokasi cadangan. 2. Periksa perangkat penyimpanan cadangan (cadangan lokal).
Batas jaringan terlampaui	Peringatan dibuat ketika jumlah maksimum jaringan awan tercapai (5 jaringan).	
Kegagalan Runbook	Peringatan akan muncul ketika eksekusi runbook gagal.	Hal ini tidak memengaruhi fungsionalitas produk, dan dapat diabaikan dengan aman. Untuk informasi lebih lanjut, lihat Membuat runbook.
Peringatan runbook	Peringatan dibuat ketika eksekusi runbook selesai dengan peringatan.	Hal ini tidak memengaruhi fungsionalitas produk, dan dapat diabaikan dengan aman. Untuk informasi lebih lanjut, lihat Membuat runbook.
Diperlukan Interaksi Pengguna Runbook	Peringatan dibuat ketika runbook menunggu interaksi pengguna.	Hal ini tidak memengaruhi fungsionalitas produk, dan dapat diabaikan dengan aman. Untuk informasi lebih lanjut, lihat Membuat runbook.
Lalu lintas internet diblokir	Peringatan dibuat ketika lalu lintas internet diblokir oleh administrator.	
Lalu lintas internet dibuka	Peringatan dibuat ketika lalu lintas internet dibuka blokirnya oleh administrator.	
Jaringan lokal tumpang tindih	Peringatan dibuat ketika jaringan lokal yang identik atau tumpang tindih terdeteksi.	
Peralihan pelisensian kuota server tidak mencukupi	Peringatan akan muncul ketika kuota server awan tidak mencukupi.	• Pastikan penyewa dan pengguna memiliki kuota server Web hosting atau kuota Server yang tersedia untuk

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
		server fisik. • Pastikan penyewa dan pengguna memiliki kuota server Web hosting atau kuota mesin Virtual yang tersedia untuk server virtual. Server virtual tidak dapat menggunakan kuota Server.
Peralihan pelisensian item penawaran tidak mencukupi	Peringatan dibuat ketika item penawaran penyimpanan pemulihan bencana dinonaktifkan.	Untuk informasi lebih lanjut, lihat Kuota pemulihan bencana.
Kesalahan penggantian pelisensian	Peringatan akan muncul ketika peningkatan pemulihan bencana mengalami kesalahan.	
Peralihan pelisensian tidak mencukupi titik komputasi	Peringatan akan muncul ketika tidak ada titik komputasi yang tersedia.	Di portal manajemen, periksa dan tingkatkan kuota keras untuk titik Komputasi.
Peralihan pelisensian server tidak mencukupi item penawaran	Peringatan dibuat ketika item penawaran server awan dinonaktifkan.	
Kebijakan gagal membuat server pemulihan	Peringatan akan muncul ketika terjadi kesalahan saat menyiapkan infrastruktur pemulihan bencana.	Buat Server Pemulihan secara manual tanpa properti Akses Internet. Untuk informasi lebih lanjut, lihat Membuat pemulihan server
Failover uji otomatis prosesor cadangan dijadwalkan ulang	Peringatan akan muncul ketika proses failover pengujian otomatis dijadwalkan ulang.	
Batas waktu failover uji otomatis prosesor cadangan tercapai	Peringatan dihasilkan ketika operasi failover pengujian otomatis berakhir. **Catatan** Setiap proses Failover Uji Otomatis akan menggunakan titik komputasi yang dapat dibebankan.	
Kegagalan keseluruhan kegagalan uji otomatis prosesor cadangan secara keseluruhan	Peringatan dibuat ketika failover pengujian otomatis terjadwal terakhir yang dijadwalkan dari server pemulihan gagal.	1. Mulai uji coba failover server pemulihan secara manual. Untuk informasi lebih lanjut, lihat Menjalankan failover uji.

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
		2. Tunggu tanggal terjadwal berikutnya ketika failover uji otomatis akan dilakukan
Kesalahan transfer data failback	Peringatan akan muncul ketika transfer data failback gagal.	
Failback gagal	Peringatan akan muncul ketika ada kesalahan dalam failback.	Anda dapat melihat lokasi yang salah di daftar penyimpanan cadangan: lokasi tersebut memiliki nomor, bukan nama (biasanya, nama lokasi cocok dengan salah satu nama pengguna akhir yang ada) dan Anda belum membuat lokasi ini. Hapus lokasi yang salah: 1. Pada Cyber Protection, navigasikan ke penyimpanan cadangan. 2. Temukan lokasinya dan klik ikon silang (x) untuk menghapusnya. 3. Konfirmasikan pilihan Anda dengan mengeklik **Hapus**. Coba lagi failover.
Failback mengonfirmasi gagal	Peringatan akan muncul ketika konfirmasi failback gagal.	
Mesin failback siap untuk peralihan	Peringatan akan muncul ketika mesin siap untuk peralihan.	
Peralihan failback selesai	Peringatan akan muncul ketika peralihan berhasil dilakukan.	Menutup peringatan secara manual dari konsol.
Agen target failback offline	Peringatan akan muncul ketika agen sedang offline.	

Peringatan proteksi Antimalware

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Aktivitas koneksi jarak jauh mencurigakan	Peringatan dibuat ketika ransomware yang berasal dari koneksi jarak jauh terdeteksi.	Menutup peringatan secara manual dari konsol.

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
terdeteksi		
Aktivitas mencurigakan terdeteksi	Peringatan dihasilkan ketika ransomware terdeteksi dalam beban kerja.	Menutup peringatan secara manual dari konsol. untuk menonaktifkan peringatan. Tergantung pada opsi yang Anda tentukan dalam rencana Active Protection, proses berbahaya dihentikan, perubahan yang dibuat oleh proses tersebut dikembalikan, atau tidak ada tindakan yang dilakukan dan Anda perlu menyelesaikan masalah ini secara manual. Baca detail peringatan untuk mengetahui proses mana yang mengenkripsi file dan file mana yang terpengaruh. Jika Anda memutuskan bahwa proses yang mengenkripsi file tersebut adalah proses yang tidak disetujui (peringatan positif palsu), tambahkan proses ini ke proses tepercaya: 1. Buka rencana Active Protection. 2. Klik **Edit** untuk memodifikasi pengaturan. 3. Pada **Proses tepercaya**, tentukan proses tepercaya yang tidak akan pernah dianggap sebagai ransomware. Tentukan jalur lengkap ke proses yang dapat dieksekusi, dimulai dengan huruf drive. Misalnya: C:\Windows\Temp\er76s7sdkh.exe.
Aktivitas cryptomining terdeteksi	Peringatan dibuat ketika cryptominer terlarang terdeteksi dalam beban kerja	Menutup peringatan secara manual dari konsol.
Pertahanan MBR: Aktivitas mencurigakan telah terdeteksi dan ditangguhkan	Peringatan dibuat ketika ransomware terdeteksi dalam beban kerja (khususnya partisi MBR / GPT yang dimodifikasi oleh ransomware).	Menutup peringatan secara manual dari konsol.
Jalur jaringan tidak didukung telah ditentukan	Peringatan akan muncul jika jalur pemulihan yang disediakan oleh administrator bukan merupakan jalur folder lokal.	Tentukan jalur lokal untuk perlindungan folder jaringan (jalur pemulihan). Menutup peringatan secara manual dari konsol

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Proses penting ditambahkan sebagai berbahaya ke rencana Active Protection	Peringatan dibuat ketika proses kritis ditambahkan sebagai proses yang diblokir dalam daftar pengecualian Perlindungan.	Menutup peringatan secara manual dari konsol.
Gagal menerapkan kebijakan Active Protection	Peringatan dibuat ketika kebijakan Active Protection gagal diterapkan.	Periksa pesan kesalahan untuk mengetahui mengapa kebijakan Active Protection tidak dapat diterapkan.
Secure Zone: Operasi tidak sah terdeteksi dan diblokir	Peringatan dibuat ketika ransomware terdeteksi dalam beban kerja (partisi ASZ dimodifikasi oleh ransomware).	Menutup peringatan secara manual dari konsol.
Layanan Active Protection tidak berjalan	Peringatan dibuat ketika layanan Active Protection berhenti/tidak berjalan.	Periksa pesan kesalahan untuk mengetahui mengapa layanan Active Protection tidak berjalan.
Layanan Active Protection tidak tersedia	Peringatan akan muncul ketika layanan Active Protection tidak tersedia karena driver tidak kompatibel atau hilang.	Periksa log peristiwa Windows untuk mengetahui adanya gangguan pada layanan Acronis Active Protection (acronis_ protection_service.exe).
Konflik dengan solusi keamanan lain	Peringatan akan muncul ketika Active Protection tidak tersedia untuk mesin '{{resourceName}}' karena terdeteksi adanya konflik dengan solusi keamanan lain. Untuk mengaktifkan Active Protection, nonaktifkan atau hapus instalasi solusi keamanan yang bertentangan.	**Solusi 1**: Jika Anda ingin menggunakan perlindungan real-time Acronis, hapus instalasi antivirus pihak ketiga di mesin. **Solusi 2**: Jika Anda ingin menggunakan antivirus pihak ketiga, nonaktifkan perlindungan real-time Acronis, penapisan URL, dan antivirus Windows defender di rencana proteksi.
Tindakan karantina gagal	Peringatan akan muncul ketika antimalware gagal mengarantina malware yang terdeteksi.	Periksa pesan kesalahan untuk mengetahui mengapa karantina gagal.
Proses berbahaya terdeteksi	Peringatan dibuat ketika malware (jenis proses) terdeteksi oleh mesin Behavior. Malware yang terdeteksi akan dikarantina.	Menutup peringatan secara manual dari konsol.
Proses berbahaya terdeteksi, tetapi tidak dikarantina	Peringatan dibuat ketika malware (jenis proses) terdeteksi oleh mesin Behavior. Malware yang terdeteksi tidak dikarantina.	Menutup peringatan secara manual dari konsol.

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Malware terdeteksi dan diblokir (ODS)	Peringatan dibuat ketika malware terdeteksi oleh pemindaian terjadwal. Malware yang terdeteksi akan dikarantina.	Menutup peringatan secara manual dari konsol.
Malware terdeteksi dan diblokir (RTP)	Peringatan dihasilkan ketika malware terdeteksi oleh perlindungan Real-Time. Malware yang terdeteksi akan dikarantina.	Menutup peringatan secara manual dari konsol.
Malware terdeteksi dalam cadangan	Peringatan dibuat ketika malware terdeteksi selama pemindaian cadangan.	Menutup peringatan secara manual dari konsol.
Konflik terdeteksi antara Perlindungan antimalware waktu nyata dan produk keamanan	Peringatan akan muncul ketika antimalware gagal mendaftar ke Windows Security Center.	Nonaktifkan atau hapus instalasi produk keamanan pihak ketiga, atau nonaktifkan proteksi antimalware real-time dalam rencana proteksi.
Gagal menjalankan modul Microsoft Security Essentials	Peringatan akan muncul ketika gagal menjalankan modul Microsoft Security Essentials.	Periksa pesan kesalahan untuk mengetahui mengapa modul Microsoft Security Essentials gagal dijalankan.
Perlindungan waktu nyata tidak tersedia karena perangkat lunak antivirus pihak ketiga diinstal	Peringatan akan muncul ketika perlindungan waktu nyata gagal dinyalakan, karena antivirus pihak ketiga masih mengaktifkan perlindungan waktu nyata.	Nonaktifkan atau hapus instalasi produk keamanan pihak ketiga, atau nonaktifkan proteksi antimalware real-time dalam rencana proteksi.
Perlindungan waktu nyata tidak tersedia karena driver tidak kompatibel atau tidak ada	Peringatan akan muncul ketika perlindungan Real-time tidak tersedia karena driver yang tidak kompatibel atau hilang.	Periksa pesan kesalahan untuk mengetahui mengapa Acronis gagal menginstal driver pada beban kerja.
Layanan Perlindungan Cyber (atau Active Protection) tidak merespons	Peringatan dibuat ketika Layanan Perlindungan Cyber merespons ping pemeriksaan kesehatan dari konsol.	Menutup peringatan secara manual dari konsol.
Pembaruan definisi keamanan gagal	Peringatan dibuat ketika pembaruan definisi keamanan gagal.	Periksa pesan kesalahan untuk mengetahui mengapa pembaruan definisi keamanan gagal.
Perlindungan Gangguan diaktifkan	Peringatan dibuat ketika pengaturan Microsoft Defender	Nonaktifkan pengaturan Perlindungan Gangguan pada beban kerja Windows.

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
	tidak dapat diubah karena perlindungan gangguan diaktifkan.	
Eksekusi modul Windows Defender gagal	Peringatan dibuat ketika eksekusi modul Windows Defender gagal.	Periksa pesan kesalahan untuk mengetahui mengapa modul Windows Defender gagal dijalankan.
Windows Defender diblokir oleh perangkat lunak antivirus pihak ketiga	Peringatan dibuat ketika Windows Defender diblokir karena Antivirus pihak ketiga diinstal pada mesin.	Nonaktifkan atau hapus instalasi produk keamanan pihak ketiga.
Konflik kebijakan grup	Peringatan dibuat ketika pengaturan Microsoft Defender tidak dapat diubah karena dikendalikan oleh kebijakan grup.	Nonaktifkan pengaturan kebijakan grup pada beban kerja Windows.
Microsoft Security Essentials mengambil tindakan untuk melindungi mesin ini dari malware	Peringatan dibuat ketika Microsoft Security Essential menghapus/mengkarantina malware.	Menutup peringatan secara manual dari konsol.
Microsoft Security Essentials mendeteksi malware	Peringatan akan muncul ketika Microsoft Security Essentials mendeteksi malware atau perangkat lunak lain yang mungkin tidak diinginkan.	Menutup peringatan secara manual dari konsol.

Peringatan pelisensian

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Kuota penyimpanan hampir tercapai	Peringatan akan muncul ketika penggunaan turun di bawah 80% (setelah pembersihan atau peningkatan kuota).	Pertimbangkan untuk membeli penyimpanan tambahan atau mengosongkan ruang di penyimpanan awan Anda.
Kuota penyimpanan terlampaui	Peringatan akan muncul ketika 100% kuota penyimpanan telah digunakan.	Beli lebih banyak ruang penyimpanan. Untuk informasi lebih lanjut tentang cara melakukannya, lihat cara membeli lebih banyak penyimpanan awan.
Kuota beban kerja tercapai	Peringatan akan muncul ketika	

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
	penggunaan untuk item penawaran > 0 dan penggunaan > kuota, tetapi penggunaan <= kuota + kelebihan pemakaian.	
Kuota beban kerja terlampaui	Peringatan akan muncul ketika penggunaan untuk item penawaran > kuota + kelebihan pemakaian.	
Beban kerja tidak memiliki kuota untuk menerapkan rencana pencadangan (sumber daya tidak memiliki kuota layanan)	Peringatan akan muncul ketika: • Kuota dihapus secara manual: **Perangkat** > **Rincian** > **Kuota layanan**, lalu klik **Ubah** dan pilih opsi **Tanpa kuota**. • Item penawaran Konsol Manajemen dinonaktifkan. • Kuota Konsol Manajemen + nilai kelebihan dari item yang ditawarkan berkurang di bawah penggunaan saat ini.	
Tidak dapat melindungi beban kerja dengan kuota yang ditetapkan	Peringatan akan muncul ketika item penawaran tidak mencukupi, dan Anda harus memilikinya: • grup yang dinamis. • rencana pencadangan yang ditugaskan ke grup tersebut. • anda menambahkan sumber daya yang termasuk dalam grup dinamis tersebut, namun memiliki beberapa kualitas yang melarang penerapan rencana pencadangan yang sama padanya.	
Lisensi berlangganan telah kedaluwarsa	Peringatan dibuat ketika pemeriksaan harian untuk peringatan kedaluwarsa lisensi/pemeliharaan, menanyakan kepada server lisensi, dan mendapat jawaban bahwa lisensi telah kedaluwarsa.	Setelah masa langganan berakhir, semua fungsionalitas produk kecuali pemulihan akan diblokir hingga pembaruan masa langganan. Data yang dicadangkan masih dapat diakses untuk pemulihan. Beli lisensi baru.

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
		Catatan Jika Anda baru saja membeli langganan baru namun masih menerima pesan bahwa langganan telah habis masa berlakunya, Anda perlu mengimpor langganan baru dari Akun Acronis: di Konsol Manajemen, masuk ke Pengaturan -> Lisensi dan klik Sinkronisasi di pojok kanan atas. Langganan akan disinkronkan.
Lisensi berlangganan akan segera kedaluwarsa	Peringatan dibuat ketika pemeriksaan harian untuk peringatan kedaluwarsa lisensi/pemeliharaan, menanyakan kepada server lisensi, dan mendapatkan jawaban bahwa lisensi akan kedaluwarsa dalam waktu kurang dari 30 hari.	Pertimbangkan untuk membeli langganan baru.

Peringatan pemfilteran URL

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
URL berbahaya diblokir	Peringatan dibuat ketika URL berbahaya diblokir oleh pemfilteran URL.	Periksa pengaturan pemfilteran URL. Pemfilteran URL adalah memblokir halaman yang seharusnya diblokir menurut pengaturan Pemfilteran URL.
Peringatan URL berbahaya diabaikan	Peringatan akan muncul ketika Anda memilih untuk melanjutkan URL berbahaya yang diblokir oleh pemfilteran URL.	Periksa pengaturan pemfilteran URL.
Konflik terdeteksi antara pemfilteran URL dan produk keamanan	Peringatan akan muncul ketika pemfilteran URL tidak dapat diaktifkan karena adanya konflik dengan produk keamanan lain.	Periksa pengaturan pemfilteran URL.
URL Situs web diblokir	Peringatan dibuat ketika URL	Periksa pengaturan pemfilteran

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
	memenuhi semua kriteria yang ditentukan dalam kategori yang diblokir untuk pemfilteran URL.	URL.

Peringatan EDR

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Insiden Terdeteksi	Peringatan dibuat ketika insiden dibuat atau ketika status untuk insiden yang sudah ada diperbarui.	Peringatan ini menginformasikan kepada Anda tentang insiden baru atau jika insiden lama telah diperbarui. Anda dapat melihat peringatan dan menutupnya. Anda dapat memilih untuk membuka insiden tersebut untuk penyelidikan lebih lanjut jika diperlukan.
Indikator penyusupan (IOC) terdeteksi	Peringatan dibuat ketika indikator penyusupan baru terdeteksi oleh layanan pencarian ancaman EDR IOC.	Peringatan ini untuk memberi tahu Anda bahwa IOC telah terdeteksi pada satu atau banyak beban kerja. Anda akan melihat peringatan dan kemudian Anda dapat mengklik tautan dalam peringatan tersebut untuk melihat detail tentang IOC.
Gagal mengisolasi beban kerja dari jaringan	Peringatan dibuat ketika pengguna memicu tindakan untuk mengisolasi mesin dari jaringan, dan tindakan isolasi gagal.	Lakukan tindakan yang diperlukan.
Gagal menghubungkan kembali beban kerja ke jaringan	Peringatan akan muncul ketika pengguna memicu tindakan untuk menyambungkan kembali mesin ke jaringan, dan tindakan tersebut gagal.	Lakukan tindakan yang diperlukan.
Pengaturan Firewall Windows Defender diubah	Peringatan akan muncul ketika pengaturan pada firewall dimodifikasi pada mesin yang terisolasi.	Peringatan ini untuk memberi tahu Anda bahwa detail firewall telah dimodifikasi pada mesin yang diisolasi. Ini hanya bersifat informatif dan Anda dapat menutup peringatan setelah

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
		melihatnya.

Peringatan Kontrol Perangkat

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Kontrol perangkat dan Pencegahan kehilangan data akan berjalan dengan fungsionalitas terbatas (CPU yang tidak kompatibel terdeteksi)	Peringatan dibuat ketika agen DeviceLock dimulai pada mesin fisik dengan CPU yang mendukung teknologi CET.	Nonaktifkan opsi pada mesin yang terpengaruh untuk menghindari peringatan.
Fungsi kontrol perangkat belum didukung di macOS Ventura	Peringatan dibuat ketika agen DeviceLock dimulai pada mesin fisik macOS Ventura, dan rencana proteksi dengan Kontrol Perangkat diterapkan ke agen. Hanya berlaku untuk versi ketika ada masalah dengan kernel panik karena driver DeviceLock.	
Transfer data sensitif yang diizinkan	Peringatan akan muncul ketika transfer untuk konten sensitivitas diizinkan.	
Transfer data sensitif yang dibenarkan	Peringatan akan muncul ketika mentransfer konten sensitivitas dibenarkan.	
Transfer data sensitif yang ditolak	Peringatan akan muncul ketika mentransfer konten sensitivitas diblokir.	
Tinjau hasil mode observasi Pencegahan Kehilangan Data	Peringatan akan muncul ketika tiba waktunya untuk meninjau hasil Observasi: • Lisensi Rencana Advanced DLP tidak diterapkan. • Sebulan berlalu sejak mode Pengamatan diaktifkan di rencana Proteksi mana pun yang diterapkan pada setidaknya satu beban kerja.	

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
	• Sebulan berlalu sejak peringatan serupa terakhir kali dimunculkan dan beberapa penggunaan DLP dalam mode Observasi terdeteksi.	
Pengenal keamanan telah diubah untuk pengguna	Peringatan dibuat ketika kita memiliki situasi ketika SID diperbarui untuk nama pengguna yang dikenal. Hal ini dapat terjadi ketika OS diinstal ulang pada PC yang bukan domain.	
Akses perangkat periferal diblokir	Peringatan dibuat ketika beberapa tindakan (operasi baca/tulis) untuk perangkat yang didukung diblokir.	
Tidak dapat terhubung ke sumber daya SSL jarak jauh.	Suatu peringatan dihasilkan ketika akses ke sumber daya SSL jarak jauh diblokir karena pencegahan jabat tangan tambahan yang digunakan di sumber daya tersebut.	Tambahkan sumber daya ke daftar izin untuk host jarak jauh.

Peringatan sistem

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Agen sudah usang	Peringatan akan muncul ketika versi agen sudah kedaluwarsa.	Buka daftar Agen dan mulai memperbarui agen.
Pembaruan otomatis gagal	Peringatan akan muncul ketika pembaruan otomatis agen gagal.	Cobalah untuk melakukan pembaruan manual.
Anda harus mulai ulang perangkat setelah menginstal agen baru	Peringatan akan muncul ketika boot ulang diperlukan setelah instalasi jarak jauh berhasil.	Mulai ulang beban kerja.
Aktivitas gagal	Peringatan akan muncul ketika aktivitas gagal.	Mulai kembali semua layanan Acronis pada mesin.
Aktivitas berhasil dengan beberapa peringatan	Peringatan dibuat ketika aktivitas berhasil namun ada beberapa peringatan yang dibuat.	

© Acronis International GmbH, 2003-2024

Peringatan	Deskripsi	Pilih cara menyelesaikan peringatan
Aktivitas tidak merespons	Peringatan dibuat ketika aktivitas yang sedang berlangsung tidak merespons.	
Penyebaran rencana gagal	Peringatan akan muncul ketika penerapan rencana proteksi gagal.	
Gagal mengonversi nama pengguna ke SID	Peringatan akan muncul ketika konversi SID jadwal gagal.	

Widget peringatan

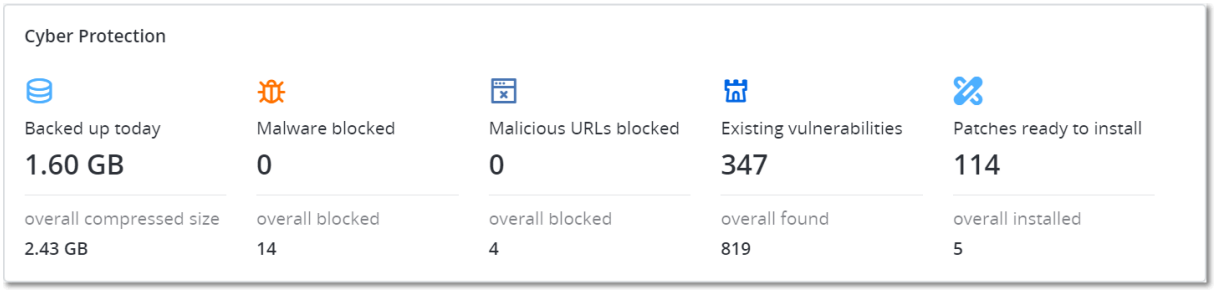
Di widget peringatan, Anda dapat melihat detail peringatan berikut terkait beban kerja Anda:

Bidang	Deskripsi
5 widget peringatan terbaru	Daftar lima peringatan terbaru.
Ringkasan peringatan riwayat	Widget grafis yang menampilkan peringatan berdasarkan tingkat keparahan peringatan, jenis peringatan, dan rentang waktu.
Ringkasan peringatan aktif	Widget grafis yang menampilkan peringatan aktif berdasarkan tingkat keparahan peringatan, jenis peringatan, serta jumlah peringatan aktif.
Riwayat peringatan	Tampilan tabel peringatan historis.
Detail peringatan aktif	Tampilan tabel peringatan aktif.

Perlindungan cyber

Widget ini menampilkan keseluruhan informasi mengenai ukuran cadangan, malware yang diblokir, URL yang diblokir, kerentanan yang ditemukan, dan patch yang diinstal.

© Acronis International GmbH, 2003-2024



Baris atas menunjukkan statistik saat ini:

- **Dicadangkan hari ini** – jumlah ukuran titik pemulihan selama 24 jam terakhir
- **Malware diblokir** – jumlah peringatan aktif saat ini tentang malware yang diblokir
- **URL yang diblokir** – jumlah peringatan aktif saat ini mengenai URL yang diblokir
- **Kerentanan yang ada** – jumlah kerentanan yang ada saat ini
- **Patch siap diinstal** – jumlah patch tersedia saat ini yang akan diinstal

Baris bawah menunjukkan keseluruhan statistik:

- Ukuran terkompresi dari semua cadangan
- Jumlah akumulasi malware yang diblokir pada semua mesin
- Jumlah akumulasi URL yang diblokir pada semua mesin
- Jumlah akumulasi kerentanan yang ditemukan pada semua mesin
- Jumlah akumulasi pembaruan/patch yang diinstal pada semua mesin

Status proteksi

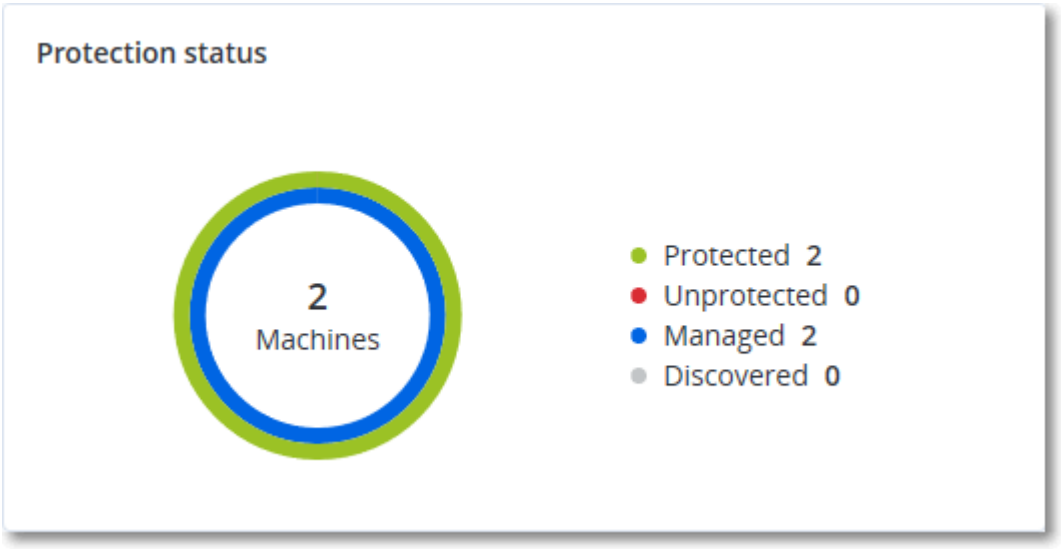
Widget ini menampilkan status perlindungan saat ini untuk semua mesin.

Suatu mesin dapat memiliki salah satu status berikut:

- **Terlindungi** – mesin dengan rencana proteksi yang diterapkan.
- **Tak terlindungi** – mesin tanpa rencana proteksi yang diterapkan. Ini mencakup mesin yang terdeteksi dan mesin yang dikelola tanpa ada rencana proteksi yang diterapkan.
- **Dikelola** – mesin dengan agen perlindungan yang sudah diinstal.
- **Ditemukan** – mesin tanpa agen perlindungan yang sudah diinstal.

Jika mengeklik status mesin, Anda akan diarahkan ke daftar mesin dengan status ini untuk keterangan lebih lanjut.

© Acronis International GmbH, 2003-2024



Mesin yang ditemukan

Widget ini menampilkan daftar mesin yang ditemukan selama rentang waktu tertentu.

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 Deteksi dan Tanggapan Titik Akhir (EDR)

Deteksi dan Tanggapan Titik Akhir (EDR) menyertakan tujuh widget, yang semuanya bisa diakses dari dasbor **Ikhtisar**; tiga widget di antaranya juga ditampilkan secara default di fungsionalitas EDR (lihat "Meninjau insiden" (hlm. 897)).

Tujuh widget yang tersedia adalah:

- Distribusi Insiden Teratas per beban kerja
- Status ancaman (ditampilkan di EDR)
- Riwayat keparahan insiden (ditampilkan di EDR)

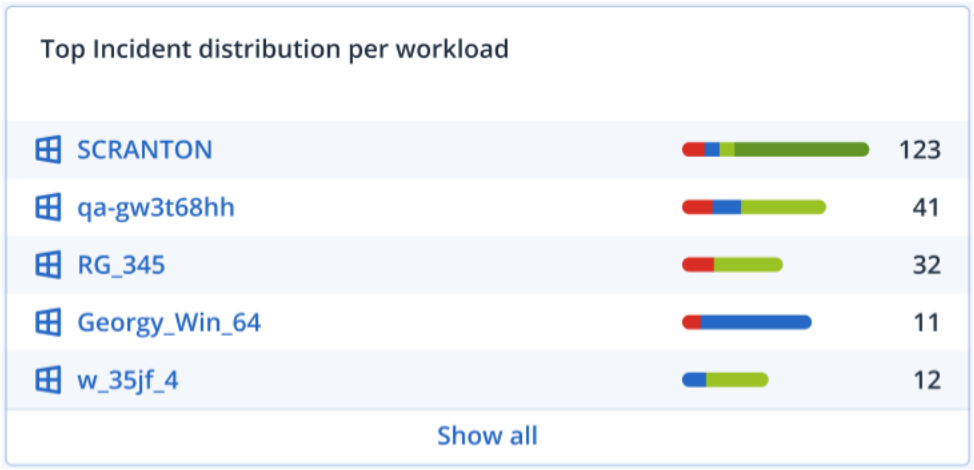
© Acronis International GmbH, 2003-2024

- MTTR insiden keamanan
- Burndown insiden keamanan
- Deteksi dengan taktik (ditampilkan di EDR)
- Status jaringan beban kerja

Distribusi Insiden Teratas per beban kerja

Widget ini menampilkan lima beban kerja teratas dengan insiden paling banyak (klik **Tampilkan semua** untuk mengarahkan langsung ke daftar insiden, yang difilter berdasarkan pengaturan widget).

Arahkan pointer mouse disekitar baris beban kerja untuk menampilkan rincian status investigasi saat ini untuk insiden tersebut; status investigasi adalah **Belum mulai**, **Menginvestigasi**, **Tertutup**, dan **Positif salah**. Lalu klik beban kerja yang ingin Anda analisis lebih lanjut; daftar insiden akan diperbarui berdasarkan pengaturan widget.

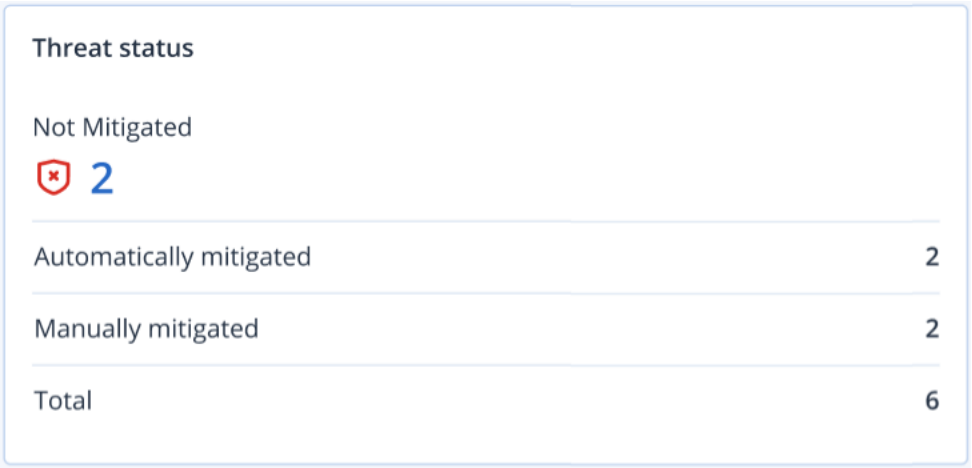


Status ancaman

Widget ini menampilkan status ancaman saat ini untuk semua beban kerja, menyorot jumlah insiden yang belum dimitigasi dan yang perlu diinvestigasi. Widget ini juga mengindikasikan jumlah insiden yang sudah dimitigasi (secara manual dan/atau secara otomatis oleh sistem).

Klik **Tidak dimitigasi** untuk menampilkan daftar insiden yang difilter untuk menampilkan insiden yang belum dimitigasi.

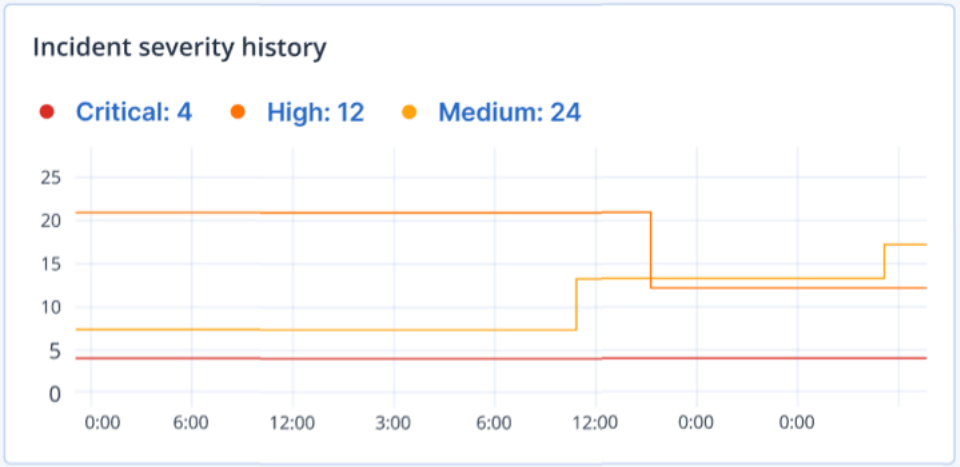
© Acronis International GmbH, 2003-2024



Riwayat keparahan insiden

Widget ini menampilkan evolusi serangan berdasarkan tingkat keparahannya, dan dapat membantu mengidentifikasi kampanye serangan. Ketika lonjakan terlihat, ini dapat menunjukkan bahwa organisasi sedang diserang.

Arahkan pointer mouse ke grafik untuk melihat uraian riwayat insiden di titik tertentu selama 24 jam sebelumnya (periode default). Klik tingkat keparahan (**Kritis**, **Tinggi**, atau **Sedang**) jika ingin melihat daftar insiden terkait; Anda akan diarahkan ke daftar insiden sebelum difilter dengan insiden yang sesuai dengan tingkat keparahan yang dipilih.

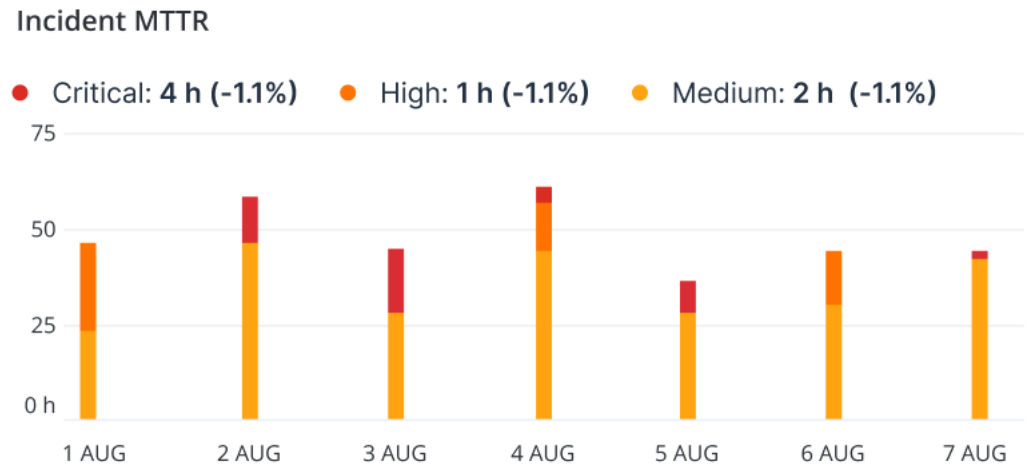


MTTR insiden keamanan

Widget ini menampilkan waktu resolusi rata-rata untuk insiden keamanan. Ini menandakan seberapa cepat insiden teridentifikasi dan terpecahkan.

Klik pada kolom untuk menampilkan rincian insiden berdasarkan keparahannya (**Kritis**, **Tinggi**, dan **Sedang**), dan indikasi yang menjelaskan seberapa lama insiden yang berdasarkan perbedaan tingkat keparahan tersebut dapat diselesaikan. Nilai dalam % yang ditampilkan dalam tanda kurung menandakan peningkatan atau penurunan dibandingkan periode waktu sebelumnya.

© Acronis International GmbH, 2003-2024

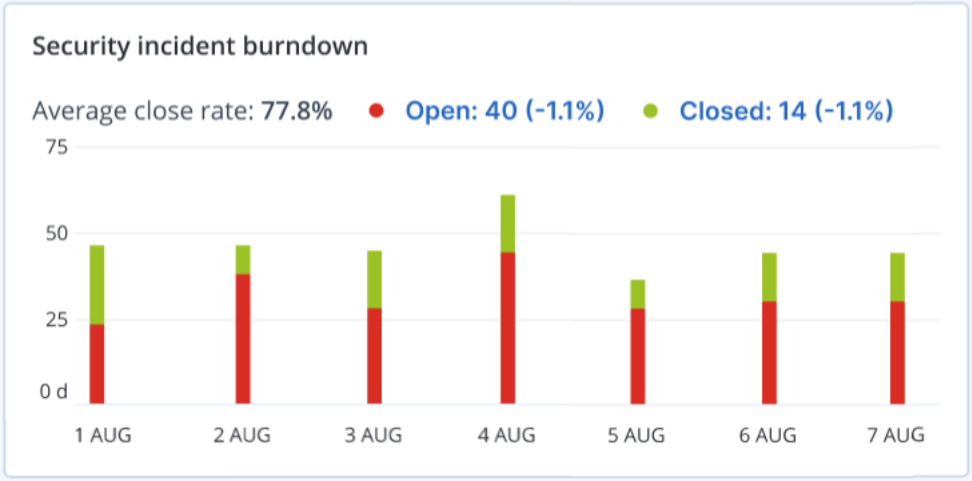


Burndown insiden keamanan

Widget ini menampilkan rentang efisiensi dalam penutupan insiden; jumlah insiden terbuka yang diukur berlawanan dengan jumlah insiden tertutup selama periode waktu tertentu.

Arahkan pointer mouse terhadap sebuah kolom untuk menampilkan uraian insiden tertutup dan terbuka untuk tanggal terpilih. Jika Anda mengeklik nilai Terbuka, daftar insiden akan ditampilkan, dan difilter untuk menampilkan insiden yang saat ini terbuka (dalam status **Menginvestigasi** atau **Belum mulai**). Jika Anda mengeklik nilai Tertutup, daftar insiden akan ditampilkan, dan difilter untuk menampilkan insiden yang tidak lagi terbuka (dalam status **Tertutup** atau **Positif palsu**).

Nilai dalam % yang ditampilkan dalam tanda kurung menandakan peningkatan atau penurunan dibandingkan periode waktu sebelumnya.



Deteksi dengan taktik

Widget ini menampilkan berapa kali teknik serangan tertentu ditemukan dalam insiden selama periode yang dipilih.

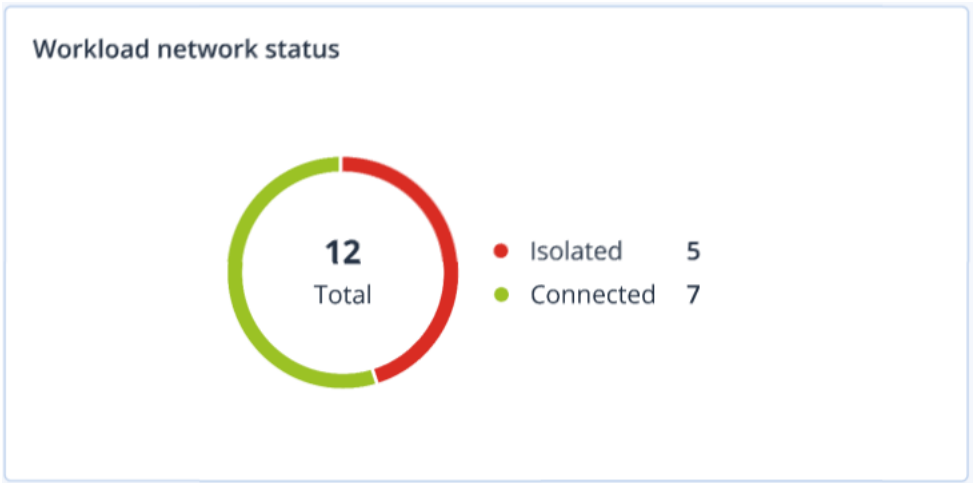
© Acronis International GmbH, 2003-2024

Nilai berwarna hijau dan merah menandakan adanya peningkatan atau penurunan selama periode waktu sebelumnya. Dalam contoh di bawah, serangan Eskalasi Hak Istimewa serta Perintah dan Kontrol mengalami peningkatan selama periode waktu sebelumnya; ini dapat menandakan bahwa manajemen kredensial Anda perlu dianalisis dan keamanannya perlu ditingkatkan.

Status jaringan beban kerja

Widget ini menampilkan status jaringan saat ini dari beban kerja Anda, dan mengindikasikan jumlah beban kerja yang terisolasi dan jumlah beban kerja yang terhubung.

Klik nilai Terisolasi untuk melihat daftar Beban Kerja dengan agen (di bawah menu **Beban kerja** di konsol Cyber Protect), yang difilter untuk menampilkan beban kerja yang terisolasi. Klik nilai Terhubung untuk melihat Beban Kerja dengan daftar agen yang difilter untuk menampilkan beban kerja yang terhubung.



Skor #CyberFit berdasarkan mesin

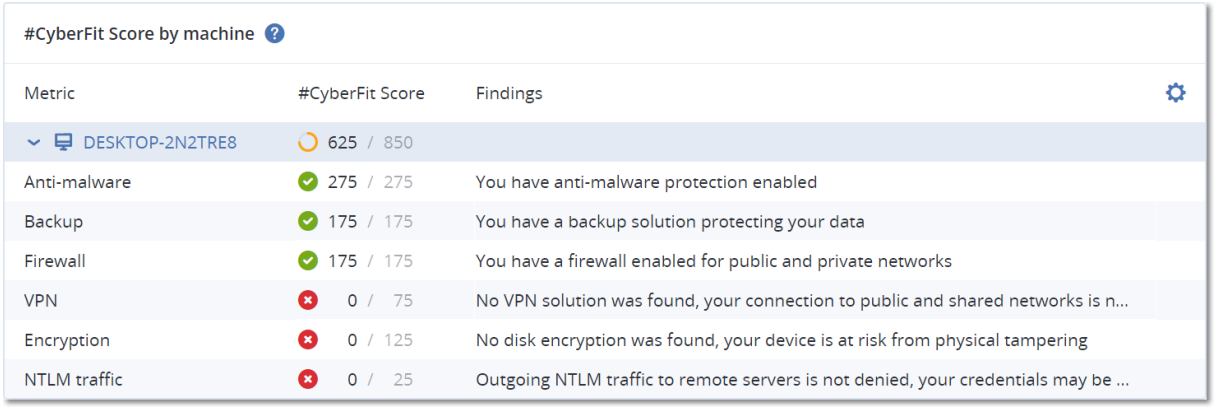
Widget ini menunjukkan total Skor #CyberFit untuk setiap mesin, skor gabungannya, dan temuan untuk setiap metrik yang dinilai:

© Acronis International GmbH, 2003-2024

- Antimalware
- Cadangan
- Firewall
- VPN
- Enkripsi
- NTLM traffic

Untuk meningkatkan skor setiap metrik, Anda dapat melihat rekomendasi yang tersedia dalam laporan.

Untuk detail selengkapnya tentang Skor #CyberFit, lihat "Skor #CyberFit untuk mesin".



Pemantauan kesehatan disk

Pemantauan kesehatan disk menyediakan informasi status kesehatan disk saat ini dan prakiraannya sehingga Anda dapat mencegah kehilangan data yang mungkin berhubungan dengan kegagalan disk. Tipe disk HDD dan SSD didukung.

Pembatasan

- Prakiraan kesehatan disk hanya didukung untuk mesin yang menjalankan Windows.
- Hanya disk mesin fisik yang dapat dipantau. Disk mesin virtual tidak dapat dipantau dan ditampilkan dalam widget kesehatan disk.
- Konfigurasi RAID tidak didukung. Widget kesehatan disk tidak menyertakan informasi apa pun tentang mesin dengan implementasi RAID.
- SSD NVMe tidak didukung.

Kesehatan disk diwakili salah satu status berikut:

- **OK**
  Kesehatan disk di antara 70% dan 100%.
- **Peringatan**
  Kesehatan disk di antara 30% dan 70%.

© Acronis International GmbH, 2003-2024

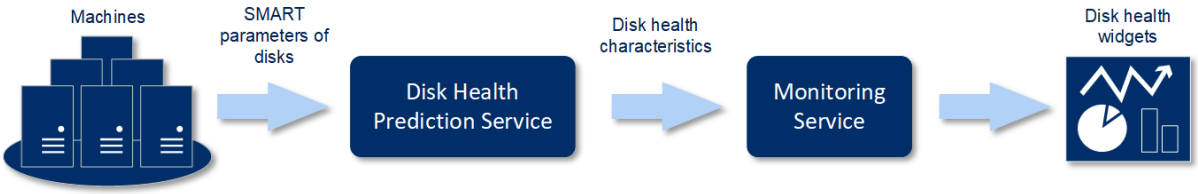
- **Kritis**
  Kesehatan disk di antara 0% dan 30%.
- **Menghitung data disk**
  Status terkini dan prakiraan disk sedang dihitung.

Cara kerjanya

Layanan Prediksi Kesehatan Disk menggunakan model prediksi berbasis AI.

1. Agen proteksi mengumpulkan parameter SMART dari disk dan meneruskan data ini ke Layanan Prediksi Kesehatan Disk:
   - SMART 5 – Hitungan sektor yang dialokasikan ulang.
   - SMART 9 – Jam menyala.
   - SMART 187 – Laporan kesalahan yang tidak dapat dikoreksi.
   - SMART 188 – Batas waktu perintah.
   - SMART 197 – Hitungan sektor tertunda terkini.
   - SMART 198 – Hitungan sektor offline yang tidak dapat dikoreksi.
   - SMART 200 – Laju kesalahan tulis.
2. Layanan Prediksi Kesehatan Disk memproses parameter SMART yang diterima, membuat prakiraan, dan memberikan karakteristik kesehatan disk berikut:
   - Status terkini kesehatan disk: OK, peringatan, kritis.
   - Prakiraan kesehatan disk: negatif, stabil, positif.
   - Persentase kemungkinan prakiraan kesehatan disk.

   Periode prediksinya satu bulan.
3. Layanan Pemantauan menerima karakteristik ini, lalu menampilkan informasi yang relevan di widget kesehatan disk di konsol Cyber Protect.



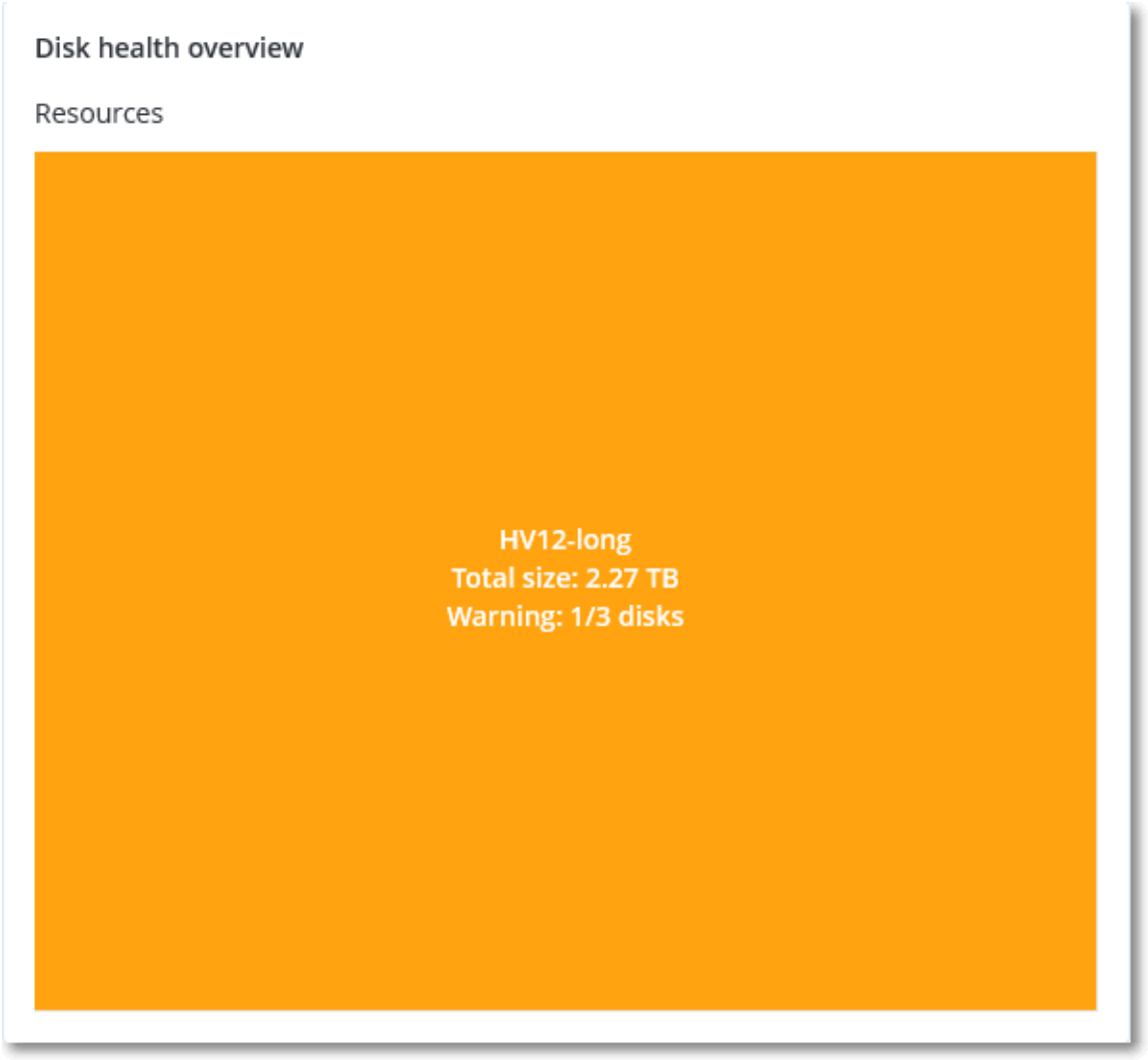
Widget kesehatan disk

Hasil pemantauan kesehatan disk disajikan dalam widget berikut yang tersedia di konsol Cyber Protect.

- **Gambaran kesehatan disk** adalah widget peta hierarki dengan dua tingkat detail yang dapat diaktifkan dengan diperinci.
  - Tingkat mesin
    Menunjukkan informasi ringkas tentang status kesehatan disk per mesin pelanggan yang

© Acronis International GmbH, 2003-2024

dipilih. Hanya status disk paling kritis yang ditunjukkan. Status lainnya ditampilkan di tooltip saat Anda mengarahkan pointer mouse ke blok tertentu. Ukuran blok mesin bergantung pada ukuran total semua disk mesin ini. Warna blok mesin bergantung pada status disk paling kritis yang ditemukan.

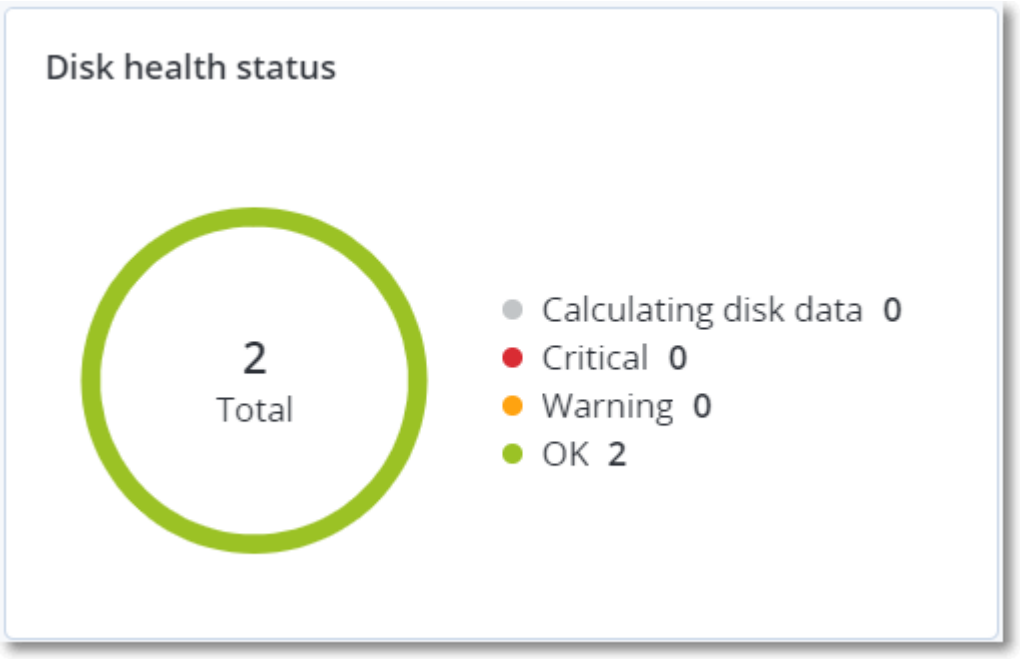


- Tingkat disk
  Menunjukkan status disk terkini dari semua disk untuk mesin yang dipilih. Setiap blok disk menunjukkan salah satu prakiraan kesehatan disk berikut dan persentase peluangnya.
  - Akan didegradasi
  - Akan tetap stabil

© Acronis International GmbH, 2003-2024

- Akan membaik

- **Status kesehatan disk** adalah widget diagram lingkaran yang menunjukkan jumlah disk untuk setiap status.



© Acronis International GmbH, 2003-2024

Peringatan status kesehatan disk

Pemeriksaan kesehatan disk berjalan setiap 30 menit, sedangkan peringatan terkait dihasilkan satu kali sehari. Saat kesehatan disk berubah dari **Peringatan** ke **Kritis**, peringatan akan muncul.

Nama peringatan	Tingkat keparahan	Status kesehatan disk	Deskripsi
Kegagalan disk mungkin terjadi	Peringatan	(30 – 70)	Disk <disk name> pada mesin ini mungkin akan gagal di masa mendatang. Jalankan pencadangan profil penuh pada disk ini sesegera mungkin, ganti lalu pulihkan profil ke disk baru.
Kegagalan disk akan terjadi	Kritis	(0 – 30)	Disk <nama disk> pada mesin ini berada dalam kondisi kritis, dan kemungkinan besar akan segera gagal. Kami tidak menyarankan pencadangan image disk ini pada saat ini, karena tekanan tambahan dapat menyebabkan kegagalan disk. Segera cadangkan semua file terpenting pada disk ini lalu ganti disk.

Peta perlindungan data

Catatan
Fitur ini tersedia dengan paket Cadangan Lanjutan.

Peta perlindungan data memungkinkan Anda untuk menemukan semua data yang penting bagi Anda dan mendapatkan informasi terperinci tentang jumlah, ukuran, lokasi, status proteksi semua file penting dalam tampilan peta pohon terukur.

Setiap ukuran blok bergantung pada jumlah/ukuran total semua file penting yang dimiliki pelanggan/mesin.

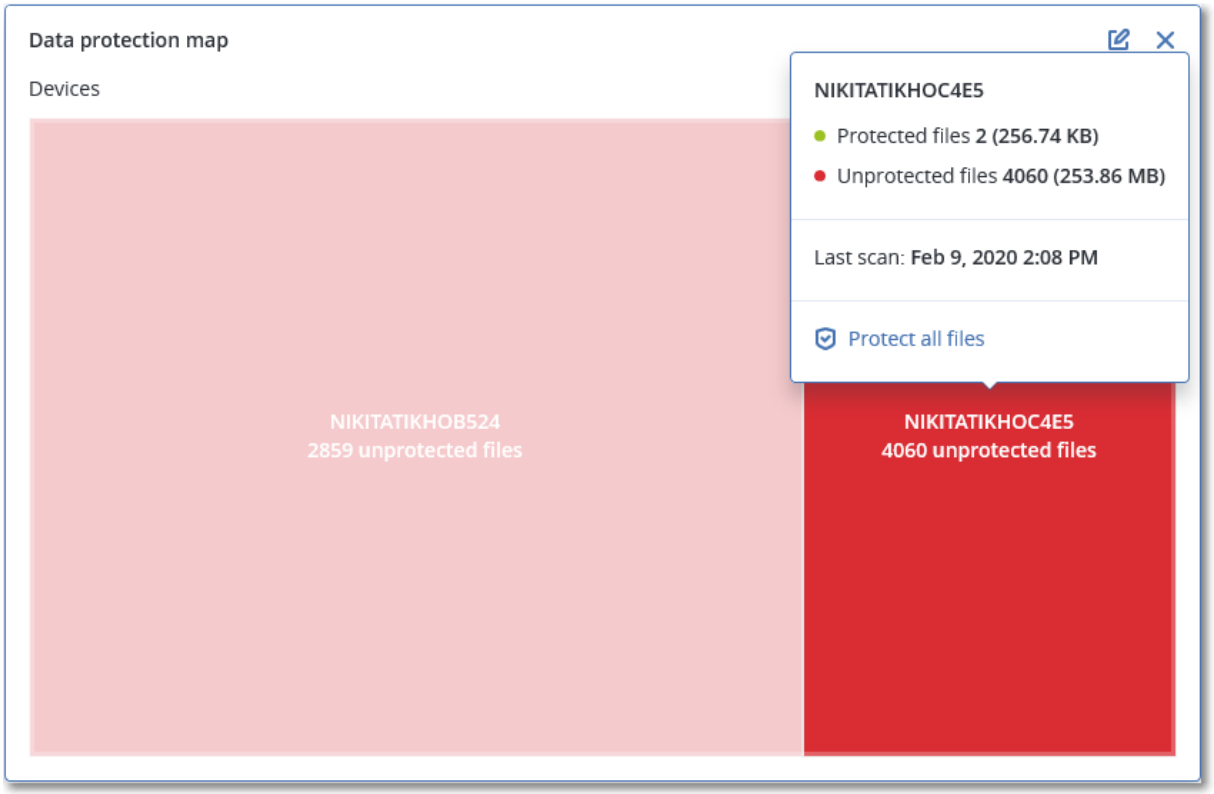
File dapat berada dalam salah satu status perlindungan berikut:

- **Kritis** – terdapat 51-100% file tidak terlindungi dengan ekstensi yang Anda tetapkan yang tidak dicadangkan dan tidak akan dicadangkan dengan pengaturan pencadangan yang ada untuk mesin/lokasi yang dipilih.
- **Rendah** – terdapat 21-50% file tidak terlindungi dengan ekstensi yang Anda tetapkan yang tidak dicadangkan dan tidak akan dicadangkan dengan pengaturan pencadangan yang ada untuk mesin/lokasi yang dipilih.
- **Sedang** – terdapat 1-20% file tidak terlindungi dengan ekstensi yang Anda tetapkan yang tidak dicadangkan dan tidak akan dicadangkan dengan pengaturan pencadangan yang ada untuk mesin/lokasi yang dipilih.
- **Tinggi** – semua file dengan ekstensi yang Anda tetapkan yang dilindungi (dicadangkan) untuk mesin/lokasi yang dipilih.

© Acronis International GmbH, 2003-2024

Hasil pemeriksaan perlindungan data dapat ditemukan di dasbor pemantauan, di widget Peta Perlindungan Data, sebuah widget peta pohon yang menunjukkan detail pada tingkat mesin:

- Tingkat mesin – menampilkan informasi tentang status proteksi file-file penting per mesin milik pelanggan yang dipilih.



Untuk melindungi file yang tidak dilindungi, beralihlah ke blok dan klik **Lindungi semua file**. Di jendela dialog, Anda dapat menemukan informasi tentang jumlah file yang tidak terlindungi dan lokasinya. Untuk melindungi file-file tersebut, klik **Lindungi semua file**.

Anda juga dapat mengunduh laporan terperinci dalam format CSV.

Widget penilaian kerentanan

Mesin yang rentan

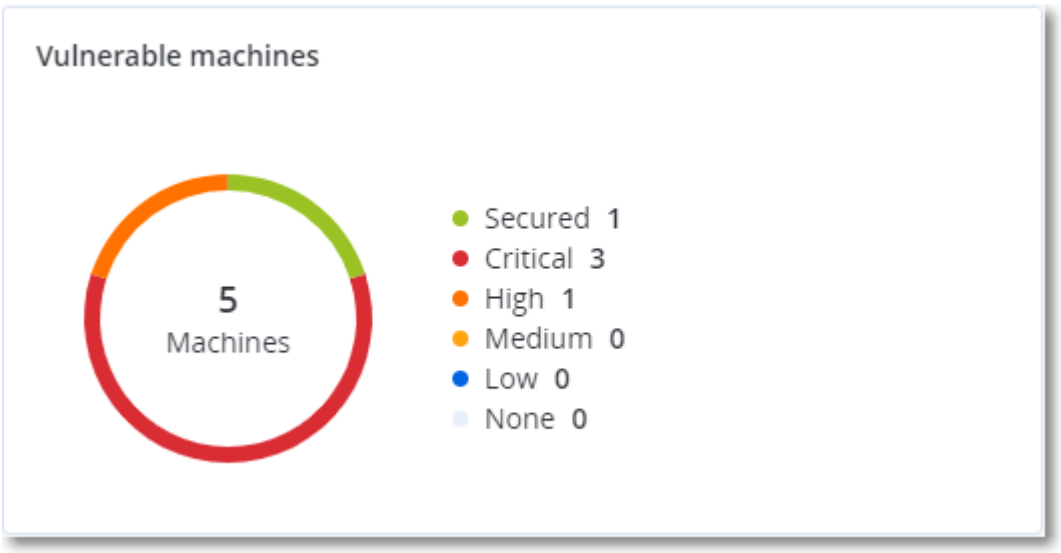
Widget ini menampilkan mesin yang rentan dengan tingkat kerentanan.

Kerentanan yang ditemukan dapat memiliki salah satu tingkat keparahan berikut berdasarkan Sistem Penilaian Kerentanan Umum (CVSS) v3.0:

- Aman: tidak ada kerentanan yang ditemukan
- Kritis: 9,0 - 10,0 CVSS
- Tinggi: 7,0 - 8,9 CVSS
- Sedang: 4,0 - 6,9 CVSS

© Acronis International GmbH, 2003-2024

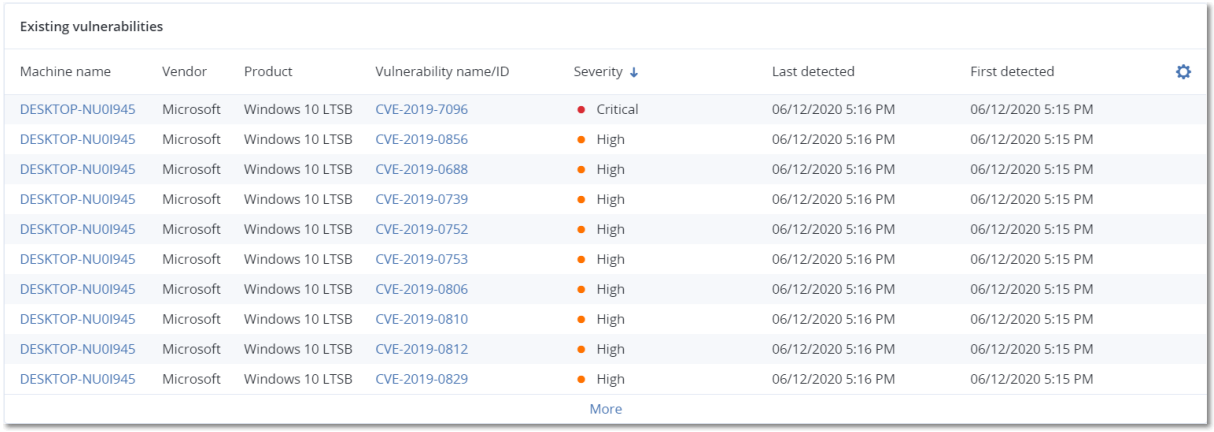
- Rendah: 0,1 - 3,9 CVSS
- Tidak ada: 0,0 CVSS



Kerentanan yang ada

Widget ini menampilkan kerentanan yang ada saat ini pada mesin. Di widget **Kerentanan yang ada**, terdapat dua kolom yang menunjukkan stempel waktu:

- **Terdeteksi pertama** – tanggal dan waktu saat kerentanan terdeteksi pertama kali pada mesin.
- **Terdeteksi terakhir** – tanggal dan waktu saat kerentanan terdeteksi terakhir kali pada mesin.



Widget instalasi patch

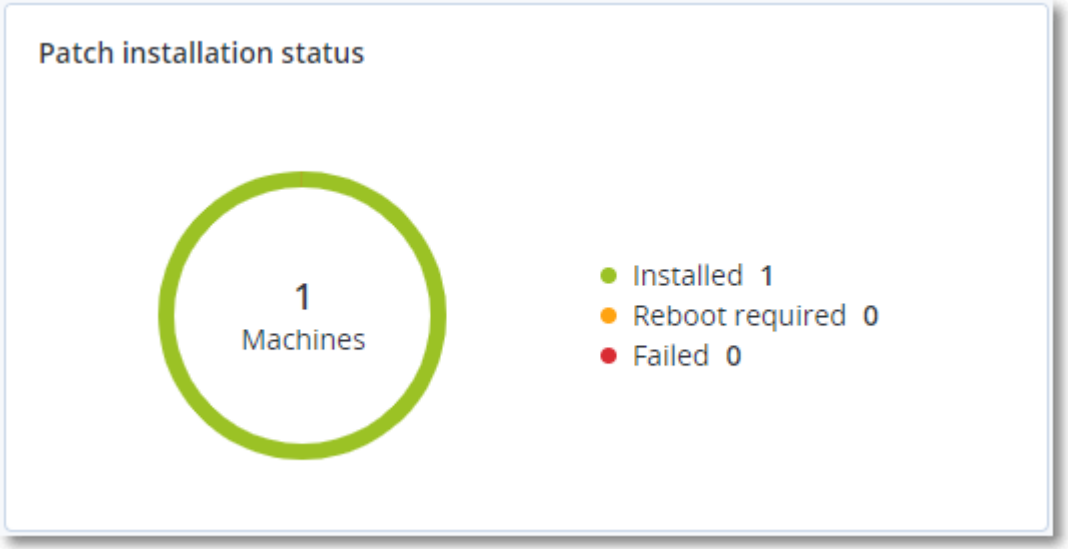
Ada empat widget terkait dengan fungsi pengelolaan patch.

Status instalasi patch

Widget ini menampilkan jumlah mesin yang dikelompokkan berdasarkan status instalasi patch.

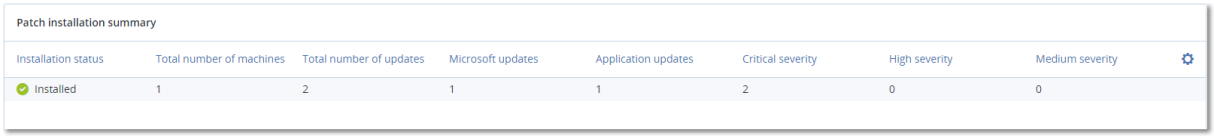
© Acronis International GmbH, 2003-2024

- **Diinstal** – semua patch yang tersedia sudah diinstal pada mesin
- **Boot ulang diperlukan** – setelah instalasi patch, boot ulang diperlukan untuk mesin
- **Gagal** – instalasi patch gagal pada mesin



Ringkasan instalasi patch

Widget ini menampilkan ringkasan patch pada mesin berdasarkan status instalasi patch.



Riwayat instalasi patch

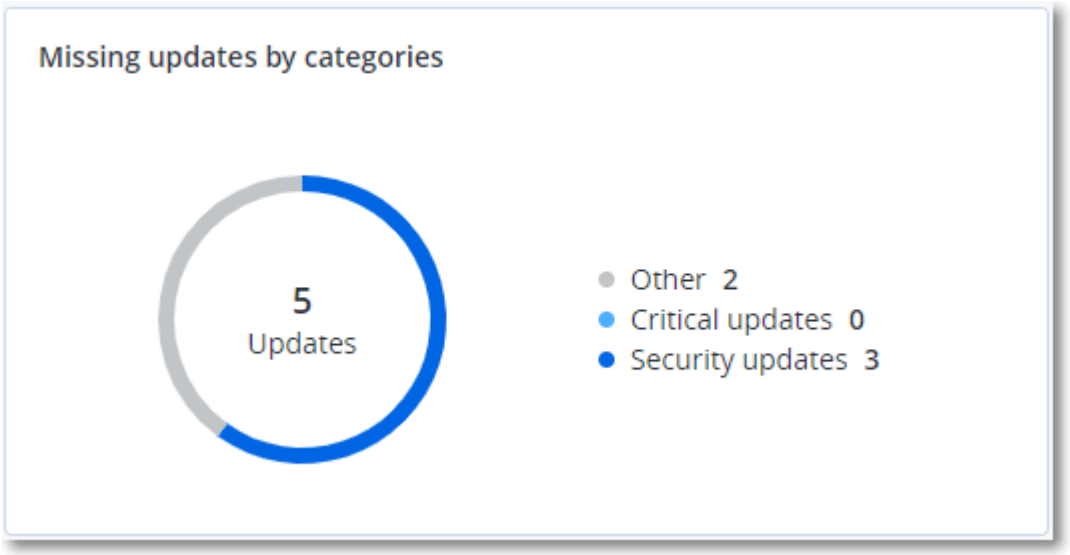
Widget ini menampilkan informasi terperinci tentang patch pada mesin.

Pembaruan yang tidak ada berdasarkan kategori

Widget ini menampilkan jumlah pembaruan yang tidak ada per kategori. Kategori berikut ini ditampilkan:

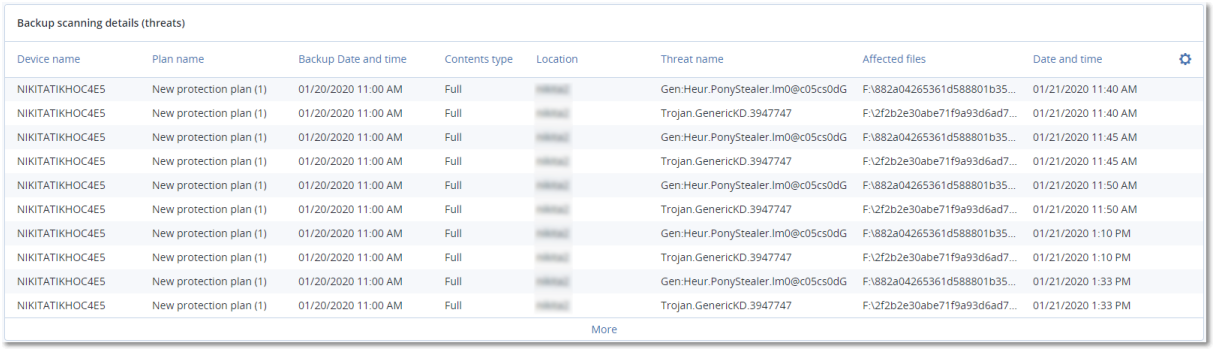
© Acronis International GmbH, 2003-2024

- Pembaruan keamanan
- Pembaruan penting
- Lain



Detail pemindaian cadangan

Widget ini menampilkan informasi terperinci tentang ancaman yang terdeteksi pada cadangan.


Backup scanning details (threats)

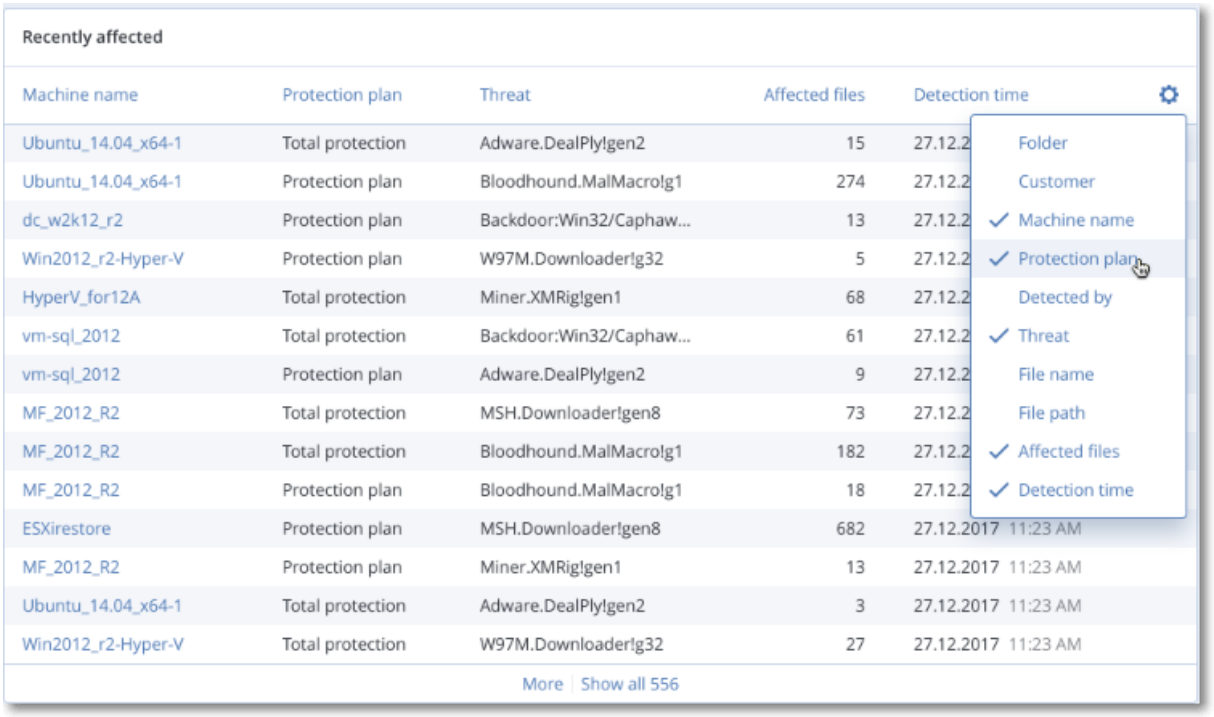
Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (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

Baru-baru ini terdampak

Widget ini menampilkan informasi mendetail tentang beban kerja yang terpengaruh oleh ancaman, seperti virus, malware, dan ramsomeware. Anda dapat menemukan informasi tentang ancaman yang terdeteksi, waktu ketika ancaman terdeteksi, dan berapa banyak file yang terpengaruh.

© Acronis International GmbH, 2003-2024



Mengunduh data untuk beban kerja yang terpengaruh baru-baru ini

Anda dapat mengunduh data untuk beban kerja yang terpengaruh baru-baru ini, membuat file CSV, dan mengirimkannya ke penerima yang Anda tentukan.

Cara mengunduh data untuk beban kerja yang terpengaruh baru-baru ini

1. Di widget **Terpengaruh baru-baru ini**, klik **Unduh data**.
2. Di bidang **Periode waktu**, masukkan jumlah hari yang Anda inginkan untuk mengunduh data. Jumlah hari maksimum yang dapat Anda masukkan adalah 200 hari.
3. Di bidang **Penerima**, masukkan alamat email semua orang yang akan menerima email dengan tautan untuk mengunduh file CSV.
4. Klik **Unduh**.

   Sistem mulai membuat file CSV dengan data untuk beban kerja yang terpengaruh dalam jangka waktu yang Anda tentukan. Ketika file CSV selesai, sistem mengirim email ke penerima. Setiap penerima kemudian dapat mengunduh file CSV.

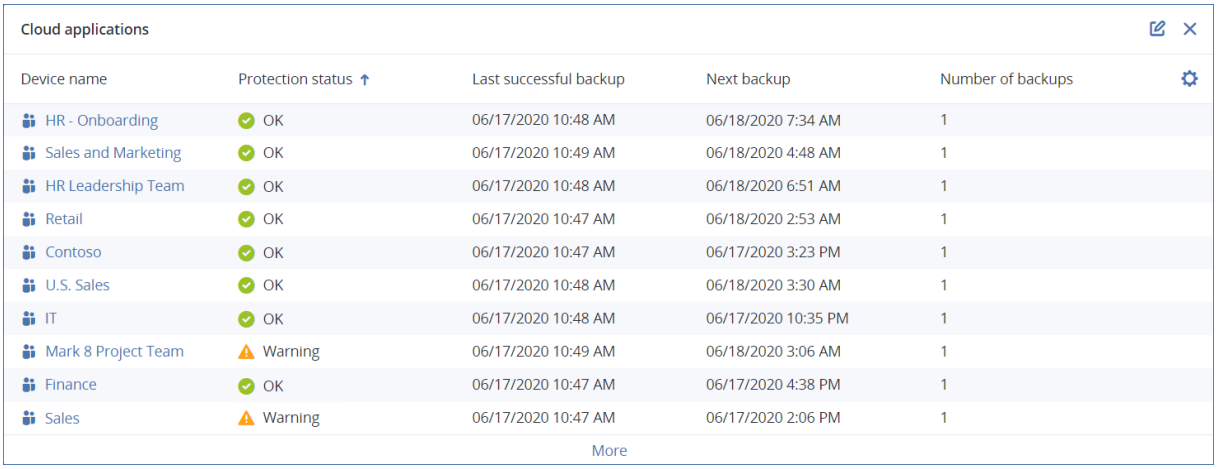
Aplikasi awan

Widget ini menampilkan informasi terperinci tentang sumber daya awan-ke-awan:

- Pengguna Microsoft 365 (kotak surat, OneDrive)
- Grup Microsoft 365 (kotak surat, situs grup)
- Folder umum Microsoft 365
- Kumpulan situs Microsoft 365

© Acronis International GmbH, 2003-2024

- Microsoft 365 Teams
- Pengguna Google Workspace (Gmail, Google Drive)
- Drive Shared Google Workspace

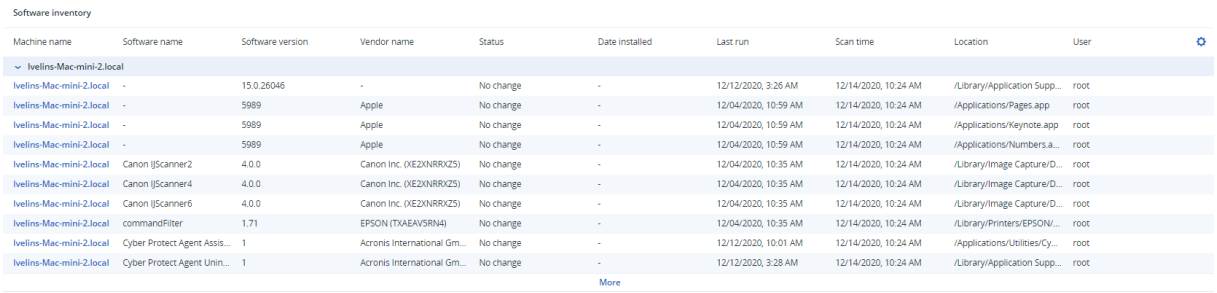


Informasi tambahan tentang sumber daya awan-ke-awan juga tersedia dalam widget berikut:

- Aktivitas
- Daftar aktivitas
- 5 peringatan terbaru
- Riwayat peringatan
- Ringkasan peringatan aktif
- Rangkuman peringatan riwayat
- Detail peringatan aktif
- Ringkasan lokasi

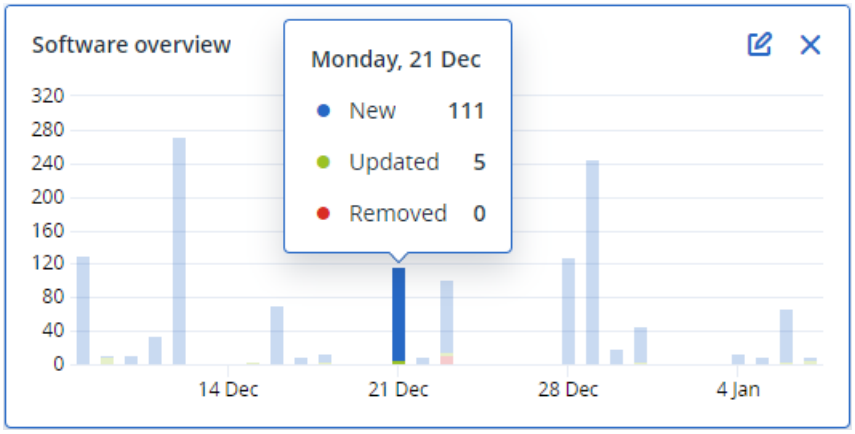
Widget inventaris perangkat lunak

Widget tabel **Inventaris perangkat lunak** menampilkan informasi terperinci tentang semua perangkat lunak yang diinstal pada perangkat Windows dan macOS di organisasi Anda.



Widget tabel **Perubahan perangkat lunak** menampilkan jumlah aplikasi baru, yang diperbarui, dan dihapus pada perangkat Windows dan macOS di organisasi klien Anda dalam kurun waktu tertentu (7 hari, 30 hari, atau bulan ini).

© Acronis International GmbH, 2003-2024



Saat Anda mengarahkan pointer mouse di atas bilah tertentu pada diagram, sebuah tooltip dengan informasi berikut menampilkan:

Baru - jumlah aplikasi yang baru diinstal.

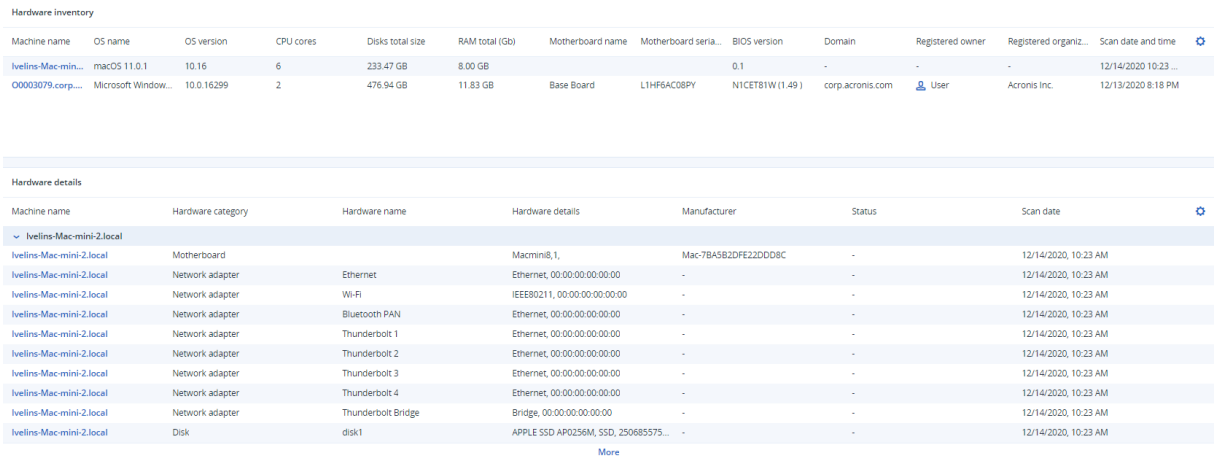
Diperbarui - jumlah aplikasi yang diperbarui.

Dihapus - jumlah aplikasi yang dihapus.

Saat Anda mengeklik bagian bilah yang sesuai dengan status tertentu, Anda akan dialihkan ke halaman **Manajemen Perangkat Lunak** -> **Inventaris Perangkat Lunak**. Informasi di halaman difilter untuk tanggal dan status yang sesuai.

Widget inventaris perangkat keras

Widget tabel **Inventaris perangkat keras** dan **Detail perangkat keras** menampilkan informasi tentang semua perangkat keras yang diinstal pada perangkat fisik dan virtual Windows dan macOS di organisasi Anda.



Widget tabel **Perubahan perangkat keras** menampilkan informasi tentang perangkat keras yang ditambahkan, dihapus, dan diubah pada perangkat fisik dan virtual Windows dan macOS di organisasi Anda untuk jangka waktu tertentu (7 hari, 30 hari, atau bulan saat ini).

© Acronis International GmbH, 2003-2024

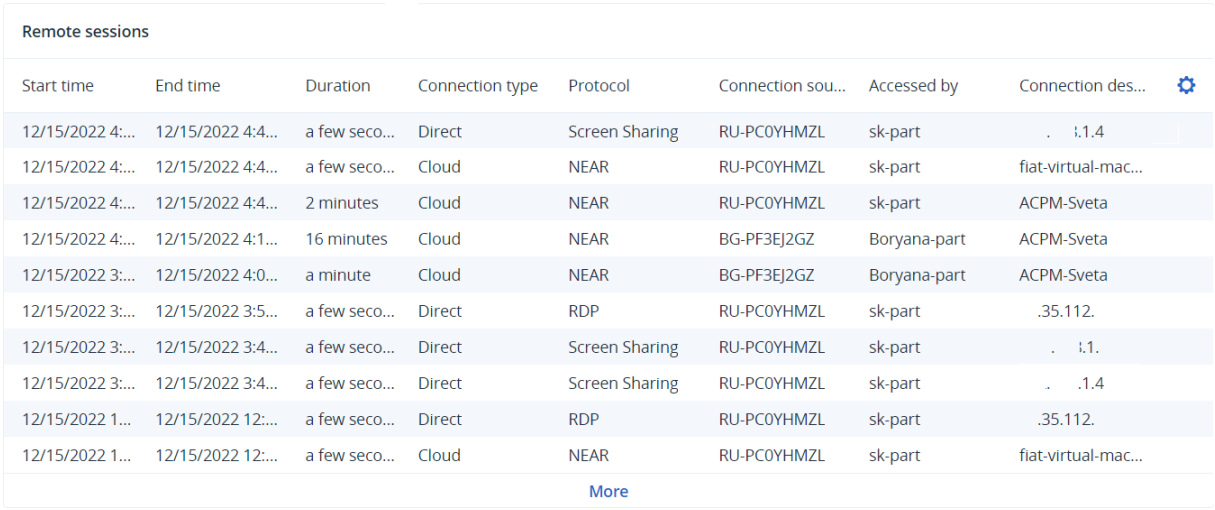
Hardware changes

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 sesi jarak jauh

Widget menunjukkan detail informasi tentang sesi desktop jarak jauh dan transfer 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

Proteksi cerdas

Umpan ancaman

Acronis Pusat Operasi Perlindungan Cyber (CPOC) mengeluarkan peringatan keamanan yang dikirimkan hanya ke wilayah yang terkait secara geografis. Peringatan keamanan ini menyediakan informasi tentang malware, kerentanan, bencana alam, kesehatan publik, dan jenis peristiwa global lainnya yang dapat berdampak pada perlindungan data Anda. Umpan ancaman memberi tahu Anda tentang potensi ancaman dan memungkinkan Anda untuk mencegahnya.

Catatan

Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Beberapa peringatan keamanan dapat diselesaikan dengan mengikuti serangkaian tindakan spesifik yang disediakan oleh pakar keamanan. Peringatan keamanan lainnya hanya memberi tahu Anda tentang ancaman yang akan datang tetapi tidak memberi saran tindakan.

© Acronis International GmbH, 2003-2024

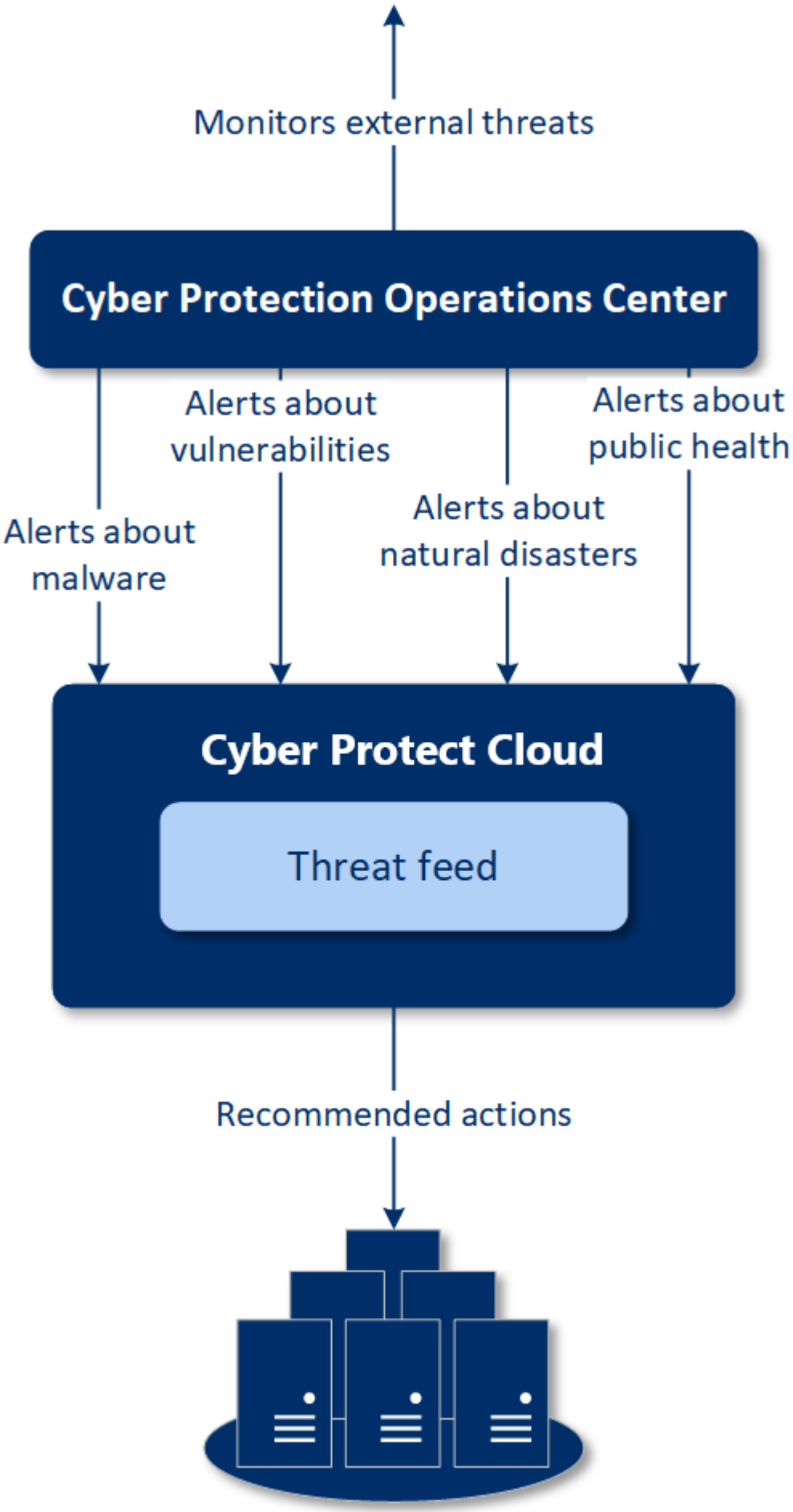
Catatan
Peringatan malware hanya diberikan untuk mesin yang memiliki agen untuk Proteksi antimalware yang terinstal.

Cara kerjanya

Pusat Operasi Perlindungan Cyber Acronis memantau ancaman eksternal dan membuat peringatan tentang ancaman malware, kerentanan, bencana alam, dan kesehatan publik. Anda akan dapat melihat semua peringatan ini di konsol Cyber Protect, di bagian **Umpan ancaman**. Anda dapat menjalankan tindakan terkait yang direkomendasikan, tergantung pada jenis peringatan.

Alur kerja utama umpan ancaman digambarkan dalam diagram berikut.

© Acronis International GmbH, 2003-2024



© Acronis International GmbH, 2003-2024

Untuk menjalankan tindakan yang direkomendasikan pada peringatan yang diterima dari Pusat Operasi Perlindungan Cyber Acronis, lakukan hal-hal berikut:

1. Di konsol Cyber Protect, buka **Pemantauan**> **Umpan ancaman** untuk meninjau apakah ada peringatan keamanan yang ada.
2. Pilih peringatan dalam daftar dan tinjau detail yang diberikan.
3. Klik **Mulai** untuk membuka wizard.
4. Aktifkan tindakan yang ingin Anda lakukan dan mesin untuk menerapkan tindakan ini. Tindakan berikut dapat direkomendasikan:
   - **Penilaian kerentanan** – untuk memindai kerentanan pada mesin
   - **Manajemen patch** – untuk menginstal patch di mesin yang dipilih
   - **Perlindungan Antimalware** – untuk menjalankan pemindaian menyeluruh pada mesin yang dipilih

     Catatan
     Tindakan ini hanya tersedia untuk mesin yang menginstal agen untuk perlindungan antimalware.

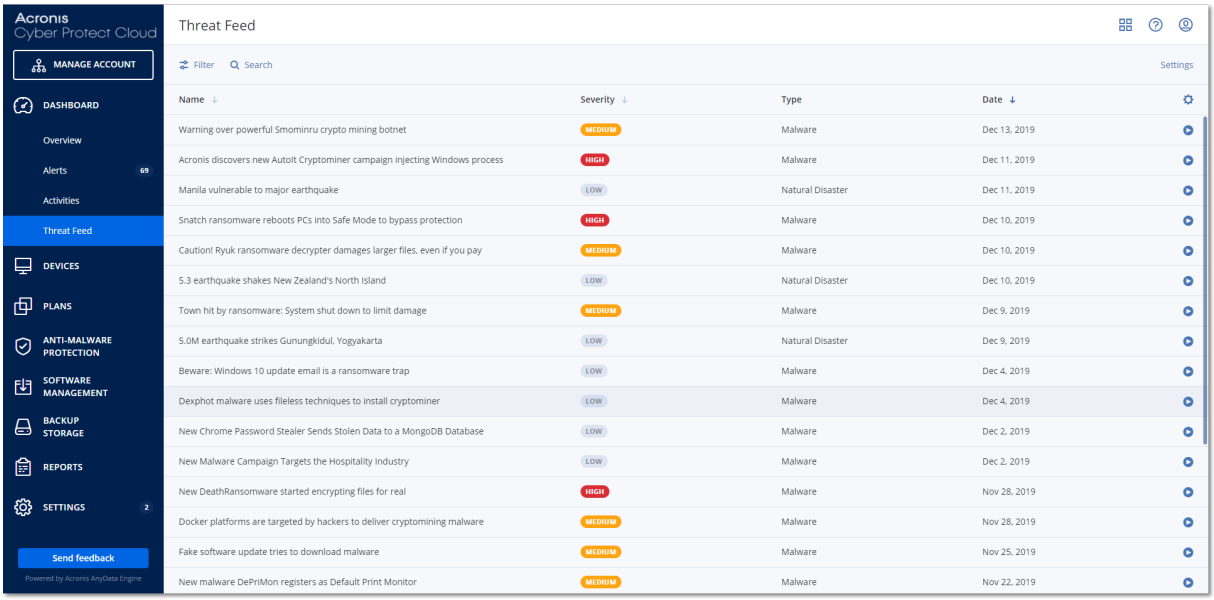
   - **Cadangan mesin yang dilindungi atau tidak dilindungi** – untuk mencadangkan beban kerja yang dilindungi dan tidak dilindungi.
     Jika belum ada cadangan untuk beban kerja (di semua lokasi yang dapat diakses, awan dan lokal), atau cadangan yang ada dienkripsi, sistem akan membuat cadangan penuh dengan format nama berikut:

     ```
     %workload_name%-Remediation
     ```

     Secara default, tujuan pencadangan adalah penyimpanan Cyber Protect Cloud, tetapi Anda dapat mengonfigurasi lokasi lain sebelum memulai operasi.

     Jika cadangan tidak terenkripsi sudah ada, sistem akan membuat cadangan bertahap di arsip yang ada.
5. Klik **Mulai**.
6. Di halaman **Aktivitas**, verifikasi bahwa aktivitas berhasil dilakukan.

© Acronis International GmbH, 2003-2024



Menghapus semua peringatan

Pembersihan otomatis dari umpan ancaman dilakukan setelah jangka waktu berikut:

- Bencana alam – 1 minggu
- Kerentanan – 1 bulan
- Malware – 1 bulan
- Kesehatan publik – 1 minggu

Peta perlindungan data

Fungsi Peta perlindungan data memungkinkan Anda untuk

- Untuk mendapatkan informasi terperinci tentang data yang disimpan (klasifikasi, lokasi, status perlindungan, dan informasi tambahan) di mesin Anda.
- Untuk mendeteksi dilindungi atau tidaknya data. Data dianggap dilindungi jika dilindungi dengan cadangan (rencana proteksi dengan modul pencadangan yang diaktifkan).
- Untuk melakukan tindakan perlindungan data.

Cara kerjanya

1. Pertama, Anda membuat rencana proteksi dengan modul Peta pencarian data diaktifkan.
2. Kemudian, setelah rencana dijalankan dan data Anda ditemukan dan dianalisis, Anda akan memperoleh representasi visual tentang perlindungan data di widget Peta perlindungan data.
3. Anda juga dapat membuka **Perangkat** > **Peta perlindungan data** dan menemukan informasi tentang file yang tidak terlindungi si setiap perangkat.
4. Anda dapat melakukan tindakan untuk melindungi file yang tidak terlindungi yang terdeteksi pada perangkat.

© Acronis International GmbH, 2003-2024

Mengelola file yang tidak terlindungi yang terdeteksi

Untuk melindungi file penting yang terdeteksi sebagai tidak terlindungi, lakukan hal berikut:

1. Di konsol Cyber Protect, buka **Perangkat** > **Peta perlindungan data**.

   Dalam daftar perangkat, Anda dapat menemukan informasi umum tentang jumlah file yang tidak terlindungi, ukuran file tersebut per perangkat, dan penemuan data terakhir.

   Untuk melindungi file pada mesin tertentu, klik ikon Elipsis lalu **Lindungi semua file**. Anda akan dialihkan ke daftar rencana di mana Anda dapat membuat rencana proteksi dengan modul pencadangan yang diaktifkan.

   Untuk menghapus perangkat tertentu dengan file yang tidak terlindungi dari daftar, klik **Sembunyikan hingga penemuan data berikutnya**.
2. Untuk melihat informasi terperinci tentang file yang tidak terlindungi pada perangkat tertentu, klik nama perangkat.

   Anda akan melihat jumlah file yang tidak terlindungi per ekstensi dan per lokasi. Tentukan ekstensi di bidang pencarian, yang ingin Anda dapatkan informasinya tentang file yang tidak terlindungi.
3. Untuk melindungi semua file yang tidak terlindungi, klik **Lindungi semua file**. Anda akan dialihkan ke daftar rencana di mana Anda dapat membuat rencana proteksi dengan modul pencadangan yang diaktifkan.

Untuk mendapatkan informasi tentang file yang tidak terlindungi dalam bentuk laporan, klik **Unduh laporan terperinci dalam CSV**.

Pengaturan peta perlindungan data

Untuk mempelajari cara membuat rencana proteksi dengan modul Peta perlindungan data, lihat "Membuat rencana proteksi".

Pengaturan berikut dapat ditetapkan untuk modul Peta perlindungan data.

Jadwal

Anda dapat menetapkan pengaturan yang berbeda untuk membuat jadwal pelaksanaan tugas peta perlindungan data.

Bidang	Deskripsi
Jadwalkan operasi tugas menggunakan peristiwa berikut	Pengaturan ini menentukan kapan tugas akan dijalankan. Nilai berikut tersedia: • **Jadwalkan berdasarkan waktu** – Ini adalah pengaturan default. Tugas akan berjalan sesuai waktu yang ditentukan. • **Saat pengguna masuk ke sistem** – Secara default, akses masuk (login) pengguna mana pun akan memicu tugas. Anda dapat mengubah pengaturan ini agar hanya akun pengguna tertentu yang dapat memicu tugas.

© Acronis International GmbH, 2003-2024

Bidang	Deskripsi
	• **Saat pengguna keluar dari sistem** – Secara default, akses keluar (logoff) pengguna mana pun akan memicu tugas. Anda dapat mengubah pengaturan ini agar hanya akun pengguna tertentu yang dapat memicu tugas. **Catatan** Tugas tidak akan berjalan saat sistem dimatikan. Mematikan dan keluar adalah peristiwa berbeda di konfigurasi penjadwalan. • **Pada startup sistem** – Tugas akan berjalan saat sistem operasi dimulai. • **Pada shutdown sistem** – Tugas akan berjalan saat sistem operasi dimatikan.
Jenis jadwal	Bidang ini muncul jika di **Jadwalkan operasi tugas menggunakan peristiwa berikut** Anda telah memilih **Jadwalkan berdasarkan waktu**. Nilai berikut tersedia: • **Bulanan** – Pilih bulan dan minggu atau hari dalam sebulan saat tugas akan berjalan. • **Harian** – Ini adalah pengaturan default. Pilih hari dalam seminggu saat tugas akan dijalankan. • **Per jam** – Pilih hari dalam pekan, jumlah pengulangan, dan interval waktu tugas akan berjalan.
Mulai pada	Bidang ini muncul jika di **Jadwalkan operasi tugas menggunakan peristiwa berikut** Anda telah memilih **Jadwalkan berdasarkan waktu** Pilih waktu yang tepat kapan tugas akan dijalankan.
Jalankan dalam rentang tanggal	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Jadwalkan berdasarkan waktu**. Atur periode waktu ketika jadwal yang sudah dikonfigurasi akan berlaku.
Tentukan akun pengguna yang akses masuknya ke sistem operasi akan memulai tugas	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Saat pengguna masuk ke sistem**. Nilai berikut tersedia: • **Semua pengguna** - Gunakan opsi ini jika Anda ingin akses masuk pengguna mana pun memicu tugas. • **Pengguna berikut** - Gunakan opsi ini jika Anda hanya ingin akses masuk akun pengguna tertentu yang memicu tugas.
Tentukan akun pengguna yang logout-nya dari	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Saat pengguna keluar dari sistem**.

© Acronis International GmbH, 2003-2024

Bidang	Deskripsi
sistem operasi akan memulai tugas	Nilai berikut tersedia: • **Pengguna mana pun** - Gunakan opsi ini jika Anda ingin logout pengguna mana pun memicu tugas. • **Pengguna berikut** - Gunakan opsi ini jika Anda hanya ingin logout akun pengguna tertentu yang memicu tugas.
Persyaratan untuk memulai	Mendefinisikan semua kondisi yang harus dipenuhi secara bersamaan agar tugas dapat dijalankan. Kondisi awal untuk pemindaian antimalware serupa dengan kondisi awal untuk **Modul cadangan** yang dijelaskan dalam "Persyaratan untuk memulai". Anda dapat menetapkan persyaratan awal tambahan berikut: • **Distribusikan waktu mulai tugas dalam rentang waktu** – Opsi ini memungkinkan Anda menentukan jangka waktu tugas untuk menghindari kemacetan jaringan. Anda dapat menentukan penundaan dalam jam atau menit. Misalnya, jika waktu mulai default adalah pukul 10.00 dan penundaannya adalah 60 menit, tugas akan dimulai antara pukul 10.00 sampai 11.00. • **Jika mesin dimatikan, jalankan tugas yang tertinggal pada saat mesin dinyalakan** • **Cegah mode tidur atau hibernasi selama menjalankan tugas** – Opsi ini hanya berlaku untuk mesin yang menjalankan Windows. • **Jika persyaratan awal tidak terpenuhi, tetap jalankan tugas setelahnya** – Tentukan periode waktu dalam jam saat tugas akan dijalankan setelahnya, terlepas dari kondisi awal lainnya. **Catatan** Persyaratan awal tidak didukung untuk Linux.

Aturan pengecualian dan ekstensi

Pada tab **Ekstensi**, Anda dapat tentukan daftar ekstensi file yang akan dianggap penting selama penemuan data dan memeriksa apakah ekstensi tersebut dilindungi. Gunakan format berikut untuk menentukan ekstensi:

```
.html, .7z, .docx, .zip, .pptx, .xml
```

Pada tab **Aturan pengecualian**, Anda dapat menentukan file dan folder mana yang tidak ingin diperiksa status proteksinya selama penemuan data.

- **File dan folder tersembunyi** – jika dipilih, file dan folder tersembunyi akan dilewati selama pemeriksaan data.
- **File dan folder sistem** – jika dipilih, file dan folder tersembunyi akan dilewati selama pemeriksaan data.

© Acronis International GmbH, 2003-2024

Tab Aktivitas

Tab **Aktivitas** memberikan gambaran umum tentang aktivitas dari 90 hari terakhir.

Untuk memfilter aktivitas pada dasbor

1. Di bidang **Nama perangkat**, tentukan mesin tempat aktivitas dilakukan.
2. Dari daftar dropdown **Status**, pilih statusnya. Misalnya, berhasil, gagal, sedang berlangsung, dibatalkan.
3. Dari daftar dropdown **Tindakan jarak jauh**, pilih tindakannya. Misalnya, menerapkan rencana, menghapus cadangan, menginstal pembaruan perangkat lunak.
4. Di bidang **Terbaru**, atur periode aktivitas. Misalnya, aktivitas terbaru, aktivitas 24 jam terakhir, atau aktivitas selama periode tertentu dalam 90 hari terakhir.
5. Jika Anda mengakses tab **Aktivitas** sebagai administrator mitra, Anda dapat memfilter aktivitas untuk pelanggan tertentu yang Anda kelola.

Untuk menyesuaikan tampilan tab **Aktivitas**, klik ikon roda gigi, dan kemudian pilih kolom yang ingin Anda lihat. Untuk melihat kemajuan aktivitas secara real time, pilih kotak centang **Refresh otomatis**.

Untuk membatalkan aktivitas yang sedang berjalan, klik namanya, lalu, pada layar **Rincian**, klik **Batalkan**.

Anda dapat mencari aktivitas yang terdaftar dengan kriteria berikut:

- Nama perangkat
  Ini adalah mesin tempat aktivitas dilakukan.
- Dimulai oleh
  Ini adalah akun yang memulai aktivitas.

Aktivitas desktop jarak jauh dapat difilter menurut properti berikut:

- Membuat rencana
- Menerapkan rencana
- Membatalkan rencana
- Menghapus rencana
- Koneksi jarak jauh
  - Koneksi desktop jarak jauh awan melalui RDP
  - Koneksi desktop jarak jauh awan melalui NEAR
  - Koneksi desktop jarak jauh awan melalui Apple Berbagi Layar
  - Koneksi desktop jarak jauh melalui klien web
  - Koneksi desktop jarak jauh melalui Bantuan Cepat
  - Koneksi desktop jarak jauh langsung melalui RDP

© Acronis International GmbH, 2003-2024

- Koneksi desktop jarak jauh langsung melalui Apple Berbagi Layar
- Transfer file
- Transfer file melalui Bantuan Cepat

- Tindakan jarak jauh
  - Mematikan beban kerja
  - Memulai ulang beban kerja
  - Mengeluarkan pengguna jarak jauh pada beban kerja
  - Mengosongkan keranjang sampah untuk pengguna pada beban kerja
  - Mengaktifkan mode tidur pada beban kerja

Monitor Cyber Protect

Cyber Protect Monitor menunjukkan informasi tentang status proteksi mesin tempat Agent untuk Windows atau Agent untuk Mac diinstal, dan memungkinkan pengguna untuk mengkonfigurasi pengaturan enkripsi cadangan dan server proxy.

Ketika Agen untuk File Sync & Share diinstal pada mesin, Cyber Protect Monitor menyediakan akses ke layanan File Sync & Share. Fungsi File Sync & Share dapat diakses setelah proses onboarding wajib. Selama itu, pengguna masuk ke akun File Sync & Share mereka sendiri dan memilih folder sinkronisasi pribadi. Untuk informasi lebih lanjut tentang Agen untuk File Sync & Share, lihat Cyber Files Cloud panduan pengguna.

Penting
Cyber Protect Monitor dapat diakses oleh pengguna yang mungkin tidak memiliki hak administratif untuk Cyber Protection atau layanan File Sync & Share.

Tabel di bawah ini merangkum operasi yang tersedia untuk pengguna tanpa hak administratif.

Agen yang dipasang	Pengguna dapat	Pengguna tidak dapat
Agen untuk Windows atau Agen untuk Mac	• Menerapkan rencana proteksi default pada mesin mereka • Memeriksa status proteksi mesin mereka • Menerima notifikasi Perlindungan Aktif • Menjeda pencadangan mesin mereka untuk sementara • Mengkonfigurasikan pengaturan server proxy • Mengubah pengaturan enkripsi cadangan	• Menerapkan rencana proteksi khusus • Mengelola rencana proteksi yang sudah diterapkan

© Acronis International GmbH, 2003-2024

Agen yang dipasang	Pengguna dapat	Pengguna tidak dapat
	Peringatan! Mengubah pengaturan enkripsi di Cyber Protect Monitor menimpa pengaturan dalam rencana proteksi dan mempengaruhi semua cadangan dari mesin. Operasi ini dapat menyebabkan beberapa rencana proteksi gagal. Untuk informasi lebih lanjut, lihat "Enkripsi" (hlm. 441). Tidak ada cara untuk memulihkan cadangan terenkripsi jika Anda menghilangkan atau lupa kata sandi.	
Agen untuk Windows dan Agen untuk Sync & Share Agen untuk Mac dan Agen untuk Sync & Share	• Menyinkronkan konten antara folder sinkronisasi lokal dan akun File Sync & Share mereka • Menjeda operasi sinkronisasi • Mengubah folder sinkronisasi • Memeriksa jenis file yang tidak dapat disinkronisasi	• Mengedit jenis file yang tidak dapat disinkronisasi

Mengonfigurasi pengaturan server proxy di Cyber Protect Monitor

Anda dapat mengonfigurasi pengaturan server proxy di Cyber Protect Monitor. Konfigurasi tersebut akan mempengaruhi semua agen yang diinstal pada mesin.

Untuk mengonfigurasi pengaturan server proxy

1. Buka Cyber Protect Monitor, lalu klik ikon roda di ujung kanan atas.
2. Klik **Pengaturan**, lalu klik **Proxy**.
3. Aktifkan tombol **Gunakan server proxy**, lalu masukkan alamat dan port server proxy.
4. [Jika akses server proxy dilindungi kata sandi] Aktifkan pilihan **Kata sandi dibutuhkan**, lalu masukkan nama pengguna dan kata sandi untuk mengakses server proxy.
5. Klik **Simpan**.

   Pengaturan server proxy disimpan di file `http-proxy.yaml`.

Laporan

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

© Acronis International GmbH, 2003-2024

Laporan tentang operasi dapat mencakup set widget dasbor apa pun. Semua widget menunjukkan informasi ringkasan untuk seluruh perusahaan.

Bergantung pada tipe widget, laporan tersebut mencakup data untuk suatu rentang waktu atau untuk saat penjelajahan atau pembuatan laporan. Lihat "Data yang dilaporkan berdasarkan tipe widget" (hlm. 315).

Semua widget historis menampilkan data untuk rentang waktu yang sama. Anda dapat mengubah rentang ini di pengaturan laporan.

Anda dapat menggunakan laporan default atau membuat laporan kustom.

Anda dapat mengunduh laporan atau mengirimnya melalui email dalam format XLSX (Excel) atau PDF.

Set laporan default bergantung dari edisi layanan Cyber Protection yang Anda miliki. Laporan default tercantum di bawah ini:

Nama laporan	Deskripsi
Skor #CyberFit berdasarkan mesin	Menampilkan Skor #CyberFit, berdasarkan evaluasi metrik kemanan dan konfigurasi untuk setiap mesin, serta rekomendasi untuk penyempurnaan.
Peringatan	Menampilkan peringatan yang terjadi selama periode waktu tertentu.
Detail pemindaian cadangan	Menampilkan informasi terperinci tentang ancaman yang terdeteksi dalam cadangan.
Aktivitas sehari-hari	Menampilkan informasi ringkasan tentang aktivitas yang dilakukan selama periode waktu tertentu.
Peta perlindungan data	Menampilkan informasi terperinci tentang jumlah, ukuran, lokasi, status proteksi semua file penting dalam mesin.
Ancaman terdeteksi	Menampilkan perincian mesin yang terdampak melalui jumlah ancaman yang diblokir serta mesin yang sehat dan rentan.
Mesin yang ditemukan	Menampilkan semua mesin yang ditemukan dalam jaringan organisasi.
Prediksi kesehatan disk	Menampilkan prediksi ketika HDD/SSD Anda akan rusak dan status disk saat ini.
Kerentanan yang ada	Menampilkan kerentanan yang ada untuk OS dan aplikasi dalam organisasi Anda. Laporan juga menampilkan rincian mesin yang terdampak dalam jaringan Anda untuk setiap produk yang tercantum.
Inventaris perangkat	Menampilkan informasi tentang perangkat lunak yang diinstal pada perangkat perusahaan Anda.

© Acronis International GmbH, 2003-2024

lunak	
Inventaris perangkat keras	Menampilkan informasi tentang perangkat keras yang tersedia pada perangkat perusahaan Anda.
Rangkuman manajemen patch	Menampilkan jumlah patch yang tidak ada, patch yang diinstal, dan patch yang diterapkan. Anda dapat memperinci laporan untuk mendapatkan informasi patch yang hilang/terinstal serta perincian semua sistem.
Ringkasan	Menampilkan informasi ringkasan tentang perangkat terlindungi untuk periode waktu tertentu.
Aktivitas mingguan	Menampilkan informasi ringkasan tentang aktivitas yang dilakukan selama periode waktu tertentu.
Sesi jarak jauh	Menampilkan informasi tentang sesi desktop jarak jauh dan transfer file.

Tindakan dengan laporan

Untuk menampilkan laporan, klik namanya.

Untuk menambahkan laporan baru

1. Di konsol Cyber Protect, buka **Laporan**.
2. Pada daftar laporan yang tersedia, klik **Tambah laporan**.
3. [Untuk menambahkan laporan yang telah ditetapkan] Klik nama laporan yang telah ditetapkan.
4. [Untuk menambahkan laporan kustom] Klik **Kustom**, lalu tambahkan widget ke laporan.
5. [Opsional] Seret dan lepas widget untuk menyusunnya kembali.

Untuk mengedit laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan yang ingin Anda edit.
   Anda dapat melakukan hal berikut:
   - Mengganti nama laporan.
   - Mengubah rentang waktu untuk semua widget dalam laporan.
   - Menentukan penerima laporan dan kapan laporan akan dikirim ke mereka. Format yang tersedia adalah PDF dan XLSX.

Untuk menghapus laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan yang ingin Anda hapus.
3. Klik ikon elipsis (...), lalu klik **Hapus**.
4. Konfirmasikan pilihan Anda dengan mengeklik **Hapus**.

© Acronis International GmbH, 2003-2024

Untuk menjadwalkan laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan yang ingin Anda jadwalkan, lalu klik **Pengaturan**.
3. Aktifkan switch **Terjadwal**.
   - Tentukan alamat email penerima.
   - Pilih format laporan.

     Catatan
     Anda dapat mengekspor hingga 1000 item dalam file PDF dan hingga 10.000 item dalam file XLSX. Tanda waktu di file PDF dan XLSX menggunakan waktu lokal mesin Anda.

   - Pilih bahasa laporan.
   - Konfigurasikan jadwal.
4. Klik **Simpan**.

Untuk mengunduh laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan, lalu klik **Unduh**.
3. Pilih format laporan.

Untuk mengirim laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan, lalu klik **Kirim**.
3. Tentukan alamat email penerima.
4. Pilih format laporan.
5. Klik **Kirim**.

Untuk mengekspor struktur laporan

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan.
3. Klik ikon elipsis (...), lalu klik **Ekspor**.

Hasilnya, struktur laporan disimpan di mesin Anda sebagai file JSON.

Untuk membuang data laporan

Dengan menggunakan opsi ini, Anda dapat mengekspor semua data selama periode kustom, tanpa filter, ke file CSV dan mengirim file CSV ke penerima email.

© Acronis International GmbH, 2003-2024

Catatan
Anda dapat mengekspor hingga 150.000 item dalam file CSV. Tanda waktu di file CSV menggunakan Waktu Universal Terkoordinasi (UTC).

1. Di konsol Cyber Protect, buka **Laporan**.
2. Di daftar laporan, pilih laporan yang datanya ingin Anda buang.
3. Klik ikon elipsis (...), lalu klik **Buang data**.
4. Tentukan alamat email penerima.
5. Di **Rentang waktu**, tentukan periode kustom kapan Anda ingin membuang data.

   Catatan
   Menyiapkan file CSV untuk periode lebih lama memakan waktu lebih lama.

6. Klik **Kirim**.

Data yang dilaporkan berdasarkan tipe widget

Berdasarkan rentang data yang ditampilkannya, widget pada dasbor terdiri dari dua tipe:

- Widget yang menampilkan data aktual pada saat penjelajahan atau pembuatan laporan.
- Widget yang menampilkan data historis.

Saat Anda mengonfigurasi rentang tanggal dalam pengaturan laporan untuk menghapus data untuk periode tertentu, rentang waktu yang dipilih akan berlaku hanya untuk widget yang menampilkan data historis. Untuk widget yang menampilkan data aktual pada saat penjelajahan, parameter rentang waktu tidak berlaku.

Tabel berikut mencantumkan widget yang tersedia dan rentang datanya.

Nama widget	Data yang ditampilkan di widget dan laporan
Skor #CyberFit berdasarkan mesin	Aktual
5 peringatan terbaru	Aktual
Detail peringatan aktif	Aktual
Ringkasan peringatan aktif	Aktual
Aktivitas	Historis
Daftar aktivitas	Historis
Riwayat peringatan	Historis
Statistik taktik serangan	Historis

© Acronis International GmbH, 2003-2024

Detail pemindaian cadangan (ancaman)	Historis
Status cadangan	Historis - dalam kolom **Total berjalan** dan **Jumlah berhasil berjalan** Aktual - di semua kolom lainnya
URL yang diblokir	Aktual
Aplikasi awan	Aktual
Cyber protection	Aktual
Peta perlindungan data	Historis
Perangkat	Aktual
Mesin yang ditemukan	Aktual
Gambaran umum kesehatan disk	Aktual
Status kesehatan disk berdasarkan perangkat fisik	Aktual
Kerentanan yang ada	Historis
Perubahan perangkat keras	Historis
Detail perangkat keras	Aktual
Inventaris perangkat keras	Aktual
Rangkuman peringatan riwayat	Historis
Riwayat keparahan insiden	Historis
Ringkasan lokasi	Aktual
Pembaruan yang tidak ada berdasarkan kategori	Aktual
Tidak terlindungi	Aktual
Riwayat instalasi patch	Historis
Status instalasi patch	Historis
Ringkasan instalasi patch	Historis
Status proteksi	Aktual
Baru-baru ini terdampak	Historis
Sesi jarak jauh	Historis
Burndown insiden keamanan	Historis

© Acronis International GmbH, 2003-2024

MTTR insiden keamanan	Historis
Inventaris perangkat lunak	Aktual
Ikhtisar perangkat lunak	Historis
Status ancaman	Aktual
Mesin yang rentan	Aktual
Status jaringan beban kerja	Aktual

© Acronis International GmbH, 2003-2024

Mengelola beban kerja di konsol Cyber Protect

Bagian ini menjelaskan cara mengelola beban kerja Anda di konsol Cyber Protect.

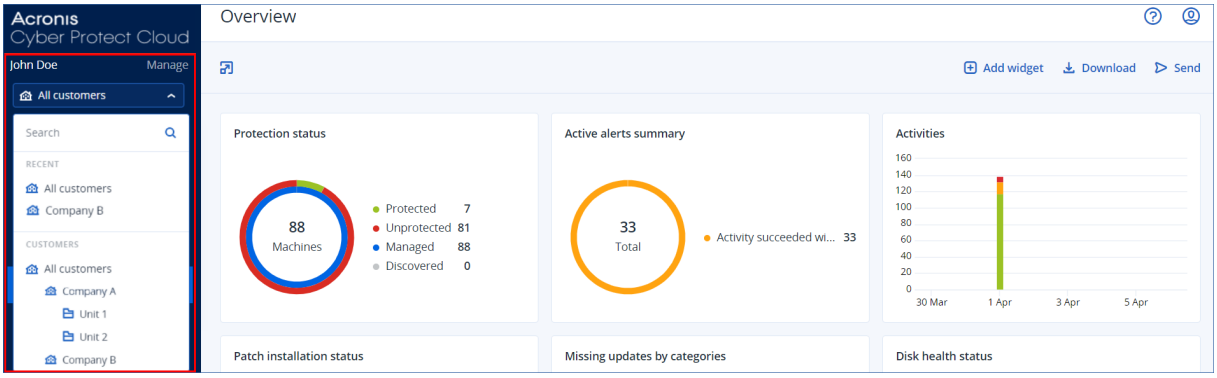
Konsol Cyber Protect

Di konsol Cyber Protect, Anda dapat mengelola beban kerja dan rencana, mengubah pengaturan proteksi, mengonfigurasi laporan, atau memeriksa penyimpanan cadangan.

Konsol Cyber Protect menyediakan akses ke layanan atau fitur tambahan, seperti File Sync & Share atau Antivirus dan Proteksi Antimalware, Manajemen patch, Kontrol perangkat, dan penilaian Kerentanan. Jenis dan jumlah layanan serta fitur ini berbeda-beda sesuai dengan lisensi Cyber Protection Anda.

Untuk memeriksa dasbor dengan informasi terpenting tentang proteksi Anda, buka **Pemantauan** > **Gambaran Umum**.

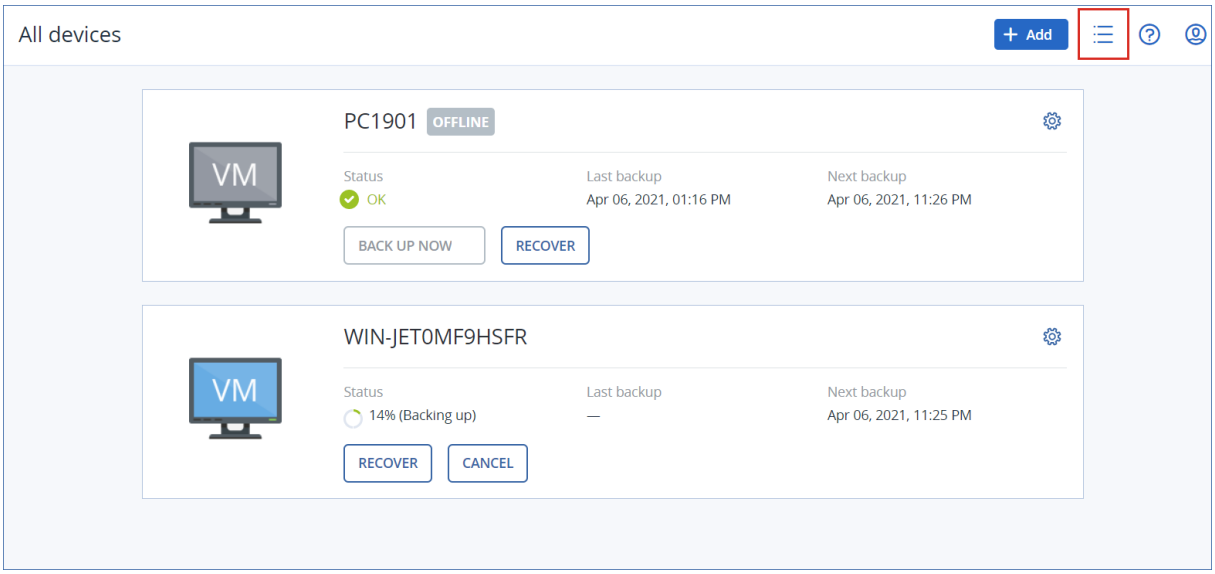
Bergantung pada izin akses, Anda dapat mengelola perlindungan untuk satu atau beberapa penyewa atau unit pelanggan pada suatu penyewa. Untuk mengganti level hierarki, gunakan daftar drop-down di menu navigasi. Hanya tingkat di mana Anda memiliki akses yang akan ditampilkan. Untuk membuka portal manajemen, klik **Kelola**.



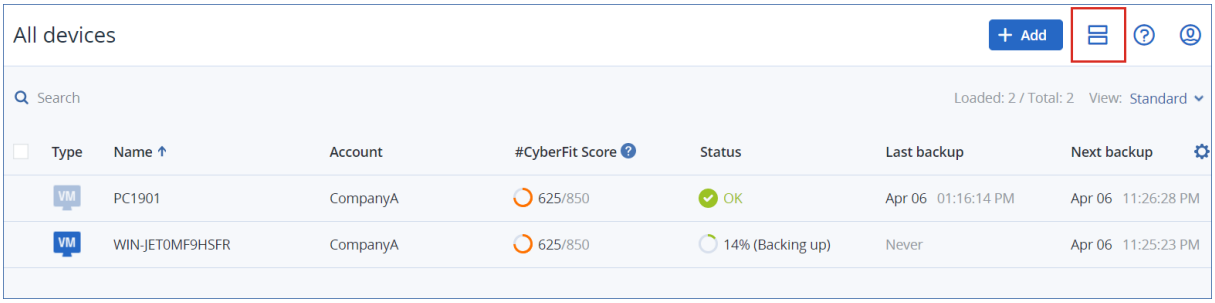
Bagian **Perangkat** tersedia dalam tampilan sederhana dan tabel. Untuk beralih antar tampilan, klik ikon yang sesuai di sudut kanan atas.

Tampilan sederhana hanya menunjukkan beberapa beban kerja.

© Acronis International GmbH, 2003-2024



Tampilan tabel diaktifkan secara otomatis saat jumlah beban kerja menjadi lebih besar.



Kedua tampilan tersebut memberikan akses ke fitur dan operasi yang sama. Dokumen ini menjelaskan akses ke operasi dari tampilan tabel.

Saat beban kerja online atau offline, diperlukan beberapa waktu untuk mengubah statusnya di konsol Cyber Protect. Status beban kerja diperiksa setiap menit. Jika agen yang diinstal pada mesin yang sesuai tidak mentransfer data, dan tidak ada jawaban untuk lima pemeriksaan berturut-turut, beban kerja ditampilkan sebagai offline. Beban kerja ditampilkan sebagai kembali online saat menjawab pemeriksaan status atau mulai mentransfer data.

Yang baru di konsol Cyber Protect

Ketika fitur baru dari Cyber Protect Cloud tersedia, Anda akan melihat jendela pop-up dengan deskripsi singkat tentang fitur ini saat masuk ke konsol Cyber Protect.

Anda juga dapat melihat deskripsi fitur baru dengan mengklik tautan **Apa yang baru** di pojok kiri bawah jendela konsol Cyber Protect utama.

Jika tidak ada fitur baru, tautan **Yang baru** tidak ditampilkan.

© Acronis International GmbH, 2003-2024

Menggunakan konsol Cyber Protect sebagai administrator mitra

Sebagai Administrator mitra, Anda dapat menggunakan Cyber Protect konsol di tingkat penyewa mitra (**Semua pelanggan**) atau di tingkat penyewa pelanggan.

Level (**Semua pelanggan**) penyewa mitra

Pada tingkat penyewa mitra (**Semua pelanggan**), Anda dapat melakukan tindakan berikut:

- Kelola rencana scripting untuk beban kerja dari semua penyewa pelanggan yang Anda kelola. Anda dapat menerapkan rencana scripting yang sama untuk beban kerja dari pelanggan yang berbeda, dan membuat grup perangkat dengan beban kerja dari pelanggan yang berbeda. Untuk mempelajari cara membuat grup perangkat statis atau grup dinamis pada level mitra, lihat "Membuat grup perangkat statis pada level mitra" (hlm. 323) dan "Membuat grup perangkat dinamis pada level mitra" (hlm. 323). Untuk informasi lebih lanjut mengenai skrip dan rencana scripting, lihat "Pembuatan Skrip Cyber" (hlm. 234).
- Buatlah rencana pemantauan untuk beban kerja dari semua penyewa pelanggan yang Anda kelola.
- Buat rencana manajemen jarak jauh untuk beban kerja dari semua penyewa pelanggan yang Anda kelola.
- Lihat dan kelola insiden Endpoint Detection and Response (EDR) untuk semua penyewa pelanggan dalam satu antarmuka manajemen insiden, daripada mengakses layar insiden setiap pelanggan secara individu.
- Lakukan autodiscovery mesin untuk semua penyewa pelanggan yang Anda kelola.

Level penyewa pelanggan

Pada level ini, Anda memiliki hak yang sama dengan administrator perusahaan tempat Anda bertindak atas namanya.

Memilih tingkat penyewa

Anda dapat memilih level penyewa untuk bekerja di Cyber Protect konsol.

Prasyarat

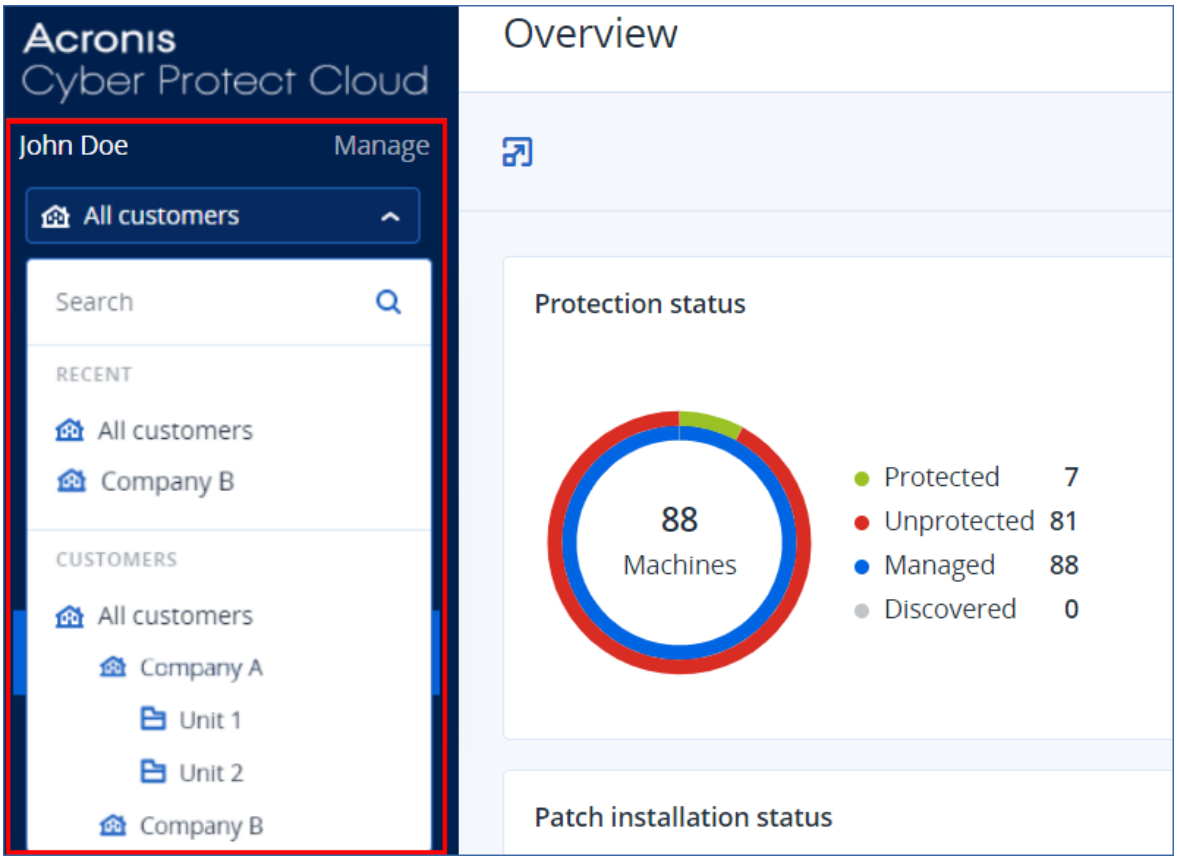
- Anda memiliki hak untuk mengakses konsol Cyber Protect dan portal manajemen.
- Anda dapat mengelola lebih dari satu penyewa atau unit.

Untuk memilih level penyewa di Cyber Protect konsol

1. Di menu navigasi di sebelah kiri, klik panah di sebelah nama penyewa pelanggan.
2. Pilih salah satu opsi berikut:
   - Untuk bekerja di level mitra, pilih **Semua pelanggan**.

© Acronis International GmbH, 2003-2024

- Untuk bekerja pada tingkat pelanggan atau unit, pilih nama pelanggan atau unit tersebut.



Tingkat penyewa mitra di Cyber Protect konsol

Ketika Anda menggunakan Cyber Protect konsol pada tingkat penyewa mitra (**Semua pelanggan**), tampilan yang dikustomisasi tersedia.

Tab **Peringatan** dan **Aktivitas** menyediakan filter terkait mitra tambahan, sedangkan tab **Perangkat** dan **Manajemen** menyediakan akses hanya ke fitur atau objek yang dapat diakses oleh administrator mitra.

Tab peringatan

Di sini, Anda dapat melihat peringatan dari semua pelanggan yang dikelola, mencarinya, dan memfilternya menurut kriteria berikut:

- Perangkat
- Pelanggan
- Rencana

Anda dapat memilih beberapa item untuk setiap kriteria ini.

© Acronis International GmbH, 2003-2024

Tab aktivitas

Di sini, Anda bisa melihat aktivitas dari semua penyewa yang Anda kelola atau aktivitas di penyewa pelanggan tertentu.

Anda dapat memfilter aktivitas berdasarkan pelanggan, status, waktu, dan jenis.

Jenis aktivitas berikut secara otomatis dipilih sebelumnya pada level ini:

- Menerapkan rencana
- Membuat rencana proteksi
- Rencana proteksi
- Membatalkan rencana
- Skrip

Tab Perangkat

Di tab **Mesin dengan agen**, Anda dapat melihat semua beban kerja dari penyewa pelanggan yang dikelola, dan Anda dapat memilih beban kerja dari satu atau beberapa penyewa. Anda juga dapat membuat grup perangkat yang menyertakan beban kerja dari penyewa yang berbeda.

Penting
Ketika Anda bekerja pada level mitra (**Semua pelanggan**), Anda dapat melakukan sejumlah operasi terbatas dengan perangkat. Misalnya, Anda tidak dapat melakukan operasi berikut:

- Lihat dan kelola rencana proteksi yang ada pada perangkat pelanggan.
- Buat rencana proteksi baru.
- Memulihkan cadangan.
- Gunakan Pemulihan Bencana.
- Akses fitur Cyber Protection Desktop.

Untuk melakukan operasi apa pun, kerjakan pada level pelanggan.

Tab manajemen perangkat lunak

Jika pemindaian inventaris perangkat lunak diaktifkan untuk beban kerja pelanggan, Anda dapat melihat hasil pemindaian perangkat lunak.

Melihat beban kerja pelanggan tertentu

Sebagai administrator mitra, Anda dapat melihat beban kerja milik penyewa pelanggan yang Anda kelola.

Untuk melihat beban kerja pelanggan tertentu

© Acronis International GmbH, 2003-2024

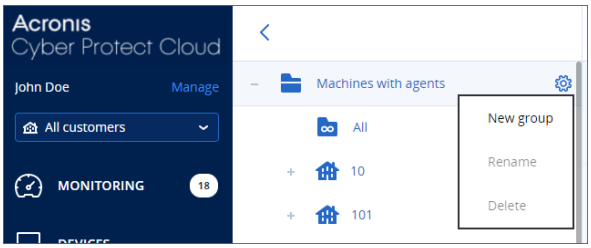
1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Di hierarki yang ditampilkan, klik **Mesin dengan agen** untuk memperluas daftar.
3. Klik nama pelanggan yang beban kerjanya ingin Anda lihat dan kelola.

Membuat grup perangkat statis pada level mitra

Anda dapat membuat grup perangkat statis pada level mitra (**Semua perangkat**).

Untuk membuat grup perangkat statis di level mitra

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Klik ikon roda gigi di samping **Mesin dengan agen**, lalu klik **Grup baru**.



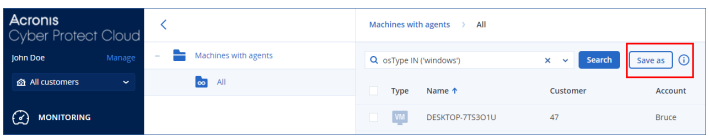
3. Tentukan nama grup.
4. [Opsional] Tambahkan deskripsi.
5. Klik **OK**.

Membuat grup perangkat dinamis pada level mitra

Anda dapat membuat grup perangkat dinamis pada tingkat mitra (**Semua perangkat**).

Untuk membuat grup perangkat dinamis di level mitra

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Di hierarki yang ditampilkan, klik **Mesin dengan agen** untuk memperluas daftar.
3. Klik **Semua**.
4. Di bidang pencarian, tentukan kriteria yang sesuai dengan keinginan Anda untuk membuat grup perangkat dinamis, lalu klik **Telusuri**.
   Untuk mempelajari lebih lanjut tentang kriteria pencarian yang tersedia, lihat "Cari atribut untuk beban kerja non-awan-ke-awan" (hlm. 346) dan "Cari atribut untuk beban kerja awan-ke-awan" (hlm. 345).
5. Klik **Simpan sebagai**, lalu tentukan nama grup.



6. [Opsional] Tambahkan deskripsi.
7. Klik **OK**.

© Acronis International GmbH, 2003-2024

Melakukan autodiscovery mesin pada level penyewa mitra

Anda dapat melakukan autodiscovery di level tenant mitra (**Semua pelanggan**).

Prasyarat

Setidaknya ada satu mesin dengan agen perlindungan yang terpasang di jaringan lokal pelanggan Anda atau Domain active directory.

Penting
Hanya agen yang diinstal pada mesin Windows yang dapat menjadi agen penemuan. Jika tidak ada agen penemuan di lingkungan pelanggan Anda, Anda tidak akan dapat menggunakan opsi **Beberapa perangkat** di panel **Tambah perangkat**.

Autodiscovery tidak didukung untuk menambahkan Pengontrol Domain karena izin tambahan diperlukan agar layanan agen berjalan.

Instalasi jarak jauh agen didukung hanya untuk mesin yang menjalankan Windows (Windows XP tidak didukung). Untuk instalasi jarak jauh pada mesin yang menjalankan Windows Server 2012 R2, Windows update KB2999226 harus diinstal.

Untuk melakukan autodiscovery mesin di tingkat penyewa mitra

1. Di Cyber Protect konsol, pilih **Semua Pelanggan**.
2. Buka **Perangkat**> **Semua perangkat**.
3. Klik **Tambah**.
4. Dalam **Beberapa perangkat**, klik **hanya Windows**. Wizard penemuan terbuka.
5. Pilih penyewa pelanggan lalu pilih agen penemuan yang akan melakukan pemindaian untuk mendeteksi mesin.
6. Pilih metode penemuan:
   - **Cari Active Directory**. Pastikan bahwa mesin dengan agen penemuan adalah anggota domain Active Directory.
   - **Pindai jaringan lokal**. Jika agen penemuan yang dipilih tidak dapat menemukan mesin apa pun, pilih agen penemuan lainnya.
   - **Tentukan secara manual atau impor dari file**. Menentukan mesin secara manual untuk ditambahkan atau mengimpor mesin dari file teks.
7. [Jika metode penemuan Active Directory dipilih] Pilih cara mencari mesin:
   - **Dalam daftar unit organisasi**. Pilih grup mesin yang akan ditambahkan.
   - **Berdasarkan kueri dialek LDAP**. Gunakan kueri dialek LDAP untuk memilih mesin. **Basis Pencarian** menetapkan tempat pernacarian, sedangkan **Filter** memungkinkan Anda untuk menentukan kriteria pemilihan mesin.

© Acronis International GmbH, 2003-2024

8. Tergantung pada metode pencarian yang Anda pilih, lakukan salah satu dari tindakan berikut:

Metode penemuan	Tindakan
Cari Active Directory	Dalam daftar mesin yang ditemukan, pilih mesin-mesin yang ingin Anda tambahkan.
Pindai jaringan lokal	Dalam daftar mesin yang ditemukan, pilih mesin-mesin yang ingin Anda tambahkan.

Tentukan secara manual atau impor dari file	Tentukan alamat IP mesin atau nama host, atau impor daftar mesin dari file teks. File harus berisi alamat IP/nama host, satu per baris. Berikut adalah contoh file:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Setelah menambah alamat mesin secara manual atau mengimpornya dari file, agen berusaha untuk mengirim ping ke mesin yang ditambahkan dan menetapkan ketersediaannya.

9. Pilih tindakan yang harus dilakukan setelah penemuan:

Opsi	Deskripsi
Instal agen dan daftarkan mesin	Anda dapat memilih komponen apa saja yang akan diinstal pada mesin dengan mengeklik **Pilih komponen**. Untuk detail lebih lanjut, lihat "Memilih komponen untuk instalasi" (hlm. 131).
Masuk akun untuk layanan agen	Pengaturan ini tersedia di layar **Pilih komponen**. Pengaturan menentukan akun tempat layanan akan dijalankan. Anda dapat memilih salah satu dari opsi berikut: • **Gunakan Akun Pengguna Layanan** (default untuk layanan agen) Akun Pengguna Layanan adalah akun sistem Windows yang digunakan untuk menjalankan layanan. Keuntungan dari pengaturan ini adalah kebijakan keamanan domain yang tidak memengaruhi hak pengguna akun ini. Secara default, agen berjalan di bawah akun **Sistem Lokal**. • **Buat akun baru** Nama akunnya adalah Agent User untuk agen. • **Gunakan akun berikut** Jika Anda menginstal agen pada pengontrol domain, sistem akan meminta Anda menentukan akun yang ada (atau akun yang sama) untuk agen. Untuk alasan keamanan, sistem tidak membuat akun baru secara otomatis di pengontrol domain. Jika Anda memilih opsi **Buat akun baru** atau **Gunakan akun berikut**, pastikan bahwa kebijakan keamanan domain tidak memengaruhi hak akun terkait. Jika akun kehilangan hak pengguna yang ditetapkan selama instalasi, komponen

© Acronis International GmbH, 2003-2024

Opsi	Deskripsi
	mungkin bekerja secara tidak semestinya atau sama sekali tidak berfungsi.
Daftarkan mesin dengan agen yang terinstal	Gunakan opsi ini jika agen sudah terpasang pada mesin, dan Anda hanya perlu mendaftarkannya di Cyber Protection. Jika tidak ada agen yang ditemukan pada mesin, mesin akan ditambahkan sebagai **Tidak Dikelola**.
Tambahkan sebagai mesin yang tidak dikelola	Jika Anda memilih opsi ini, agen tidak akan diinstal pada mesin. Anda akan dapat melihatnya di konsol dan menginstal atau mendaftarkan agen nanti.
Mulai ulang mesin, jika diperlukan	Opsi ini muncul ketika **Menginstal agen dan mendaftarkan mesin** dipilih. Jika Anda memilih opsi ini, mesin akan di-restart sebanyak yang diperlukan untuk menyelesaikan instalasi. Memulai ulang mesin mungkin perlu dilakukan pada salah satu kasus berikut: • Instalasi prasyarat telah selesai, dan diperlukan restart untuk melanjutkan instalasi. • Instalasi selesai tetapi memulai ulang diperlukan karena beberapa file terkunci selama instalasi. • Instalasi selesai tetapi memulai ulang perlu dilakukan untuk perangkat lunak lain yang diinstal sebelumnya.
Jangan memulai ulang jika pengguna login	Opsi ini muncul ketika **Mulai ulang mesin jika diperlukan** dipilih. Jika Anda memilih opsi ini, mesin tidak akan memulai ulang secara otomatis jika pengguna masuk ke dalam sistem. Misalnya, jika pengguna sedang bekerja sementara instalasi harus dinyalakan ulang, sistem tidak akan memulai ulang secara otomatis. Jika prasyarat telah dipasang tetapi mesin tidak dimulai ulang karena ada pengguna yang sedang masuk, Anda harus memulai ulang mesin dan menjalankan instalasi hingga selesai. Jika agen telah diinstal tetapi kemudian mesin tidak dimulai ulang, Anda harus memulai ulang mesin tersebut.
Pengguna tempat mendaftarkan mesin	[Jika ada unit di organisasi Anda] Pilih akun pengguna unit atau unit bawahan tempat Anda ingin mendaftarkan mesin. [Ketika melakukan autodiscovery pada level penyewa mitra] Dalam daftar penyewa pelanggan yang Anda kelola, perluas struktur pohon, lalu pilih akun pengguna yang ingin Anda daftarkan mesinnya. [Ketika melakukan autodiscovery sebagai administrator pelanggan] Jika Anda memilih **Instal agen dan daftarkan mesin** atau **Daftarkan mesin dengan agen yang terinstal**, ada juga opsi untuk menerapkan rencana proteksi ke mesin. Jika Anda memiliki beberapa rencana proteksi, Anda dapat memilih mana yang akan digunakan.

10. Tentukan kredensial pengguna dengan hak Administrator untuk semua mesin.

© Acronis International GmbH, 2003-2024

Penting
Instalasi agen secara jarak jauh dapat berfungsi tanpa persiapan apa pun hanya jika Anda menetapkan kredensial untuk akun Administrator bawaan (akun pertama yang dibuat saat sistem operasi diinstal). Jika Anda ingin menentukan kredensial administrator kustom, Anda harus melakukan persiapan tambahan seperti yang dijelaskan di "Prasyarat" (hlm. 324).

11. Sistem memeriksa konektivitas ke semua mesin. Jika koneksi ke beberapa mesin gagal, Anda dapat mengubah kredensial untuk mesin tersebut.

Setelah aktivasi penemuan mesin dimulai, Anda dapat melihat tugas yang sesuai di **Monitoring**> **Aktivitas** > aktivitas **Menemukan mesin**.

Dukungan beberapa penyewaan

Layanan Cyber Protection mendukung beberapa penyewaan, yang menyiratkan administrasi pada level berikut:

- [Untuk penyedia layanan] Level penyewa mitra (**Semua pelanggan**)
  Level ini hanya tersedia untuk administrator mitra yang mengelola penyewa pelanggan.
- Level penyewa pelanggan
  Level ini dikelola oleh administrator perusahaan.
  Administrator mitra juga dapat bekerja pada level ini di penyewa pelanggan yang mereka kelola. Pada level ini, administrator mitra memiliki hak yang sama dengan administrator pelanggan atas nama siapa mereka bertindak.
- Level unit
  Level ini dikelola oleh administrator unit dan oleh administrator perusahaan dari penyewa pelanggan induk.
  Administrator mitra yang mengelola penyewa pelanggan induk juga dapat mengakses level unit. Pada level ini, mereka memiliki hak yang sama dengan administrator pelanggan atas nama siapa mereka bertindak.

Administrator dapat mengelola objek di penyewa mereka sendiri dan di penyewa anak. Mereka tidak dapat melihat atau mengakses objek pada level administrasi atas, jika ada.

Misalnya, administrator perusahaan dapat mengelola rencana proteksi baik di level penyewa pelanggan maupun di level unit. Administrator unit hanya dapat mengelola rencana proteksi mereka sendiri di level unit. Mereka tidak dapat mengelola rencana proteksi apa pun di level penyewa pelanggan dan tidak dapat mengelola rencana proteksi yang dibuat oleh administrator pelanggan di level unit.

Selain itu, administrator mitra dapat membuat dan menerapkan rencana skrip di penyewa pelanggan yang mereka kelola. Administrator perusahaan di penyewa tersebut hanya memiliki akses hanya baca ke rencana skrip yang diterapkan pada beban kerja mereka oleh administrator mitra. Namun, administrator pelanggan dapat membuat dan menerapkan skrip atau rencana proteksi mereka sendiri.

© Acronis International GmbH, 2003-2024

Beban kerja

Beban kerja adalah semua jenis sumber daya yang dilindungi - misalnya, mesin fisik, mesin virtual, kotak surat, atau instans database. Di konsol Cyber Protect, beban kerja ditampilkan sebagai objek yang dapat Anda terapkan rencana (rencana proteksi, rencana pencadangan, atau rencana skrip).

Beberapa beban kerja memerlukan pemasangan agen perlindungan atau penerapan alat virtual. Anda dapat menginstal agen dengan menggunakan antarmuka pengguna grafis atau dengan menggunakan antarmuka baris perintah (instalasi tanpa pengawasan). Anda dapat menggunakan instalasi tanpa pengawasan untuk mengotomatiskan prosedur instalasi. Untuk informasi selengkapnya tentang cara menginstal agen perlindungan, lihat "Menginstal dan menyebarkan agen Cyber Protection" (hlm. 58).

Alat virtual (VA) adalah mesin virtual siap pakai yang berisi agen perlindungan. Dengan alat virtual, Anda dapat mencadangkan mesin virtual lain di lingkungan yang sama tanpa menginstal agen perlindungan pada mesin tersebut (pencadangan tanpa agen). Peralatan virtual tersedia dalam format khusus hypervisor, seperti .ovf, .ova, atau .qcow. Untuk informasi selengkapnya tentang platform virtualisasi mana yang mendukung pencadangan tanpa agen, lihat "Platform virtualisasi yang didukung" (hlm. 32).

Penting
Agen harus online setidaknya sekali setiap 30 hari. Jika tidak, rencana mereka akan batal dan beban kerja menjadi tidak terlindungi.

Tabel di bawah ini merangkum jenis beban kerja dan agen masing-masing.

Jenis beban kerja	Agen	Contoh (daftar yang tidak lengkap)
Mesin fisik	Agen perlindungan dipasang pada setiap mesin yang dilindungi.	Stasiun Kerja Laptop Server
Mesin virtual	Bergantung pada platform virtualisasi, metode pencadangan berikut ini mungkin tersedia: • Cadangan berbasis agen - Agen perlindungan diinstal pada setiap mesin yang dilindungi. • Cadangan tanpa agen - Agen perlindungan diinstal hanya pada host hypervisor, pada mesin virtual khusus, atau digunakan sebagai alat virtual. Agen ini mencadangkan semua mesin virtual di lingkungan.	Mesin virtual VMware Mesin virtual Hyper-V Mesin Virtual berbasis kernel (KVM) yang dikelola oleh oVirt
Beban kerja	Beban kerja ini didukung oleh agen awan yang tidak memerlukan	Kotak surat

© Acronis International GmbH, 2003-2024

Jenis beban kerja	Agen	Contoh (daftar yang tidak lengkap)
Microsoft 365 Business Beban kerja Google Workspace	instalasi. Untuk menggunakan agen awan, Anda perlu menambahkan organisasi Microsoft 365 atau Google Workspace ke konsol Cyber Protect. Selain itu, Agen lokal untuk Office 365 juga tersedia. Ini memerlukan instalasi dan hanya dapat digunakan untuk membuat cadangan kotak surat Exchange Online. Untuk informasi lebih lanjut mengenai perbedaan antara agen lokal dan agen cloud, lihat "Melindungi data Microsoft 365" (hlm. 596). .	Microsoft 365 Microsoft 365 OneDrive Microsoft Teams Situs SharePoint Kotak surat Google Google Drive
Aplikasi	Data aplikasi tertentu dicadangkan oleh agen khusus, seperti Agen untuk SQL, Agen untuk Exchange, Agen untuk MySQL/MariaDB, atau Active Directory.	Database SQL Server Database MySQL/MariaDB Database Oracle Active Directory
Perangkat seluler	Apl seluler terinstal di perangkat dilindungi.	Perangkat Android atau iOS
Situs web	Situs web dicadangkan oleh agen awan yang tidak memerlukan instalasi.	Situs web yang diakses melalui protokol SFTP atau SSH

Untuk informasi lebih lanjut tentang agen mana yang Anda butuhkan dan di mana menginstalnya, lihat "Agen mana yang saya perlukan?" (hlm. 61)

Menambahkan beban kerja ke konsol Cyber Protect

Untuk mulai melindungi beban kerja Anda, tambahkan terlebih dahulu ke konsol Cyber Protect.

Catatan
Jenis beban kerja yang dapat Anda tambahkan tergantung pada kuota layanan untuk akun Anda. Jika jenis beban kerja tertentu tidak ada, panel **Tambah perangkat** maka akan berwarna abu-abu.

Administrator mitra dapat mengaktifkan kuota layanan yang diperlukan di portal Manajemen. Untuk perincian, lihat "Informasi untuk administrator mitra" (hlm. 334).

Untuk menambahkan beban kerja

© Acronis International GmbH, 2003-2024

1. Masuk ke konsol Cyber Protect.
2. Buka **Perangkat** > **Seluruh perangkat**, lalu klik **Tambah**.
   Panel **Tambah peranti** terbuka di sebelah kanan.
3. Pilih saluran rilis.
4. Klik jenis beban kerja yang ingin Anda tambahkan, lalu ikuti petunjuk untuk beban kerja spesifik yang Anda pilih.

Tabel berikut ini merangkum jenis beban kerja dan tindakan yang diperlukan.

Beban kerja yang akan ditambahkan	Tindakan yang diperlukan	Prosedur yang harus diikuti
Beberapa mesin Windows	Lakukan autodiscovery di lingkungan Anda. Untuk melakukan autodiscovery, Anda membutuhkan setidaknya satu mesin dengan agen perlindungan terinstal di jaringan lokal atau domain Active Directory Anda. Agen ini digunakan sebagai agen penemuan.	"Melakukan autodiscovery dan manual discovery" (hlm. 127)
Stasiun kerja Windows Server Windows	Instal Agen untuk Windows.	"Menginstal agen proteksi di Windows" (hlm. 76) atau "Instalasi atau penghapusan instalasi tanpa pengawasan di Windows" (hlm. 86)
Stasiun kerja macOS	Instal Agen untuk macOS.	"Menginstal agen proteksi di macOS" (hlm. 81) atau "Instalasi dan penghapusan instalasi tanpa pengawasan di macOS" (hlm. 110)
Server Linux	Instal Agen untuk Linux.	"Menginstal agen proteksi di Linux" (hlm. 78) atau "Instalasi atau penghapusan tanpa pengawasan di Linux" (hlm. 104)
Perangkat seluler (iOS, Android)	Instal apl seluler.	"Melindungi perangkat seluler" (hlm. 588)
Beban kerja awan-ke-awan		

© Acronis International GmbH, 2003-2024

Beban kerja yang akan ditambahkan	Tindakan yang diperlukan	Prosedur yang harus diikuti
Microsoft 365 Business	Tambahkan organisasi Microsoft 365 Anda ke konsol Cyber Protect dan gunakan agen awan untuk melindungi kotak surat online Exchange, file OneDrive, Microsoft Teams, dan situs SharePoint. Atau, Anda dapat menginstal Agen lokal untuk Office 365. Ini hanya menyediakan cadangan kotak surat Exchange Online. Untuk informasi lebih lanjut tentang perbedaan antara agen lokal dan agen awan, lihat "Melindungi data Microsoft 365" (hlm. 596).	"Melindungi data Microsoft 365" (hlm. 596)
Google Workspace	Tambahkan organisasi Google Workspace Anda ke konsol Cyber Protect dan gunakan agen awan untuk melindungi kotak surat Gmail dan file Google Drive.	"Melindungi data Google Workspace" (hlm. 638)
Mesin virtual		
VMware ESXi	Sebarkan Agen untuk VMware (Alat Virtual) di lingkungan Anda.	"Menyebarkan Agen untuk VMware (Virtual Appliance)" (hlm. 135)
	Instal Agen untuk VMware (Windows).	"Menginstal agen proteksi di Windows" (hlm. 76) atau "Instalasi atau penghapusan instalasi tanpa pengawasan di Windows" (hlm. 86)
Virtuozzo Hybrid Infrastructure	Sebarkan Agen untuk Virtuozzo Hybrid Infrastructure (Alat virtual) di lingkungan Anda.	"Menyebarkan Agen untuk Virtuozzo Hybrid Infrastructure (Alat Virtual)" (hlm. 144)
Hyper-V	Instal Agen untuk Hyper-V.	"Menginstal agen proteksi di Windows" (hlm. 76) atau "Instalasi atau penghapusan instalasi tanpa pengawasan di Windows" (hlm. 86)
Virtuozzo	Instal Agen untuk Virtuozzo.	"Menginstal agen proteksi di Linux"

© Acronis International GmbH, 2003-2024

Beban kerja yang akan ditambahkan	Tindakan yang diperlukan	Prosedur yang harus diikuti
		(hlm. 78) atau "Instalasi atau penghapusan tanpa pengawasan di Linux" (hlm. 104)
KVM	Instal Agen untuk Windows.	"Menginstal agen proteksi di Windows" (hlm. 76) atau "Instalasi atau penghapusan instalasi tanpa pengawasan di Windows" (hlm. 86)
	Instal Agen untuk Linux.	"Menginstal agen proteksi di Linux" (hlm. 78) atau "Instalasi atau penghapusan tanpa pengawasan di Linux" (hlm. 104)
Red Hat Virtualization (oVirt)	Sebarkan Agen untuk oVirt (Alat Virtual) di lingkungan Anda.	"Menyebarkan Agen untuk oVirt (Alat Virtual)" (hlm. 152)
Citrix XenServer	Instal Agen untuk Windows.	"Menginstal agen proteksi di Windows" (hlm. 76) atau "Instalasi atau penghapusan instalasi tanpa pengawasan di Windows" (hlm. 86)
	Instal Agen untuk Linux.	"Menginstal agen proteksi di Linux" (hlm. 78) atau "Instalasi atau penghapusan tanpa pengawasan di Linux" (hlm. 104)
Nutanix AHV	Instal Agen untuk Windows.	"Menginstal agen proteksi di Windows" (hlm. 76) atau "Instalasi atau penghapusan instalasi tanpa pengawasan di Windows" (hlm. 86)
	Instal Agen untuk Linux.	"Menginstal agen proteksi di Linux"

© Acronis International GmbH, 2003-2024

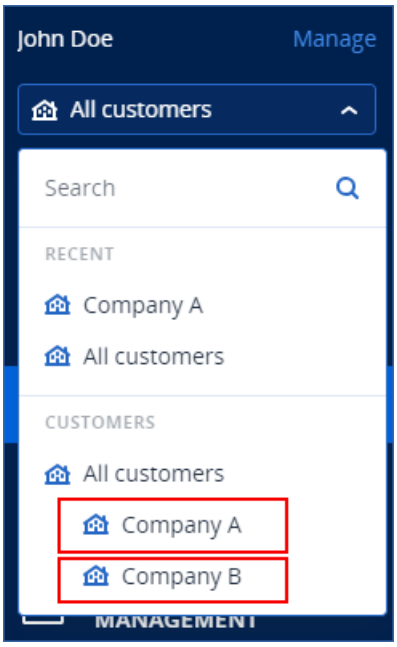
Beban kerja yang akan ditambahkan	Tindakan yang diperlukan	Prosedur yang harus diikuti
		(hlm. 78) atau "Instalasi atau penghapusan tanpa pengawasan di Linux" (hlm. 104)
Oracle VM	Instal Agen untuk Windows.	"Menginstal agen proteksi di Windows" (hlm. 76) atau "Instalasi atau penghapusan instalasi tanpa pengawasan di Windows" (hlm. 86)
	Instal Agen untuk Linux.	"Menginstal agen proteksi di Linux" (hlm. 78) atau "Instalasi atau penghapusan tanpa pengawasan di Linux" (hlm. 104)
Scale Computing HC3	Menyebarkan Agen untuk Scale Computing HC3 (Alat Virtual) di lingkungan Anda.	"Menyebarkan Agen untuk Scale Computing HC3 (Alat Virtual)" (hlm. 139)
Penyimpanan terhubung ke jaringan		
Synology	Menyebarkan Agen untuk Synology (Alat Virtual) di lingkungan Anda.	"Menyebarkan Agen untuk Synology" (hlm. 158)
Aplikasi		
Microsoft SQL Server	Instal Agen untuk SQL.	"Menginstal agen proteksi di Windows" (hlm. 76) atau "Instalasi atau penghapusan instalasi tanpa pengawasan di Windows" (hlm. 86)
Microsoft Exchange Server	Instal Agen untuk Exchange.	
Microsoft Active Directory	Instal Agen Untuk Active Directory.	
Database Oracle	Instal Agen untuk Oracle.	"Melindungi Database Oracle" (hlm. 664)
Situs web	Mengonfigurasi koneksi ke situs web.	"Melindungi situs web dan server hosting" (hlm. 671)

Untuk informasi lebih lanjut tentang agen perlindungan yang tersedia dan tempat instalasinya, lihat "Agen mana yang saya perlukan?" (hlm. 61)

© Acronis International GmbH, 2003-2024

Informasi untuk administrator mitra

- Jenis beban kerja mungkin tidak ada di panel **Tambah peranti** jika kuota layanan yang diperlukan tidak diaktifkan di portal Manajemen. Untuk informasi lebih lanjut tentang kuota layanan mana yang diperlukan untuk beban kerja yang mana, lihat Mengaktifkan atau menonaktifkan item penawaran dalam panduan administrator Mitra.
- Sebagai administrator mitra, Anda tidak dapat menambahkan beban kerja pada level **Semua pelanggan**. Untuk menambahkan beban kerja, pilih penyewa pelanggan perorangan.



Menghapus beban kerja dari konsol Cyber Protect

Anda dapat menghapus dari konsol Cyber Protect pada beban kerja yang tidak perlu Anda lindungi lagi. Prosedur tergantung pada jenis beban kerja.

Sebagai alternatif, Anda dapat menghapus instalasi agen pada beban kerja yang diproteksi. Saat Anda menghapus instalasi agen, beban kerja yang diproteksi secara otomatis dihapus dari konsol Cyber Protect.

Penting
Saat Anda menghapus beban kerja dari konsol Cyber Protect, semua rencana yang diterapkan pada beban kerja tersebut akan batal. Menghapus beban kerja tidak menghapus rencana atau cadangan apa pun, dan tidak menghapus instalasi agen perlindungan.

Tabel berikut ini merangkum jenis beban kerja dan tindakan yang diperlukan.

© Acronis International GmbH, 2003-2024

Beban kerja yang akan dihapus	Tindakan yang diperlukan	Prosedur yang harus diikuti
Mesin fisik dan virtual		
Mesin fisik atau virtual tempat agen perlindungan diinstal	1. Hapus beban kerja dari konsol Cyber Protect. 2. [Opsional] Hapus instalasi agen proteksi.	"Untuk menghapus beban kerja dari konsol Cyber Protect" (hlm. 336) (Beban kerja dengan agen perlindungan)
Mesin virtual yang dicadangkan pada level hypervisor (cadangan tanpa agen)	1. Pada konsol Cyber Protect, hapus mesin tempat agen perlindungan diinstal. Semua mesin virtual yang dicadangkan oleh agen ini akan secara otomatis dihapus dari konsol. 2. [Opsional] Hapus instalasi agen proteksi.	"Untuk menghapus beban kerja dari konsol Cyber Protect" (hlm. 336) (Beban kerja tanpa agen perlindungan)
Beban kerja awan-ke-awan		
Beban kerja Microsoft 365 Business Beban kerja Google Workspace	Hapus organisasi Microsoft 365 atau Google Workspace dari konsol Cyber Protect. Semua sumber daya dalam organisasi tersebut akan secara otomatis dihapus dari konsol.	"Untuk menghapus beban kerja dari konsol Cyber Protect" (hlm. 336) (Beban kerja awan-ke-awan)
Perangkat seluler		
Perangkat Android Perangkat iOS	1. Menghapus perangkat bergerak dari konsol Cyber	"Untuk menghapus beban kerja dari konsol Cyber Protect" (hlm. 336) (Perangkat bergerak)

© Acronis International GmbH, 2003-2024

Beban kerja yang akan dihapus	Tindakan yang diperlukan	Prosedur yang harus diikuti
	Protect. 2. [Opsional] Pada perangkat bergerak, hapus instalasi aplikasi.	
Penyimpanan terhubung ke jaringan		
Synology	1. Hapus beban kerja dari konsol Cyber Protect. 2. [Opsional] Hapus instalasi agen proteksi.	"Untuk menghapus beban kerja dari konsol Cyber Protect" (hlm. 336) (Beban kerja dengan agen perlindungan)
Aplikasi		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Database Oracle	1. Pada konsol Cyber Protect, hapus mesin tempat agen perlindungan diinstal. Objek yang dicadangkan oleh agen ini akan secara otomatis dihapus dari konsol. 2. [Opsional] Hapus instalasi agen proteksi.	"Untuk menghapus beban kerja dari konsol Cyber Protect" (hlm. 336) (Beban kerja tanpa agen perlindungan)
Situs web	Hapus situs web dari konsol Cyber Protect.	"Untuk menghapus beban kerja dari konsol Cyber Protect" (hlm. 336) (Situs web)

Untuk menghapus beban kerja dari konsol Cyber Protect

Beban kerja dengan agen perlindungan

Anda dapat menghapus jenis beban kerja ini secara langsung.

1. Pada konsol Cyber Protect, navigasi ke **Perangkat** > **Semua perangkat**.
2. Pilih kotak centang di samping satu atau beberapa beban kerja yang ingin Anda hapus.

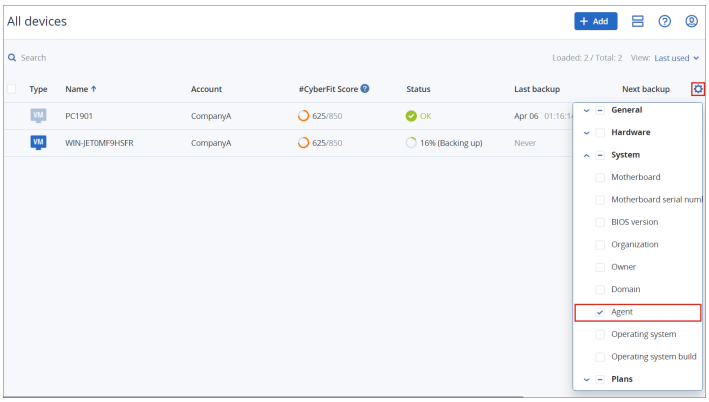
© Acronis International GmbH, 2003-2024

3. Di panel **Tindakan**, pilih **Hapus**.
4. Konfirmasikan pilihan Anda dengan mengeklik **Hapus**.
5. [Opsional] Hapus instalasi agen seperti yang dijelaskan di "Menghapus instalasi agen" (hlm. 180).

Beban kerja tanpa agen perlindungan

Untuk menghapus jenis beban kerja ini, Anda perlu melepas mesin tempat agen perlindungan diinstal.

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Di sudut kanan atas, klik ikon roda gigi, lalu pilih kotak centang **Agen**.



   Kolom **Agen** akan muncul.
3. Pada kolom **Agen**, centang nama mesin tempat agen perlindungan diinstal.
4. Pada konsol Cyber Protect, pilih kotak centang di samping mesin tempat agen perlindungan diinstal.
5. Di panel **Tindakan**, pilih **Hapus**.
6. Konfirmasikan pilihan Anda dengan mengeklik **Hapus**.
7. [Opsional] Hapus instalasi agen seperti yang dijelaskan di "Menghapus instalasi agen" (hlm. 180).

Beban kerja awan-ke-awan

Untuk menghapus beban kerja yang dicadangkan oleh agen awan, hapus organisasi Microsoft 365 atau Google Workspace dari konsol Cyber Protect.

1. Di konsol Cyber Protect, navigasi ke **Perangkat** > **Microsoft 365** or **Perangkat** > **Google Workspace**.
2. Klik nama organisasi Microsoft 365 atau Google Workspace Anda.
3. Di panel **Tindakan**, pilih **Hapus grup**.
4. Klik **Hapus** untuk mengonfirmasi tindakan Anda.

Perangkat seluler

1. Pada konsol Cyber Protect, navigasi ke **Perangkat** > **Semua perangkat**.
2. Pilih kotak centang di samping beban kerja yang ingin Anda hapus.

© Acronis International GmbH, 2003-2024

3. Di panel **Tindakan**, pilih **Hapus**.
4. Konfirmasikan pilihan Anda dengan mengeklik **Hapus**.
5. [Opsional] Hapus instalasi apl dari perangkat bergerak.

Situs web

1. Pada konsol Cyber Protect, navigasi ke **Perangkat** > **Semua perangkat**.
2. Pilih kotak centang di samping beban kerja yang ingin Anda hapus.
3. Di panel **Tindakan**, pilih **Hapus**.
4. Konfirmasikan pilihan Anda dengan mengeklik **Hapus**.

Grup perangkat

Dengan grup perangkat, Anda dapat melindungi beberapa beban kerja serupa dengan rencana grup. Rencana tersebut berlaku untuk seluruh grup dan tidak dapat dicabut dari anggota grup.

Beban kerja dapat menjadi anggota di lebih dari satu grup. Beban kerja yang termasuk dalam grup perangkat masih dapat dilindungi oleh rencana individual.

Anda hanya dapat menambahkan beban kerja dengan jenis yang sama ke grup perangkat. Misalnya, di bagian **Hyper-V**, Anda hanya dapat membuat grup mesin virtual Hyper-V. Di bagian **Mesin dengan agen**, Anda hanya dapat membuat grup mesin dengan agen yang diinstal.

Anda tidak dapat membuat grup perangkat dalam grup **Semua** jenis, seperti grup root **Semua perangkat**, atau grup bawaan seperti **Mesin dengan agen** > **Semua**, **Microsoft 365** > organisasi Anda > **Pengguna** > **Semua pengguna**.

Grup bawaan dan grup khusus

Grup bawaan

Setelah Anda mendaftarkan beban kerja di konsol Cyber Protect, beban kerja muncul di salah satu grup root bawaan di tab **Perangkat**, seperti **Mesin dengan agen**, **Microsoft 365**, atau **Hyper-V**.

Semua beban kerja non-awan-ke-awan yang terdaftar juga tercantum di grup root **Semua perangkat**. Grup root bawaan terpisah yang diberi nama menurut penyewa Anda berisi semua beban kerja non-awan-ke-awan dan semua unit di penyewa ini.

Anda tidak dapat menghapus atau mengedit grup root, atau menerapkan rencana ke grup tersebut.

Beberapa grup root berisi satu atau lebih level subgrup bawaan, misalnya, **Mesin dengan agen** > **Semua**, **Microsoft 365** > organisasi Anda > **Tim** > **Semua tim**, **Google Workspace** > organisasi Anda > **Drive Bersama** > **Semua Drive Bersama**.

Anda tidak dapat mengedit atau menghapus subgrup bawaan.

© Acronis International GmbH, 2003-2024

Grup kustom

Melindungi semua beban kerja dalam grup bawaan mungkin tidak mudah, karena mungkin ada beban kerja yang memerlukan pengaturan perlindungan berbeda atau jadwal perlindungan berbeda.

Di beberapa grup root, misalnya di **Mesin dengan agen**, **Microsoft 365**, atau **Google Workspace**, Anda dapat membuat subgrup khusus. Subgrup ini bisa bersifat statis atau dinamis.

Anda dapat mengedit, mengganti nama, atau menghapus grup kustom apa pun.

Grup statis dan grup dinamis

Anda dapat membuat jenis grup kustom berikut:

- Statis
- Dinamis

Grup statis

Grup statis berisi beban kerja yang ditambahkan secara manual.

Konten grup statis hanya berubah ketika Anda dengan sengaja menambahkan atau menghapus beban kerja.

Contoh: Anda membuat grup statis untuk departemen akuntansi di perusahaan Anda, dan secara manual menambahkan mesin akuntan ke grup ini. Saat Anda menerapkan rencana grup, mesin di grup tersebut akan menjadi terlindungi. Jika merekrut akuntan baru, Anda harus menambahkan mesin akuntan baru ke grup statis secara manual.

Grup dinamis

Grup dinamis berisi beban kerja yang sesuai dengan kriteria tertentu. Anda menentukan kriteria ini sebelumnya dengan membuat kueri pencarian yang menyertakan atribut (misalnya, `osType`), nilainya (misalnya, `Windows`), dan operator pencariannya (misalnya, `IN`).

Anda dapat membuat grup dinamis untuk semua mesin dengan sistem operasi Windows atau grup dinamis yang berisi semua pengguna di organisasi Microsoft 365 Anda, yang alamat emailnya diawali dengan nama `john`.

Semua beban kerja yang memiliki atribut dan nilai yang diperlukan akan ditambahkan secara otomatis ke grup dan beban kerja yang kehilangan atribut atau nilai yang diperlukan akan dikeluarkan dari grup secara otomatis.

Contoh 1: Nama host dari mesin yang dimiliki oleh departemen akuntansi mengandung kata accounting. Anda mencari mesin yang namanya mengandung kata accounting, lalu menyimpan hasil pencariannya sebagai grup dinamis. Selanjutnya, Anda menerapkan rencana proteksi ke grup. Jika merekrut akuntan baru, nama mesin akuntan akan mengandung accounting dan akan secara

© Acronis International GmbH, 2003-2024

otomatis ditambahkan ke grup dinamis segera setelah Anda mendaftarkan mesin ke konsol Cyber Protect.

Contoh 2: Departemen akuntansi membentuk unit organisasi (OU) Active Directory yang terpisah. Anda menetapkan OU akuntan sebagai atribut yang diperlukan, dan kemudian Anda menyimpan hasil pencariannya sebagai grup dinamis. Selanjutnya, Anda menerapkan rencana proteksi ke grup. Jika merekrut akuntan baru, mesin akuntan akan ditambahkan ke grup dinamis segera setelah mesinnya ditambahkan ke Active Directory OU dan terdaftar di konsol Cyber Protect (mana pun yang terjadi lebih dahulu).

Grup awan-ke-awan dan grup non-awan-ke-awan

Grup awan-ke-awan berisi beban kerja Microsoft 365 atau Google Workspace yang dicadangkan oleh agen awan.

Grup non-awan-ke-awan berisi semua jenis beban kerja lainnya.

Rencana yang didukung untuk grup perangkat

Tabel berikut merangkum rencana yang dapat Anda terapkan ke grup perangkat.

Grup	Rencana yang tersedia	Lokasi patch
Beban kerja awan-ke-awan (Beban kerja Microsoft 365 dan Google Workspace)	Rencana pencadangan	**Manajemen** > **Pencadangan aplikasi awan**
Beban kerja non-awan-ke-awan	Rencana proteksi	**Manajemen** > **Rencana proteksi**
	Rencana manajemen jarak jauh	**Manajemen** > **Rencana manajemen jarak jauh**
	Rencana skrip	**Manajemen** > **Rencana skrip**

Sumber daya awan, seperti pengguna Microsoft 365 atau Google Workspace, OneDrive dan Google Drive, Microsoft Teams, atau grup Azure AD disinkronkan ke konsol Cyber Protect tepat setelah Anda menambahkan organisasi Microsoft 365 atau Google Workspace ke konsol. Setiap perubahan lebih lanjut dalam suatu organisasi disinkronkan sekali sehari.

Jika Anda perlu segera menyinkronkan perubahan, di konsol Cyber Protect, navigasikan ke **Perangkat** > **Microsoft 365** atau **Perangkat** > **Google Workspace**, pilih organisasi yang diperlukan, lalu klik **Menyegarkan**.

Membuat grup statis

Anda dapat membuat grup statis kosong dan menambahkan beban kerja ke dalamnya.

Alternatifnya, Anda dapat memilih beban kerja dan membuat grup statis baru dari pilihan Anda.

© Acronis International GmbH, 2003-2024

Anda tidak dapat membuat grup perangkat dalam grup **Semua** jenis, seperti grup root **Semua perangkat**, atau grup bawaan seperti **Mesin dengan agen** > **Semua**, **Microsoft 365** > organisasi Anda > **Pengguna** > **Semua pengguna**.

Untuk membuat grup statis

Di jendela utama

1. Klik **Perangkat**, lalu pilih grup root berisi beban kerja yang ingin Anda buatkan grup statis.
2. [Opsional] Untuk membuat grup bersarang, navigasikan ke grup statis yang ada.

   Catatan
   Membuat grup statis bertingkat tidak tersedia untuk beban kerja awan-ke-awan.

3. Klik **+ Grup statis baru** di bawah pohon grup atau klik **Grup statis baru** di panel **Tindakan**.
4. Tentukan nama untuk grup baru.
5. [Opsional] Tambahkan komentar untuk grup.
6. Klik **OK**.

Di pohon grup

1. Klik **Perangkat**, lalu pilih grup root berisi beban kerja yang ingin Anda buatkan grup statis.
2. Klik ikon roda di samping nama grup tempat Anda ingin membuat grup statis baru.

   Catatan
   Membuat grup statis bertingkat tidak tersedia untuk beban kerja awan-ke-awan.

3. Klik **Grup statis baru**.
4. Tentukan nama untuk grup baru.
5. [Opsional] Tambahkan komentar untuk grup.
6. Klik **OK**.

Dari seleksi

1. Klik **Perangkat**, lalu pilih grup root berisi beban kerja yang ingin Anda buatkan grup statis.

   Catatan
   Anda tidak dapat membuat grup perangkat dalam grup **Semua** jenis, seperti grup root **Semua perangkat**, atau grup bawaan seperti **Mesin dengan agen** > **Semua**, **Microsoft 365** > organisasi Anda > **Pengguna** > **Semua pengguna**.

2. Pilih kotak centang di samping beban kerja yang ingin Anda buatkan grup baru, lalu klik **Tambahkan ke grup**.
3. Di pohon folder, pilih tingkat induk untuk grup baru, lalu klik **Grup statis baru**.

© Acronis International GmbH, 2003-2024

Catatan
Membuat grup statis bertingkat tidak tersedia untuk beban kerja awan-ke-awan.

4. Tentukan nama untuk grup baru.
5. [Opsional] Tambahkan komentar untuk grup.
6. Klik **OK**.
   Grup baru muncul di pohon folder.
7. Klik **Selesai**.

Menambahkan beban kerja ke grup statis

Anda dapat memilih grup target terlebih dahulu, lalu menambahkan beban kerja ke dalamnya.

Alternatifnya, Anda dapat memilih beban kerja terlebih dahulu, lalu menambahkannya ke grup.

Untuk menambahkan beban kerja ke grup statis

Memilih grup target terlebih dahulu

1. Klik **Perangkat**, lalu navigasikan ke grup target Anda.
2. Pilih grup target, lalu klik **Tambah peranti**.
3. Di pohon folder, pilih grup yang berisi beban kerja yang diperlukan.
4. Pilih kotak centang di samping beban kerja yang ingin Anda tambahkan, lalu klik **Tambahkan**.

Memilih beban kerja terlebih dahulu

1. Klik **Perangkat**, lalu pilih grup root berisi beban kerja yang diperlukan.
2. Pilih kotak centang di samping beban kerja yang ingin Anda tambahkan, lalu klik **Tambahkan ke grup**.
3. Di pohon folder, pilih grup target, lalu klik **Selesai**.

Membuat grup dinamis

Anda membuat grup dinamis dengan mencari beban kerja yang memiliki atribut khusus yang nilainya Anda tetapkan dalam kueri penelusuran. Kemudian Anda menyimpan hasil pencarian sebagai grup dinamis.

Atribut yang didukung untuk pencarian dan pembuatan grup dinamis berbeda antara untuk beban kerja cloud-to-cloud dan beban kerja non-cloud-to-cloud. Untuk informasi lebih lanjut tentang atribut yang didukung, lihat "Cari atribut untuk beban kerja non-awan-ke-awan" (hlm. 346) dan "Cari atribut untuk beban kerja awan-ke-awan" (hlm. 345).

Grup dinamis dibuat di grup root masing-masing. Grup dinamis bersarang tidak didukung.

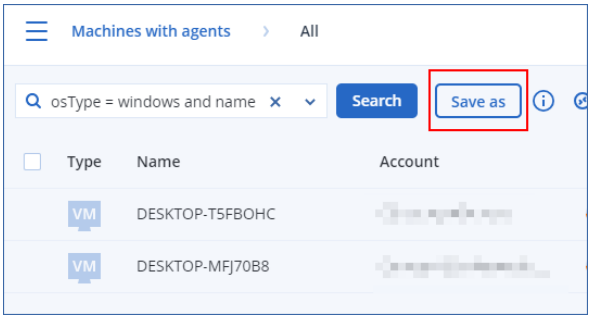
© Acronis International GmbH, 2003-2024

Anda tidak dapat membuat grup perangkat dalam grup **Semua** jenis, seperti grup root **Semua perangkat**, atau grup bawaan seperti **Mesin dengan agen** > **Semua**, **Microsoft 365** > organisasi Anda > **Pengguna** > **Semua pengguna**.

Untuk membuat grup dinamis

Beban kerja non-awan-ke-awan

1. Klik **Perangkat**, lalu pilih grup berisi beban kerja yang ingin Anda buatkan grup dinamis baru.
2. Cari beban kerja menggunakan atribut dan operator pencarian yang didukung.
   Anda dapat menggunakan beberapa atribut dan operator dalam satu kueri. Untuk informasi lebih lanjut tentang atribut yang didukung, lihat "Cari atribut untuk beban kerja non-awan-ke-awan" (hlm. 346).
3. Klik **Simpan sebagai** di sebelah bidang pencarian.



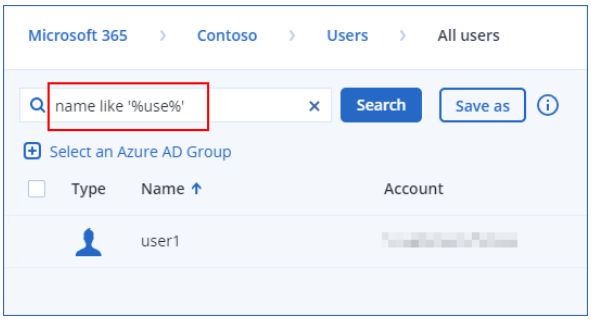
Catatan
Tombol **Simpan sebagai** tidak tersedia ketika Anda tidak diizinkan untuk membuat Grup dinamis pada level tertentu. Misalnya, dalam grup root **Perangkat** > **Semua perangkat**.
Pilih level lain (misalnya, **Perangkat** > **Mesin dengan agen** > **Semua**), dan kemudian ulangi langkah-langkah di atas. Dengan pencarian ini, Anda dapat membuat Grup dinamis dalam **Mesin dengan agen**, dan bukan dalam **Mesin dengan agen** > **Semua**.

4. Tentukan nama untuk grup baru.
5. [Opsional] Di bidang **Komentar**, tambahkan deskripsi untuk grup baru.
6. Klik **OK**.

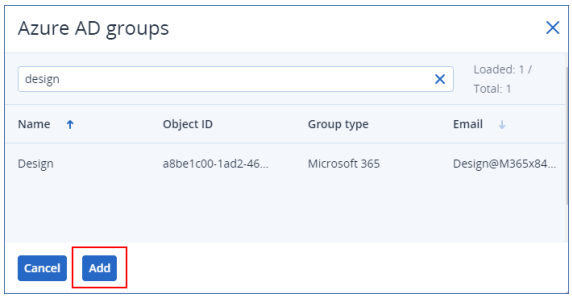
Beban kerja awan-ke-awan

1. Klik **Perangkat**, lalu pilih **Microsoft 365** atau **Google Workspace**.
2. Pilih grup yang berisi beban kerja yang ingin Anda buat sebagai Grup dinamis baru. Misalnya, **Pengguna** > **Semua pengguna**.
3. Cari beban kerja menggunakan operator dan atribut pencarian yang didukung atau dengan memilih pengguna Microsoft 365 dari grup Active Directory tertentu.
   Anda dapat menggunakan beberapa atribut dan operator dalam satu kueri. Untuk informasi lebih lanjut tentang atribut yang didukung, lihat "Cari atribut untuk beban kerja awan-ke-awan" (hlm. 345).

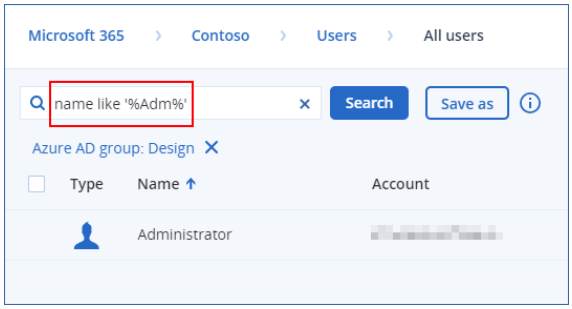
© Acronis International GmbH, 2003-2024



4. [Hanya untuk **Microsoft 365** > **Pengguna**] Untuk memilih pengguna dari grup Active Directory tertentu, lakukan hal berikut:
   a. Buka **Pengguna** > **Semua pengguna**.
   b. Klik **Pilih Grup Azure AD**.
      Daftar grup Active Directory di organisasi Anda akan terbuka.
      Dalam daftar ini, Anda dapat mencari grup tertentu atau mengurutkan grup berdasarkan nama atau email.
   c. Pilih grup Active Directory yang Anda inginkan, lalu klik **Tambahkan**.



   d. [Opsional] Untuk menyertakan atau mengecualikan pengguna tertentu dari grup Active Directory yang dipilih, buat kueri penelusuran menggunakan operator dan atribut penelusuran yang didukung.
      Anda dapat menggunakan beberapa atribut dan operator dalam satu kueri. Untuk informasi lebih lanjut tentang atribut yang didukung, lihat "Cari atribut untuk beban kerja awan-ke-awan" (hlm. 345).



5. Klik **Simpan sebagai** di sebelah bidang pencarian.

© Acronis International GmbH, 2003-2024

Catatan
Tombol **Simpan sebagai** tidak tersedia ketika Anda tidak diizinkan untuk membuat Grup dinamis pada level tertentu. Misalnya, di **Microsoft 365** > organisasi Anda > **Pengguna**.
Pilih level lain (misalnya, **Microsoft 365** > organisasi Anda > **Pengguna** > **Semua**), lalu ulangi langkah-langkah di atas. Dengan pencarian ini, Anda dapat membuat Grup dinamis dalam **Microsoft 365** > organisasi Anda > **Pengguna** >, dan bukan dalam **Pengguna** > **Semua**.

6. Tentukan nama untuk grup baru.
7. [Opsional] Di bidang **Komentar**, tambahkan deskripsi untuk grup baru.
8. Klik **OK**.

Cari atribut untuk beban kerja awan-ke-awan

Tabel berikut meringkas atribut yang dapat Anda gunakan dalam kueri pencarian untuk beban kerja Microsoft 365 dan Google Workspace.

Untuk melihat atribut mana yang dapat Anda gunakan dalam permintaan pencarian untuk jenis beban kerja lainnya, lihat "Cari atribut untuk beban kerja non-awan-ke-awan" (hlm. 346).

Atribut	Maksud	Dapat digunakan di	Contoh kueri pencarian	Didukung untuk pembuatan grup
`name`	Nama tampilan beban kerja Microsoft 365 atau Google Workspace	Semua sumber daya awan-ke-awan	`name = 'My Name'` `name LIKE '*nam*'`	Iya

`email`	Alamat email untuk pengguna atau grup Microsoft 365, atau pengguna Google Workspace	Microsoft 365 > Grup
		Microsoft 365 > Pengguna
		Google Workspace > Pengguna
			`email = 'my_group_email@mycompany.com'`
			`email LIKE '*@company*'`
			`email NOT LIKE '*enterprise.com'`
				Iya

`siteName`	Nama situs yang terkait dengan grup Microsoft 365	Microsoft 365 > Grup	`siteName = 'my_site'` `siteName LIKE '*company.com*support*'`	Iya
`url`	Alamat web untuk grup Microsoft 365 atau situs SharePoint	Microsoft 365 > Grup Microsoft 365 > Koleksi situs	`url = 'https://www.mycompany.com/'` `url LIKE '*www.mycompany.com*'`	Iya

© Acronis International GmbH, 2003-2024

Cari atribut untuk beban kerja non-awan-ke-awan

Tabel berikut meringkas atribut yang dapat Anda gunakan dalam kueri penelusuran untuk beban kerja non-awan-ke-awan.

Untuk melihat atribut mana yang dapat Anda gunakan dalam kueri penelusuran untuk beban kerja awan-ke-awan, lihat "Cari atribut untuk beban kerja awan-ke-awan" (hlm. 345).

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
Umum			
`name`	Nama beban kerja, misalnya: • Nama host untuk mesin fisik • Nama mesin virtual • Nama database • Alamat email untuk kotak surat	`name = 'en-00'`	Iya
`id`	ID Perangkat. Untuk mendapatkan ID perangkat, pada **Perangkat**, pilih perangkat, klik **Detail** > **Semua properti**. ID ditampilkan di bidang `id`.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Iya
`resourceType`	Jenis beban kerja. Nilai yang dimungkinkan: • `'machine'` • `'exchange'` • `'mssql_server'` • `'mssql_instance'` • `'mssql_database'` • `'mssql_database_folder'` • `'msexchange_database'` • `'msexchange_storage_group'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Iya

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	• 'msexchange_mailbox.msexchange' • 'msexchange_mailbox.office365' • 'mssql_aag_group' • 'mssql_aag_database' • 'virtual_machine.vmww' • 'virtual_machine.vmwesx' • 'virtual_host.vmwesx' • 'virtual_cluster.vmwesx' • 'virtual_appliance.vmwesx' • 'virtual_application.vmwesx' • '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'		

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	• `'datastore.mshyperv'` • `'virtual_machine.msvs'` • `'virtual_machine.parallelsw'` • `'virtual_host.parallelsw'` • `'virtual_cluster.parallelsw'` • `'virtual_machine.rhev'` • `'virtual_machine.kvm'` • `'virtual_machine.xen'` • `'bootable_media'`		
`chassis`	Jenis sasis. Nilai yang dimungkinkan: • `laptop` • `desktop` • `server` • `other` • `unknown`	`chassis = 'laptop'` `chassis IN ('laptop', 'desktop')`	Iya
`ip`	Alamat IP (hanya untuk mesin fisik).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Iya
`comment`	Komentar untuk perangkat. Komentar dapat ditentukan secara otomatis atau manual. Nilai defaultnya: • Untuk mesin fisik yang menjalankan Windows, deskripsi komputer di Windows disalin secara otomatis sebagai komentar. Nilai ini akan disinkronisasi setiap 15 menit. • Kosong untuk	`comment = 'important machine'` `comment = ''` (semua mesin tanpa komentar)	Iya

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup

	perangkat lain.
	
	Catatan
	Sinkronisasi otomatis dinonaktifkan jika ada teks yang ditambahkan secara manual di kolom komentar. Untuk mengaktifkan sinkronisasi lagi, hapus teks ini.
	
	Untuk me-refresh komentar yang disinkronkan secara otomatis untuk beban kerja Anda, mulai ulang Managed Machine Service di **Layanan Windows** atau jalankan perintah berikut pada saran perintah:
	
	`net stop mms`
	
	`net start mms`
	
	Untuk melihat komentar perangkat, dalam **Perangkat**, pilih perangkat, klik **Detail**, lalu cari bagian **Komentar**.
	
	Untuk menambahkan atau mengubah komentar secara manual, klik **Tambah** atau **Edit**.
	
	Untuk perangkat di mana agen proteksi diinstal, ada dua bidang komentar terpisah:
	
	• Komentar agen
	◦ Untuk mesin fisik		

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	yang menjalankan Windows, deskripsi komputer di Windows disalin secara otomatis sebagai komentar. Nilai ini akan disinkronisasi setiap 15 menit. ◦ Kosong untuk perangkat lain. **Catatan** Sinkronisasi otomatis dinonaktifkan jika ada teks yang ditambahkan secara manual di kolom komentar. Untuk mengaktifkan sinkronisasi lagi, hapus teks ini. • Komentar perangkat ◦ Jika komentar agen ditentukan secara otomatis, komentar akan disalin sebagai komentar perangkat. Komentar agen yang ditambahkan secara manual tidak disalin sebagai komentar perangkat. ◦ Komentar perangkat tidak disalin sebagai komentar agen. Perangkat dapat mengatur agar satu atau kedua komentar ini ditentukan, atau membiarkan keduanya kosong. Jika		

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	kedua komentar ditentukan, komentar perangkat yang diprioritaskan. Untuk melihat komentar agen, di bawah **Pengaturan** > **Agen**, pilih perangkat dengan agen, klik **Detail**, lalu cari bagian **Komentar**. Untuk melihat komentar perangkat, dalam **Perangkat**, pilih perangkat, klik **Detail**, lalu cari bagian **Komentar**. Untuk menambahkan atau mengubah komentar secara manual, klik **Tambah** atau **Edit**.		
`isOnline`	Ketersediaan beban kerja. Nilai yang dimungkinkan: • `true` • `false`	`isOnline = true`	Tidak
`hasAsz`	Ketersediaan Secure Zone. Nilai yang dimungkinkan: • `true` • `false`	`hasAsz = true`	Iya

`tzOffset`	Pergeseran zona waktu dari Waktu Universal Terkoordinasi (UTC), dalam menit.	`tzOffset = 120`
		`tzOffset > 120`
		`tzOffset < 120`
			Iya

CPU, memori, disk			
`cpuArch`	Arsitektur CPU. Nilai yang dimungkinkan:	`cpuArch = 'x64'`	Iya

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	• `'x64'` • `'x86'`		
`cpuName`	Nama CPU.	`cpuName LIKE '%XEON%'`	Iya
`memorySize`	Ukuran RAM dalam megabyte.	`memorySize < 1024`	Iya
`diskSize`	Ukuran hard drive dalam gigabyte atau megabyte (hanya untuk mesin fisik).	`diskSize < 300GB` `diskSize >= 3000000MB`	Tidak
Sistem operasi			
`osName`	Nama sistem operasi	`osName LIKE '%Windows XP%'`	Iya
`osType`	Jenis sistem operasi. Nilai yang dimungkinkan: • `'windows'` • `'linux'` • `'macosx'`	`osType = 'windows'` `osType IN ('linux', 'macosx')`	Iya
`osArch`	Arsitektur sistem operasi. Nilai yang dimungkinkan: • `'x64'` • `'x86'`	`cpuArch = 'x86'`	Iya
`osProductType`	Jenis produk sistem operasi. Nilai yang dimungkinkan: • `'dc'` Singkatan dari Pengontrol Domain.	`osProductType = 'server'`	Iya

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	Catatan Catatan Ketika peran pengontrol domain ditetapkan di server Windows, `osProductType` berubah dari `server` menjadi `dc`. Mesin seperti itu tidak akan disertakan dalam hasil pencarian untuk filter `osProductType='server'`. • `'server'` • `'workstation'`		
`osSp`	Paket layanan sistem operasi.	`osSp = 1`	Iya
`osVersionMajor`	Versi besar sistem operasi.	`osVersionMajor = 1`	Iya
`osVersionMinor`	Versi kecil sistem operasi.	`osVersionMinor > 1`	Iya
Agen			
`agentVersion`	Versi agen perlindungan yang diinstal.	`agentVersion LIKE '12.0.*'`	Iya
`hostId`	ID internal agen perlindungan. Untuk mendapatkan ID Agen perlindungan, pada **Perangkat**, pilih perangkat, klik **Detail** > **Semua properti**. Gunakan nilai `id` properti `agen`.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Iya
`virtualType`	Tipe mesin virtual. Nilai yang dimungkinkan: • `'vmwesx'` Mesin virtual VMware. • `'mshyperv'`	`virtualType = 'vmwesx'`	Iya

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	Mesin virtual Hyper-V. • `'pcs'` Mesin virtual Virtuozzo. • `'hci'` Mesin virtual Virtuozzo Hybrid Infrastructure. • `'scale'` Mesin virtual Scale Computing HC3. • `'ovirt'` Mesin virtual oVirt		
`insideVm`	Mesin virtual dengan agen di dalamnya. Nilai yang dimungkinkan: • `true` • `false`	`insideVm = true`	Iya
Lokasi			
`tenant`	Nama penyewa yang memiliki perangkat tersebut.	`tenant = 'Unit 1'`	Iya
`tenantId`	Pengidentifikasi Penyewa yang dimiliki perangkat. Untuk mendapatkan ID penyewa, pada **Perangkat**, pilih perangkat, klik **Detail** > **Semua properti**. ID ditampilkan di bidang `ownerId`.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Iya
`ou`	Perangkat yang dimiliki unit organisasi Active Directory yang ditentukan.	`ou IN ('RnD', 'Computers')`	Iya
Status			
`state`	Status perangkat. Nilai yang dimungkinkan:	`state = 'backup'`	Tidak

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	• 'idle' • 'interactionRequired' • 'canceling' • 'backup' • 'recover' • 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'		
status	Status perlindungan. Nilai yang dimungkinkan: • ok • warning • error • critical • protected • notProtected	status = 'ok' status IN ('error', 'warning')	Tidak
protectedByPlan	Perangkat yang dilindungi oleh rencana proteksi dengan ID tertentu. Untuk melihat ID rencana, di **Manajemen** > **Rencana proteksi**, pilih rencana, klik bilah di kolom **Status**, lalu klik nama status. Pencarian baru dengan ID rencana akan dibuat.	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Tidak
okByPlan	Perangkat yang dilindungi oleh rencana proteksi dengan ID tertentu dan	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Tidak

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	memiliki status **OK**.		
`errorByPlan`	Perangkat yang dilindungi oleh rencana proteksi dengan ID tertentu dan memiliki status **Kesalahan**.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Tidak
`warningByPlan`	Perangkat yang dilindungi oleh rencana proteksi dengan ID tertentu dan memiliki status **Peringatan**.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Tidak
`runningByPlan`	Perangkat yang dilindungi oleh rencana proteksi dengan ID tertentu dan memiliki status **Berjalan**.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Tidak
`interactionByPlan`	Perangkat yang dilindungi oleh rencana proteksi dengan ID tertentu dan memiliki status **Interaksi Diperlukan**.	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Tidak

`lastBackupTime`*	Tanggal dan waktu pencadangan terakhir yang berhasil.
	Formatnya adalah `'YYYY-MM-DD HH: MM'`.
		`lastBackupTime > '2023-03-11'`
		`lastBackupTime <= '2023-03-11 00:15'`
		`lastBackupTime is null`
			Tidak

`lastBackupTryTime`*	Waktu percobaan pencadangan terakhir. Formatnya adalah `'YYYY-MM-DD HH: MM'`.	`lastBackupTryTime >= '2023-03-11'`	Tidak
`nextBackupTime`*	Waktu pencadangan berikutnya. Formatnya adalah `'YYYY-MM-DD HH: MM'`.	`nextBackupTime >= '2023-08-11'`	Tidak
`lastVAScanTime`*	Tanggal dan waktu penilaian kerentanan terakhir yang berhasil dilakukan.	`lastVAScanTime > '2023-03-11'` `lastVAScanTime <= '2023-03-11 00:15'`	Iya

© Acronis International GmbH, 2003-2024

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	Formatnya adalah `'YYYY-MM-DD HH: MM'`.	`lastVAScanTime is null`	
`lastVAScanTryTime*`	Waktu upaya penilaian kerentanan terakhir. Formatnya adalah `'YYYY-MM-DD HH: MM'`.	`lastVAScanTimeTryTime >= '2022-03-11'`	Iya
`nextVAScanTime*`	Waktu penilaian kerentanan berikutnya. Formatnya adalah `'YYYY-MM-DD HH: MM'`.	`nextVAScanTime <= '2023-08-11'`	Iya
`network_status`	Status isolasi jaringan untuk Deteksi dan Tanggapan Titik Akhir (EDR). Nilai yang dimungkinkan: • `connected` • `isolated`	`network_status= 'connected'`	Iya

Catatan
Jika Anda melewatkan nilai jam dan menit, waktu mulai dianggap YYYY-MM-DD 00:00, dan waktu selesai dianggap YYYY-MM-DD 23:59:59. Contohnya, `lastBackupTime = 2023-01-20`, berarti hasil pencarian akan menyertakan semua cadangan dari interval `lastBackupTime >= 2023-01-20 00:00` dan `lastBackup time <= 2023-01-20 23:59:59`.

Operator pencarian

Tabel berikut merangkum operator yang bisa Anda gunakan untuk kueri pencarian.

Anda dapat menggunakan lebih dari satu operator dalam kueri tunggal.

Operator	Didukung untuk	Maksud	Contoh
`AND`	Semua beban kerja	Operator konjungsi logis	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Semua	Operator disjungsi	`state = 'backup' OR state =`

© Acronis International GmbH, 2003-2024

Operator	Didukung untuk	Maksud	Contoh
	beban kerja	logis	`'interactionRequired'`
`NOT`	Semua beban kerja	Operator negasi logis	`NOT(osProductType = 'workstation')`
`IN (<value1>,... <valueN>)`	Semua beban kerja	Operator ini memeriksa apakah suatu ekspresi cocok dengan setiap nilai dalam daftar nilai.	`osType IN ('windows', 'linux')`
`NOT IN`	Semua beban kerja	Operator ini berlawanan dengan operator `IN`.	`NOT osType IN ('windows', 'linux')`

`LIKE 'wildcard pattern'`	Semua beban kerja	Operator ini memeriksa apakah suatu ekspresi cocok dengan pola wildcard.
		Anda dapat menggunakan operator wildcard berikut:
		• * atau % Tanda bintang dan persen mewakili nol, satu, atau beberapa karakter
		• _ Garis bawah mewakili satu karakter
			`name LIKE 'en-00'`
			`name LIKE '*en-00'`
			`name LIKE '*en-00*'`
			`name LIKE 'en-00_'`

`NOT LIKE 'wildcard pattern'`	Semua beban kerja	Operator ini berlawanan dengan operator `LIKE`.
		Anda dapat menggunakan operator wildcard berikut:
		• * atau % Tanda bintang dan
			`NOT name LIKE 'en-00'`
			`NOT name LIKE '*en-00'`
			`NOT name LIKE '*en-00*'`
			`NOT name LIKE 'en-00_'`

© Acronis International GmbH, 2003-2024

Operator	Didukung untuk	Maksud	Contoh
		persen mewakili nol, satu, atau beberapa karakter • _ Garis bawah mewakili satu karakter	

`RANGE (<starting_value>, <ending_value>)`	Semua beban kerja	Operator ini memeriksa apakah suatu ekspresi berada dalam rentang nilai (inklusif).
		Kueri pencarian dengan string alfanumerik menggunakan urutan ASCII tetapi tidak peka huruf besar-kecil.
			`ip RANGE('10.250.176.1','10.250.176.50')`
			`name RANGE('a','d')`
			Dengan kueri ini, Anda dapat memfilter semua nama yang dimulai dengan A, B, dan C, seperti `Alice`, `Bob`, `Claire`. Namun, hanya satu huruf D yang memenuhi syarat, jadi nama dengan lebih banyak huruf, seperti `Diana` atau `Don` tidak akan disertakan.
			Untuk mencapai hasil yang sama, Anda juga dapat menggunakan kueri berikut:
			`name >= 'a' AND name <= 'd'`

= atau ==	Semua beban kerja	Operator *sama dengan*	`osProductType = 'server'`
!= atau <>	Semua beban kerja	Operator *tidak sama dengan*	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
<	Beban kerja non-awan-ke-awan	Operator *kurang dari*	`memorySize < 1024`
>	Beban kerja non-awan-ke-awan	Operator *lebih besar dari*.	`diskSize > 300GB`
<=	Beban kerja non-awan-ke-awan	Operator *kurang dari atau sama dengan*	`lastBackupTime <= '2022-03-11 00:15'`
>=	Beban kerja non-awan-ke-awan	Operator *lebih dari atau sama dengan*	`nextBackupTime >= '2022-08-11'`

© Acronis International GmbH, 2003-2024

Mengedit grup dinamis

Anda mengedit grup dinamis dengan mengubah permintaan pencarian yang menentukan konten grup.

Dalam grup dinamis yang berbasis Active Directory, Anda juga dapat mengubah grup Active Directory.

Untuk mengedit grup dinamis

Dengan mengubah permintaan pencarian

1. Klik **Perangkat**, navigasikan ke grup dinamis yang ingin Anda edit, lalu pilih.
2. Klik ikon roda di samping nama grup, lalu klik **Edit**. Atau, klik **Edit** di panel **Tindakan**.
3. Ubah kueri pencarian dengan mengubah atribut pencarian, nilai, atau operator pencarian, lalu klik **Cari**.
4. Klik **Simpan** di samping bidang pencarian.

Dengan mengubah grup Active Directory

Catatan
Prosedur ini berlaku untuk grup dinamis berbasis Active Directory. Grup dinamis berbasis Active Directory hanya tersedia di **Microsoft 365** > **Pengguna**.

1. Klik **Perangkat**, arahkan ke **Perangkat** > **Microsoft 365** > organisasi Anda > **Pengguna**.
2. Pilih grup dinamis yang ingin Anda edit.
3. Klik ikon roda di samping nama grup, lalu klik **Edit**. Atau, klik **Edit** di panel **Tindakan**.
4. Ubah konten grup dengan melakukan salah satu hal berikut:
   - Ubah grup Active Directory yang sudah dipilih dengan mengeklik namanya, lalu pilih grup Active Directory baru dari daftar yang terbuka.
   - Edit kueri pencarian, lalu klik **Cari**.
     Kueri pencarian terbatas pada grup Active Directory yang dipilih saat ini.
5. Klik **Simpan** di samping bidang pencarian.

Anda juga dapat menyimpan hasil edit tanpa menimpa grup saat ini. Untuk menyimpan konfigurasi yang telah diedit sebagai grup baru, klik tombol panah di samping bidang pencarian, lalu klik **Simpan sebagai**.

Menghapus grup

Saat Anda menghapus grup perangkat, semua rencana yang diterapkan ke grup tersebut akan dicabut. Beban kerja dalam grup akan menjadi tidak terlindungi jika tidak ada rencana lain yang diterapkan padanya.

Untuk menghapus grup perangkat

© Acronis International GmbH, 2003-2024

1. Klik **Perangkat**, lalu navigasikan ke grup yang ingin Anda hapus.
2. Klik ikon roda di samping nama grup, lalu klik **Hapus**.
3. Konfirmasikan pilihan Anda dengan mengeklik **Hapus**.

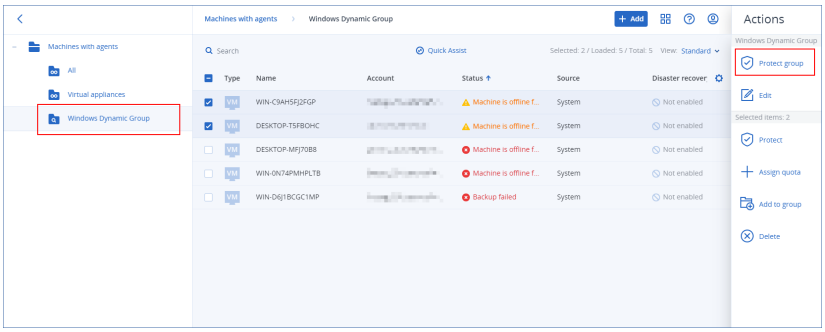
Menerapkan rencana ke grup

Anda dapat menerapkan rencana ke grup dengan memilih grup terlebih dahulu, lalu menerapkan rencana ke grup tersebut.

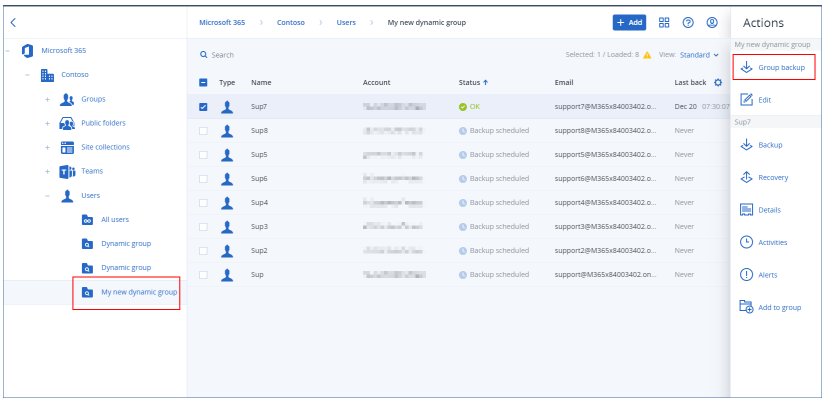
Alternatifnya, Anda dapat membuka rencana untuk diedit, lalu menambahkan grup ke dalamnya.

Untuk menerapkan rencana ke grup

1. Klik **Perangkat**, lalu navigasikan ke grup tempat Anda ingin menerapkan rencana.
2. [Untuk beban kerja non-awan-ke-awan] Klik **Lindungi grup**.



   Daftar rencana yang dapat diterapkan ditampilkan.
3. [Untuk beban kerja awan-ke-awan] Klik **Pencadangan grup**.



   Daftar rencana pencadangan yang dapat diterapkan ditampilkan.
4. [Untuk menerapkan rencana yang sudah ada] Pilih rencana, lalu klik **Terapkan**.
5. [Untuk membuat rencana baru] Klik **Buat rencana**, pilih jenis rencana, lalu buat rencana baru.

   Untuk informasi selengkapnya tentang jenis rencana yang tersedia dan cara membuatnya, lihat "Rencana yang didukung untuk grup perangkat" (hlm. 340).

© Acronis International GmbH, 2003-2024

Catatan
Rencana pencadangan yang diterapkan ke grup perangkat awan-ke-awan dijadwalkan secara otomatis untuk berjalan sekali sehari. Anda tidak dapat menjalankan rencana ini sesuai permintaan dengan mengeklik **Jalankan sekarang**.

Batalkan rencana dari grup

Anda dapat membatalkan rencana dari grup dengan memilih grupnya terlebih dahulu, lalu membatalkan rencananya.

Atau, Anda dapat membuka rencana untuk diedit, lalu menghapus grupnya.

Untuk membatalkan rencana dari grup

1. Klik **Perangkat**, lalu buka grup tempat Anda ingin membatalkan rencana.
2. [Untuk beban kerja non-awan-ke-awan] Klik **Lindungi grup**.
   Daftar rencana yang dapat diterapkan ke grup akan ditampilkan.
3. [Untuk beban kerja awan-ke-awan] Klik **Pencadangan grup**.
   Daftar rencana pencadangan yang diterapkan pada grup akan ditampilkan.
4. Pilih rencana yang ingin Anda batalkan.
5. [Untuk beban kerja non-awan-ke-awan] Klik ikon elipsis (...), lalu klik **Batalkan**.
6. [Untuk beban kerja awan-ke-awan] Klik ikon roda gigi, lalu klik **Batalkan**.

Bekerja dengan modul kontrol Perangkat

Sebagai bagian dari Cyber Protection rencana proteksi layanan, modul kontrol perangkat[1] memanfaatkan subset fungsional dari agen Pencegah Kehilangan Data[2] pada setiap komputer terlindungi demi mendeteksi dan mencegah akses dan transmisi data tanpa izin melalui saluran komputer lokal. Modul kontrol perangkat menyediakan kontrol halus pada jalur kebocoran data yang luas, termasuk pertukaran data menggunakan media yang dapat dilepas, printer, perangkat virtual dan yang dialihkan, dan papan klip Windows.

---

[1]Sebagai bagian dari rencana proteksi, modul kontrol perangkat memanfaatkan subset fungsional dari agen pencegah hilangnya data pada tiap komputer terlindungi demi mendeteksi, dan mencegah akses dan transmisi data tanpa izin melalui saluran komputer lokal. Hal ini mencakup akses pengguna ke perangkat periferal dan port, pencetakan dokumen, operasi salin/tempel papan klip, operasi format dan keluarkan media, maupun sinkronisasi dengan perangkat bergerak yang terhubung di lokasi terkait. Modul kontrol perangkat menyediakan kendali granural dan kontekstual pada tipe perangkat dan port yang dapat diakses pengguna di komputer terlindungi dan tindakan yang dapat dilakukan pengguna ke perangkat tersebut.
[2]Komponen klien dari sistem pencegah hilangnya data yang melindungi komputer host dari penggunaan tanpa izin, transmisi, dan penyimpanan data rahasia, terlindungi, atau sensitif dengan menerapkan kombinasi teknik analisis konteks dan konten, serta menegakkan kebijakan pencegah hilangnya data yang dikelola secara terpusat. Perlindungan cyber menyediakan agen pencegah hilangnya data berfitur lengkap. Akan tetapi, fungsionalitas agen pada komputer terlindungi terbatas pada set fitur pencegah hilangnya data yang tersedia untuk pelisensian dalam Perlindungan cyber, dan bergantung pada rencana proteksi yang berlaku pada komputer tersebut.

© Acronis International GmbH, 2003-2024

Modul ini tersedia untuk edisi Cyber Product Essentials, Cyber Protect Standard, dan Cyber Protect Advanced yang berlisensi per beban kerja.

Catatan
Pada mesin Windows, fitur kontrol perangkat memerlukan instalasi Agen untuk Pencegahan Kehilangan Data. Fitur akan diinstal secara otomatis demi beban kerja yang terlindungi jika modul **Kontrol perangkat** diaktifkan dalam rencana proteksinya.

Modul kontrol perangkat bergantung pada fungsi pencegah kehilangan data[1] milik agen untuk menegakkan kontrol kontekstual terhadap operasi akses dan transfer data pada komputer terlindungi. Ini termasuk akses pengguna ke perangkat periferal dan port, pencetakan dokumen, operasi salin/tempel papan klip, operasi format dan keluarkan media, maupun sinkronisasi dengan perangkat seluler yang terhubung secara lokal. Agen Pencegah Kehilangan Data termasuk kerangka kerja untuk semua komponen manajemen dan administrasi pusat milik modul kontrol perangkat sehingga harus diinstal di setiap komputer agar terlindungi dengan modul kontrol perangkat. Agen ini mengizinkan, membatasi, atau menolak tindakan pengguna berdasarkan pengaturan kontrol perangkat yang diterima dari rencana proteksi yang diterapkan di komputer terlindungi.

Modul kontrol perangkat mengontrol akses ke berbagai perangkat periferal, baik yang digunakan secara langsung di komputer terlindungi atau yang dialihkan di lingkungan virtualisasi yang di-host di komputer terlindungi. Modul tersebut mengenali perangkat yang dialihkan di Microsoft Remote Desktop Server, Citrix XenDesktop / XenApp / XenServer, dan VMware Horizon. Modul itu juga dapat mengontrol operasi salin data antara papan klip sistem operasi tamu yang berjalan di VMware Workstation / Player, Oracle VM VirtualBox, atau Windows Virtual PC, dan papan klip sistem operasi host yang berjalan di komputer terlindungi.

Modul kontrol perangkat dapat melindungi komputer yang menjalankan sistem operasi berikut:

Kontrol perangkat

- Microsoft Windows 7 Service Pack 1 dan versi lebih baru
- Microsoft Windows Server 2008 R2 dan versi lebih baru
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

Catatan
Agen untuk Pencegahan Kehilangan Data untuk macOS hanya mendukung prosesor x64. Prosesor berbasis Apple silicon ARM tidak didukung.

[1]Sistem teknologi terintegrasi dan prosedur organisasi yang bertujuan untuk mendeteksi dan mencegah penyingkapan/akses secara sengaja atau tidak ke data rahasia, terlindungi, atau sensitif yang dilakukan oleh entitas tanpa izin di luar atau dalam organisasi, atau pengiriman data tersebut ke lingkungan yang tidak tepercaya.

© Acronis International GmbH, 2003-2024

Pencegah kehilangan data

- Microsoft Windows 7 Service Pack 1 dan versi lebih baru
- Microsoft Windows Server 2008 R2 dan versi lebih baru

Catatan
Agen untuk Pencegahan Kehilangan Data dapat diinstal pada sistem macOS yang tidak didukung karena merupakan bagian integral dari Agen untuk Mac. Pada kasus ini, konsol Cyber Protect akan mengindikasikan bahwa Agen untuk Pencegahan Kehilangan Data sudah diinstal di komputer, tetapi fungsionalitas kontrol perangkat dan pencegahan kehilangan data tidak akan berfungsi. Fungsionalitas kontrol perangkat hanya akan berfungsi pada sistem macOS yang didukung oleh Agen untuk Pencegahan Kehilangan Data.

Keterbatasan pada penggunaan agen untuk Pencegahan Kehilangan Data dengan Hyper-V

Jangan instal Agen untuk Pencegahan Kehilangan Data pada host Hyper-V di kluster Hyper-V karena dapat menyebabkan masalah BSOD, terutama di kluster Hyper-V dengan Volume Bersama Kluster (CSV).

Jika Anda menggunakan salah satu versi Agen untuk Hyper-V berikut, Anda perlu menghapus Agen untuk Pencegahan Kehilangan Data secara manual:

- 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)

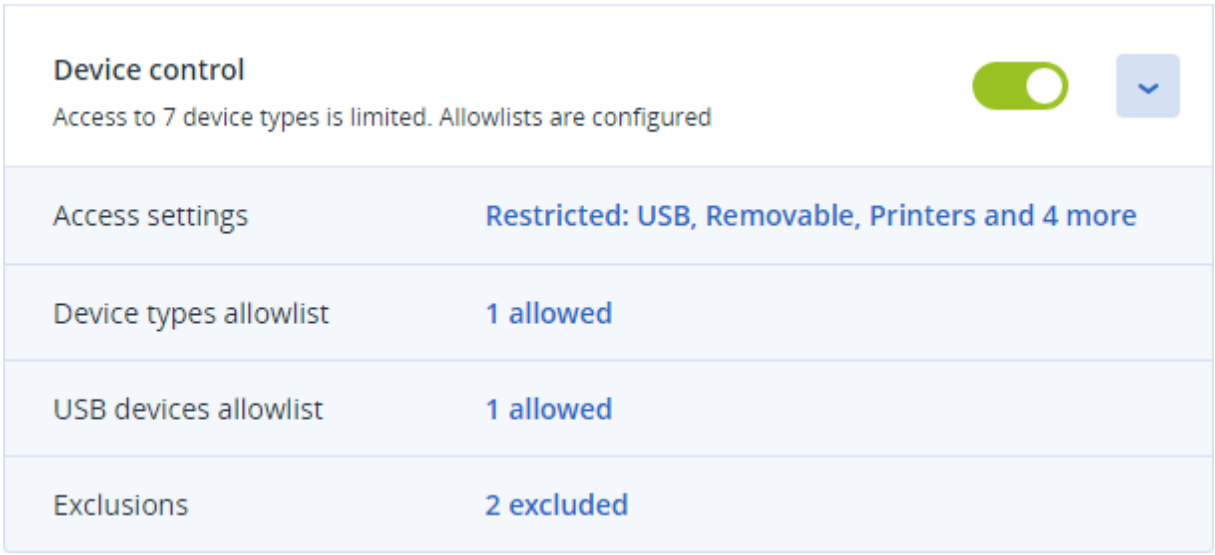
Untuk menghapus Agen untuk Pencegahan Kehilangan Data, di host Hyper-V, jalankan penginstal secara manual dan kosongkan kotak centang Agen untuk Pencegahan Kehilangan Data, atau jalankan perintah berikut:

```
<installer_name> --remove-components=agentForDlp -quiet
```

Anda dapat mengaktifkan dan mengonfigurasi modul kontrol perangkat di bagian **Kontrol perangkat** dari rencana proteksi Anda di konsol Cyber Protect. Untuk instruksi, lihat langkah-langkah mengaktifkan atau menonaktifkan kontrol perangkat.

© Acronis International GmbH, 2003-2024

Bagian **Kontrol perangkat** menampilkan rangkuman konfigurasi modul:



- Pengaturan akses - Menunjukkan rangkuman tipe perangkat dan port dengan akses terbatas (ditolak atau hanya baca), jika ada. Jika tidak, ia menunjukkan semua tipe perangkat yang diizinkan. Klik rangkuman ini untuk melihat atau mengubah pengaturan akses (lihat langkah-langkah melihat atau mengubah pengaturan akses).
- Daftar izin tipe perangkat - Menunjukkan jumlah subklas perangkat yang diizinkan dengan mengecualikannya dari kontrol akses perangkat, jika ada. Jika tidak, ia menunjukkan daftar izin yang kosong. Klik rangkuman ini untuk melihat atau mengubah pilihan subklas perangkat yang diizinkan (lihat langkah-langkah mengecualikan subklas perangkat dari kontrol akses).
- Daftar izin perangkat USB - Menunjukkan jumlah perangkat/model USB yang diizinkan dengan mengecualikannya dari kontrol akses perangkat, jika ada. Jika tidak, ia menunjukkan daftar izin yang kosong. Klik rangkuman ini untuk melihat atau mengubah pilihan perangkat/model USB yang diizinkan (lihat langkah-langkah mengecualikan masing-masing perangkat USB dari kontrol akses).
- Pengecualian - Menunjukkan jumlah pengecualian kontrol akses yang telah ditetapkan untuk papan klip Windows, tangkapan layar, printer, dan perangkat seluler.

Menggunakan kontrol perangkat

Bagian ini mencakup instruksi langkah-demi-langkah untuk tugas mendasar saat menggunakan modul kontrol perangkat.

Aktifkan atau nonaktifkan kontrol perangkat

Anda dapat mengaktifkan kontrol perangkat saat membuat rencana proteksi. Anda dapat mengubah rencana proteksi yang ada untuk mengaktifkan atau menonaktifkan kontrol perangkat.

Untuk mengaktifkan atau menonaktifkan kontrol perangkat

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Lakukan salah satu langkah berikut untuk membuka panel rencana proteksi:
   - Jika Anda ingin membuat rencana proteksi baru, pilih mesin untuk melindungi, klik **Lindungi**, lalu klik **Buat rencana**.
   - Jika Anda ingin mengubah rencana proteksi yang ada, pilih mesin terlindungi, klik **Lindungi**, klik elipsis (...) di sebelah nama rencana proteksi, lalu klik **Edit**.
3. Di panel rencana proteksi, navigasikan ke area **Kontrol perangkat**, lalu klik untuk mengaktifkan atau menonaktifkan **Kontrol perangkat**.
4. Lakukan salah satu langkah berikut untuk menerapkan perubahan Anda:
   - Jika membuat rencana proteksi, klik **Buat**.
   - Jika mengedit rencana proteksi, klik **Simpan**.

Anda juga dapat mengakses panel rencana proteksi dari Tab manajemen. Namun, belum tentu tersedia di semua edisi layanan Cyber Protection.

Mengaktifkan penggunaan modul kontrol perangkat pada macOS

Pengaturan kontrol perangkat pada rencana proteksi akan berlaku hanya setelah memuat driver kontrol perangkat pada beban kerja yang dilindungi. Bagian ini menjelaskan cara memuat driver kontrol perangkat untuk mengaktifkan penggunaan modul kontrol perangkat pada macOS. Ini adalah operasi satu kali yang memerlukan hak istimewa administrator pada mesin titik akhir.

Versi macOS yang didukung:

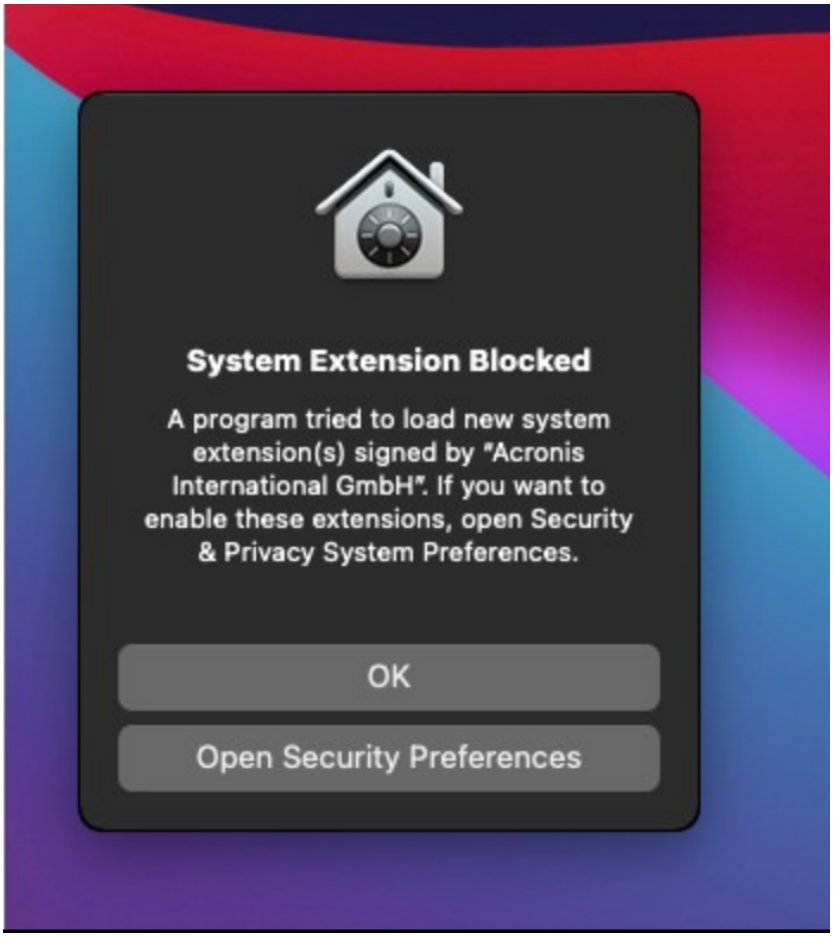
- macOS 10.15 (Catalina) dan versi lebih baru
- macOS 11.2.3 (Big Sure) dan versi lebih baru
- macOS 12.2 (Monterey) dan versi lebih baru
- macOS 13.2 (Ventura) dan versi lebih baru

Untuk mengaktifkan penggunaan modul kontrol perangkat pada macOS

1. Instal Agen untuk Mac pada mesin yang ingin Anda lindungi.
2. Aktifkan pengaturan kontrol perangkat dalam rencana proteksi.
3. Terapkan rencana proteksi.

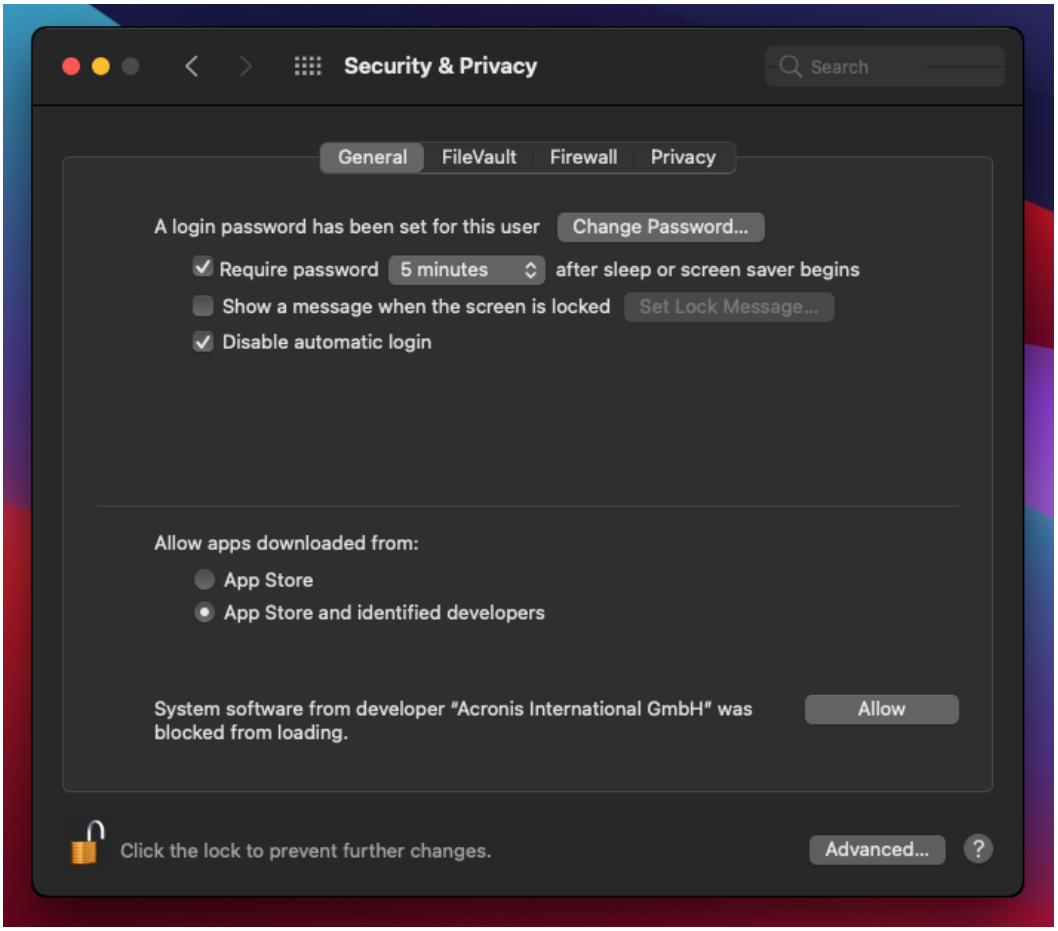
© Acronis International GmbH, 2003-2024

4. Peringatan "Ekstensi Sistem Diblokir" akan muncul di beban kerja yang diproteksi. Klik **Buka Preferensi Keamanan**.



© Acronis International GmbH, 2003-2024

5. Pada panel **Keamanan & Privasi** yang muncul, pilih **App Store dan pengembang yang teridentifikasi** lalu klik **Izinkan**.



6. Dalam dialog yang muncul, klik **Mulai ulang** untuk memulai ulang beban kerja dan mengaktifkan pengaturan kontrol perangkat.

Catatan
Anda tidak perlu mengulangi langkah ini jika pengaturan kontrol perangkat dinonaktifkan lalu diaktifkan kembali.

Lihat atau ubah pengaturan akses

Dari panel rencana proteksi, Anda dapat mengelola pengaturan akses perangkat untuk modul kontrol perangkat. Dengan ini, Anda dapat mengizinkan atau menolak akses ke tipe perangkat tertentu, sekaligus mengaktifkan atau menonaktifkan notifikasi dan peringatan.

Untuk melihat atau mengubah pengaturan akses

1. Buka panel rencana proteksi dan aktifkan kontrol perangkat di rencana tersebut (lihat langkah-langkah mengaktifkan atau menonaktifkan kontrol perangkat).
2. Klik ikon panah di sebelah saklar **Kontrol perangkat** untuk memperluas pengaturan, lalu klik tautan di sebelah **Pengaturan akses**.

© Acronis International GmbH, 2003-2024

3. Di halaman mengelola pengaturan akses yang muncul, lihat atau ubah pengaturan akses sebagaimana dibutuhkan.

Catatan
Pengaturan akses yang dikonfigurasi dalam Kontrol perangkat mungkin akan diganti saat menggunakan Kontrol perangkat dan Advanced DLP untuk melindungi beban kerja. Lihat "Mengaktifkan Advanced Data Loss Prevention di rencana proteksi" (hlm. 874).

Aktifkan atau nonaktifkan notifikasi OS dan peringatan layanan.

Saat mengelola pengaturan akses, Anda dapat mengaktifkan atau menonaktifkan notifikasi OS dan peringatan layanan, memberi tahu jika ada pengguna yang mencoba tindakan terlarang.

Untuk mengaktifkan atau menonaktifkan notifikasi OS

1. Ikuti langkah-langkah melihat atau mengubah pengaturan akses.
2. Di halaman untuk mengelola akses perangkat, pilih atau kosongkan kotak centang **Tampilkan pemberitahuan OS kepada pengguna akhir jika mereka mencoba menggunakan tipe atau port perangkat yang terblokir**.

Untuk mengaktifkan atau menonaktifkan peringatan layanan

1. Ikuti langkah-langkah melihat atau mengubah pengaturan akses.
2. Pada halaman untuk mengelola akses perangkat, pilih atau kosongkan kotak centang **Tampilkan peringatan** untuk tipe perangkat yang diinginkan.

Kotak centang **Tampilkan peringatan** tersedia hanya untuk tipe perangkat dengan akses terbatas (akses Hanya-baca atau Ditolak), kecuali tangkapan layar.

Kecualikan subklas perangkat dari kontrol akses

Dari panel rencana proteksi, Anda dapat memilih subklas perangkat yang dikecualikan dari kontrol akses. Hasilnya, akses ke perangkat tersebut diizinkan terlepas dari pengaturan akses kontrol perangkat.

Untuk mengecualikan subklas perangkat dari kontrol akses

1. Buka panel rencana proteksi dan aktifkan kontrol perangkat di rencana tersebut (lihat langkah-langkah mengaktifkan atau menonaktifkan kontrol perangkat).
2. Klik ikon panah di sebelah saklar **Kontrol perangkat** untuk memperluas pengaturan, lalu klik tautan di sebelah **Daftar izin tipe perangkat**.
3. Di halaman mengelola daftar izin yang muncul, lihat atau ubah pilihan subklas perangkat untuk dikecualikan dari kontrol akses.

Kecualikan maisng-masing perangkat USB dari kontrol akses

Dari panel rencana proteksi, Anda dapat memilih masing-masing perangkat atau model USB untuk dikecualikan dari kontrol akses. Hasilnya, akses ke perangkat tersebut diizinkan, terlepas dari

© Acronis International GmbH, 2003-2024

pengaturan akses kontrol perangkat.

Untuk mengecualikan perangkat USB dari kontrol akses

1. Buka panel rencana proteksi dan aktifkan kontrol perangkat di rencana tersebut (lihat langkah-langkah mengaktifkan atau menonaktifkan kontrol perangkat).
2. Klik ikon panah di sebelah saklar **Kontrol perangkat** untuk memperluas pengaturan, lalu klik tautan di sebelah **Daftar izin perangkat USB**.
3. Di halaman mengelola daftar izin yang muncul, klik **Tambahkan dari database**.
4. Di halaman untuk memilih perangkat USB yang muncul, pilih perangkat yang diinginkan dari yang didaftarkan dengan database perangkat USB.
5. Klik tombol **Tambahkan ke daftar izin**.

Untuk berhenti mengecualikan perangkat USB dari kontrol akses

1. Buka panel rencana proteksi dan aktifkan kontrol perangkat di rencana tersebut (lihat langkah-langkah mengaktifkan atau menonaktifkan kontrol perangkat).
2. Klik ikon panah di sebelah saklar **Kontrol perangkat** untuk memperluas pengaturan, lalu klik tautan di sebelah **Daftar izin perangkat USB**.
3. Di halaman mengelola daftar izin yang muncul, klik ikon hapus di akhir item yang mewakili perangkat USB diinginkan.

Tambah atau hapus perangkat USB dari database

Untuk mengecualikan perangkat USB tertentu dari kontrol akses, Anda perlu menambahkannya ke database perangkat USB. Lalu, Anda dapat menambahkan perangkat ke daftar izin dengan memilih dari database tersebut.

Prosedur berikut ini berlaku untuk rencana proteksi dengan fitur kontrol perangkat yang diaktifkan.

Untuk menambahkan perangkat USB ke database

1. Buka rencana proteksi salah satu perangkat untuk mengedit:
   Klik elipsis (...) di samping nama rencana proteksi dan pilih **Edit**.

   Catatan
   Kontrol perangkat harus diaktifkan dalam rencana sehingga Anda dapat mengakses pengaturan Kontrol perangkat.

2. Klik ikon panah di sebelah saklar **Kontrol perangkat** untuk memperluas pengaturan, lalu klik tautan di sebelah **Daftar izin perangkat USB**.
3. Di halaman **daftar izin perangkat USB** yang muncul, klik **Tambahkan dari database**.
4. Di halaman manajemen database perangkat USB yang muncul, klik **Tambahkan ke database**.
5. Pada dialog **Tambahkan perangkat USB** yang muncul, klik mesin tempat perangkat USB terhubung.
   Hanya mesin yang sedang online yang ditampilkan dalam daftar komputer.

© Acronis International GmbH, 2003-2024

Daftar perangkat USB ditampilkan hanya bagi mesin yang di dalamnya sudah terinstal agen untuk Pencegahan Kehilangan Data.

Perangkat USB dicantumkan dalam tampilan hierarki. Tingkat pertama hierarki mewakili model perangkat. Tingkat kedua mewakili perangkat tertentu dari model tersebut.

Ikon berwarna biru di samping deskripsi perangkat menunjukkan bahwa perangkat sedang terhubung ke komputer. Jika perangkatnya tidak terhubung ke komputer, ikonnya berwarna abu-abu.

6. Pilih kotak centang untuk perangkat USB yang ingin Anda tambahkan ke database, lalu klik **Tambahkan ke database**.
   Perangkat USB yang dipilih ditambahkan ke database.
7. Tutup atau simpan rencana proteksi.

Untuk menambahkan perangkat USB ke database dari panel Detail komputer

Catatan
Prosedur ini hanya berlaku untuk perangkat yang sedang online dan memiliki agen untuk Pencegahan Hilangnya Data yang terinstal padanya. Anda tidak dapat menampilkan daftar perangkat USB untuk komputer yang sedang offline atau tidak memiliki instalasi agen Pencegahan Hilangnya Data.

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih komputer yang pernah dihubungkan dengan perangkat USB yang diinginkan, lalu pada menu di sebelah kanan, klik **Inventaris**.
   Panel detail komputer terbuka.
3. Di panel detail komputer, klik tab **Perangkat USB**.
   Daftar perangkat USB yang dikenal di komputer yang dipilih kemudian terbuka.
   Perangkat USB dicantumkan dalam tampilan hierarki. Tingkat pertama hierarki mewakili model perangkat. Tingkat kedua mewakili perangkat tertentu dari model tersebut.
   Ikon berwarna biru di samping deskripsi perangkat menunjukkan bahwa perangkat sedang terhubung ke komputer. Jika perangkatnya tidak terhubung ke komputer, ikonnya berwarna abu-abu.
4. Pilih kotak centang untuk perangkat USB yang ingin Anda tambahkan ke database, kemudian klik **Tambahkan ke database**.

Untuk menambahkan perangkat USB ke database dari peringatan layanan

1. Di konsol Cyber Protect, buka **Pemantauan** > **Peringatan**.
2. Temukan peringatan kontrol perangkat yang memberi tahu akses yang ditolak ke perangkat USB.
3. Di tampilan sederhana peringatan, klik**Izinkan perangkat USB ini**.
   Fungsi ini mengecualikan perangkat USB dari kontrol akses dan menambahkannya ke database untuk rujukan lebih lanjut.

Untuk menambahkan perangkat USB dengan mengimpor daftar perangkat ke database

© Acronis International GmbH, 2003-2024

Anda dapat mengimpor file JSON yang berisi daftar perangkat USB ke database. Lihat "Impor daftar perangkat USB ke database" (hlm. 383).

Untuk menghapus perangkat USB dari database

1. Buka rencana proteksi salah satu perangkat untuk mengedit:
   Klik elipsis (...) di samping nama rencana proteksi dan pilih **Edit**.

   Catatan
   Kontrol perangkat harus diaktifkan dalam rencana sehingga Anda dapat mengakses pengaturan Kontrol perangkat.

2. Klik panah di samping tombol **Kontrol perangkat** untuk memperluas pengaturan, lalu klik baris **Daftar izin perangkat USB**.
3. Di halaman untuk mengelola daftar izin yang muncul, klik **Tambahkan dari database**.
4. Di halaman untuk memilih perangkat USB dari database, klik elipsis (...) di akhir daftar item yang mewakili perangkat, klik **Hapus**, lalu konfirmasi penghapusan.
   Perangkat USB dihapus dari database.
5. Tutup atau simpan rencana proteksi.

Lihat peringatan kontrol perangkat

Modul kontrol perangkat dapat dikonfigurasi untuk memberi peringatan yang memberi tahu upaya penolakan penggunaan tipe perangkat tertentu (lihat Aktifkan atau nonaktifkan notifikasi dan peringatan layanan OS). Gunakan langkah-langkah berikut untuk melihat peringatan.

Untuk melihat peringatan kontrol perangkat

1. Di konsol Cyber Protect, buka **Pemantauan** > **Peringatan**.
2. Cari peringatan dengan status berikut: "Akses perangkat periferal diblokir".

Lihat Peringatan kontrol perangkat untuk detail lebih lanjut.

Pengaturan akses

Di halaman **Pengaturan akses**, Anda dapat mengizinkan atau menolak akses ke tipe perangkat tertentu, sekaligus mengaktifkan atau menonaktifkan notifikasi OS dan peringatan kontrol perangkat.

Catatan
Pengaturan akses yang dikonfigurasi dalam Kontrol perangkat mungkin akan diganti saat menggunakan Kontrol perangkat dan Advanced DLP untuk melindungi beban kerja. Lihat "Mengaktifkan Advanced Data Loss Prevention di rencana proteksi" (hlm. 874).

Pengaturan akses memungkinkan Anda membatasi akses pengguna ke tipe dan port perangkat berikut:

© Acronis International GmbH, 2003-2024

- **Dapat dilepas** (kontrol akses berdasarkan tipe perangkat) - Perangkat dengan antarmuka untuk dihubungkan ke komputer (USB, FireWire, PCMCIA, IDE, SATA, SCSI, dll.) yang dikenali sistem operasi sebagai perangkat penyimpanan yang dapat dilepas (contohnya, stik USB, pembaca kartu, drive magneto-optik, dll.). Kontrol perangkat mengelompokkan semua hard drive yang terhubung via USB, FireWire, dan PCMCIA sebagai perangkat yang dapat dilepas. Ia juga mengelompokkan beberapa hard drive (biasanya SATA dan SCSI) sebagai perangkat yang dapat dilepas jika mendukung fungsi hot-plug dan tidak terinstal sistem operasi yang berjalan di dalamnya.

  Anda dapat mengizinkan akses penuh, akses hanya baca, atau menolak akses ke perangkat yang dapat dilepas untuk mengontrol operasi penyalinan data ke dan dari perangkat yang dapat dilepas pada komputer yang dilindungi. Hak akses tidak memengaruhi perangkat yang dienkripsi dengan BitLocker atau FileVault (hanya sistem file HFS+).

  Tipe perangkat ini didukung di Windows dan macOS.
- **Dienkripsi dan dapat dilepas** (kontrol akses menurut jenis perangkat) - Perangkat dapat dilepas yang dienkripsi dengan enkripsi drive BitLocker (pada Windows) atau FileVault (pada macOS).

  Pada macOS, hanya perangkat dapat dilepas dan dienkripsi yang menggunakan sistem file HFS+ (disebut juga dengan HFS Plus, Mac OS Extended, atau HFS Extended) yang didukung. Perangkat dapat dilepas dan dienkripsi yang menggunakan sistem file APFS diperlakukan sebagai perangkat yang dapat dilepas.

  Anda dapat mengizinkan akses penuh, akses hanya baca, atau menolak akses ke perangkat yang dapat dilepas dan dienkripsi untuk mengontrol operasi penyalinan data ke dan dari perangkat yang dapat dilepas dan dienkripsi apa pun di komputer yang dilindungi. Hak akses hanya memengaruhi perangkat yang dienkripsi dengan BitLocker atau FileVault (hanya sistem file HFS+).

  Tipe perangkat ini didukung di Windows dan macOS.
- **Printer** (kontrol akses berdasarkan tipe perangkat) - Printer fisik dengan antarmuka untuk dihubungkan komputer (USB, LPT, Bluetooth, dll.), serta printer yang diakses dari komputer jaringan.

  Anda dapat mengizinkan atau menolak akses ke printer untuk mengontrol pencetakan dokumen pada printer apa pun di komputer yang dilindungi.

  Catatan
  Ketika Anda mengubah pengaturan akses untuk printer menjadi **Tolak**, aplikasi dan proses yang mengakses printer harus dimulai ulang untuk menerapkan pengaturan akses yang baru dikonfigurasi. Untuk memastikan bahwa pengaturan akses diberlakukan dengan benar, mulai ulang beban kerja yang dilindungi.

  Tipe perangkat ini didukung hanya di Windows.
- **Papan klip** (kontrol akses berdasarkan tipe perangkat) - Papan klip Windows.

  Anda dapat mengizinkan atau menolak akses ke papan klip untuk mengontrol operasi salin dan tempel melalui papan klip Windows di komputer yang dilindungi.

© Acronis International GmbH, 2003-2024

Catatan
Saat Anda mengubah pengaturan akses untuk papan klip menjadi **Tolak**, aplikasi dan proses yang mengakses papan klip harus dimulai ulang untuk menerapkan pengaturan akses yang baru dikonfigurasi. Untuk memastikan bahwa pengaturan akses diberlakukan dengan benar, mulai ulang beban kerja yang dilindungi.

Tipe perangkat ini didukung hanya di Windows.

- **Tangkapan layar** (kontrol akses berdasarkan jenis perangkat) - Memungkinkan pengambilan tangkapan seluruh layar, jendela aktif, atau bagian layar yang dipilih.
  Anda dapat mengizinkan atau menolak akses ke tangkapan layar untuk mengontrol pengambilan tangkapan layar di komputer yang dilindungi.

Catatan
Saat Anda mengubah pengaturan akses untuk tangkapan layar menjadi **Tolak**, aplikasi dan proses yang mengakses tangkapan layar harus dimulai ulang untuk menerapkan pengaturan akses yang baru dikonfigurasi. Untuk memastikan bahwa pengaturan akses diberlakukan dengan benar, mulai ulang beban kerja yang dilindungi.

Tipe perangkat ini didukung hanya di Windows.

- **Perangkat seluler** (kontrol akses berdasarkan tipe perangkat) - Perangkat (misalnya ponsel pintar Android, dll.) yang berkomunikasi dengan komputer via Media Transfer Protocol (MTP), dengan antarmuka untuk dihubungkan ke komputer (USB, IP, Bluetooth).
  Anda dapat mengizinkan akses penuh, mengizinkan akses hanya baca, atau menolak akses ke perangkat seluler untuk mengontrol operasi penyalinan data ke dan dari perangkat seluler berbasis MTP apa pun di komputer yang dilindungi.

Catatan
Saat Anda mengubah pengaturan akses untuk perangkat seluler menjadi **Hanya baca** atau **Tolak**, aplikasi dan proses yang mengakses perangkat seluler harus dimulai ulang untuk menerapkan pengaturan akses yang baru dikonfigurasi. Untuk memastikan bahwa pengaturan akses diberlakukan dengan benar, mulai ulang beban kerja yang dilindungi.

Tipe perangkat ini didukung hanya di Windows.

- **Bluetooth** (kontrol akses berdasarkan tipe perangkat) - Perangkat Bluetooth eksternal dan internal dengan antarmuka untuk dihubungkan ke komputer (USB, PCMCIA, dll.). Pengaturan ini mengontrol penggunaan perangkat tipe ini, alih-alih pertukaran data memakai perangkat tersebut.
  Anda dapat mengizinkan atau menolak akses ke Bluetooth untuk mengontrol penggunaan perangkat Bluetooth apa pun di komputer yang dilindungi.

© Acronis International GmbH, 2003-2024

Catatan

Pada macOS, hak akses untuk Bluetooth tidak memengaruhi perangkat HID Bluetooth. Akses ke perangkat ini selalu diizinkan untuk mencegah dinonaktifkannya perangkat HID nirkabel (mouse dan keyboard) pada perangkat keras iMac dan Mac Pro.

Tipe perangkat ini didukung di Windows dan macOS.

- **Drive optik** (kontrol akses berdasarkan tipe perangkat) - Drive CD/DVD/BD eksternal dan internal (termasuk penulis) dengan antarmuka untuk dihubungkan komputer (IDE, SATA, USB, FireWire, PCMCIA, dll.).

  Anda dapat mengizinkan akses penuh, mengizinkan akses hanya baca, atau menolak akses ke drive optik untuk mengontrol operasi penyalinan data ke dan dari drive optik mana pun pada komputer yang dilindungi.

  Tipe perangkat ini didukung di Windows dan macOS.
- **Drive floppy** (kontrol akses berdasarkan tipe perangkat) - Drive floppy eksternal dan internal dengan antarmuka untuk dihubungkan komputer (IDE, USB, PCMCIA, dll.). Ada beberapa model drive floppy yang dikenali sistem operasi sebagai perangkat yang dapat dilepas, dalam hal ini kontrol perangkat juga mengenali drive tersebut sebagai perangkat yang dapat dilepas.

  Anda dapat mengizinkan akses penuh, mengizinkan akses hanya baca, atau menolak akses ke floppy drive untuk mengontrol operasi penyalinan data ke dan dari floppy drive pada komputer yang dilindungi.

  Tipe perangkat ini didukung hanya di Windows.
- **USB** (kontrol akses berdasarkan antarmuka perangkat) - Perangkat apa pun yang terhubung ke port USB, kecuali hub.

  Anda dapat mengizinkan akses penuh, mengizinkan akses hanya baca, atau menolak akses ke port USB untuk mengontrol operasi penyalinan data ke dan dari perangkat yang terhubung ke port USB apa pun pada komputer yang dilindungi.

  Tipe perangkat ini didukung di Windows dan macOS.
- **FireWire** (kontrol akses berdasarkan antarmuka perangkat) - Perangkat apa pun yang terhubung ke port FireWire (IEEE 1394), kecuali hub.

  Anda dapat mengizinkan akses penuh, mengizinkan akses hanya baca, atau menolak akses ke port FireWire untuk mengontrol operasi penyalinan data ke dan dari perangkat yang terhubung ke port FireWire mana pun pada komputer yang dilindungi.

  Tipe perangkat ini didukung di Windows dan macOS.
- **Perangkat yang dialihkan** (kontrol akses berdasarkan antarmuka perangkat) - Drive yang dipetakan (hard drive, dapat dilepas, dan optik), perangkat USB, dan papan klip yang dialihkan ke sesi aplikasi/desktop virtual.

  Kontrol perangkat mengenali perangkat yang dialihkan via Microsoft RDP, Citrix ICA, VMware PCoIP, dan HTML5/WebSockets menjauhkan protokol di lingkungan virtualisasi Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer, dan VMware Horizon yang di-host di komputer Windows terlindungi. Modul itu juga dapat mengontrol operasi salin data antara papan klip Windows pada sistem operasi tamu yang berjalan di VMware Workstation, VMware Player, Oracle

© Acronis International GmbH, 2003-2024

VM VirtualBox, atau Windows Virtual PC, dan papan klip sistem operasi host yang berjalan di komputer Windows terlindungi.

Tipe perangkat ini didukung hanya di Windows.

Anda dapat mengonfigurasi akses ke perangkat yang dialihkan sebagai berikut:

- **Drive yang dipetakan** - Mengizinkan akses penuh, mengizinkan akses hanya baca, atau menolak akses untuk mengontrol operasi penyalinan data ke dan dari hard drive, drive yang dapat dilepas, atau drive optik yang dialihkan ke sesi yang dihosting di komputer yang dilindungi.
- **Papan klip yang masuk** - Mengizinkan atau menolak akses untuk mengontrol operasi penyalinan data melalui papan klip ke sesi yang dihosting di komputer yang dilindungi.

  Catatan
  Saat Anda mengubah pengaturan akses untuk papan klip yang masuk menjadi **Tolak**, aplikasi dan proses yang mengakses papan klip harus dimulai ulang untuk menerapkan pengaturan akses yang baru dikonfigurasi. Untuk memastikan bahwa pengaturan akses diberlakukan dengan benar, mulai ulang beban kerja yang dilindungi.

- **Papan klip yang keluar** - Mengizinkan atau menolak akses untuk mengontrol operasi penyalinan data melalui papan klip dari sesi yang di-hosting di komputer yang dilindungi.

  Catatan
  Saat Anda mengubah pengaturan akses untuk papan klip yang keluar menjadi **Tolak**, aplikasi dan proses yang mengakses papan klip harus dimulai ulang untuk menerapkan pengaturan akses yang baru dikonfigurasi. Untuk memastikan bahwa pengaturan akses diberlakukan dengan benar, mulai ulang beban kerja yang dilindungi.

- **Port USB** - Mengizinkan atau menolak akses untuk mengontrol operasi penyalinan data ke dan dari perangkat yang terhubung ke port USB mana pun yang diarahkan ke sesi yang dihosting pada komputer yang dilindungi.

Pengaturan kontrol perangkat berpengaruh ke semua pengguna secara rata. Contohnya, jika Anda menolak akses ke perangkat yang dapat dilepas, Anda mencegah pengguna mana pun untuk menyalin data ke dan dari perangkat tersebut di komputer yang dilindungi. Anda dapat mengizinkan akses secara selektif ke masing-masing perangkat USB dengan mengecualikan mereka dari kontrol akses (lihat Daftar izin tipe perangkat dan Daftar izin perangkat USB).

Saat akses ke suatu perangkat dikontrol oleh tipe dan antarmukanya, diutamakan menolak akses di tingkat antarmuka. Contohnya, jika akses ke port USB ditolak (antarmuka perangkat), maka akses ke perangkat seluler yang terhubung ke port USB ditolak terlepas dari akses ke perangkat seluler diizinkan atau tidak (tipe perangkat). Untuk mengizinkan akses ke perangkat tersebut, Anda perlu mengizinkan baik antarmukanya maupun tipenya.

Catatan
Jika rencana proteksi yang digunakan di macOS memiliki pengaturan untuk tipe perangkat yang hanya didukung di Windows, maka pengaturan untuk tipe perangkat ini akan diabaikan di macOS.

© Acronis International GmbH, 2003-2024

Penting
Saat perangkat yang dapat dilepas, perangkat yang dapat dilepas dan dienkripsi, printer, atau perangkat Bluetooth dihubungkan ke port USB, mengizinkan akses ke perangkat tersebut menggantikan set penolakan akses pada tingkat antarmuka USB. Jika Anda mengizinkan tipe perangkat itu, akses ke perangkat itu diizinkan terlepas dari akses ke port USB ditolak atau tidak.

Notifikasi OS dan peringatan layanan

Anda dapat mengonfigurasi kontrol perangkat untuk menampilkan notifikasi OS kepada pengguna akhir jika mereka mencoba menggunakan tipe atau port perangkat terblokir pada komputer terproteksi. Saat kotak centang **Tampilkan notifikasi OS ke pengguna akhir jika mereka mencoba menggunakan tipe atau port perangkat terblokir** dipilih di pengaturan akses, agen memunculkan pesan di area notifikasi komputer terproteksi jika salah satu peristiwa ini terjadi:

- Percobaan menggunakan perangkat pada port USB atau FireWire yang ditolak. Notifikasi ini muncul ketika pengguna memasukkan perangkat USB atau FireWire yang ditolak di tingkat antarmuka (contohnya, saat menolak akses ke port USB) atau di tingkat tipe (contohnya, saat menolak penggunaan perangkat yang dapat dilepas). Notifikasi ini memberi tahu bahwa pengguna ini tidak diizinkan mengakses perangkat/drive tertentu.
- Percobaan menyalin objek data (seperti file) dari perangkat tertentu yang ditolak. Notifikasi ini muncul saat menolak akses baca ke perangkat berikut: floppy drive, drive optik, perangkat yang dapat dilepas, perangkat yang dapat dilepas yang dienkripsi, perangkat seluler, drive yang dipetakan dialihkan, dan data masuk papan klip yang dialihkan. Notifikasi ini memberi tahu bahwa pengguna ini tidak diizinkan mendapat objek data tertentu dari perangkat tertentu.
  Notifikasi baca yang ditolak juga ditampilkan ketika menolak akses baca/tulis ke Bluetooth, port FireWire, port USB, dan port USB yang dialihkan.
- Percobaan menyalin objek data (seperti file) ke perangkat tertentu yang ditolak. Notifikasi ini muncul saat menolak akses tulis ke perangkat berikut: floppy drive, drive optik, perangkat yang dapat dilepas, perangkat yang dapat dilepas dan dienkripsi, perangkat seluler, papan klip lokal, tangkapan layar, printer, drive yang dipetakan dan dialihkan, dan data keluar papan klip yang dialihkan. Notifikasi ini memberi tahu bahwa pengguna ini tidak diizinkan mengirim objek data tertentu ke perangkat tertentu.

Upaya pengguna untuk mengakses jenis perangkat yang diblokir pada komputer yang dilindungi dapat memunculkan peringatan yang masuk ke dalam konsol Cyber Protect. Anda dapat mengaktifkan peringatan untuk setiap jenis perangkat (tidak termasuk tangkapan layar) atau port secara terpisah dengan memilih kotak centang **Tampilkan peringatan** di pengaturan akses. Misalnya, jika akses ke perangkat yang dapat dilepas dibatasi menjadi hanya-baca, dan kotak centang **Tampilkan peringatan** dipilih untuk tipe perangkat tersebut, peringatan dicatat setiap kali pengguna di komputer terproteksi mencoba menyalin data ke perangkat yang dapat dilepas. Lihat Peringatan kontrol perangkat untuk detail lebih lanjut.

Lihat juga langkah untuk mengaktifkan atau menonaktifkan notifikasi OS dan peringatan layanan.

© Acronis International GmbH, 2003-2024

Daftar izin jenis perangkat

Di halaman **Daftar izin tipe perangkat**, Anda dapat memilih subklas perangkat yang dikecualikan dari kontrol akses perangkat. Hasilnya, akses ke perangkat tersebut diizinkan terlepas dari pengaturan akses di modul kontrol perangkat.

Modul kontrol perangkat menyediakan opsi untuk mengizinkan akses ke subklas perangkat tertentu dalam tipe perangkat yang ditolak. Opsi ini memungkinkan Anda untuk menolak semua perangkat di tipe tertentu, kecuali beberapa subklas perangkat tipe tersebut. Opsi ini dapat jadi bermanfaat, contohnya jika Anda perlu menolak akses ke semua port USB namun mengizinkan penggunaan keyboard dan mouse USB.

Saat mengonfigurasi modul kontrol perangkat, Anda dapat menentukan subklas perangkat yang dikecualikan dari kontrol akses perangkat. Saat suatu perangkat termasuk ke dalam subklas yang dikecualikan, akses ke perangkat itu diizinkan, terlepas tipe atau port perangkatnya ditolak atau tidak. Anda dapat mengecualikan subklas perangkat berikut dari kontrol akses perangkat secara selektif:

- **HID USB (mouse, keyboard, dll.)** - Saat dipilih, mengizinkan akses ke Perangkat Antarmuka Manusia (mouse, keyboard, dan lainnya) yang terhubung ke port USB, meskipun port tersebut ditolak. Secara default, item ini terpilih sehingga menolak akses ke port USB tidak akan menonaktifkan keyboard atau mouse.
  Didukung di Windows dan macOS.
- **Kartu jaringan USB dan FireWire** - Saat dipilih, mengizinkan akses ke kartu jaringan yang terhubung ke port USB atau FireWire (IEEE 1394) meski port USB/FireWire ditolak.
  Didukung di Windows dan macOS.
- **Pemindai dan perangkat citra diam USB** - Saat dipilih, mengizinkan akses ke pemindai dan perangkat citra diam yang terhubung ke port USB, meskipun port tersebut ditolak.
  Didukung hanya pada Windows.
- **Perangkat audio USB** - Saat dipilih, mengizinkan akses ke perangkat audio, seperti headset dan mikrofon, yang terhubung ke port USB meskipun port tersebut ditolak.
  Didukung hanya pada Windows.
- **Kamera USB** - Saat dipilih, mengizinkan akses ke kamera Web yang terhubung ke port USB meskipun port tersebut ditolak.
  Didukung hanya pada Windows.
- **HID Bluetooth (mouse, keyboard, dll.)** - Saat dipilih, mengizinkan akses ke Perangkat Antarmuka Manusia (mouse, keyboard, dan lainnya) yang terhubung via Bluetooth meskipun Bluetooth ditolak.
  Didukung hanya pada Windows.
- **Salin/tempel papan klip dalam aplikasi** - Saat dipilih, mengizinkan salin/tempel data melalui papan klip dalam aplikasi yang sama meskipun papan klip ditolak.
  Didukung hanya pada Windows.

© Acronis International GmbH, 2003-2024

Catatan
Pengaturan untuk subkelas perangkat yang tidak didukung akan diabaikan jika pengaturan ini dikonfigurasi dalam rencana proteksi yang diterapkan.

Saat membuat daftar izin tipe perangkat, pertimbangkan hal berikut:

- Dengan daftar izin tipe perangkat, Anda hanya dapat mengizinkan keseluruhan subklas perangkat. Anda tidak dapat mengizinkan model perangkat spesifik sambil menolak perangkat lain dalam subklas yang sama. Contohnya, dengan mengecualikan kamera USB dari kontrol akses perangkat, Anda mengizinkan penggunaan semua kamera USB, terlepas dari model atau merknya. Untuk cara mengizinkan masing-masing perangkat/model, lihat daftar izin perangkat USB.
- Tipe perangkat hanya dapat dipilih dari daftar subklas perangkat tertutup. Jika perangkat yang ingin diizinkan memiliki subklas berbeda, maka tidak dapat diizinkan dengan daftar izin tipe perangkat. Contohnya, subklas seperti pembaca kartu cerdas USB tidak dapat ditambahkan ke daftar izin. Untuk mengizinkan pembaca kartu cerdas USB saat port USB ditolak, ikuti instruksi di daftar izin perangkat USB.
- Daftar izin perangkat hanya bekerja untuk perangkat yang menggunakan driver Windows standar. Kontrol perangkat mungkin tidak mengenali subklas beberapa perangkat USB dengan driver perorangan. Oleh karena itu, Anda tidak dapat mengizinkan akses ke perangkat USB tersebut menggunakan daftar izin tipe perangkat. Dalam kasus ini, Anda dapat mengizinkan akses secara per-perangkat/model (lihat daftar izin perangkat USB).

Daftar izin perangkat USB

Daftar izin dapat mengizinkan penggunaan perangkat USB tertentu, terlepas dari pengaturan kontrol perangkat lainnya. Anda dapat menambahkan masing-masing perangkat atau model ke daftar izin untuk menonaktifkan kontrol akses ke perangkat tersebut. Contohnya, jika Anda menambahkan perangkat seluler dengan ID unik ke daftar izin, Anda mengizinkan penggunaan perangkat spesifik tersebut, meskipun perangkat USB lain ditolak.

Di halaman **Daftar izin perangkat USB**, Anda dapat memilih masing-masing perangkat atau model USB yang dikecualikan dari kontrol akses perangkat. Hasilnya, akses ke perangkat tersebut diizinkan, terlepas dari pengaturan akses di modul kontrol perangkat.

Ada dua cara untuk mengenali perangkat di daftar izin:

- Model perangkat - Secara kolektif mengenali semua perangkat model tertentu. Setiap model perangkat diidentifikasi dengan ID vendor (VID) dan ID produk (PID), misalnya USB\VID_0FCE&PID_E19E.

  Kombinasi VID dan PID ini bukanlah identitas satu perangkat spesifik, tetapi seluruh model perangkat. Dengan menambahkan model perangkat ke daftar izin, Anda mengizinkan akses ke perangkat apa pun dengan model tersebut. Contohnya, dengan ini Anda dapat mengizinkan printer USB bermodel tertentu.

© Acronis International GmbH, 2003-2024

- Perangkat unik - Mengenali perangkat tertentu. Setiap perangkat unik diidentifikasi dengan ID vendor (VID) dan ID produk (PID), serta nomor seri, misalnya USB\VID_0FCE&PID_E19E\D55E7FCA.
  Tidak semua perangkat USB memiliki nomor seri. Anda dapat menambahkan perangkat ke daftar izin sebagai perangkat unik hanya jika perangkat itu telah diberi nomor seri saat produksi. Contohnya, stik USB yang memiliki nomor seri unik.

Untuk menambahkan perangkat ke daftar izin, pertama Anda perlu menambahkannya ke database perangkat USB. Lalu, Anda dapat menambahkan perangkat ke daftar izin dengan memilih dari database tersebut.

Daftar izin dikelola di halaman konfigurasi terpisah, bernama **daftar izin perangkat USB**. Setiap item di daftar ini mewakili perangkat atau model dan memiliki bidang berikut:

- **Deskripsi** - Sistem operasi menetapkan deskripsi tertentu saat menghubungkan perangkat USB. Anda dapat mengubah deskripsinya di database perangkat USB (lihat halaman manajemen database USB).
- **Tipe perangkat** - Menampilkan Unik jika item merupakan perangkat unik, atau Model jika mewakili model perangkat.
- **Hanya baca** - Saat dipilih, hanya mengizinkan penerimaan data dari perangkat. Jika perangkatnya tidak mendukung akses hanya baca, maka akses ke perangkat tersebut diblokir. Kosongkan kotak centang ini untuk mengizinkan akses penuh ke perangkat.
- **Reinisialisasi** - Saat dipilih, menyebabkan perangkat menyimulasikan pemutusan/penyambungan kembali saat pengguna baru masuk. Beberapa perangkat USB memerlukan inisialisasi ulang agar dapat berfungsi, jadi kami menyarankan Anda mencentang kotak ini untuk perangkat tersebut (mouse, keyboard, dll.). Kami juga menyarankan Anda mengosongkan kotak centang ini untuk perangkat penyimpanan data (stik USB, drive optik, hard drive eksternal, dll.).
  Kontrol perangkat mungkin tidak dapat mereinisialisasi beberapa perangkat USB dengan driver perorangan. Jika tidak ada akses ke perangkat tersebut, Anda harus melepaskan perangkat USB dari port USB, lalu memasukkannya kembali.

Catatan
Bidang **Reinisialisasi** tersembunyi secara default. Untuk menampilkannya di tabel, klik ikon roda gigi di sudut kanan atas tabel, lalu pilih kotak centang **Reinisialisasi**.

Catatan
Bidang **Hanya-baca** dan **Reinisialisasi** tidak didukung di macOS. Jika bidang ini dikonfigurasi dalam rencana proteksi yang diterapkan, bidang ini akan diabaikan.

Anda dapat menambahkan atau menghapus perangkat/modul dari daftar izin seperti berikut:

- Klik **Tambahkan dari database** di atas daftar, lalu pilih perangkat yang diinginkan dari yang didaftarkan dengan database perangkat USB. Perangkat yang dipilih ditambahkan ke daftar, lalu Anda dapat mengonfigurasi pengaturannya dan mengonfirmasi perubahan.

© Acronis International GmbH, 2003-2024

- Klik **Izinkan perangkat USB ini** di peringatan yang memberi tahu bahwa akses ke perangkat USB ditolak (lihat Peringatan kontrol perangkat). Fungsi ini akan menambahkan perangkat ke daftar izin dan ke database perangkat USB.
- Klik ikon hapus di akhir item dalam daftar. Fungsi ini akan menghapus perangkat/model tersebut dari daftar izin.

Database perangkat USB

Modul kontrol perangkat menyimpan database perangkat USB yang dapat Anda ditambahkan ke daftar pengecualian (lihat daftar izin perangkat USB). Perangkat USB dapat didaftarkan ke database dengan salah satu cara ini:

- Tambahkan perangkat di halaman yang muncul saat menambahkan perangkat ke daftar pengecualian (lihat halaman manajemen database perangkat USB).
- Tambahkan perangkat dari tab Perangkat USB di panel Inventaris komputer di konsol Cyber Protect (lihat Daftar perangkat USB di komputer).
- Izinkan perangkat dari peringatan yang menolak akses ke perangkat USB (lihat Peringatan kontrol perangkat).

Lihat juga langkah-langkah menambahkan atau menghapus perangkat USB dari database.

Halaman manajemen database perangkat USB

Saat mengonfigurasi daftar izin perangkat USB, Anda memiliki opsi untuk menambahkan perangkat dari database. Jika Anda memilih opsi ini, halaman manajemen akan muncul dengan daftar perangkat. Di halaman ini, Anda dapat melihat daftar semua perangkat yang terdaftar dengan database tersebut, memilih perangkat untuk ditambahkan ke daftar izin, serta melakukan operasi berikut:

Mendaftarkan perangkat dengan database

1. Klik **Tambahkan ke database** di bagian atas halaman.
2. Pada dialog **Tambahkan perangkat USB** yang muncul, pilih mesin tempat perangkat USB terhubung.
   Hanya mesin yang sedang online yang ditampilkan dalam daftar komputer.
   Daftar perangkat USB ditampilkan hanya bagi mesin yang di dalamnya sudah terinstal agen untuk Pencegahan Kehilangan Data.
   Perangkat USB dicantumkan dalam tampilan hierarki. Tingkat pertama hierarki mewakili model perangkat. Tingkat kedua mewakili perangkat tertentu dari model tersebut.
   Ikon berwarna biru di samping deskripsi perangkat menunjukkan bahwa perangkat sedang terhubung ke komputer. Jika perangkatnya tidak terhubung ke komputer, ikonnya berwarna abu-abu.
3. Pilih kotak centang untuk perangkat USB yang ingin Anda daftarkan, lalu klik **Tambahkan ke database**.

Mengubah deskripsi perangkat

© Acronis International GmbH, 2003-2024

1. Di halaman **Database perangkat USB**, klik elipsis (...) di akhir item daftar yang mewakili perangkat, lalu klik **Edit**.
2. Ubah deskripsi di kotak dialog yang muncul.

Menghapus perangkat dari database

1. Klik elipsis (...) di akhir item daftar yang mewakili perangkat.
2. Klik **Hapus**, lalu konfirmasi penghapusan.

Untuk setiap perangkat, daftar di halaman itu menyediakan informasi berikut:

- **Deskripsi** - Pengidentifikasi perangkat yang dapat dibaca. Anda dapat mengubah deksripsi sesuai kebutuhan.
- **Tipe perangkat** - Menampilkan Unik jika item merupakan perangkat unik, atau Model jika mewakili model perangkat. Suatu perangkat unik harus memiliki nomor seri berikut ID vendor (VID) dan ID produk (PID), sementara model perangkat dikenali dari kombinasi VID dan PID.
- **ID vendor**, **ID produk**, **Nomor seri** - Nilai-nilai tersebut menyusun ID perangkat dalam bentuk USB\VID_<vendor ID>&PID_<product ID>\<serial number>.
- **Akun** - Menunjukkan penyewa yang memiliki perangkat ini. Inilah penyewa yang berisi akun pengguna yang digunakan untuk pendaftaran perangkat dengan database.

> **Catatan**
> Kolom ini tersembunyi secara default. Untuk menampilkannya di tabel, klik ikon roda gigi di pojok kanan atas tabel, lalu pilih **Akun**.

Kolom paling kiri dimaksudkan untuk memilih perangkat yang ditambahkan ke daftar izin: Pilih kotak centang untuk menambahkan setiap perangkat, lalu klik tombol **Tambahkan ke daftar izin**. Untuk memilih atau mengosongkan semua kotak centang, klik kotak centang di atas kolom.

Anda dapat mencari atau memfilter daftar perangkat:

- Klik **Cari** di atas halaman dan masukkan pencarian. Daftar akan menampilkan perangkat dengan deskripsi yang cocok dengan pencarian.
- Klik **Filter**, lalu konfigurasikan dan terapkan filter di kotak dialog yang muncul. Daftarnya terbatas pada perangkat dengan tipe, ID vendor, ID produk, dan akun yang Anda pilih saat mengonfigurasi filter. Untuk membatalkan filter dan mencantumkan semua perangkat, klik **Setel ulang ke default**.

Ekspor daftar perangkat USB di database

Anda dapat mengekspor daftar perangkat USB yang ditambahkan ke database.

1. Buka rencana proteksi salah satu perangkat untuk mengedit.
2. Klik ikon panah di samping tombol **Kontrol perangkat** untuk memperluas pengaturan, lalu klik baris **Daftar izin perangkat USB**.
3. Di halaman daftar izin perangkat USB, klik **Tambahkan dari database**.

© Acronis International GmbH, 2003-2024

4. Di halaman manajemen database perangkat USB yang muncul, klik **Ekspor**.
   Dialog Jelajahi standar terbuka.
5. Pilih lokasi untuk menyimpan file, masukkan nama file baru jika diperlukan, lalu klik **Simpan**.

Daftar perangkat USB diekspor ke file JSON.

Anda dapat mengedit file JSON yang dihasilkan untuk menambahkan atau menghapus perangkat, lalu melakukan perubahan massal pada deskripsi perangkat.

Impor daftar perangkat USB ke database

Alih-alih menambahkan perangkat USB dari konsol Cyber Protect, Anda dapat mengimpor daftar perangkat USB. Daftar berupa file dalam format JSON.

Catatan
Anda dapat mengimpor file JSON ke database yang tidak berisi perangkat yang dijelaskan dalam file tersebut. Untuk mengimpor file yang sudah diubah ke database asalnya, Anda harus mengosongkan database terlebih dahulu karena entri duplikat tidak dapat diimpor. Jika Anda mengekspor daftar perangkat USB, mengubahnya, lalu mencoba mengimpornya ke database yang sama tanpa mengosongkannya, proses impor akan gagal.

1. Buka rencana proteksi salah satu perangkat untuk mengedit.
2. Klik ikon panah di samping tombol **Kontrol perangkat** untuk memperluas pengaturan, lalu klik baris **Daftar izin perangkat USB**.
3. Di halaman daftar izin perangkat USB, klik **Tambahkan dari database**.
4. Di halaman manajemen database perangkat USB yang muncul, klik **Impor**.
   Dialog Impor perangkat USB dari file terbuka.
5. Gunakan fitur seret dan letakkan (atau temukan) file yang ingin Anda impor.

Konsol Cyber Protect memeriksa apakah daftar berisi entri duplikat yang sudah ada di database dan melewatkannya. Perangkat USB yang tidak ditemukan dalam database ditambahkan padanya.

Daftar perangkat USB di komputer

Panel Inventaris komputer di konsol Cyber Protect termasuk tab **Perangkat USB**. Jika komputer sedang online dan agen untuk Pencegahan Kehilangan Data diinstal ke komputer, tab **Perangkat USB** menampilkan daftar semua perangkat USB yang pernah dihubungkan ke komputer tersebut.

Perangkat USB dicantumkan dalam tampilan hierarki. Tingkat pertama hierarki mewakili model perangkat. Tingkat kedua mewakili perangkat tertentu dari model tersebut.

Untuk setiap perangkat, daftar di halaman itu menyediakan informasi berikut:

- **Deskripsi** - Sistem operasi menetapkan deskripsi saat menghubungkan perangkat USB. Deskripsi ini berguna sebagai pengidentifikasi perangkat yang dapat dibaca.

© Acronis International GmbH, 2003-2024

Ikon berwarna biru di samping deskripsi perangkat menunjukkan bahwa perangkat sedang terhubung ke komputer. Jika perangkatnya tidak terhubung ke komputer, ikonnya berwarna abu-abu.

- **ID perangkat** - Pengidentifikasi yang ditetapkan sistem operasi ke perangkat tersebut. Pengidentifikasi ini memiliki format berikut: USB\VID_<vendor ID>&PID_<product ID>\<serial number> dengan <serial number> yang opsional. Contoh: USB\VID_0FCE&PID_ADDE\D55E7FCA (perangkat bernomor seri); USB\VID_0FCE&PID_ADDE (perangkat tanpa nomor seri).

Untuk menambahkan perangkat ke database perangkat USB, pilih kotak centang perangkat yang diinginkan, lalu klik tombol **Tambahkan ke database**.

Mengecualikan proses dari kontrol akses

Akses ke papan klip Windows, tangkapan layar, printer, dan perangkat seluler dikontrol melalui pengait yang dimasukkan ke dalam proses. Jika proses tidak dikaitkan, akses ke perangkat ini tidak akan dikontrol.

Catatan
Mengecualikan proses dari kontrol akses tidak didukung dalam macOS. Jika daftar proses yang dikecualikan dikonfigurasikan dalam rencana proteksi yang diterapkan, daftar tersebut akan diabaikan.

Pada halaman **Pengecualian**, Anda dapat menentukan daftar proses yang tidak akan dikaitkan. Artinya, papan klip (lokal dan dialihkan), tangkapan layar, printer, dan kontrol akses perangkat seluler tidak akan diterapkan ke proses tersebut.

Misalnya, Anda menerapkan rencana proteksi yang menolak akses ke printer, lalu memulai aplikasi Microsoft Word. Upaya untuk mencetak dari aplikasi ini akan diblokir. Namun, jika Anda menambahkan proses Microsoft Word ke daftar pengecualian, aplikasi tersebut tidak akan dikaitkan. Akibatnya, pencetakan dari Microsoft Word tidak akan diblokir, sedangkan pencetakan dari aplikasi lain tetap akan diblokir.

Untuk menambahkan proses ke pengecualian

1. Buka rencana proteksi salah satu perangkat untuk mengedit:
   Klik elipsis (...) di samping nama rencana proteksi dan pilih **Edit**.

   Catatan
   Kontrol perangkat harus diaktifkan dalam rencana sehingga Anda dapat mengakses pengaturan Kontrol perangkat.

2. Klik panah di samping tombol **Kontrol perangkat** untuk memperluas pengaturan, lalu klik baris **Pengecualian**.
3. Di halaman **Pengecualian**, di baris **Proses dan folder**, klik **+Tambahkan**.
4. Tambahkan proses yang ingin Anda kecualikan dari kontrol akses.
   Misalnya, `C:\Folder\subfolder\process.exe`.

© Acronis International GmbH, 2003-2024

Anda dapat menggunakan wildcard:

- * menggantikan berapa pun jumlah karakter.
- ? menggantikan satu karakter.

Misalnya:

```
C:\Folder\*
*\Folder\SubFolder?\*
*\process.exe
```

5. Klik tanda centang, lalu klik **Selesai**.
6. Dalam rencana proteksi, klik **Simpan**.
7. Mulai ulang proses yang Anda kecualikan untuk memastikan bahwa pengait telah dilepas dengan benar.

Proses yang dikecualikan akan memiliki akses ke papan klip, tangkapan layar, printer, dan perangkat seluler terlepas dari pengaturan akses untuk perangkat tersebut.

Untuk menghapus proses dari pengecualian

Buka rencana proteksi salah satu perangkat untuk mengedit:

Klik elipsis (...) di samping nama rencana proteksi dan pilih **Edit**.

Catatan
Kontrol perangkat harus diaktifkan dalam rencana sehingga Anda dapat mengakses pengaturan Kontrol perangkat.

1. Klik panah di samping tombol **Kontrol perangkat** untuk memperluas pengaturan, lalu klik baris **Pengecualian**.
2. Di halaman **Pengecualian**, klik ikon tempat sampah di samping proses yang ingin Anda hapus dari pengecualian.
3. Klik **Selesai**.
4. Dalam rencana proteksi, klik **Simpan**.
5. Mulai ulang proses untuk memastikan bahwa pengait telah dimasukkan dengan benar.

Pengaturan akses dari rencana proteksi akan diterapkan ke proses yang Anda hapus dari pengecualian.

Untuk mengedit proses dalam pengecualian

1. Buka rencana proteksi salah satu perangkat untuk mengedit:
   Klik elipsis (...) di samping nama rencana proteksi dan pilih **Edit**.

Catatan
Kontrol perangkat harus diaktifkan dalam rencana sehingga Anda dapat mengakses pengaturan Kontrol perangkat.

© Acronis International GmbH, 2003-2024

2. Klik panah di samping tombol **Kontrol perangkat** untuk memperluas pengaturan, lalu klik baris **Pengecualian**.
3. Di halaman **Pengecualian**, klik ikon **Edit** di samping proses yang ingin Anda edit.
4. Terapkan perubahan dan klik tanda centang untuk mengonfirmasi.
5. Klik **Selesai**.
6. Dalam rencana proteksi, klik **Simpan**.
7. Mulai ulang proses yang terpengaruh untuk memastikan perubahan Anda diterapkan dengan benar.

Peringatan kontrol perangkat

Kontrol perangkat memelihara log peristiwa dengan melacak percobaan pengguna yang mengakses tipe perangkat, port, atau antarmuka terkontrol. Peristiwa tertentu dapat memunculkan peringatan yang dicatat di konsol Cyber Protect. Contohnya, modul kontrol perangkat dapat dikonfigurasi untuk mencegah penggunaan perangkat yang dapat dilepas, dengan peringatan yang dilog setiap kali pengguna mencoba menyalin data ke atau dari perangkat tersebut.

Saat mengonfigurasi modul kontrol perangkat, Anda dapat mengaktifkan peringatan untuk sebagian besar item yang terdaftar pada Port atau Jenis (kecuali tangkapan layar) perangkat. Jika peringatan diaktifkan, setiap upaya oleh pengguna untuk melakukan operasi yang tidak diizinkan menghasilkan peringatan. Misalnya, jika akses ke perangkat yang dapat dilepas dibatasi menjadi hanya baca, dan opsi **Tampilkan peringatan** dipilih untuk tipe perangkat tersebut, peringatan dibuat setiap kali pengguna di komputer terproteksi mencoba menyalin data ke perangkat yang dapat dilepas.

Untuk melihat peringatan di konsol Cyber Protect, buka **Pemantauan** > **Peringatan**. Dalam setiap peringatan kontrol perangkat, konsol menyediakan informasi peristiwa berikut:

- **Tipe**—Peringatan.
- **Status**—Menampilkan "Akses perangkat periferal diblokir".
- **Pesan**—Menampilkan "Akses ke '<tipe perangkat atau port>' pada '<nama komputer>' diblokir". Contohnya, "Akses ke 'Dapat dilepas' pada 'pc-akuntan' diblokir".
- **Tanggal dan waktu**—Tanggal dan waktu kejadian peristiwa.
- **Perangkat**—Nama komputer tempat kejadian peristiwa.
- **Nama rencana**—Nama rencana proteksi yang menyebabkan peristiwa tersebut.
- **Sumber**—Tipe perangkat atau port yang terlibat dalam peristiwa tersebut. Contohnya, saat pengguna yang ditolak mencoba mengakses perangkat yang dapat dilepas, bidang ini berisi Perangkat yang dapat dilepas.
- **Tindakan**—Operasi yang memicu peristiwa tersebut. Contohnya, saat pengguna yang ditolak mencoba menyalin data ke perangkat, bidang ini berisi Tulis. Untuk informasi lebih lanjut, lihat Nilai bidang tindakan.

© Acronis International GmbH, 2003-2024

- **Nama**—Nama objek target peristiwa, misalnya file yang dicoba disalin pengguna atau perangkat yang dicoba digunakan pengguna. Tidak ditampilkan jika objek target tidak dapat diidentifikasi.
- **Informasi**—Informasi tambahan tentang perangkat target peristiwa, seperti ID perangkat untuk perangkat USB. Tidak ditampilkan jika informasi tambahan tentang perangkat target tidak tersedia.
- **Pengguna**—Nama pengguna yang memicu peristiwa.
- **Proses**—Jalur terbatas lengkap menuju file yang dapat dieksekusi milik aplikasi yang memicu peristiwa. Di beberapa kasus, nama proses mungkin ditampilkan alih-alih jalurnya. Tidak ditampilkan jika informasi proses tidak tersedia.

Jika peringatan diterapkan ke perangkat USB (termasuk perangkat yang dapat dilepas dan perangkat yang dapat dilepas dan dienkripsi), maka, langsung dari peringatan tersebut, administrator dapat menambahkan perangkat ke daftar yang diizinkan, yang mencegah modul kontrol perangkat membatasi akses ke perangkat tersebut. Mengeklik **Izinkan perangkat USB ini** menambahkannya ke daftar izin perangkat USB di konfigurasi modul kontrol perangkat, serta menambahkannya ke database perangkat USB untuk rujukan lebih lanjut.

Lihat juga langkah-langkah melihat peringatan kontrol perangkat.

Nilai bidang tindakan

Bidang peringatan **Tindakan** dapat berisi nilai berikut:

- **Baca** - Mengambil data dari perangkat atau port.
- **Tulis** - Mengirimkan data ke perangkat atau port.
- **Format** - Akses langsung (pemformatan, pemeriksaan disk, dll.) ke perangkat. Dalam hal port, berlaku untuk perangkat yang terhubung ke port tersebut.
- **Keluarkan** - Mengeluarkan perangkat dari sistem atau mengeluarkan media dari perangkat. Dalam hal port, berlaku untuk perangkat yang terhubung ke port tersebut.
- **Cetak** - Mengirim dokumen ke printer.
- **Salin audio** - Menyalin/menempel data audio via papan klip lokal.
- **Salin file** - Menyalin/menempel file via papan klip lokal.
- **Salin citra** - Menyalin/menempel citra via papan klip lokal.
- **Salin teks** - Menyalin/menempel teks via papan klip lokal.
- **Salin konten tak teridentifikasi** - Menyalin/menempel data lain via papan klip lokal.
- **Salin data RTF (citra)** - Menyalin/menempel citra via papan klip lokal menggunakan Rich Text Format.
- **Salin data RTF (file)** - Menyalin/menempel file via papan klip lokal menggunakan Rich Text Format.
- **Salin data RTF (teks, citra)** - Menyalin/menempel teks bersama citra via papan klip lokal menggunakan Rich Text Format.

© Acronis International GmbH, 2003-2024

- **Salin data RTF (teks, file)** - Menyalin/menempel teks bersama file via papan klip lokal menggunakan Rich Text Format.
- **Salin data RTF (citra, file)** - Menyalin/menempel citra bersama file via papan klip lokal menggunakan Rich Text Format.
- **Salin data RTF (teks, citra, file)** - Menyalin/menempel teks bersama citra dan file via papan klip lokal menggunakan Rich Text Format.
- **Hapus** - Menghapus data dari perangkat (contohnya, perangkat yang dapat dilepas, perangkat seluler, dan lainnya).
- **Akses perangkat** - Akses ke beberapa perangkat atau port (contohnya, perangkat Bluetooth, port USB, dan lainnya).
- **Audio masuk** - Menyalin/menempel data audio dari komputer klien ke sesi yang di-host via papan klip yang dialihkan.
- **File masuk** - Menyalin/menempel file dari komputer klien ke sesi yang di-host via papan klip yang dialihkan.
- **Citra masuk** - Menyalin/menempel citra dari komputer klien ke sesi yang di-host via papan klip yang dialihkan.
- **Teks masuk** - Menyalin/menempel teks dari komputer klien ke sesi yang di-host via papan klip yang dialihkan.
- **Konten tak teridentifikasi masuk** - Menyalin/menempel data lain dari komputer klien ke sesi yang di-host via papan klip yang dialihkan.
- **Data RTF (citra) masuk** - Menyalin/menempel citra dari komputer klien ke sesi yang di-host via papan klip yang dialihkan menggunakan Rich Text Format.
- **Data RTF (file) masuk** - Menyalin/menempel file dari komputer klien ke sesi yang di-host via papan klip yang dialihkan menggunakan Rich Text Format.
- **Data RTF (teks, citra) masuk** - Menyalin/menempel teks bersama citra dari komputer klien ke sesi yang di-host via papan klip yang dialihkan menggunakan Rich Text Format.
- **Data RTF (teks, file) masuk** - Menyalin/menempel teks bersama file dari komputer klien ke sesi yang di-host via papan klip yang dialihkan menggunakan Rich Text Format.
- **Data RTF (citra, file) masuk** - Menyalin/menempel citra bersama file dari komputer klien ke sesi yang di-host via papan klip yang dialihkan menggunakan Rich Text Format.
- **Data RTF (teks, citra, file) masuk** - Menyalin/menempel teks bersama citra dan file dari komputer klien ke sesi yang di-host via papan klip yang dialihkan menggunakan Rich Text Format.
- **Masukkan** - Hubungkan perangkat USB atau perangkat FireWire.
- **Audio keluar** - Menyalin/menempel data audio dari sesi yang di-host ke komputer klien via papan klip yang dialihkan.
- **File keluar** - Menyalin/menempel file dari sesi yang di-host ke komputer klien via papan klip yang dialihkan.
- **Citra keluar** - Menyalin/menempel citra dari sesi yang di-host ke komputer klien via papan klip yang dialihkan.
- **Teks keluar** - Menyalin/menempel teks dari sesi yang di-host ke komputer klien via papan klip yang dialihkan.

© Acronis International GmbH, 2003-2024

- **Konten tak teridentifikasi keluar** - Menyalin/menempel data lain dari sesi yang di-host ke komputer klien via papan klip yang dialihkan.
- **Data RTF (citra) keluar** - Menyalin/menempel citra dari sesi yang di-host ke komputer klien via papan klip yang dialihkan menggunakan Rich Text Format.
- **Data RTF (file) keluar** - Menyalin/menempel file dari sesi yang di-host ke komputer klien via papan klip yang dialihkan menggunakan Rich Text Format.
- **Data RTF (teks, citra) keluar** - Menyalin/menempel teks bersama citra dari sesi yang di-host ke komputer klien via papan klip yang dialihkan menggunakan Rich Text Format.
- **Data RTF (teks, file) keluar** - Menyalin/menempel teks bersama file dari sesi yang di-host ke komputer klien via papan klip yang dialihkan menggunakan Rich Text Format.
- **Data RTF (citra, file) keluar** - Menyalin/menempel citra bersama file dari sesi yang di-host ke komputer klien via papan klip yang dialihkan menggunakan Rich Text Format.
- **Data RTF (teks, citra, file) keluar** - Menyalin/menempel teks bersama citra dan file dari sesi yang di-host ke komputer klien via papan klip yang dialihkan menggunakan Rich Text Format.
- **Ubah nama** - Mengubah nama file pada perangkat (contohnya, di perangkat yang dapat dilepas, perangkat seluler, dan lainnya).

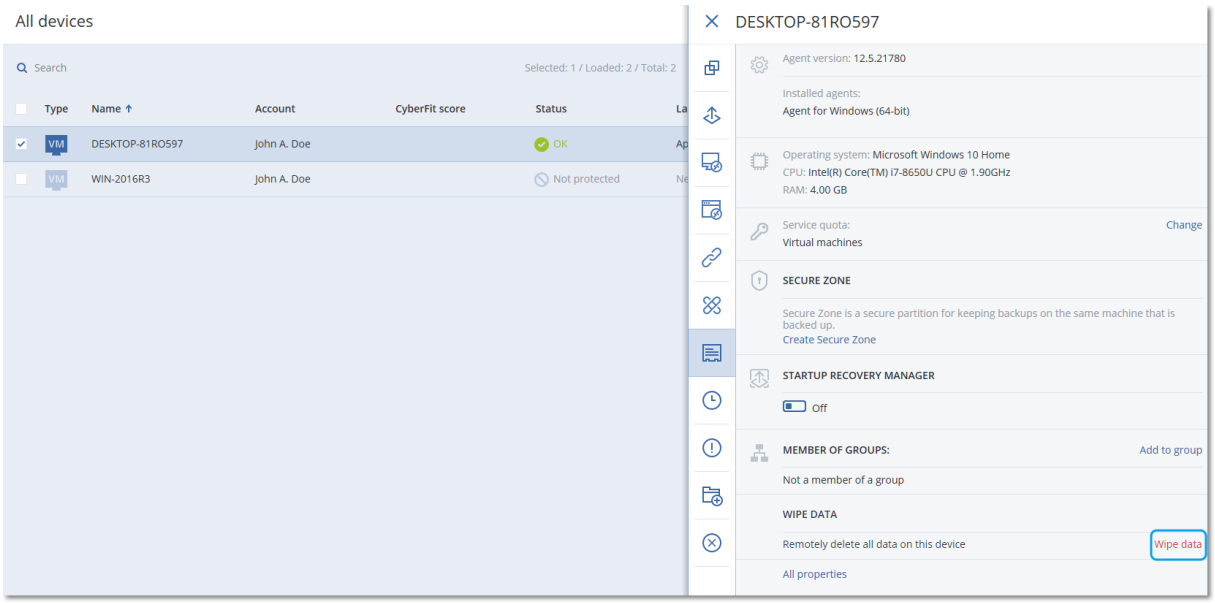
Penghapusan aman data dari beban kerja yang terkelola

Catatan
Penghapusan jarak jauh tersedia dengan paket Keamanan Tingkat Lanjut.

Penghapusan jarak jauh memungkinkan administrator layanan Cyber Protection dan pemilik mesin untuk menghapus data pada mesin yang dikelola – contohnya, jika mesin hilang atau dicuri. Sehingga akses yang tidak sah terhadap informasi sensitif akan dapat dicegah.

Penghapusan jarak jauh hanya tersedia untuk mesin yang menjalankan Windows versi 10 dan yang lebih baru. Untuk menerima perintah penghapusan, mesin harus menyala dan terhubung ke Internet.

© Acronis International GmbH, 2003-2024



Untuk menghapus data dari mesin

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih mesin yang datanya ingin Anda hapus.

   Catatan
   Anda dapat menghapus data dari satu mesin pada satu waktu.

3. Klik **Detail**, lalu klik **Hapus data**.
   Jika mesin yang Anda pilih sedang offline, opsi **Hapus data** dengan aman tidak dapat diakses.
4. Konfirmasi pilihan Anda.
5. Masukkan kredensial administrator lokal mesin, lalu klik **Hapus data**.

   Catatan
   Anda dapat memeriksa detail mengenai proses penghapusan aman dan siapa yang memulainya di **Pemantauan** > **Aktivitas**.

Beban kerja CyberApp

Beban kerja CyberApp dibuat oleh ISV (Independent software vendors/Vendor perangkat lunak independen) dan muncul di konsol Cyber Protect setelah Anda mengaktifkan integrasi CyberApp. Syarat berikut harus terpenuhi:

- Titik ekstensi **beban kerja dan tindakan** harus diaktifkan di CyberApp.
- Tentukan minimal satu **Jenis beban kerja** di CyberApp.
- Layanan penghubung yang di-host oleh ISV harus memastikan bahwa beban kerja CyberApp telah ditambahkan dan diperbarui ke platform Acronis.

© Acronis International GmbH, 2003-2024

Untuk informasi lebih lanjut mengenai Portal Vendor dan membuat CyberApp, lihat Panduan Pengguna Portal Vendor.

Beban kerja terakumulasi

Beban kerja fisik mungkin memiliki Cyber Protect agen dan satu atau beberapa agen CyberApp yang terinstal dalam waktu bersamaan. Pada kasus ini, beban kerja yang sama akan memiliki lebih dari satu perwakilan di layar **Semua Perangkat**—catatan terpisah akan ditampilkan untuk beban kerja Acronis, dan untuk masing-masing beban kerja CyberApp. Jika penggabungan otomatis terhadap beban kerja diaktifkan dan dikonfigurasikan dari Portal Vendor atau dari konsol Acronis, sistem akan membandingkan alamat host dan alamat MAC dari beban kerja Cyber Protect dan beban kerja CyberApp, dan akan menggabungkan semua perwakilan ke dalam satu beban kerja terakumulasi. Anda juga dapat menggabungkan dan memisahkan beban kerja secara manual di konsol Cyber Protect.

Bekerja dengan beban kerja CyberApp

Terlepas dari tindakan standar yang sudah diatur ke dalam konsol Cyber Protect, Anda dapat melakukakan tindakan yang tersedia setelah beban kerja CyberApp muncul dalam konsol: gabungkan beban kerja secara manual ke dalam beban kerja yang terkumpul dan lakukan tindakan kustom yang dikonfigurasikan dalam CyberApps.

Gabungkan

Prasyarat

- Tersedia beban kerja dari sumber yang berbeda untuk tenant.

Anda dapat menggabungkan beban kerja Acronis dengan satu atau beberapa beban kerja CyberApp ke dalam satu beban kerja yang terkumpul.

Untuk menggabungkan beban kerja secara manual ke dalam beban kerja yang terkumpul

1. Dalam layar **Semua perangkat**, pilih beban kerja yang ingin Anda gabungkan.

   Catatan
   Tindakan penggabungan ditampilkan jika Anda memilih beban kerja dari sumber yang berbeda, seperti beban kerja Acronis dan beban kerja CyberApp.

2. Klik **Gabungkan beban kerja**.

Lakukan tindakan kustom

Prasyarat

- Tersedia integrasi CyberApp yang memiliki **Tindakan beban kerja** terderfinisi untuk tenant.

Tindakan kustom adalah tindakan yang dikonfigurasi dalam CyberApps, dan tersedia untuk beban kerja CyberApp terkait saat Anda mengaktifkan integrasi CyberApp untuk tenant.

© Acronis International GmbH, 2003-2024

Untuk melakukan tindakan kustom

1. Dalam layar **Semua perangkat**, klik beban kerja.
2. Klik **Tindakan Aplikasi Terintegrasi**.
3. Klik tindakan.

Bekerja dengan beban kerja yang terkumpul

Terlepas dari tindakan standar yang sudah diatur ke dalam konsol Cyber Protect, Anda dapat melakukakn operasi berikut dengan beban kerja yang terkumpul: lihat rincian, pisahkan beban kerja sumber, dan lakukan tindakan yang dikonfigurasikan dalam CyberApps.

Lihat detail

Prasyarat

- Setidaknya satu beban kerja tersedia untuk penyewa.

Untuk melihat detail beban kerja yang terkumpul

1. Dalam layar **Semua perangkat**, klik beban kerja yang terkumpul.
2. Klik **Detail**.
   Rincian dalam beban kerja yang terkumpul terpisah menjadi tab. Tiap tab menunjukkan rincian dari setiap penggambaran tiap beban kerja.

Batalkan penggabungan

Prasyarat

- Setidaknya satu beban kerja tersedia untuk penyewa.

Saat Anda memisahkan beban kerja yang dikumpulkan, maka beban tersebut tidak akan ditampilkan dalam daftar perangkat. Alih-alih, Anda akan melihat entri terpisah untuk setiap beban kerja sumber yang telah digabung menjadi beban kerja agregat.

Untuk memisahkan beban kerja yang terkumpul

1. Dalam layar **Semua perangkat**, klik beban kerja yang terkumpul yang ingin Anda pisah.
2. Klik **Batalkan penggabungan beban kerja**.
3. Di jendela konfirmasi, klik **Batalkan penggabungan**.

Lakukan tindakan kustom

Prasyarat

- Setidaknya satu integrasi CyberApp dengan **Tindakan beban kerja** terdefinisi tersedia untuk tenant.

© Acronis International GmbH, 2003-2024

Tindakan kustom adalah tindakan yang dikonfigurasi dalam CyberApps dan tersedia untuk beban kerja CyberApp terkait saat Anda mengaktifkan integrasi CyberApp untuk tenant.

Untuk melakukan tindakan kustom

1. Dalam layar **Semua perangkat**, klik beban kerja.
2. Klik **Tindakan Aplikasi Terintegrasi**.
3. Tergantung tindakan kustom yang ada, lakukan salah satu tindakan berikut.
   - Jika beban kerja yang terkumpul memiliki satu beban kerja CyberApp, klik tindakannya.
   - Jika beban kerja yang terkumpul memilik beban kerja CyberApp lebih dari satu, klik nama CyberApp, lalu klik tindakannya.

Temukan pengguna yang terakhir masuk

Agar administrator dapat mengelola perangkat, mereka harus mengidentifikasi pengguna mana yang sedang dan telah masuk ke perangkat. Informasi ini ditampilkan di Dasbor atau di detail beban kerja.

Anda dapat mengaktifkan atau menonaktifkan tampilan informasi login terakhir di Rencana manajemen jarak jauh.

Di Dasbor:

1. Klik **Perangkat**. Jendela **Semua perangkat** ditampilkan.
2. Pada kolom **Masuk terakhir**, nama pengguna yang masuk terakhir kali untuk setiap perangkat ditampilkan.
3. Pada kolom **Waktu masuk terakhir**, nama pengguna yang masuk terakhir kali untuk setiap perangkat ditampilkan.

Pada Rincian Perangkat:

1. Klik **Perangkat**. Jendela **Semua perangkat** ditampilkan.
2. Klik pada perangkat yang ingin Anda verifikasi detailnya.
3. Klik ikon **Rincian**. Nama pengguna, tanggal dan waktu masuk terakhir untuk perangkat yang dipilih ditampilkan di bagian **Pengguna terakhir masuk**.

Catatan
Pada bagian **Pengguna terakhir yang masuk** akan ditampilkan hingga 5 pengguna berbeda yang masuk ke perangkat.

Untuk menampilkan atau menyembunyikan kolom Masuk terakhir dan Waktu masuk terakhir di Dasbor

© Acronis International GmbH, 2003-2024

1. Klik **Perangkat**. Jendela **Semua perangkat** ditampilkan.
2. Klik ikon roda gigi di sudut kanan atas, dan lakukan salah satu hal berikut ini di bagian **Umum**:
   - Aktifkan kolom **Masuk terakhir** dan **Waktu masuk terakhir**, jika Anda ingin menampilkannya di Dasbor.
   - Nonaktifkan kolom **Masuk terakhir** dan **Waktu masuk terakhir**, jika Anda ingin menyembunyikannya dari Dasbor.

© Acronis International GmbH, 2003-2024

Mengelola pencadangan serta pemulihan beban kerja dan file

Modul pencadangan mengaktifkan pencadangan dan pemulihan mesin fisik dan virtual, file, serta database ke penyimpanan lokal atau awan.

Cadangan

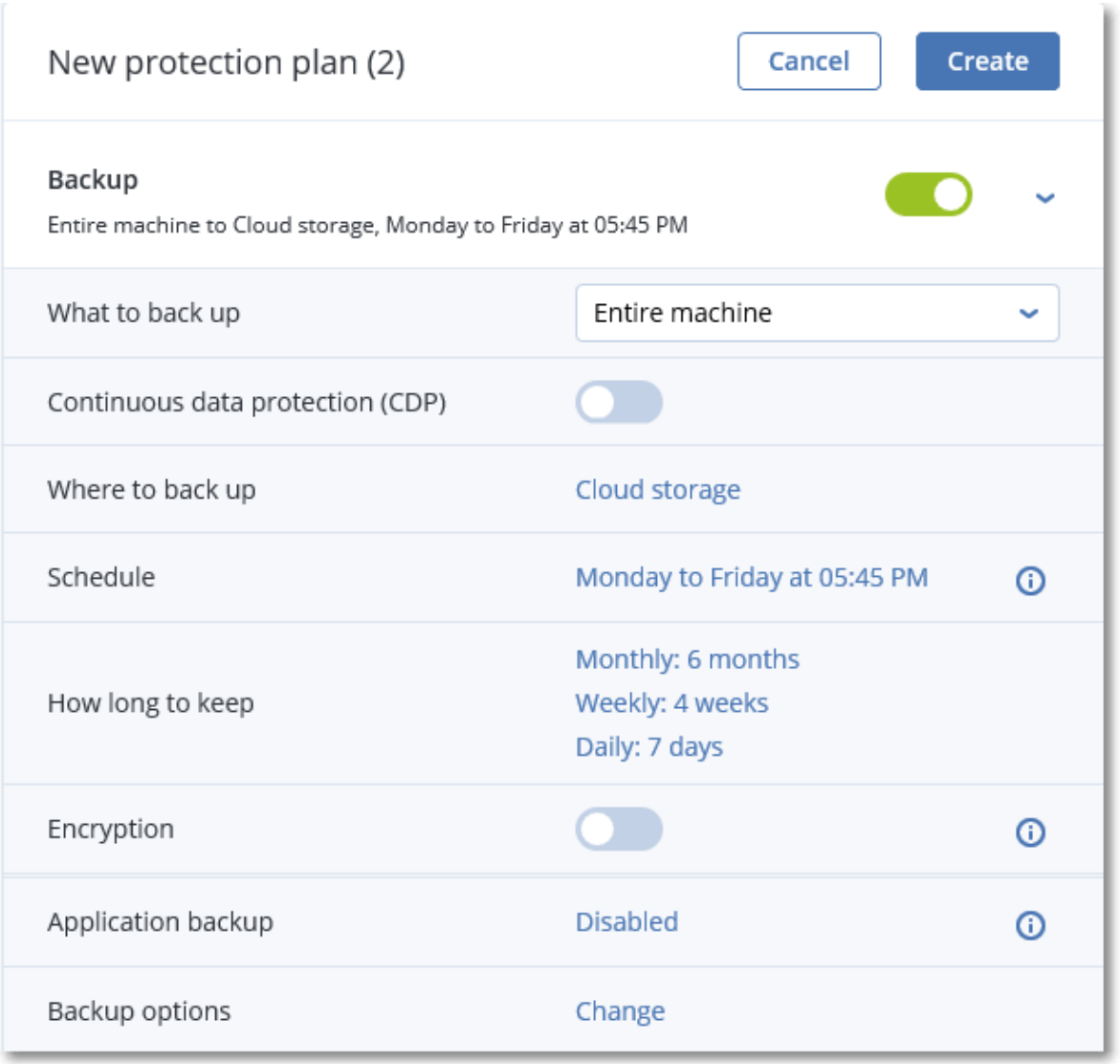
Rencana proteksi dengan Modul pencadangan yang diaktifkan adalah sekumpulan aturan yang menetapkan bagaimana data yang diberikan akan dilindungi pada mesin tertentu.

Rencana proteksi dapat diterapkan pada beberapa mesin pada saat pembuatannya, atau di lain waktu.

Untuk membuat rencana proteksi pertama dengan modul Pencadangan yang diaktifkan

1. Pilih mesin yang ingin Anda cadangkan.
2. Klik **Lindungi**.
   Rencana proteksi yang diterapkan pada mesin ditampilkan. Jika mesin tidak memiliki rencana yang sudah ditetapkan padanya, Anda akan melihat rencana proteksi default yang dapat diterapkan. Anda dapat menyesuaikan pengaturan bila diperlukan dan menerapkan rencana ini atau membuat rencana baru.
3. Untuk membuat rencana baru, klik **Buat rencana**. Aktifkan modul **Cadangan** dan buka Pengaturan.

© Acronis International GmbH, 2003-2024

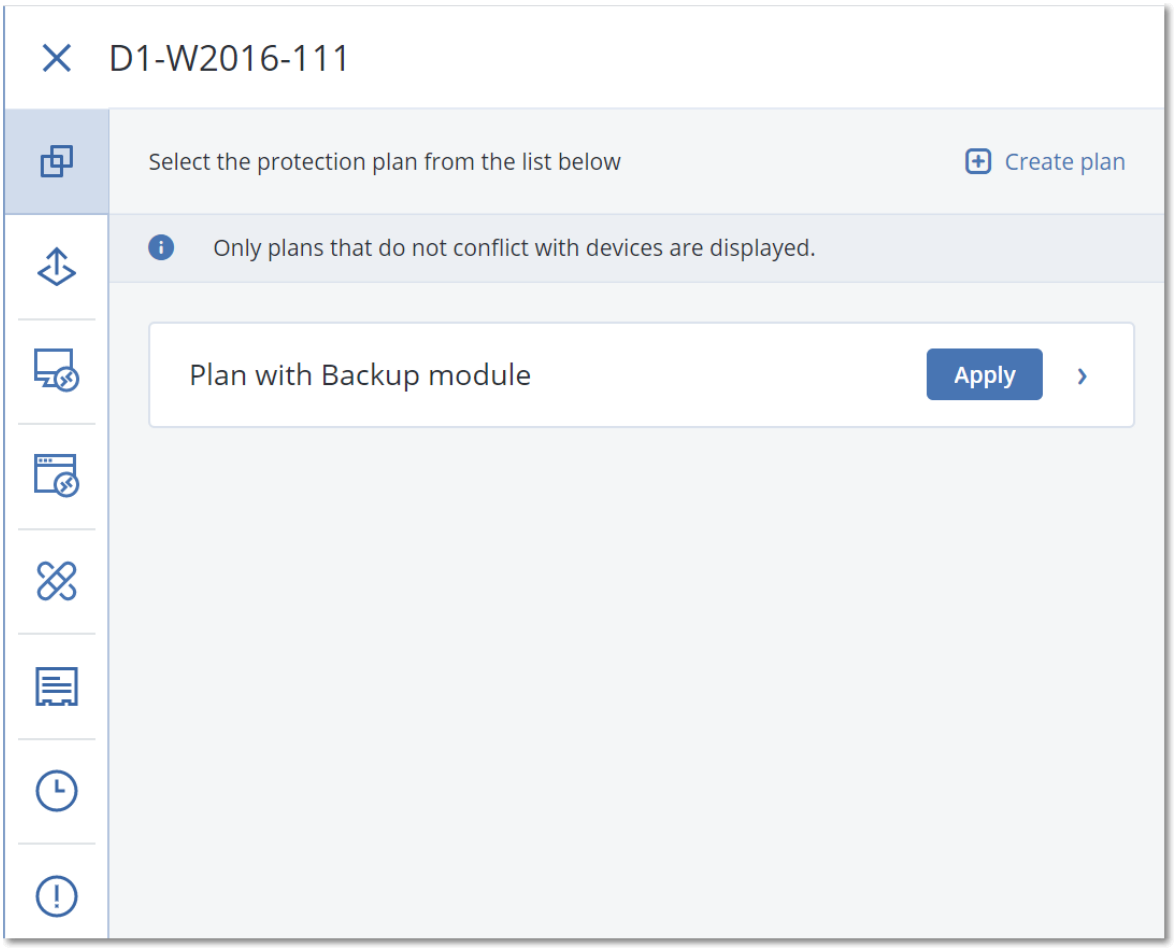


4. [Opsional] Untuk mengubah nama rencana proteksi, klik nama default.
5. [Opsional] Untuk memodifikasi parameter Pencadangan, klik pengaturan yang sesuai pada panel rencana proteksi.
6. [Opsional] Untuk memodifikasi opsi pencadangan, klik **Ubah** di samping **Opsi pencadangan**.
7. Klik **Buat**.

Untuk menerapkan rencana proteksi yang sudah ada

1. Pilih mesin yang ingin Anda cadangkan.
2. Klik **Lindungi**. Jika rencana proteksi umum sudah diterapkan pada mesin yang dipilih, klik **Tambah rencana**.
   Perangkat lunak menampilkan rencana proteksi yang telah dibuat sebelumnya.

© Acronis International GmbH, 2003-2024



3. Pilih rencana proteksi untuk diterapkan.
4. Klik **Terapkan**.

Referensi cepat rencana proteksi

Tabel berikut merangkum parameter rencana proteksi yang tersedia. Gunakan tabel untuk membuat rencana proteksi yang paling sesuai dengan kebutuhan Anda.

APA YANG AKAN DICADANGKAN	ITEM UNTUK DICADANGKAN Metode seleksi	TEMPAT MENYIMPAN CADANGAN	JADWAL Skema cadangan	BERAPA LAMA AKAN DISIMPAN
Disk/volume (mesin fisik[1])	Pemilihan langsung Aturan kebijakan Filter file	Awan Folder lokal Folder jaringan NFS* Secure Zone**	Selalu inkremental (file tunggal) Selalu penuh Mingguan penuh, Kenaikan	Berdasarkan umur cadangan (aturan tunggal/per set cadangan) Berdasarkan

[1]Mesin yang dicadangkan oleh agen yang diinstal di sistem operasi.

© Acronis International GmbH, 2003-2024

			harian Bulanan penuh, Mingguan diferensial, Harian inkremental (GFS) Kustom (F-D-I)	jumlah cadangan Berdasarkan ukuran total cadangan*** Simpan tanpa batas waktu

© Acronis International GmbH, 2003-2024

Disk/volume (mesin virtual[1])		Aturan kebijakan Filter file	Awan Folder lokal Folder jaringan NFS*	
File (hanya mesin fisik[2])		Pemilihan langsung Aturan kebijakan Filter file	Awan Folder lokal Folder jaringan NFS* Secure Zone**	Selalu inkremental (file tunggal) Selalu penuh Mingguan penuh, Kenaikan harian Bulanan penuh, Mingguan diferensial, Harian inkremental (GFS) Kustom (F-D-I)
Konfigurasi ESXi		Pemilihan langsung	Folder lokal Folder jaringan NFS*	
Situs web (file dan database MySQL)		Pemilihan langsung	Awan	—
Status sistem		Pemilihan langsung	Awan Folder lokal Folder jaringan	Selalu penuh Mingguan penuh, Kenaikan harian Kustom (F-I) Selalu inkremental (File tunggal) - hanya untuk database SQL
Database SQL				
Basis data Exchange				
Microsoft 365	Kotak surat (Agen untuk Microsoft 365 lokal)	Pemilihan langsung	Awan Folder lokal Folder jaringan	Selalu inkremental (file tunggal)

[1]Mesin virtual yang dicadangkan di level hypervisor oleh agen eksternal seperti Agen untuk VMware atau Agen untuk Hyper-V. Mesin virtual dengan agen di dalamnya diperlakukan sebagai fisik dari sudut pencadangan.
[2]Mesin yang dicadangkan oleh agen yang diinstal di sistem operasi.

© Acronis International GmbH, 2003-2024

	Kotak surat (Agen untuk Microsoft 365 awan)	Pemilihan langsung	Awan	Hingga 6 cadangan per hari	
	Folder publik				
	Teams				
	File OneDrive	Pemilihan langsung Aturan kebijakan			
	Data SharePoint Online				
Google Workspace	Kotak surat Gmail	Pemilihan langsung	Awan	Hingga 6 cadangan per hari	
	File Google Drive	Pemilihan langsung Aturan kebijakan			
	File drive Shared				

* Cadangkan ke NFS bersama tidak tersedia di Windows.

** Secure Zone tidak dapat dibuat di Mac.

*** Aturan retensi **Berdasarkan ukuran total cadangan** tidak tersedia dengan skema pencadangan **Selalu inkremental (file tunggal)** atau saat mencadangkan ke penyimpanan awan.

Memilih data yang akan dicadangkan

Memilih keseluruhan mesin

Cadangan keseluruhan mesin berarti cadangan dari semua disk-nya yang tidak dapat dilepas. Untuk informasi lebih lanjut tentang cadangan disk, lihat "Memilih disk atau volume" (hlm. 401).

Pembatasan

- Pencadangan tingkat disk tidak didukung untuk volume APFS terenkripsi yang terkunci. Selama pencadangan keseluruhan mesin, volume tersebut dilewatkan.
- Folder root OneDrive tidak disertakan dari operasi pencadangan secara default. Jika Anda memilih untuk mencadangkan file dan folder OneDrive tertentu, file dan folder tersebut akan dicadangkan. File yang tidak tersedia di perangkat akan memiliki konten yang tidak valid dalam cadangan yang diatur pada beban kerja yang ingin Anda lindungi.

© Acronis International GmbH, 2003-2024

Memilih disk atau volume

Cadangan tingkat disk berisi salinan disk atau volume dalam bentuk paket. Dari pencadangan tingkat disk, Anda dapat memulihkan disk, volume, folder, dan file.

Anda dapat memilih disk atau volume yang akan dicadangkan untuk setiap beban kerja individual dalam rencana proteksi (pilihan langsung) atau Anda dapat mengonfigurasi aturan kebijakan untuk beberapa beban kerja. Selain itu, Anda dapat mengecualikan file tertentu dari cadangan, atau hanya menyertakan file tertentu ke dalamnya, dengan mengonfigurasi filter file. Untuk informasi lebih lanjut, lihat "Filter file (Penyertaan/Pengecualian)" (hlm. 460).

Untuk memilih disk atau volume

Pemilihan langsung

Pemilihan langsung hanya tersedia untuk mesin fisik.

1. Di **Apa yang akan dicadangkan**, pilih **Disk/volume**.
2. Klik **Item untuk dicadangkan**.
3. Di **Pilih item untuk dicadangkan**, pilih **Secara langsung**.
4. Untuk setiap beban kerja yang termasuk dalam rencana proteksi, pilih kotak centang di sebelah disk atau volume yang akan dicadangkan.
5. Klik **Selesai**.

Berdasarkan aturan kebijakan

1. Di **Apa yang akan dicadangkan**, pilih **Disk/volume**.
2. Klik **Item untuk dicadangkan**.
3. Di **Pilih item untuk dicadangkan**, pilih **Gunakan aturan kebijakan**.
4. Pilih salah satu aturan yang telah ditetapkan, ketik aturan Anda sendiri, atau kombinasikan keduanya.

   Untuk informasi lebih lanjut tentang aturan kebijakan yang tersedia, lihat "Aturan kebijakan untuk disk dan volume" (hlm. 403).

   Aturan kebijakan akan diterapkan pada semua beban kerja yang termasuk dalam rencana proteksi.

   Jika tidak ada aturan yang ditentukan yang dapat diterapkan pada beban kerja, pencadangan beban kerja tersebut akan gagal.
5. Klik **Selesai**.

Pembatasan

- Pencadangan tingkat disk tidak didukung untuk volume APFS terenkripsi yang terkunci. Selama pencadangan keseluruhan mesin, volume tersebut dilewatkan.

© Acronis International GmbH, 2003-2024

- Folder root OneDrive tidak disertakan dari operasi pencadangan secara default. Jika Anda memilih untuk mencadangkan file dan folder OneDrive tertentu, file dan folder tersebut akan dicadangkan. File yang tidak tersedia di perangkat akan memiliki konten yang tidak valid dalam cadangan yang diatur pada beban kerja yang ingin Anda lindungi.
- Anda dapat mencadangkan disk yang terhubung melalui protokol iSCSI ke mesin fisik. Namun, batasan berlaku jika Anda menggunakan Agen untuk VMware atau Agen untuk Hyper-V untuk mencadangkan disk yang terhubung dengan iSCSI. Untuk informasi lebih lanjut, lihat "Pembatasan" (hlm. 33).

Apa manfaat penyimpanan cadangan disk atau volume?

Cadangan disk atau volume menyimpan disk atau volume **sistem file** secara keseluruhan dan memasukkan semua informasi yang diperlukan dalam sistem operasi untuk boot. Jenis cadangan ini memungkinkan Anda untuk memulihkan disk atau volume secara keseluruhan dari pencadangan tersebut serta folder atau file individual.

Dengan diaktifkannya **opsi pencadangan** sektor per sektor (mode mentah), cadangan disk akan menyimpan semua sektor disk. Pencadangan sektor per sektor dapat digunakan untuk mencadangkan disk dengan sistem file yang tidak dikenal atau tidak didukung dan format data kepemilikan lainnya.

Windows

Cadangan volume menyimpan semua file dan folder volume yang dipilih secara mandiri dari atributnya (termasuk file tersembunyi dan sistem), rekaman boot, tabel alokasi file (FAT) jika ada, root dan trek nol dari hard disk dengan master boot record (MBR).

Cadangan disk menyimpan semua volume disk yang dipilih (termasuk volume tersembunyi seperti partisi pemeliharaan vendor) dan trek nol dengan master boot record.

Item berikut *tidak* dimasukkan dalam cadangan disk atau volume (serta dalam pencadangan tingkat file):

- File swap (pagefile.sys) dan file yang menyimpan isi RAM ketika mesin beralih ke mode hibernasi (hiberfil.sys). Setelah pemulihan, file akan dibuat ulang di tempat yang sesuai dengan ukuran nol.
- Jika pencadangan dilakukan di dalam sistem operasi (sebagai kebalikan dari media yang dapat di-boot atau mencadangkan mesin virtual pada tingkat hypervisor):
  - Penyimpanan bayangan Windows. Jalur ke penyimpanan ditentukan dengan nilai registri **Penyedia Default VSS**yang dapat ditemukan di kunci registri **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. Ini berarti bahwa dalam sistem operasi yang dimulai dengan Windows Vista, Windows Restore Points tidak dicadangkan.
  - Jika opsi pencadangan **Layanan Menyalin Bayangan Volume (VSS)** diaktifkan, file dan folder yang ditentukan dalam kunci registri **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**.

© Acronis International GmbH, 2003-2024

Linux

Cadangan volume menyimpan semua file dan direktori dari volume yang dipilih secara independen dari atributnya, rekaman boot, dan blok super sistem file.

Cadangan disk menyimpan semua volume disk serta trek nol dengan master boot record.

Mac

Cadangan disk atau volume menyimpan semua file dan direktori dari disk atau volume yang dipilih, ditambah deskripsi tata letak volume.

Item berikut akan dikecualikan:

- Metadata sistem, seperti jurnal sistem file dan indeks Spotlight
- Sampah
- Pencadangan mesin waktu

Secara fisik, disk dan volume pada Mac dicadangkan di tingkat file. Pemulihan bare metal dari cadangan disk dan volume dimungkinkan, namun mode cadangan sektor per sektor tidak tersedia.

Aturan kebijakan untuk disk dan volume

Saat Anda memilih disk atau volume untuk dicadangkan, Anda dapat menggunakan aturan kebijakan berikut, sesuai dengan sistem operasi beban kerja yang dilindungi.

Windows

- `[All Volumes]` memilih semua volume pada mesin.
- Huruf drive (misalnya, `C:\`) memilih volume dengan huruf drive yang ditentukan.
- `[Fixed Volumes (physical machines)]` memilih semua volume mesin fisik, selain media yang dapat dipindahkan. Volume tetap mencakup volume pada perangkat SCSI, ATAPI, ATA, SSA, SAS, dan SATA, dan pada array RAID.
- `[BOOT+SISTEM]` memilih volume sistem dan boot. Ini adalah kombinasi minimal yang dapat digunakan untuk memulihkan sistem operasi.
- `[Disk 1]` memilih disk pertama mesin, termasuk semua volume pada disk tersebut. Untuk memilih disk lain, ketik nomor yang sesuai.

Linux

- `[All Volumes]` memilih semua volume yang dipasang pada mesin.
- `/dev/hda1` memilih volume pertama pada hard disk IDE pertama.
- `/dev/sda1` memilih volume pertama pada hard disk SCSI pertama.
- `/dev/md1` memilih hard disk RAID perangkat lunak pertama.

© Acronis International GmbH, 2003-2024

- Untuk memilih volume dasar lainnya, tentukan `/dev/xdyN`, di mana:
  - "x" sesuai dengan jenis disk
  - "y" sesuai dengan nomor disk (a untuk disk pertama, b untuk disk kedua, dan seterusnya)
  - "N" adalah nomor volume.
- Untuk memilih volume logis, tentukan jalurnya saat muncul setelah menjalankan perintah `ls /dev/mapper` di bawah akun akar.

  Misalnya:

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  Keluaran ini menunjukkan dua volume logis, `lv1` dan `lv2`, yang termasuk dalam grup volume `vg_1`. Untuk mencadangkan volume ini, tentukan:

  `/dev/mapper/vg_1-lv1`

  `/dev/mapper/vg-l-lv2`

macOS

- `[All Volumes]` memilih semua volume yang dipasang pada mesin.
- `[Disk 1]` Memilih disk pertama mesin, termasuk semua volume pada disk tersebut. Untuk memilih disk lain, tentukan nomor yang sesuai.

Memilih file atau folder

Gunakan cadangan tingkat file untuk melindungi data tertentu saja, misalnya file dalam proyek Anda saat ini. Pencadangan tingkat file lebih kecil daripada pencadangan tingkat disk dan menghemat ruang penyimpanan.

Penting
Anda tidak dapat memulihkan sistem operasi dari cadangan tingkat file.

Anda dapat memilih file dan folder yang akan dicadangkan untuk setiap beban kerja individual dalam rencana proteksi (pilihan langsung) atau Anda dapat mengonfigurasi aturan kebijakan untuk beberapa beban kerja. Selain itu, Anda dapat mengecualikan file tertentu dari cadangan, atau hanya menyertakan file tertentu di dalamnya, dengan mengonfigurasi filter. Untuk informasi lebih lanjut, lihat "Filter file (Penyertaan/Pengecualian)" (hlm. 460).

Untuk memilih file atau folder

Pemilihan langsung

1. Di **Apa yang akan dicadangkan**, pilih **File/folder**.
2. Di **Item untuk dicadangkan**, klik **Tentukan**.
3. Di **Pilih item untuk dicadangkan**, pilih **Secara langsung**.

© Acronis International GmbH, 2003-2024

4. Tentukan file atau folder yang akan dicadangkan untuk setiap beban kerja dalam rencana proteksi.
   a. Klik **Pilih file dan folder**.
   b. Klik **Folder lokal** atau **Folder jaringan**.
      Folder jaringan harus dapat diakses dari mesin yang dipilih.
      Saat Anda memilih **Folder jaringan** sebagai sumber, Anda dapat mencadangkan data dari penyimpanan yang terpasang di jaringan (NAS), seperti perangkat NetApp. Perangkat NAS dari semua vendor didukung.
   c. Di pohon folder, navigasikan ke file atau folder yang diperlukan.
      Alternatifnya, tentukan jalur ke sana, lalu klik tombol panah.
   d. [Untuk folder bersama] Saat diminta, tentukan kredensial akses ke folder bersama.
      Mencadangkan folder dengan akses anonim tidak didukung.
   e. Pilih file dan folder yang diperlukan.
   f. Klik **Selesai**.

Berdasarkan aturan kebijakan

1. Di **Apa yang akan dicadangkan**, pilih **File/folder**.
2. Di **Item untuk dicadangkan**, klik **Tentukan**.
3. Di **Pilih item untuk dicadangkan**, pilih **Gunakan aturan kebijakan**.
4. Pilih salah satu aturan yang telah ditetapkan, ketik aturan Anda sendiri, atau kombinasikan keduanya.
   Untuk informasi lebih lanjut tentang aturan kebijakan yang tersedia, lihat "Aturan kebijakan untuk file dan folder" (hlm. 406).
   Aturan kebijakan akan diterapkan pada semua beban kerja yang termasuk dalam rencana proteksi.
   Jika tidak ada aturan yang ditentukan yang dapat diterapkan pada beban kerja, pencadangan beban kerja tersebut akan gagal.
5. Klik **Selesai**.

Pembatasan

- Anda dapat memilih file dan folder saat Anda mencadangkan mesin fisik atau mesin virtual tempat agen diinstal (pencadangan berbasis agen). Pencadangan tingkat file tidak tersedia untuk mesin virtual yang Anda cadangankan dalam mode tanpa agen. Untuk informasi lebih lanjut tentang perbedaan antara jenis cadangan ini, lihat "Pencadangan berbasis agen dan tanpa agen" (hlm. 65).
- Folder root OneDrive tidak disertakan dari operasi pencadangan secara default. Jika Anda memilih untuk mencadangkan file dan folder OneDrive tertentu, file dan folder tersebut akan dicadangkan. File yang tidak tersedia di perangkat akan memiliki konten yang tidak valid dalam cadangan yang diatur pada beban kerja yang ingin Anda lindungi.

© Acronis International GmbH, 2003-2024

- Anda dapat mencadangkan file dan folder yang terletak di disk yang terhubung melalui protokol iSCSI ke mesin fisik. Beberapa batasan berlaku jika Anda menggunakan Agen untuk VMware atau Agen untuk Hyper-V untuk mencadangkan data pada disk yang terhubung dengan iSCSI.

Aturan kebijakan untuk file dan folder

Saat Anda memilih file atau folder untuk dicadangkan, Anda dapat menggunakan aturan kebijakan berikut, sesuai dengan sistem operasi beban kerja yang dilindungi.

Windows

- Jalur lengkap ke file atau folder. Misalnya, `D:\Work\Text.doc` atau `C:\Windows`.
- Aturan yang telah ditentukan sebelumnya:
  - `[All Files]` memilih semua file pada semua volume mesin.
  - `[All Profiles Folder]` memilih folder tempat semua profil pengguna berada. Misalnya, `C:\Users` atau `C:\Documents and Settings`.
- Variabel lingkungan:
  - `%ALLUSERSPROFILE%` memilih folder tempat data umum semua profil pengguna berada. Misalnya `C:\ProgramData` atau `C:\Documents and Settings\All Users`.
  - `%PROGRAMFILES%` memilih folder `Program File`. Misalnya, `C:\Program Files`.
  - `%WINDIR%` memilih folder `Windows`. Misalnya, `C:\Windows`.

  Anda dapat menggunakan variabel lingkungan lain atau kombinasi variabel lingkungan dan teks. Misalnya, untuk memilih folder Java di folder Program Files, tentukan: `%PROGRAMFILES%\Java`.

Linux

- Jalur lengkap ke file atau direktori.

  Misalnya, untuk mencadangkan file `file.txt` pada volume `/dev/hda3` yang dipasang pada `/home/usr/docs`, tentukan `/dev/hda3/file.txt` atau `/home/usr/docs/file.txt`.
- Aturan yang telah ditentukan sebelumnya:
  - `[All Profiles Folder]` memilih `/home`. Secara default, semua profil pengguna disimpan di folder ini.
  - `/home` memilih direktori asal dari pengguna umum.
  - `/root` memilih direktori asal pengguna root.
  - `/usr` memilih direktori untuk semua program terkait pengguna.
  - `/etc` memilih direktori untuk file konfigurasi sistem.

macOS

- Jalur lengkap ke file atau direktori.

  Misalnya:
  - Untuk mencadangkan `file.txt` di desktop pengguna, tentukan `/Users/<nama pengguna>/Desktop/file.txt`.

© Acronis International GmbH, 2003-2024

- Untuk mencadangkan folder `Desktop`, `Documents`, dan `Downloads` milik pengguna, tentukan `/Users/<user name>/Desktop`, `/Users/<user name>/Documents`, dan `/Users/<user name>/Downloads`.
- Untuk mencadangkan folder utama semua pengguna yang memiliki akun di mesin ini, tentukan `/Users`.
- Untuk membuat cadangan folder tempat aplikasi diinstal, tentukan `/Applications`.

- Aturan yang telah ditentukan sebelumnya
  - `[All Profiles Folder]` memilih `/Users`. Secara default, semua profil pengguna disimpan di folder ini.

Memilih status sistem

Catatan
Pencadangan status sistem tersedia untuk mesin yang menjalankan Windows 7 dan versi lebih baru tempat Agen untuk Windows diinstal. Status sistem cadangan tidak tersedia untuk mesin virtual yang dicadangkan di level hypervisor (cadangan tanpa agen).

Untuk mencadangkan status sistem, di **Apa yang akan dicadangkan**, pilih **Status sistem**.

Pencadangan status sistem terdiri dari file berikut:

- Konfigurasi penjadwal tugas
- VSS Metadata Store
- Informasi konfigurasi penghitung performa
- MSSearch Service
- Background Intelligent Transfer Service (BITS)
- Registri
- Windows Management Instrumentation (WMI)
- Database pendaftaran Component Services Class

Memilih konfigurasi ESXi

Cadangan dari konfigurasi host ESXi memungkinkan Anda untuk memulihkan host ESXi ke bare metal. Pemulihan dilakukan dengan media yang dapat di-boot.

Mesin virtual yang berjalan pada host tidak termasuk dalam cadangan. Mesin virtual tersebut dapat dicadangkan dan dipulihkan secara terpisah.

Cadangan konfigurasi host ESXi termasuk:

- Partisi bootloader dan bank boot dari host.
- Status host (konfigurasi jaringan dan penyimpanan virtual, kunci SSL, pengaturan jaringan server, dan informasi pengguna lokal).

© Acronis International GmbH, 2003-2024

- Ekstensi dan patch diinstal atau ditempel pada host.
- File log.

Prasyarat

- SSH harus diaktifkan di **Security Profile** konfigurasi host ESXi.
- Anda harus mengetahui kata sandi untuk akun 'root' di host ESXi.

Pembatasan

- Pencadangan konfigurasi ESXi tidak didukung untuk host yang menjalankan VMware ESXi 7.0 dan yang lebih baru.
- Konfigurasi ESXi tidak dapat dicadangkan ke penyimpanan awan.

Untuk memilih konfigurasi ESXi

1. Klik **Perangkat** > **Semua perangkat**, lalu pilih host ESXi yang ingin Anda cadangkan.
2. Klik **Lindungi**.
3. Di **Apa yang akan dicadangkan**, pilih **Konfigurasi ESXI**.
4. Di **kata sandi 'root' ESXi**, tentukan kata sandi untuk akun 'root' pada masing-masing host yang dipilih atau terapkan kata sandi yang sama untuk semua host.

Perlindungan data berkelanjutan (CDP)

Perlindungan data berkelanjutan (CDP) merupakan bagian dari paket Cadangan Tingkat Lanjut. Ini mencadangkan data penting segera setelah data ini diubah, memastikan bahwa tidak ada perubahan yang hilang jika sistem Anda gagal antara dua pencadangan terjadwal. Anda dapat mengonfigurasi Perlindungan data berkelanjutan untuk data berikut:

- File atau folder di lokasi tertentu
- File yang dimodifikasi dengan aplikasi tertentu

Perlindungan data berkelanjutan didukung hanya untuk sistem file NTFS dan sistem operasi berikut:

- Desktop: Windows 7 dan versi lebih baru
- Server: Windows Server 2008 R2 dan versi lebih baru

Hanya folder lokal yang didukung. Folder jaringan tidak dapat dipilih untuk Perlindungan data berkelanjutan.

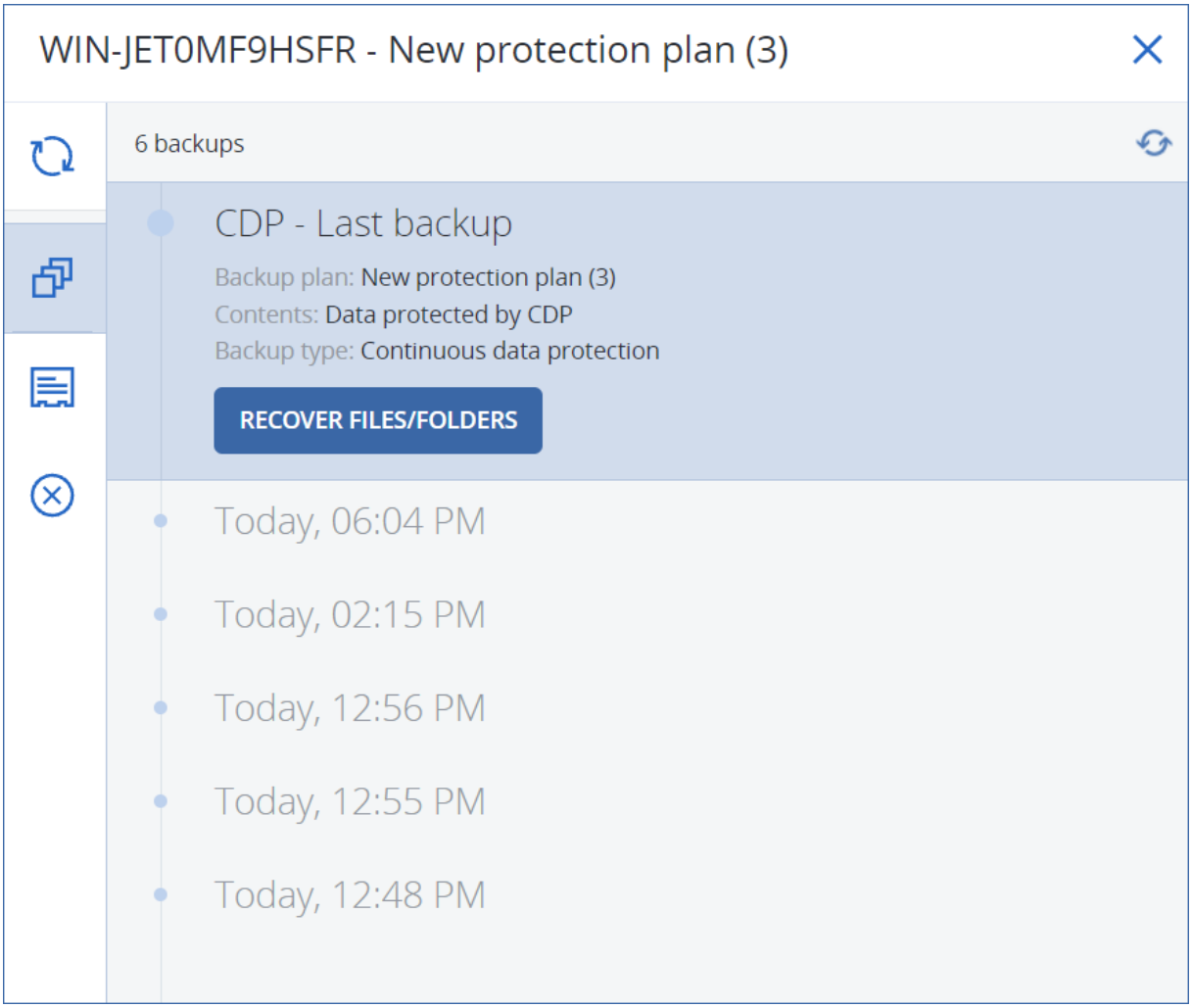
Perlindungan data berkelanjutan tidak kompatibel dengan opsi **Cadangan aplikasi**.

Cara kerjanya

Perubahan dalam file dan folder yang terlacak oleh Perlindungan data berkelanjutan segera disimpan ke cadangan CDP khusus. Hanya ada satu cadangan CDP dalam set cadangan, dan selalu

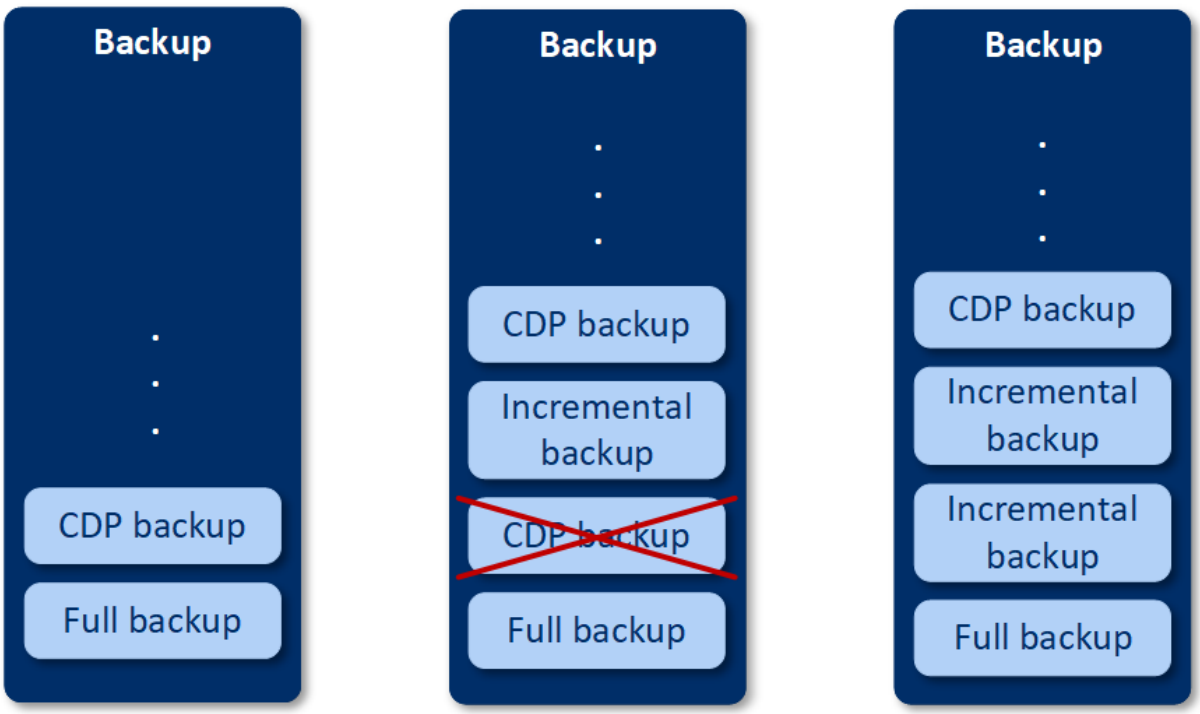
© Acronis International GmbH, 2003-2024

yang terbaru.



Ketika pencadangan regular terjadwal dimulai, Perlindungan data berkelanjutan akan ditunda karena data terkini disertakan dalam pencadangan terjadwal. Saat pencadangan terjadwal selesai, Perlindungan data berkelanjutan dilanjutkan, pencadangan CDP lama dihapus, dan pencadangan CDP baru dibuat. Maka, cadangan CDP selalu menjadi cadangan terbaru dalam set cadangan dan menyimpan hanya file atau folder terlacak dalam keadaan terbaru.

© Acronis International GmbH, 2003-2024



Jika mesin Anda mengalami gangguan selama pencadangan reguler, Perlindungan data berkelanjutan berlanjut secara otomatis setelah mesin memulai ulang dan membuat cadangan CDP sebagai tambahan untuk cadangan terjadwal terakhir yang berhasil.

Perlindungan data berkelanjutan mengharuskan agar setidaknya satu cadangan reguler dibuat sebelum cadangan CDP. Inilah alasan dibuatnya cadangan penuh ketika Anda menjalankan rencana proteksi dengan Perlindungan data berkelanjutan untuk pertama kalinya, dan cadangan CDP segera ditambahkan padanya. Jika Anda mengaktifkan opsi **Perlindungan data berkelanjutan** untuk rencana proteksi yang sudah ada, cadangan CDP ditambahkan ke set cadangan yang sudah ada.

Catatan
Perlindungan Data Berkelanjutan diaktifkan secara default untuk rencana proteksi yang Anda buat dari tab **Perangkat**, jika fungsionalitas Cadangan Tingkat Lanjut diaktifkan bagi Anda dan Anda tidak menggunakan fitur Cadangan Tingkat Lanjut untuk mesin yang dipilih. Jika Anda sudah memiliki rencana dengan Perlindungan data berkelanjutan untuk mesin yang dipilih, Perlindungan data berkelanjutan tidak akan diaktifkan secara default untuk mesin tersebut di dalam rencana yang baru dibuat.
Perlindungan data berkelanjutan tidak diaktifkan secara default untuk rencana yang dibuat untuk grup perangkat.

Sumber data yang didukung

Anda dapat mengonfigurasi Perlindungan data berkelanjutan untuk sumber data berikut:

- Seluruh mesin
- Disk/volume

© Acronis International GmbH, 2003-2024

- File/folder

Setelah memilih sumber data di bagian **Apa yang harus dicadangkan** dalam rencana proteksi, di bagian **Item yang harus dilindungi secara berkelanjutan**, pilih file, folder, atau aplikasi untuk Perlindungan data berkelanjutan. Untuk informasi lebih lanjut tentang cara mengonfigurasi Perlindungan data berkelanjutan, lihat "Mengonfigurasi cadangan CDP" (hlm. 411).

Tujuan yang didukung

Anda dapat mengonfigurasi Perlindungan data berkelanjutan untuk tujuan berikut:

- Folder lokal
- Folder jaringan
- Penyimpanan awan
- Acronis Cyber Infrastructure
- Lokasi ditentukan oleh skrip

Catatan
Anda dapat menentukan dengan skrip hanya untuk lokasi yang tercantum di atas.

Mengonfigurasi cadangan CDP

Anda dapat mengonfigurasi Perlindungan data berkelanjutan dalam modul **Cadangan** pada rencana proteksi. Untuk informasi lebih lanjut tentang cara membuat rencana proteksi, lihat "Membuat rencana proteksi" (hlm. 214).

Cara mengonfigurasi pengaturan Perlindungan data berkelanjutan

1. Dalam modul **Cadangan** pada rencana proteksi, aktifkan switch **Perlindungan data berkelanjutan (CDP)**.
   Switch ini tersedia hanya untuk sumber data berikut:
   - Seluruh mesin
   - Disk/volume
   - File/folder
2. Dalam **Item yang harus dilindungi secara berkelanjutan**, konfigurasi Perlindungan data berkelanjutan untuk **Aplikasi** atau **File/folder**, atau keduanya.
   - Klik **Aplikasi** guna mengonfigurasi cadangan CDP untuk file yang dimodifikasi dengan aplikasi tertentu.
     Anda dapat memilih aplikasi dari kategori yang sudah ditetapkan sebelumnya atau menambahkan aplikasi lain dengan menentukan jalur ke file aplikasi yang dapat dieksekusi, misalnya:
     - `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
     - `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

© Acronis International GmbH, 2003-2024

- Klik **File/folder** guna mengonfigurasi cadangan CDP untuk file di lokasi tertentu.
  Anda dapat menetapkan lokasi ini menggunakan aturan pemilihan, atau dengan memilih file dan folder secara langsung.
  - [Untuk semua mesin] Untuk membuat aturan pemilihan, gunakan kotak teks.
    Anda dapat menggunakan jalur lengkap menuju file atau jalur dengan karakter wildcard (* dan ?). Tanda bintang cocok dengan nol atau lebih banyak karakter. Tanda tanya cocok dengan satu karakter.

    Penting
    Guna membuat cadangan CDP untuk suatu folder, Anda harus menetapkan kontennya menggunakan karakter wildcard tanda bintang:
    Jalur yang benar:`D:\Data\*`
    Jalur yang salah: `D:\Data\`
  - [Untuk mesin online] Cara memilih file dan folder secara langsung:
    - Dalam **Mesin untuk menelusuri**, pilih mesin yang terdapat file atau folder.
    - Klik **Pilih file dan folder** untuk menelusuri mesin yang dipilih.
      Pemilihan langsung Anda akan membuat aturan pemilihan. Jika Anda menerapkan rencana proteksi ke beberapa mesin dan aturan pemilihan tidak valid untuk suatu mesin, rencana tersebut akan dilewati untuk mesin ini.
3. Pada panel rencana proteksi, klik **Buat**.

Hasilnya, data yang Anda tetapkan akan dicadangkan terus-menerus antara pencadangan terjadwal.

Memilih tujuan

Klik **Tempat menyimpan cadangan**, lalu pilih salah satu dari opsi berikut:

- **Penyimpanan awan**
  File akan disimpan di pusat data awan.
- **Folder lokal**
  Jika mesin tunggal dipilih, jelajahi ke folder di mesin yang dipilih atau ketik jalur folder.
  Jika beberapa mesin dipilih, ketik jalur folder. Cadangan akan disimpan dalam folder ini pada setiap mesin fisik yang dipilih atau pada mesin tempat agen untuk mesin virtual diinstal. Jika foldernya tidak ada, folder akan dibuat.
- **Folder jaringan**
  Ini adalah folder yang dibagikan melalui SMB/CIFS/DFS.
  Jelajahi folder bersama yang diperlukan atau masukkan jalur dengan format berikut:
  - Untuk SMB/CIFS bersama: `\\<nama host>\<jalur>\` atau `smb://<nama host>/<jalur>/`
  - Untuk DFS bersama: `\\<nama domain DNS yang lengkap>\<DFS akar>\<jalur>`
    Misalnya, `\\contoh.perusahaan.com\bersama\file`

© Acronis International GmbH, 2003-2024

Lalu, klik tombol panah. Jika diminta, tentukan nama pengguna dan kata sandi untuk folder bersama. Anda dapat mengubah kredensial setiap saat dengan mengeklik ikon kunci di samping nama folder.

Mencadangkan ke folder dengan akses anonim tidak didukung.

- **Cloud publik**

  Opsi ini tersedia sebagai bagian dari paket Backup Lanjutan.

  Dengan ini, Anda dapat mengonfigurasi pencadangan langsung ke penyimpanan cloud publik yang kompatibel, tanpa perlu menyebarkan komponen tambahan (seperti Microsoft Azure atau mesin virtual lainnya sebagai gateway). Pilih dan sambungkan ke cloud publik yang relevan, sesuai kebutuhan.

  Untuk informasi lebih lanjut, lihat "Mencadangkan beban kerja ke cloud publik" (hlm. 538).

- **Folder NFS** (tersedia untuk mesin yang menjalankan Linux atau macOS)

  Verifikasi bahwa paket nfs-utils diinstal di server Linux di mana Agen untuk Linux diinstal.

  Jelajahi folder NFS yang diperlukan atau masukkan jalur dengan format berikut:

  `nfs://<nama host>/<diekspor folder>:/<subfolder>`

  Lalu, klik tombol panah.

  Catatan
  Tidak dimungkinkan untuk mencadangkan ke folder NFS yang dilindungi dengan kata sandi.

- **Secure Zone** (tersedia jika ada di masing-masing mesin yang dipilih)

  Secure Zone adalah partisi aman pada disk mesin yang dicadangkan. Partisi ini harus dibuat secara manual sebelum mengonfigurasi cadangan. Untuk informasi tentang cara membuat Secure Zone, kelebihan dan kekurangannya, lihat "Tentang Secure Zone" (hlm. 414).

Opsi penyimpanan lanjutan

Catatan
Fungsi ini hanya tersedia di edisi Advanced pada layanan Cyber Protection.

Didefinisikan oleh skrip (tersedia untuk mesin yang menjalankan Windows)

Anda dapat menyimpan cadangan setiap mesin dalam folder yang didefinisikan oleh skrip. Perangkat lunak ini mendukung skrip yang ditulis dalam JScript, VBScript, atau Python 3.5. Saat menyebarkan rencana proteksi, perangkat lunak menjalankan skrip di setiap mesin. Output skrip untuk setiap mesin harus berupa jalur folder lokal atau jaringan. Jika folder tidak ditemukan, maka folder akan dibuat (batasan: skrip yang ditulis dengan Python tidak dapat membuat folder di jaringan bersama). Pada tab **Penyimpanan cadangan**, setiap folder ditampilkan sebagai lokasi cadangan terpisah.

Di **Jenis skrip**, pilih jenis skrip (**JScript**, **VBScript**, atau **Python**), lalu impor, atau salin dan tempelkan skrip. Untuk folder jaringan, tentukan kredensial akses dengan izin baca/tulis.

Contoh:

© Acronis International GmbH, 2003-2024

- Skrip JScript berikut menampilkan lokasi cadangan untuk mesin dalam format `\\bkpsrv\<nama mesin>`:

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  Hasilnya, cadangan dari setiap mesin akan disimpan dalam folder dengan nama yang sama di server **bkpsrv**.
- Skrip JScript berikut menghasilkan output lokasi cadangan dalam folder pada mesin tempat skrip berjalan:

  ```
  WScript.Echo("C:\\Backup");
  ```

  Sebagai hasilnya, cadangan mesin ini akan disimpan di folder `C:\Backup` pada mesin yang sama.

Catatan
Jalur lokasi skrip ini peka huruf kecil dan besar. Oleh karena itu, `C:\Backup` dan `C:\backup` ditampilkan sebagai lokasi yang berbeda di konsol Cyber Protect. Selain itu, gunakan huruf besar untuk huruf drive.

Tentang Secure Zone

Secure Zone adalah partisi aman pada disk mesin yang dicadangkan. Partisi tersebut dapat menyimpan cadangan disk atau file mesin ini.

Jika disk mengalami kegagalan fisik, cadangan yang ada di dalam Secure Zone dapat hilang. Itulah mengapa Secure Zone sebaiknya tidak menjadi satu-satunya lokasi penyimpanan cadangan. Di lingkungan enterprise, Secure Zone dapat dianggap sebagai lokasi kedua yang digunakan untuk cadangan jika lokasi biasa sedang tidak tersedia atau terhubung ke saluran yang lambat atau sibuk.

Mengapa perlu menggunakan Secure Zone?

Secure Zone:

- Memungkinkan pemulihan disk ke disk yang sama di mana cadangan disk berada.
- Menawarkan efektivitas biaya dan cara yang mudah untuk melindungi data dari malafungsi perangkat lunak, serangan virus, eror manusia.
- Mengeliminasi kebutuhan akan media terpisah atau koneksi jaringan untuk pencadangan atau pemulihan data. Hal ini berguna khususnya bagi pengguna roaming.
- Dapat berlaku sebagai tujuan utama saat menggunakan replikasi cadangan.

Pembatasan

- Secure Zone tidak dapat dikelola di Mac.
- Secure Zone adalah partisi pada disk standar. Tidak dapat dikelola pada disk dinamis atau dibuat sebagai volume logis (dikelola oleh LVM).

© Acronis International GmbH, 2003-2024

- Secure Zone diformat menggunakan sistem file FAT32. Karena FAT32 memiliki batas ukuran file sebesar 4 GB, cadangan yang lebih besar akan dibagi ketika disimpan ke Secure Zone. Hal ini tidak memengaruhi prosedur dan kecepatan pemulihan.

Bagaimana pembuatan Secure Zone mengubah disk

- Secure Zone selalu dibuat di bagian akhir hard disk.
- Jika tidak ada atau tidak cukup ruang yang tidak teralokasi di bagian akhir disk, namun terdapat ruang yang tidak teralokasi di antara volume, volume akan dipindahkan untuk menambah ruang yang tidak teralokasi di bagian akhir disk.
- Ketika semua ruang yang tidak teralokasi terkumpul namun masih belum cukup, program akan mengambil ruang bebas dari volume yang Anda pilih, sehingga mengurangi ukuran volume secara proporsional.
- Namun, harus ada ruang bebas pada volume, sehingga sistem operasi dan aplikasi dapat berjalan; misalnya, membuat file sementara. Perangkat lunak ini tidak akan mengurangi volume di mana ruang bebas menjadi lebih kecil 25 persen dari total ukuran volume. Hanya saat semua volume pada disk memiliki ruang bebas sebesar 25 persen atau kurang, perangkat lunak akan terus mengurangi volume secara proporsional.

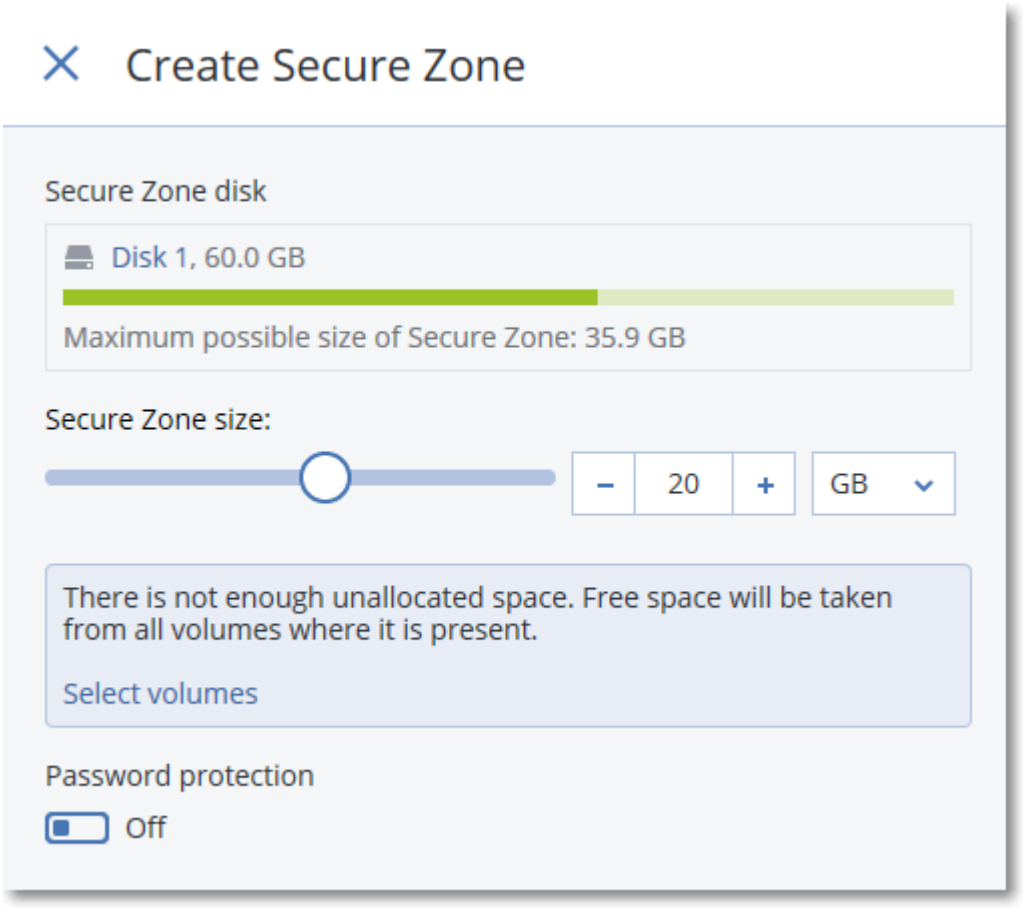
Seperti telah dijelaskan di atas, menentukan ukuran Secure Zone maksimum yang paling memungkinkan tidaklah dianjurkan. Anda akhirnya tidak akan memiliki ruang bebas pada volume, sehingga dapat menyebabkan sistem operasi atau aplikasi tidak bekerja dengan stabil dan bahkan gagal memulai.

Penting
Memindahkan atau mengubah ukuran volume yang darinya sistem di-boot memerlukan reboot.

Cara membuat Secure Zone

1. Pilih mesin yang ingin Anda buat Secure Zone.
2. Klik **Detail** > **Buat Secure Zone** .
3. Pada **Secure Zone disk**, klik **Pilih**, lalu pilih hard disk (jika ada beberapa) yang akan dijadikan zona.
   Perangkat lunak menghitung ukuran maksimum yang dimungkinkan dari Secure Zone.
4. Masukkan ukuran Secure Zone atau seret slider untuk memilih ukuran antara minimum dan maksimum.
   Ukuran minimum sekitar 50 MB, tergantung pada geometri hard disk. Ukuran maksimum sama dengan ruang disk yang tidak teralokasi ditambah ruang kosong total pada semua volume disk.
5. Jika semua ruang yang tidak teralokasi tidak cukup untuk ukuran yang Anda tentukan, perangkat lunak akan mengambil ruang kosong dari volume yang ada. Secara default, semua volume dipilih. Jika Anda ingin mengecualikan beberapa volume, klik **Pilih volume**. Jika tidak, lewati langkah ini.

© Acronis International GmbH, 2003-2024



6. [Opsional] Aktifkan switch **Perlindungan kata sandi**, lalu tentukan kata sandi.
   Kata sandi akan diperlukan untuk mengakses cadangan yang berada di Secure Zone. Mencadangkan ke Secure Zone tidak memerlukan kata sandi, kecuali jika pencadangan dilakukan di bawah media yang dapat di-boot.
7. Klik **Buat**.
   Perangkat lunak menampilkan tata letak yang diperkirakan. Klik **OK**.
8. Tunggu saat perangkat lunak membuat Secure Zone.

Anda sekarang dapat memilih Secure Zone di **Tempat menyimpan cadangan** saat membuat rencana proteksi.

Cara menghapus Secure Zone

1. Pilih mesin dengan Secure Zone.
2. Klik **Detail**.
3. Klik ikon roda gigi di sebelah **Secure Zone** , lalu klik **Hapus**.
4. [Opsional] Tentukan volume di mana ruang yang dibebaskan dari zona akan ditambahkan. Secara default, semua volume dipilih.
   Ruang akan didistribusikan secara merata ke seluruh volume yang dipilih. Jika Anda tidak memilih volume apa pun, ruang yang dibebaskan akan menjadi tidak terisi.

© Acronis International GmbH, 2003-2024

Mengubah ukuran volume yang darinya sistem di-boot membutuhkan reboot.

5. Klik **Hapus**.

Hasilnya, Secure Zone akan dihapus bersama dengan semua cadangan yang tersimpan di dalamnya.

Jadwal pencadangan

Anda dapat mengonfigurasi pencadangan agar berjalan secara otomatis pada waktu tertentu, interval tertentu, atau peristiwa tertentu.

Pencadangan terjadwal untuk sumber daya non-cloud-ke-cloud dijalankan sesuai dengan pengaturan zona waktu beban kerja tempat agen perlindungan diinstal. Misalnya, jika Anda menerapkan rencana proteksi yang sama pada beban kerja dengan pengaturan zona waktu berbeda, pencadangan akan dimulai sesuai dengan zona waktu lokal setiap beban kerja.

Menjadwalkan pencadangan mencakup tindakan berikut:

- Memilih skema cadangan
- Mengonfigurasi waktu atau memilih peristiwa yang memicu pencadangan
- Mengonfigurasi pengaturan opsional dan kondisi awal

Skema cadangan

Skema pencadangan adalah bagian dari jadwal rencana proteksi yang menentukan jenis pencadangan (penuh, diferensial, atau inkremental) yang dibuat dan kapan. Anda dapat memilih salah satu skema pencadangan yang telah ditentukan sebelumnya atau membuat skema kustom.

Skema dan jenis pencadangan yang tersedia bergantung pada lokasi dan sumber pencadangan. Misalnya, pencadangan diferensial tidak tersedia saat Anda mencadangkan data SQL, data Exchange, atau status sistem. Skema **Selalu inkremental (file tunggal)** tidak didukung untuk alat rekaman.

Skema cadangan	Deskripsi	Elemen yang dapat dikonfigurasi
Selalu inkremental (file tunggal)	Pencadangan pertama sudah penuh dan mungkin memakan waktu. Pencadangan berikutnya bersifat inkremental dan jauh lebih cepat. Cadangannya menggunakan format cadangan file	• Jenis jadwal: bulanan, mingguan, harian, setiap jam • Pemicu cadangan:

© Acronis International GmbH, 2003-2024

Skema cadangan	Deskripsi	Elemen yang dapat dikonfigurasi
	tunggal[1]*. Secara default, pencadangan dilakukan setiap hari, Senin hingga Jumat. Kami menyarankan Anda menggunakan skema ini saat menyimpan cadangan di penyimpanan cloud, karena pencadangan inkremental bersifat cepat dan melibatkan lebih sedikit lalu lintas jaringan.	waktu atau peristiwa • Waktu mulai • Persyaratan untuk memulai • Opsi tambahan
Selalu penuh	Semua cadangan dalam set adalah cadangan penuh. Secara default, pencadangan dilakukan setiap hari, Senin hingga Jumat.	• Jenis jadwal: bulanan, mingguan, harian, setiap jam • Pemicu cadangan: waktu atau peristiwa • Waktu mulai • Persyaratan untuk memulai • Opsi tambahan
Mingguan penuh, kenaikan Harian	Pencadangan penuh dibuat seminggu sekali dan pencadangan lainnya dilakukan secara inkremental. Pencadangan pertama sudah penuh dan pencadangan lainnya selama seminggu bersifat inkremental, lalu siklus berulang. Untuk memilih hari pembuatan cadangan penuh mingguan, dalam rencana proteksi, klik ikon roda gigi, lalu buka **Opsi pencadangan** > **Pencadangan mingguan**. Secara default, pencadangan dilakukan setiap hari, Senin hingga Jumat.	• Pemicu cadangan: waktu atau peristiwa • Waktu mulai • Persyaratan untuk memulai • Opsi tambahan
Bulanan penuh, Mingguan diferensial, Harian inkremental (GFS)	Secara default, pencadangan tambahan dilakukan setiap hari, Senin hingga Jumat. Pencadangan diferensial dilakukan setiap hari Sabtu. Pencadangan penuh dilakukan pada hari pertama setiap bulan.	• Ubah jadwal yang ada per jenis cadangan: ◦ Jenis jadwal: bulanan, mingguan, harian,

[1]Format cadangan, di mana cadangan penuh awal dan bertahap selanjutnya akan disimpan ke file .tibx tunggal. Format ini memanfaatkan kecepatan metode pencadangan inkremental, sekaligus menghindari kekurangan utamanya, yaitu kesulitan menghapus cadangan yang lama. Perangkat lunak menandai blok yang digunakan oleh cadangan lama sebagai "kosong" dan menulis cadangan baru ke blok ini. Format ini menghasilkan pembersihan yang sangat cepat, dengan sedikit pemakaian sumber daya. Format cadangan file tunggal tidak tersedia saat mencadangkan ke lokasi yang tidak mendukung akses-acak baca dan tulis.

© Acronis International GmbH, 2003-2024

Skema cadangan	Deskripsi	Elemen yang dapat dikonfigurasi
	Catatan Ini adalah skema kustom yang telah ditentukan sebelumnya. Dalam rencana proteksi, ini ditampilkan sebagai **Kustom**.	setiap jam ◦ Pemicu cadangan: waktu atau peristiwa ◦ Waktu mulai ◦ Persyaratan untuk memulai ◦ Opsi tambahan • Tambahkan jadwal baru per jenis cadangan
Kustom	Anda harus memilih jenis pencadangan (penuh, diferensial, dan inkremental), dan mengonfigurasi jadwal terpisah untuk masing-masing pencadangan*.	• Ubah jadwal yang ada per jenis cadangan: ◦ Jenis jadwal: bulanan, mingguan, harian, setiap jam ◦ Pemicu cadangan: waktu atau peristiwa ◦ Waktu mulai ◦ Persyaratan untuk memulai ◦ Opsi tambahan • Tambahkan jadwal baru per jenis cadangan

* Setelah Anda membuat rencana proteksi, Anda tidak dapat beralih di antara keduanya **Selalu inkremental (file tunggal)** dan skema cadangan lainnya, dan sebaliknya. **Selalu inkremental (file tunggal)** adalah skema format file tunggal, dan skema lainnya adalah format multi-file. Jika Anda ingin beralih antar format, buat rencana proteksi baru.

Jenis cadangan

Jenis cadangan berikut tersedia:

- Penuh—cadangan penuh berisi semua data sumber. Cadangan ini bersifat mandiri. Untuk memulihkan data, Anda tidak memerlukan akses ke cadangan lainnya.

  Catatan
  Cadangan pertama yang dibuat oleh rencana proteksi apa pun adalah cadangan penuh.

© Acronis International GmbH, 2003-2024

- Inkremental—pencadangan inkremental menyimpan perubahan pada data sejak pencadangan terbaru, terlepas dari apakah pencadangan terbaru bersifat penuh, diferensial, atau inkremental. Untuk memulihkan data, Anda memerlukan seluruh rantai pencadangan yang menjadi sandaran pencadangan inkremental, kembali ke pencadangan penuh awal.
- Diferensial—cadangan diferensial menyimpan perubahan pada data sejak pencadangan penuh terbaru. Untuk memulihkan data, Anda memerlukan pencadangan diferensial dan pencadangan penuh terkait yang menjadi sandaran pencadangan diferensial.

Menjalankan pencadangan sesuai jadwal

Untuk menjalankan pencadangan secara otomatis pada waktu tertentu atau pada peristiwa tertentu, aktifkan jadwal dalam rencana proteksi.

Untuk menonaktifkan jadwal

1. Dalam rencana proteksi, perbesar modul **Cadangan**.
2. Klik **Jadwal**.
3. Aktifkan sakelar jadwal.
4. Pilih skema pencadangan.
5. Konfigurasikan jadwal sesuai kebutuhan, lalu klik **Selesai**.
   Untuk informasi selengkapnya tentang opsi penjadwalan yang tersedia, lihat "Jadwalkan berdasarkan waktu" (hlm. 420) dan "Jadwalkan berdasarkan event" (hlm. 423).
6. [Opsional] Konfigurasikan kondisi awal atau opsi penjadwalan tambahan.
7. Simpan rencana proteksi.

Hasilnya, operasi pencadangan dimulai setiap kali kondisi jadwal terpenuhi.

Untuk menonaktifkan jadwal

1. Dalam rencana proteksi, perbesar modul **Cadangan**.
2. Klik **Jadwal**.
3. Nonaktifkan sakelar jadwal.
4. Simpan rencana proteksi.

Akibatnya, pencadangan hanya berjalan jika Anda memulainya secara manual.

Catatan
Jika jadwal dinonaktifkan, aturan retensi tidak diterapkan secara otomatis. Untuk menerapkannya, jalankan pencadangan secara manual.

Jadwalkan berdasarkan waktu

Tabel berikut merangkum opsi penjadwalan yang didasarkan pada waktu. Ketersediaan opsi ini bergantung pada skema pencadangan. Untuk informasi lebih lanjut, lihat "Skema cadangan" (hlm. 417).

© Acronis International GmbH, 2003-2024

Opsi	Deskripsi	Contoh
Bulanan	Pilih bulan, hari dalam sebulan, atau hari dalam seminggu, lalu pilih waktu mulai pencadangan.	Jalankan pencadangan pada tanggal 1 Januari dan 3 Februari pukul 00.00. Jalankan pencadangan pada hari pertama setiap bulan, pukul 10.00. Jalankan pencadangan pada tanggal 1 Maret, 5 Maret, 1 April, dan 5 April, pukul 09.00. Jalankan pencadangan pada hari Jumat kedua dan ketiga setiap bulan, pukul 11.00. Jalankan pencadangan pada hari Rabu terakhir setiap bulan, pukul 22.30.
Mingguan	Pilih hari dalam seminggu, lalu pilih waktu mulai pencadangan.	Jalankan pencadangan Senin hingga Jumat, pukul 10.00. Jalankan pencadangan pada hari Senin, pukul 23.00. Jalankan pencadangan pada hari Selasa dan Sabtu, pukul 08.00.
Harian	Pilih hari (setiap hari atau hari kerja saja), lalu pilih waktu mulai pencadangan.	Jalankan pencadangan setiap hari, pada pukul 11.45. Jalankan pencadangan Senin hingga Jumat, pukul 21.30.
Per jam	Pilih hari dalam seminggu, lalu pilih interval waktu antara dua pencadangan berturut-turut dan rentang waktu saat pencadangan dijalankan. Saat Anda mengonfigurasi interval dalam menit, Anda dapat memilih interval yang disarankan antara 10 dan 60 menit, atau menentukan interval khusus, misalnya, 45 atau 75 menit.	Jalankan pencadangan setiap jam antara pukul 08.00 hingga 18.00, Senin hingga Jumat. Jalankan pencadangan setiap 3 jam antara pukul 01.00 hingga 18.00, pada hari Sabtu dan Minggu.

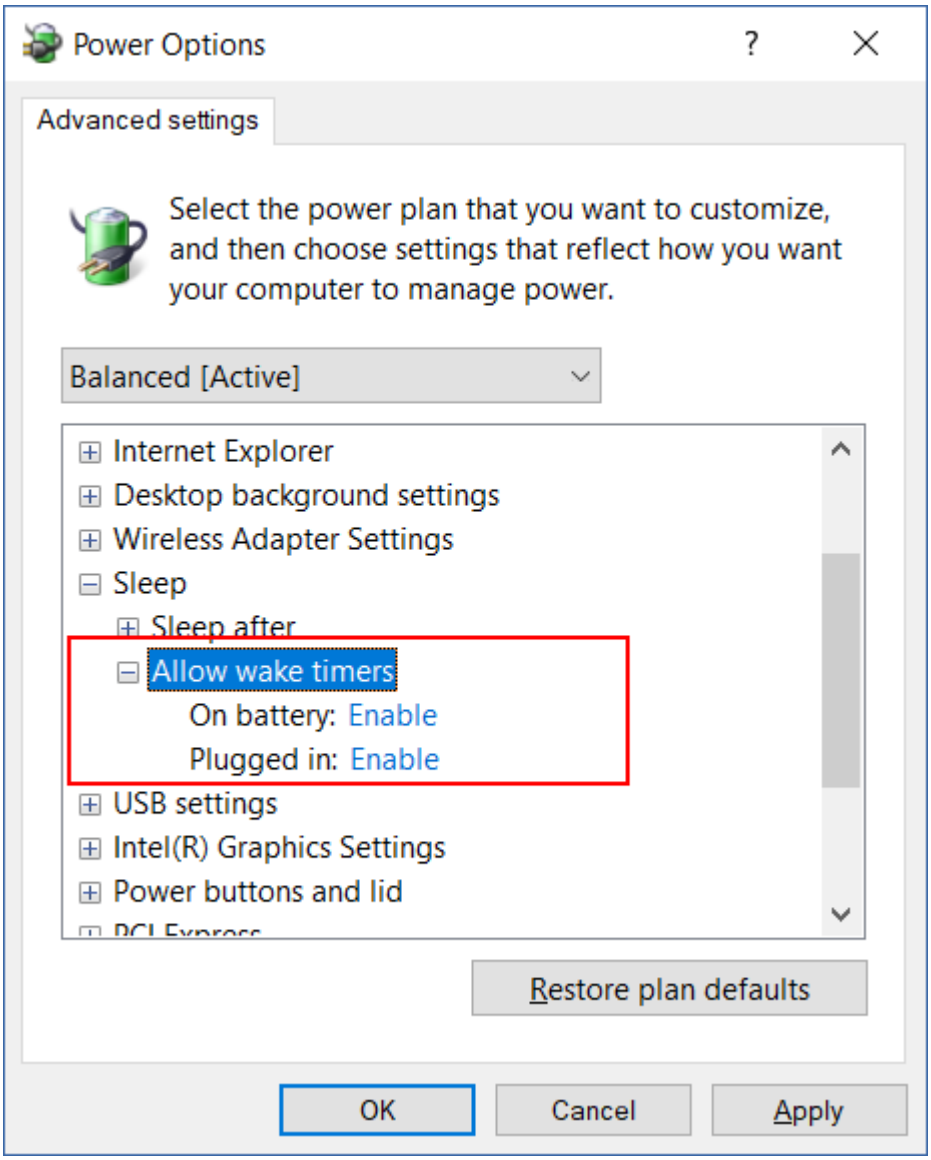
Opsi tambahan

Saat Anda menjadwalkan pencadangan berdasarkan waktu, opsi penjadwalan tambahan berikut akan tersedia.

Untuk mengaksesnya, di panel **Jadwal**, klik **Tampilkan lebih banyak**.

© Acronis International GmbH, 2003-2024

- **Jika mesin dimatikan, jalankan tugas yang tertinggal pada saat mesin dinyalakan**
  Pengaturan default: Dinonaktifkan.
- **Cegah mode tidur atau hibernasi selama pencadangan**
  Opsi ini hanya berlaku untuk mesin yang menjalankan Windows.
  Pengaturan default: Diaktifkan.
- **Bangun dari mode tidur atau hibernasi untuk memulai pencadangan terjadwal**
  Opsi ini hanya berlaku untuk mesin yang menjalankan Windows, dalam rencana daya yang mengaktifkan opsi **Izinkan penghitung waktu aktif**.



  Opsi ini tidak menggunakan fungsionalitas Wake-on-LAN dan tidak berlaku untuk mesin yang dimatikan.
  Pengaturan default: Dinonaktifkan.

© Acronis International GmbH, 2003-2024

Jadwalkan berdasarkan event

Untuk mengonfigurasi cadangan yang dijalankan pada peristiwa tertentu, pilih salah satu opsi berikut.

Opsi	Deskripsi	Contoh
Sejak waktu pencadangan terakhir	Pencadangan berjalan setelah jangka waktu tertentu setelah pencadangan terakhir berhasil. **Catatan** Opsi ini bergantung pada bagaimana pencadangan sebelumnya diselesaikan. Jika pencadangan gagal, pencadangan berikutnya tidak akan dimulai secara otomatis. Dalam hal ini, Anda harus menjalankan pencadangan secara manual dan memastikan pencadangan berhasil diselesaikan untuk dapat mengatur ulang jadwal.	Jalankan pencadangan satu hari setelah pencadangan terakhir berhasil. Jalankan pencadangan empat jam setelah pencadangan terakhir berhasil.
Ketika pengguna masuk ke sistem	Pencadangan berjalan saat pengguna masuk ke mesin. Anda dapat mengonfigurasi opsi ini untuk login apa pun atau untuk login pengguna tertentu. **Catatan** Masuk dengan profil pengguna sementara tidak akan memulai pencadangan.	Jalankan pencadangan saat pengguna John Doe login.
Ketika pengguna keluar dari sistem	Pencadangan dimulai saat pengguna keluar dari mesin. Anda dapat mengonfigurasi opsi ini untuk logoff apa pun atau logoff pengguna tertentu. **Catatan** Masuk dengan profil pengguna sementara tidak akan memulai pencadangan. Mematikan mesin tidak akan memulai pencadangan.	Jalankan pencadangan saat setiap pengguna logout.
Pada startup sistem	Pencadangan dijalankan saat mesin yang dilindungi dinyalakan.	Jalankan pencadangan saat pengguna memulai mesin.

© Acronis International GmbH, 2003-2024

Opsi	Deskripsi	Contoh
Pada sistem shutdown	Pencadangan dijalankan saat mesin yang dilindungi dimatikan.	Jalankan pencadangan saat pengguna mematikan mesin.
Pada event Windows Event Log	Pencadangan dijalankan pada peristiwa Windows yang Anda tentukan.	Jalankan pencadangan ketika peristiwa 7 dari kesalahan jenis dan disk sumber direkam di log Sistem Windows.

Ketersediaan opsi ini bergantung pada sumber pencadangan dan sistem operasi beban kerja yang dilindungi. Tabel di bawah ini merangkum opsi yang tersedia untuk Windows, Linux, dan macOS.

Event	Sumber cadangan (Apa yang harus dicadangkan)					
	Seluruh mesin, Disk/volume, atau File/folder (mesin fisik)	**Seluruh mesin atau Disk/volume (mesin virtual)**	**Konfigurasi ESXi**	**Kotak surat Microsoft 365**	**Database dan kotak surat Exchange**	**Database SQL**
Sejak waktu pencadangan terakhir	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Ketika pengguna masuk ke sistem	Windows	N/A	N/A	N/A	N/A	N/A
Ketika pengguna keluar dari sistem	Windows	N/A	N/A	N/A	N/A	N/A
Pada startup sistem	Windows, Linux, macOS	N/A	N/A	N/A	N/A	N/A
Pada sistem shutdown	Windows	N/A	N/A	N/A	N/A	N/A
Pada event Windows Event Log	Windows	N/A	N/A	Windows	Windows	Windows

Pada event Windows Event Log

Anda dapat menjalankan pencadangan secara otomatis ketika peristiwa tertentu dicatat dalam log Peristiwa Windows, seperti log Aplikasi, log Keamanan, atau log Sistem.

© Acronis International GmbH, 2003-2024

Catatan
Anda dapat menelusuri peristiwa dan melihat propertinya di **Manajemen Komputer** > **Event Viewer** di Windows. Untuk membuka log Keamanan, Anda memerlukan hak administrator.

Parameter peristiwa

Tabel berikut merangkum parameter yang harus Anda tentukan saat mengonfigurasi opsi **Pada event Windows Event Log**.

Parameter	Deskripsi
Nama log	Nama log. Pilih nama log standar (Aplikasi, Keamanan, Sistem) atau tentukan nama log lainnya. Misalnya, Sesi Microsoft Office.
Sumber peristiwa	Sumber peristiwa menunjukkan program atau komponen sistem yang menyebabkan peristiwa tersebut. Misalnya, disk. Sumber peristiwa apa pun yang berisi string teks tertentu akan memicu pencadangan terjadwal. Opsi ini tidak peka huruf besar-kecil. Misalnya, jika Anda menentukan `service`, sumber peristiwa Service Control Manager dan Time-Service akan memicu pencadangan.
Jenis event	Jenis peristiwa: Kesalahan, Peringatan, Informasi, Audit berhasil, atau Audit gagal.
ID peristiwa	ID peristiwa mengidentifikasi jenis peristiwa tertentu dalam sumber peristiwa. Misalnya, peristiwa Kesalahan dengan sumber peristiwa disk dan ID peristiwa 7 terjadi ketika Windows menemukan blok buruk pada disk, sedangkan peristiwa Kesalahan dengan sumber peristiwa disk dan ID peristiwa 15 terjadi ketika disk belum siap untuk diakses.

Contoh: Cadangan darurat jika terjadi blok buruk pada hard disk

Satu atau lebih blok buruk pada hard disk drive mungkin mengindikasikan kegagalan yang akan terjadi. Itu sebabnya Anda mungkin ingin membuat cadangan ketika blok buruk terdeteksi.

Ketika Windows mendeteksi blok buruk pada disk, peristiwa kesalahan dengan sumber peristiwa disk dan nomor peristiwa 7 dicatat ke log sistem. Dalam rencana proteksi, konfigurasikan jadwal berikut:

- Jadwal: Pada event Windows Event log
- Nama log: Sistem
- Sumber peristiwa: disk

© Acronis International GmbH, 2003-2024

- Jenis event: Eror
- ID peristiwa: 7

Penting
Untuk memastikan bahwa pencadangan selesai meskipun ada blok buruk, di **Opsi pencadangan**, buka **Penanganan kesalahan**, lalu pilih kotak centang **Abaikan sektor buruk**.

Persyaratan untuk memulai

Untuk membuat pencadangan hanya berjalan jika kondisi tertentu terpenuhi, konfigurasikan satu atau beberapa kondisi awal. Jika Anda mengonfigurasi beberapa ketentuan, semuanya harus dipenuhi secara bersamaan agar pencadangan dapat dimulai. Anda dapat menentukan jangka waktu kapan pencadangan akan dijalankan, terlepas dari apakah kondisinya terpenuhi atau tidak. Untuk informasi lebih lanjut tentang opsi pencadangan ini, lihat "Syarat mulai tugas" (hlm. 490).

Kondisi awal tidak berlaku saat Anda memulai pencadangan secara manual.

Tabel di bawah ini berisi syarat awal yang tersedia untuk berbagai data di Windows, Linux, dan macOS.

Kondisi awal	Sumber cadangan (Apa yang harus dicadangkan)					
	Seluruh mesin, Disk/volume, atau File/folder (mesin fisik)	**Seluruh mesin atau Disk/volume (mesin virtual)**	**Konfigurasi ESXi**	**Kotak surat Microsoft 365**	**Database dan kotak surat Exchange**	**Database SQL**
Pengguna idle	Windows	N/A	N/A	N/A	N/A	N/A
Host lokasi cadangan tersedia	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Pengguna telah keluar	Windows	N/A	N/A	N/A	N/A	N/A
Sesuai interval waktu	Windows, Linux, macOS	Windows, Linux	N/A	N/A	N/A	N/A
Hemat daya baterai	Windows	N/A	N/A	N/A	N/A	N/A
Jangan dimulai	Windows	N/A	N/A	N/A	N/A	N/A

© Acronis International GmbH, 2003-2024

Kondisi awal	Sumber cadangan (Apa yang harus dicadangkan)					
	Seluruh mesin, Disk/volume, atau File/folder (mesin fisik)	**Seluruh mesin atau Disk/volume (mesin virtual)**	**Konfigurasi ESXi**	**Kotak surat Microsoft 365**	**Database dan kotak surat Exchange**	**Database SQL**
ketika memakai koneksi bermeter						
Jangan dimulai ketika terkoneksi ke jaringan Wi-Fi berikut	Windows	N/A	N/A	N/A	N/A	N/A
Cek alamat IP perangkat	Windows	N/A	N/A	N/A	N/A	N/A

Pengguna idle

"Pengguna idle" berarti bahwa screen saver berjalan di mesin atau mesin terkunci.

Contoh

Jalankan pencadangan setiap hari pada pukul 21.00, sebaiknya saat pengguna sedang menganggur. Jika pengguna masih aktif pada pukul 23.00, tetap jalankan pencadangan.

- Jadwal: **Harian**, **Jalankan setiap hari**. Mulai pada: **21.00**.
- Syarat: **Pengguna idle**.
- Syarat mulai pencadangan: **Tunggu hingga kondisi terpenuhi**, **Mulai saja pencadangan setelah 2** jam.

Hasilnya:

- Jika pengguna menganggur sebelum pukul 21.00, pencadangan dimulai pada pukul 21.00.
- Jika pengguna menganggur antara pukul 21.00 hingga 23.00, pencadangan akan segera dimulai.
- Jika pengguna masih aktif pada pukul 23.00, pencadangan dimulai pada pukul 23.00.

© Acronis International GmbH, 2003-2024

Host lokasi cadangan tersedia

"Host lokasi cadangan tersedia" berarti mesin yang menjadi host lokasi pencadangan tersedia melalui jaringan.

Kondisi ini berlaku untuk folder jaringan, penyimpanan cloud, dan lokasi yang dikelola oleh simpul penyimpanan.

Kondisi ini tidak mencakup ketersediaan lokasi itu sendiri—hanya ketersediaan host. Misalnya, jika host tersedia, namun folder jaringan pada host ini tidak dibagikan atau kredensial untuk folder ini sudah tidak valid, syarat masih dianggap terpenuhi.

Contoh

Anda menjalankan pencadangan ke folder jaringan setiap hari kerja pada pukul 21.00. Jika mesin yang menjadi host folder tersebut tidak tersedia pada saat itu (misalnya, karena pemeliharaan), Anda perlu melewati pencadangan dan menunggu jadwal mulai pada hari kerja berikutnya.

- Jadwal: **Harian**, **Jalankan Senin hingga Jumat**. Mulai pada: **21.00**.
- Syarat: **Host lokasi cadangan tersedia**.
- Syarat mulai pencadangan: **Lewati jadwal pencadangan**.

Hasilnya:

- Jika host tersedia pada pukul 21.00, pencadangan akan segera dimulai.
- Jika host tidak tersedia pada pukul 21.00, pencadangan dimulai pada hari kerja berikutnya (jika host tersedia pada pukul 21.00 pada hari itu).
- Jika host tidak pernah tersedia pada hari kerja pukul 21.00, pencadangan tidak akan pernah dimulai.

Pengguna telah keluar

Gunakan kondisi awal ini untuk menunda pencadangan hingga semua pengguna logout dari mesin Windows.

Contoh

Anda menjalankan pencadangan setiap hari Jumat pukul 20.00, sebaiknya saat semua pengguna logout. Jika salah satu pengguna masih login pada pukul 23.00, tetap jalankan pencadangan.

- Jadwal: **Mingguan**, pada hari Jumat. Mulai pada: **20.00**.
- Syarat: **Pengguna telah keluar**.
- Syarat mulai pencadangan: **Tunggu hingga kondisi terpenuhi**, **Tetap mulai pencadangan setelah 3** jam.

Hasilnya:

© Acronis International GmbH, 2003-2024

- Jika semua pengguna logout pada pukul 20.00, pencadangan dimulai pada pukul 20.00.
- Jika pengguna terakhir logout antara pukul 20.00 dan 23.00, pencadangan akan segera dimulai.
- Jika masih ada pengguna yang masuk pada pukul 23.00, pencadangan dimulai pada pukul 23.00.

Sesuai interval waktu

Gunakan kondisi awal ini untuk membatasi permulaan pencadangan pada interval tertentu.

Contoh

Perusahaan mencadangkan data pengguna dan server ke lokasi berbeda pada penyimpanan yang terhubung ke jaringan yang sama.

Hari kerja dimulai pada pukul 08.00 dan berakhir pada pukul 17.00. Data pengguna harus dicadangkan segera setelah pengguna logout, tetapi tidak lebih awal dari pukul 16.30.

Server perusahaan dicadangkan setiap hari pada pukul 23.00. Data pengguna sebaiknya dicadangkan sebelum pukul 23.00, untuk mengosongkan bandwidth jaringan untuk pencadangan server.

Mencadangkan data pengguna tidak lebih dari satu jam, jadi waktu mulai pencadangan terakhir adalah pukul 22.00. Jika pengguna masih login dalam interval waktu yang ditentukan, atau logout di waktu lain, pencadangan data pengguna harus dilewati.

- Event: **Ketika pengguna keluar dari sistem**. Tentukan akun pengguna: **Pengguna mana pun**.
- Syarat: **Sesuai dengan interval waktu** dari **16.30** hingga **22.00**.
- Syarat mulai pencadangan: **Lewati jadwal pencadangan**.

Hasilnya:

- Jika pengguna logout antara pukul 16.30 dan 22.00, pencadangan akan segera dimulai.
- Jika pengguna logout pada waktu lain, pencadangan akan dilewati.

Hemat daya baterai

Gunakan kondisi awal ini untuk mencegah pencadangan jika mesin (misalnya, laptop atau tablet) tidak tersambung ke sumber listrik. Tergantung pada nilai opsi Kondisi awal pencadangan, pencadangan yang dilewati akan atau tidak akan dimulai setelah mesin terhubung ke sumber listrik.

Opsi berikut tersedia:

- **Jangan dimulai ketika memakai daya baterai**
  Pencadangan akan dimulai hanya jika mesin terhubung ke sumber listrik.
- **Mulai ketika memakai daya baterai jika level baterai lebih tinggi dari**
  Pencadangan akan dimulai jika mesin tersambung ke sumber listrik atau jika level baterai lebih tinggi dari nilai yang ditentukan.

© Acronis International GmbH, 2003-2024

Contoh

Anda mencadangkan data Anda setiap hari kerja pada pukul 21.00. Jika mesin Anda tidak terhubung ke sumber listrik, Anda ingin melewatkan pencadangan untuk menghemat daya baterai dan menunggu hingga Anda menghubungkan mesin ke sumber listrik.

- Jadwal: **Harian**, **Jalankan Senin hingga Jumat**. Mulai pada: **21.00**.
- Syarat: **Hemat daya baterai**, **Jangan dimulai ketika memakai daya baterai**.
- Syarat mulai pencadangan: **Tunggu sampai syarat terpenuhi**.

Hasilnya:

- Jika mesin terhubung ke sumber listrik pada pukul 21.00, pencadangan akan segera dimulai.
- Jika mesin berjalan dengan daya baterai pada pukul 21.00, pencadangan dimulai saat Anda menyambungkan mesin ke sumber listrik.

Jangan dimulai ketika memakai koneksi bermeter

Gunakan kondisi awal ini untuk mencegah pencadangan (termasuk pencadangan ke disk lokal) jika mesin tersambung ke Internet melalui koneksi yang diatur sebagai koneksi bermeter di Windows. Untuk informasi lebih lanjut tentang koneksi bermeter di Windows, lihat https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

Kondisi awal tambahan **Jangan dimulai ketika terkoneksi ke jaringan Wi-Fi berikut** secara otomatis diaktifkan saat Anda mengaktifkan kondisi **Jangan dimulai ketika memakai koneksi bermeter**. Ini adalah tindakan tambahan untuk mencegah pencadangan melalui hotspot seluler. Nama jaringan berikut ditentukan secara default: android, telepon, ponsel, dan modem.

Untuk menghapus nama-nama ini dari daftar, klik tanda X. Untuk menambahkan nama baru, ketikkan di kolom kosong.

Contoh

Anda mencadangkan data Anda setiap hari kerja pada pukul 21.00. Jika mesin terhubung ke Internet menggunakan koneksi bermeter, Anda perlu melewati pencadangan untuk menghemat lalu lintas jaringan dan menunggu jadwal mulai pada hari kerja berikutnya.

- Jadwal: **Harian**, **Jalankan Senin hingga Jumat**. Mulai pada: **21.00**.
- Syarat: **Jangan dimulai ketika memakai koneksi bermeter**.
- Syarat mulai pencadangan: **Lewati jadwal pencadangan**.

Hasilnya:

- Pada pukul 21.00, jika mesin tidak tersambung ke Internet melalui koneksi bermeter, pencadangan akan segera dimulai.
- Pada pukul 21.00, jika mesin terhubung ke Internet melalui koneksi bermeter, pencadangan dimulai pada hari kerja berikutnya.

© Acronis International GmbH, 2003-2024

- Jika mesin selalu terhubung ke Internet melalui koneksi bermeter pada hari kerja pukul 21.00, pencadangan tidak akan pernah dimulai.

Jangan dimulai ketika terkoneksi ke jaringan Wi-Fi berikut

Gunakan kondisi awal ini untuk mencegah pencadangan (termasuk pencadangan ke disk lokal) jika mesin terhubung ke salah satu jaringan nirkabel yang ditentukan (misalnya, jika Anda ingin membatasi pencadangan melalui hotspot ponsel).

Anda dapat menentukan nama jaringan Wi-Fi, disebut juga sebagai service set identifier (SSID). Pembatasan ini berlaku untuk semua jaringan yang berisi nama tertentu sebagai substring dalam namanya, tidak peka huruf besar-kecil. Misalnya, jika Anda menentukan `phone` sebagai nama jaringan, pencadangan tidak akan dimulai ketika mesin terhubung ke salah satu jaringan berikut: `John's iPhone`, `phone_wifi`, atau `my_PHONE_wifi`.

Kondisi awal **Jangan dimulai ketika terkoneksi ke Wi-Fi berikut** diaktifkan secara otomatis saat Anda mengaktifkan kondisi **Jangan dimulai ketika memakai koneksi bermeter**. Nama jaringan berikut ditentukan secara default: android, `telepon`, `ponsel`, dan modem.

Untuk menghapus nama-nama ini dari daftar, klik tanda X. Untuk menambahkan nama baru, ketikkan di kolom kosong.

Contoh

Anda mencadangkan data Anda setiap hari kerja pada pukul 21.00. Jika mesin terhubung ke Internet melalui hotspot seluler, Anda perlu melewati pencadangan dan menunggu jadwal mulai pada hari kerja berikutnya.

- Jadwal: **Harian**, **Jalankan Senin hingga Jumat**. Mulai pada: **21.00**.
- Syarat: **Jangan dimulai ketika terhubung ke jaringan berikut**, **Nama jaringan**: `<SSID jaringan hotspot>`.
- Syarat mulai pencadangan: **Lewati jadwal pencadangan**.

Hasilnya:

- Jika mesin tidak terhubung ke jaringan yang ditentukan pada pukul 21.00, pencadangan akan segera dimulai.
- Jika mesin terhubung ke jaringan yang ditentukan pada pukul 21.00, pencadangan dimulai pada hari kerja berikutnya.
- Jika mesin selalu terhubung ke jaringan yang ditentukan pada hari kerja pukul 21.00, pencadangan tidak akan pernah dimulai.

Cek alamat IP perangkat

Gunakan kondisi awal ini untuk mencegah pencadangan (termasuk pencadangan ke disk lokal) jika salah satu alamat IP mesin berada di dalam atau di luar rentang alamat IP yang ditentukan. Jadi, misalnya, Anda dapat menghindari biaya transit data yang besar saat mencadangkan mesin

© Acronis International GmbH, 2003-2024

pengguna yang berada di luar negeri, atau Anda dapat mencegah pencadangan melalui koneksi Jaringan Privat Virtual (VPN).

Opsi berikut tersedia:

- **Mulai jika di luar rentang IP**
- **Mulai jika di dalam rentang IP**

Dengan opsi tersebut, Anda dapat menentukan beberapa nilai rentang. Hanya mendukung alamat IPv4.

Contoh

Anda mencadangkan data Anda setiap hari kerja pada pukul 21.00. Jika mesin terhubung ke jaringan perusahaan menggunakan terowongan VPN, Anda ingin melewati pencadangan.

- Jadwal: **Harian**, **Jalankan Senin hingga Jumat**. Mulai pukul **21.00**.
- Syarat: **Cek alamat IP perangkat**, **Mulai jika di luar rentang IP**, **Dari**: `<awal dari rentang alamat IP VPN>`, **Hingga**: `<akhir dari rentang alamat IP VPN>`.
- Syarat mulai pencadangan: **Tunggu sampai syarat terpenuhi**.

Hasilnya:

- Jika alamat IP mesin tidak berada dalam kisaran yang ditentukan pada pukul 21.00, pencadangan akan segera dimulai.
- Jika alamat IP mesin berada dalam kisaran yang ditentukan pada pukul 21.00, pencadangan dimulai ketika mesin memperoleh alamat IP non-VPN.
- Jika alamat IP mesin selalu berada dalam kisaran yang ditentukan pada hari kerja pukul 21.00, pencadangan tidak akan pernah dimulai.

Opsi penjadwalan tambahan

Anda dapat mengonfigurasi pencadangan agar dijalankan hanya jika kondisi tertentu terpenuhi, dijalankan hanya selama jangka waktu tertentu, atau dijalankan dengan penundaan dibandingkan jadwal.

Untuk mengonfigurasi kondisi awal

1. Dalam rencana proteksi, perbesar modul **Cadangan**.
2. Klik **Jadwal**.
3. Pada panel **Jadwal**, klik **Tampilkan lebih banyak**.
4. Pilih kotak centang di samping kondisi awal yang ingin Anda sertakan, lalu klik **Selesai**.
   Untuk informasi lebih lanjut tentang kondisi awal yang tersedia dan cara mengonfigurasinya, lihat "Persyaratan untuk memulai" (hlm. 426).
5. Simpan rencana proteksi.

Untuk mengonfigurasi rentang waktu

© Acronis International GmbH, 2003-2024

1. Dalam rencana proteksi, perbesar modul **Cadangan**.
2. Klik **Jadwal**.
3. Pilih kotak centang **Jalankan rencana dalam rentang tanggal**.
4. Tentukan jangka waktunya sesuai kebutuhan Anda, lalu klik **Selesai**.
5. Simpan rencana proteksi.

Akibatnya, pencadangan hanya akan berjalan selama jangka waktu yang ditentukan.

Untuk mengkonfigurasi penundaan

Untuk menghindari beban jaringan yang berlebihan saat Anda mencadangkan beberapa beban kerja di lokasi jaringan, penundaan acak singkat akan dikonfigurasi sebagai opsi pencadangan. Anda dapat menonaktifkannya atau mengubah pengaturannya.

1. Dalam rencana proteksi, perbesar modul **Cadangan**.
2. Klik **Opsi pencadangan**, lalu pilih **Penjadwalan**.
   Nilai penundaan untuk setiap beban kerja dipilih secara acak antara nol dan nilai maksimum yang Anda tentukan. Secara default, nilai maksimumnya adalah 30 menit.
   Untuk informasi lebih lanjut tentang opsi pencadangan ini, lihat "Penjadwalan" (hlm. 488)
   Nilai penundaan untuk setiap beban kerja dihitung saat Anda menerapkan rencana proteksi pada beban kerja tersebut, dan tetap sama hingga Anda mengedit nilai penundaan maksimum.
3. Tentukan jangka waktunya sesuai kebutuhan Anda, lalu klik **Selesai**.
4. Simpan rencana proteksi.

Menjalankan pencadangan secara manual

Anda dapat menjalankan pencadangan terjadwal dan tidak terjadwal secara manual.

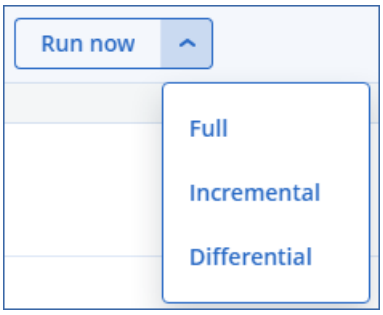
Untuk menjalankan pencadangan secara manual

1. Di konsol Cyber Protect, buka **Perangkat**.
2. Pilih beban kerja yang ingin Anda jalankan pencadangannya, lalu klik **Protect**.
3. Pilih rencana proteksi yang ingin Anda buat cadangannya.
   Jika tidak ada rencana proteksi yang diterapkan pada beban kerja, terapkan rencana yang sudah ada atau buat rencana baru.
   Untuk informasi selengkapnya tentang cara membuat rencana proteksi, lihat "Membuat rencana proteksi" (hlm. 214).
4. [Untuk membuat jenis cadangan default] Dalam rencana proteksi, klik ikon **Jalankan sekarang**.

© Acronis International GmbH, 2003-2024

Alternatifnya, dalam rencana proteksi, perluas modul **Cadangan**, lalu klik tombol **Jalankan sekarang**.

5. [Untuk membuat jenis cadangan tertentu] Dalam rencana proteksi, perluas modul **Cadangan**, klik panah di sebelah tombol **Jalankan sekarang**, lalu pilih jenis cadangan.



Catatan
Memilih jenis tidak tersedia untuk skema pencadangan yang hanya menggunakan satu metode pencadangan, misalnya, **Selalu inkremental (file tunggal)** atau **Selalu penuh**.

Akibatnya, operasi pencadangan dimulai. Anda dapat memeriksa kemajuannya dan hasilnya di tab **Perangkat**, di kolom **Status**.

Aturan retensi

Untuk menghapus cadangan lama secara otomatis, konfigurasikan aturan retensi cadangan dalam rencana proteksi.

Anda dapat mendasarkan aturan retensi pada salah satu properti cadangan berikut:

- Nomor
- Usia
- Ukuran

Aturan retensi yang tersedia dan pilihannya bergantung pada skema pencadangan. Aturan ini juga relevan terhadap agen, beban kerja, dan cloud untuk cadangan cloud. Untuk informasi lebih lanjut, lihat "Aturan retensi sesuai dengan skema pencadangan" (hlm. 435).

Anda dapat menonaktifkan pembersihan otomatis cadangan lama dengan memilih opsi **Menyimpan cadangan tanpa batas** saat mengonfigurasi aturan retensi. Hal ini mungkin mengakibatkan peningkatan penggunaan penyimpanan, dan Anda harus menghapus cadangan lama yang tidak diperlukan secara manual.

© Acronis International GmbH, 2003-2024

Kiat penting

- Aturan retensi adalah bagian dari rencana perlindungan. Jika Anda mencabut atau menghapus suatu rencana, aturan retensi dalam rencana tersebut tidak akan diterapkan lagi. Untuk informasi lebih lanjut tentang cara menghapus cadangan yang tidak lagi Anda perlukan, lihat "Menghapus beberapa cadangan" (hlm. 532).
- Jika, sesuai dengan skema pencadangan dan format pencadangan, setiap cadangan disimpan sebagai file terpisah, Anda tidak dapat menghapus cadangan yang menjadi dependen cadangan tambahan atau diferensial lainnya. Cadangan ini akan dihapus sesuai dengan aturan penyimpanan yang diterapkan pada cadangan dependen. Konfigurasi ini dapat mengakibatkan peningkatan penggunaan penyimpanan karena penghapusan beberapa cadangan ditunda. Selain itu, usia, jumlah, atau ukuran cadangan mungkin melebihi nilai yang Anda tentukan. Untuk informasi selengkapnya tentang cara mengubah perilaku ini, lihat"Konsolidasi cadangan" (hlm. 449).
- Secara default, cadangan terbaru yang dibuat oleh rencana proteksi tidak pernah dihapus. Namun, jika Anda mengonfigurasi aturan retensi untuk membersihkan cadangan sebelum memulai operasi pencadangan baru, dan mengatur jumlah cadangan agar tetap nol, cadangan terbaru juga akan dihapus.

Peringatan!
Jika Anda menerapkan aturan retensi ini ke kumpulan cadangan dengan satu cadangan, dan operasi pencadangan gagal, Anda tidak akan dapat memulihkan data, karena cadangan yang ada akan dihapus sebelum cadangan baru dibuat.

Aturan retensi sesuai dengan skema pencadangan

Aturan retensi yang tersedia dan pengaturannya bergantung pada skema pencadangan yang Anda gunakan dalam rencana proteksi. Untuk informasi lebih lanjut tentang skema pencadangan, lihat "Skema cadangan" (hlm. 417).

Tabel berikut merangkum aturan retensi yang tersedia dan pengaturannya.

Skema cadangan	Jadwal	Aturan dan pengaturan retensi yang tersedia
Selalu inkremental (file tunggal)	Bulanan Mingguan Harian Per jam Pencadangan yang dipicu oleh peristiwa	Berdasarkan jumlah cadangan Berdasarkan usia pencadangan (pengaturan terpisah untuk pencadangan bulanan, mingguan, harian, dan per jam) Simpan cadangan tanpa batas
Selalu penuh	Bulanan Mingguan	Berdasarkan jumlah cadangan Berdasarkan usia pencadangan (pengaturan

© Acronis International GmbH, 2003-2024

Skema cadangan	Jadwal	Aturan dan pengaturan retensi yang tersedia
	Harian Per jam Pencadangan yang dipicu oleh peristiwa	terpisah untuk pencadangan bulanan, mingguan, harian, dan per jam) Berdasarkan ukuran total cadangan Simpan cadangan tanpa batas
Mingguan penuh, kenaikan Harian	Harian Pencadangan yang dipicu oleh peristiwa	Berdasarkan jumlah cadangan Berdasarkan usia pencadangan (pengaturan terpisah untuk pencadangan mingguan dan harian) Berdasarkan ukuran total cadangan Simpan cadangan tanpa batas
Bulanan lengkap, Mingguan diferensial, harian inkremental	Bulanan Mingguan Harian Per jam Pencadangan yang dipicu oleh peristiwa	Berdasarkan jumlah cadangan Berdasarkan usia pencadangan (pengaturan terpisah untuk pencadangan penuh, diferensial, dan tambahan) Berdasarkan ukuran total cadangan Simpan cadangan tanpa batas
Kustom	Bulanan Mingguan Harian Per jam Pencadangan yang dipicu oleh peristiwa	Berdasarkan jumlah cadangan Berdasarkan usia pencadangan (pengaturan terpisah untuk pencadangan penuh, diferensial, dan tambahan) Berdasarkan ukuran total cadangan Simpan cadangan tanpa batas

Mengapa ada cadangan bulanan dengan skema per jam?

Tergantung pada skema pencadangan, Anda dapat mengonfigurasi opsi **Berdasarkan umur cadangan** untuk salah satu pencadangan berikut:

- Pencadangan bulanan, mingguan, harian, dan setiap jam.

  Pengaturan ini tersedia dengan semua skema pencadangan non-kustom, dan didasarkan pada waktu. Semua pencadangan ini (bulanan, mingguan, harian, dan setiap jam) tersedia, bahkan jika Anda mengonfigurasi pencadangan untuk dijalankan setiap jam. Lihat contoh di bawah ini.

Cadangan	Deskripsi
Bulanan	Cadangan bulanan adalah cadangan pertama setiap bulan.
Mingguan	Pencadangan mingguan adalah pencadangan pertama pada hari dalam

© Acronis International GmbH, 2003-2024

Cadangan	Deskripsi
	seminggu yang Anda tentukan di opsi Cadangan mingguan. Hari ini dianggap sebagai awal minggu menurut aturan retensi. Jika pencadangan mingguan juga merupakan pencadangan pertama pada bulan tersebut, maka pencadangan tersebut dianggap sebagai pencadangan bulanan. Dalam hal ini, cadangan mingguan dibuat pada hari yang dipilih pada minggu berikutnya.
Harian	Pencadangan harian adalah pencadangan pertama pada satu hari, kecuali jika pencadangan ini termasuk dalam definisi pencadangan bulanan atau mingguan. Dalam hal ini, cadangan harian dibuat pada hari berikutnya.
Per jam	Pencadangan setiap jam adalah pencadangan pertama pada jam tersebut, kecuali jika pencadangan ini termasuk dalam definisi pencadangan bulanan, mingguan, atau harian. Dalam hal ini, cadangan setiap jam dibuat pada jam berikutnya.

- Pencadangan penuh, diferensial, dan tambahan.

  Pengaturan ini tersedia untuk skema pencadangan **Kustom**, dan didasarkan pada metode pencadangan. **Penuh bulanan, Diferensial mingguan, Tambahan harian** adalah skema kustom yang telah dikonfigurasi sebelumnya.

Contoh

Anda menggunakan skema pencadangan **Selalu inkremental (file tunggal)** dengan pengaturan default untuk pencadangan setiap jam:

- Dijadwalkan berdasarkan waktu.
- Pencadangan dijalankan setiap jam: Senin sampai Jumat, setiap 1 jam, mulai pukul 08.00 hingga 18.00.
- Opsi **Pencadangan mingguan** diatur ke hari Senin.

Di bagian **Berapa lama akan disimpan** pada rencana perlindungan, Anda dapat menerapkan aturan retensi pada pencadangan bulanan, mingguan, harian, dan per jam.

Tabel berikut merangkum jenis cadangan yang dibuat selama periode 8 hari.

Tanggal	Hari dalam seminggu	Deskripsi
1 Juli	Senin	Pencadangan pertama setiap bulan adalah pencadangan bulanan, jadi pencadangan pertama hari ini adalah pencadangan bulanan. Cadangan lainnya pada siang hari dilakukan setiap jam. Minggu ini, pencadangan pertama dianggap sebagai pencadangan bulanan. Itu sebabnya tidak ada cadangan

© Acronis International GmbH, 2003-2024

Tanggal	Hari dalam seminggu	Deskripsi
		mingguan. Cadangan pertama minggu depan akan menjadi cadangan mingguan.
2 Juli	Selasa	Pencadangan pertama dilakukan setiap hari, pencadangan lainnya pada siang hari dilakukan setiap jam.
3 Juli	Rabu	Pencadangan pertama dilakukan setiap hari, pencadangan lainnya pada siang hari dilakukan setiap jam.
4 Juli	Kamis	Pencadangan pertama dilakukan setiap hari, pencadangan lainnya pada siang hari dilakukan setiap jam.
5 Juli	Jumat	Pencadangan pertama dilakukan setiap hari, pencadangan lainnya pada siang hari dilakukan setiap jam.
6 Juli	Sabtu	Pencadangan pertama dilakukan setiap hari, pencadangan lainnya pada siang hari dilakukan setiap jam.
7 Juli	Minggu	Pencadangan pertama dilakukan setiap hari, pencadangan lainnya pada siang hari dilakukan setiap jam.
8 Juli	Senin	Pencadangan pertama dilakukan setiap minggu, pencadangan lainnya pada siang hari dilakukan setiap jam.

Mengonfigurasi aturan retensi

Aturan retensi adalah bagian dari rencana proteksi, dan ketersediaan serta opsinya bergantung pada skema pencadangan. Untuk informasi lebih lanjut, lihat "Aturan retensi sesuai dengan skema pencadangan" (hlm. 435).

Untuk mengonfigurasi aturan retensi

1. Dalam rencana proteksi, perbesar modul **Cadangan**.
2. Klik **Berapa banyak akan disimpan**.
3. Pilih salah satu opsi berikut:
   - **Berdasarkan jumlah cadangan**
   - **Berdasarkan usia cadangan**

     Tersedia pengaturan terpisah untuk pencadangan bulanan, mingguan, harian, dan per jam. Nilai maksimum untuk semua tipe adalah 9999.

     Anda juga dapat menggunakan satu pengaturan untuk semua cadangan.
   - **Berdasarkan ukuran total cadangan**

     Pengaturan ini tidak tersedia dengan skema pencadangan **Selalu inkremental (file tunggal)**.
   - **Simpan cadangan tanpa batas**

© Acronis International GmbH, 2003-2024

4. [Jika Anda tidak memilih **Simpan cadangan tanpa batas**] Konfigurasikan nilai untuk opsi yang dipilih.
5. [Jika Anda tidak memilih **Simpan cadangan tanpa batas**] Pilih kapan aturan retensi diterapkan:
   - Setelah pencadangan
   - Sebelum pencadangan

     Opsi ini tidak tersedia saat mencadangkan klaster Microsoft SQL Server atau klaster Microsoft Exchange Server.
6. Klik **Selesai**.
7. Simpan rencana proteksi.

Replikasi

Dengan replikasi, setiap cadangan baru disalin secara otomatis ke lokasi replikasi. Cadangan di lokasi replikasi tidak bergantung pada cadangan yang berada di lokasi sumber dan sebaliknya.

Hanya cadangan terakhir dalam lokasi sumber yang direplikasi. Namun, apabila cadangan sebelumnya tidak direplikasi (misalnya, karena masalah koneksi jaringan). operasi replikasi akan menyertakan semua cadangan yang dibuat setelah replikasi yang berhasil dilakukan terakhir kali.

Jika operasi replikasi terganggu, data yang diproses akan digunakan oleh operasi replikasi selanjutnya.

Catatan
Topik ini menjelaskan replikasi sebagai bagian dari rencana proteksi. Anda juga dapat membuat rencana replikasi cadangan terpisah. Untuk informasi lebih lanjut, lihat "Replikasi cadangan" (hlm. 198).

Contoh penggunaan

- Memastikan pemulihan yang dapat diandalkan

  Simpan cadangan Anda baik di situs (untuk pemulihan cepat) dan di luar situs (untuk mengamankan cadangan dari kegagalan penyimpanan atau bencana alam yang memengaruhi lokasi utama).
- Menggunakan penyimpanan awan untuk melindungi data dari bencana alam

  Mereplikasi cadangan ke penyimpanan awan dengan hanya mentransfer perubahan data.
- Hanya menyimpan titik pemulihan terbaru

  Konfigurasi aturan retensi untuk menghapus cadangan lama dari penyimpanan cepat, untuk menghemat biaya penyimpanan.

© Acronis International GmbH, 2003-2024

Lokasi yang didukung

Lokasi	Sebagai lokasi sumber	Sebagai lokasi replikasi
Folder lokal	+	+
Folder jaringan	+	+
Penyimpanan awan	-	+
Secure Zone	+	–
Cloud publik	+	+

Untuk mengaktifkan replikasi

1. Dalam rencana proteksi, perbesar modul **Cadangan**, kemudian klik **Tambah lokasi**.

   Catatan
   Opsi **Tambah lokasi** tidak tersedia ketika Anda memilih penyimpanan cloud di **Tempat menyimpan cadangan**.

2. Dari daftar lokasi yang tersedia, pilih lokasi replikasi.
   Lokasi tersebut muncul dalam rencana proteksi sebagai **lokasi ke-2**, **lokasi ke-3**, **lokasi ke-4**, atau **lokasi ke-5**, bergantung pada jumlah lokasi yang ditambahkan untuk replikasi.
3. [Opsional] Klik pada ikon roda untuk mengonfigurasi opsi untuk lokasi replikasi.
   - **Pengaturan kinerja dan cadangan jendela** – atur jendela pencadangan untuk lokasi yang dipilih, seperti dijelaskan dalam "Pengaturan kinerja dan cadangan jendela" (hlm. 478). Pengaturan ini menentukan performa replikasi.
   - **Hapus lokasi** – hapus lokasi replikasi yang dipilih saat ini.
   - [Hanya untuk penyimpanan cloud] **Pengiriman Data Fisik** – menyimpan cadangan awal pada perangkat penyimpanan yang dapat dilepas dan mengirimnya untuk diunggah ke cloud, alih-alih mereplikasinya di Internet.
     Opsi ini cocok untuk lokasi dengan koneksi jaringan yang lambat atau saat Anda ingin menghemat bandwidth pada pengiriman file besar melalui jaringan. Mengaktifkan opsi tersebut tidak memerlukan kuota layanan Cyber Protect lanjutan, tapi Anda akan membutuhkan kuota layanan Pengiriman Data Fisik untuk membuat pesanan pengiriman dan melacaknya. Lihat "Pengiriman Data Fisik" (hlm. 482).

     Catatan
     Opsi ini didukung dengan versi agen proteksi dari rilis C21.06 atau versi yang lebih baru.

4. [Opsional] Pada baris **Jumlah yang akan disimpan** di bawah lokasi replikasi, konfigurasikan aturan retensi untuk lokasi tersebut, seperti yang dijelaskan dalam "Aturan retensi" (hlm. 434).
5. [Opsional] Ulangi langkah 1 – 4 untuk menambahkan lebih banyak lokasi replikasi.

© Acronis International GmbH, 2003-2024

Anda dapat mengonfigurasi hingga empat lokasi replikasi (**lokasi ke-2**, **lokasi ke-3**, **lokasi ke-4**, dan **lokasi ke-5**). Jika Anda memiliih **Penyimpanan cloud**, Anda tidak dapat menambah lagi lokasi replikasi.

Penting
Jika Anda mengaktifkan cadangan dan replikasi dalam rencana proteksi yang sama, pastikan bahwa replikasi selesai sebelum pencadangan terjadwal berikutnya. Jika replikasi masih berlangsung, pencadangan terjadwal tidak akan dimulai—misalnya, pencadangan terjadwal yang berjalan setiap 24 jam sekali tidak akan dimulai jika replikasi membutuhkan waktu 26 jam untuk diselesaikan.

Untuk menghindari dependensi ini, gunakan rencana terpisah untuk replikasi cadangan. Untuk informasi lebih lanjut tentang paket khusus ini, lihat "Replikasi cadangan" (hlm. 198).

Enkripsi

Standar Enkripsi Lanjutan (AES) algoritme kriptografi beroperasi dalam mode Galois/Counter (GCM) dan menggunakan kunci acak 256-bit. Kode enkripsi kemudian dienkripsi dengan algoritme AES-256 dengan menggunakan hash SHA-2 (256-bit) dari kata sandi sebagai kunci. Kata sandi itu sendiri tidak disimpan di mana pun di disk atau dalam cadangan, dan hash kata sandi digunakan untuk verifikasi.

Dengan keamanan dua level ini, data cadangan terlindungi dari akses yang tidak sah, tetapi Anda tidak dimungkinkan untuk memulihkan kata sandi yang hilang.

Catatan
Menggunakan algoritma AES-256 dengan kata sandi yang kuat memberikan enkripsi yang tahan terhadap kuantum. Ini aman terhadap serangan analisis kriptografi yang mengandalkan komputasi kuantum.

Kami menyarankan Anda untuk mengenkripsi semua cadangan yang disimpan dalam penyimpanan awan, terutama jika perusahaan tunduk pada kepatuhan peraturan.

Anda dapat mengonfigurasi enkripsi dengan cara berikut:

- Dalam rencana proteksi
- Sebagai properti mesin, dengan menggunakan Cyber Protect Monitor atau antarmuka baris perintah

Mengonfigurasi enkripsi dalam rencana proteksi

Dalam rencana proteksi, enkripsi diaktifkan secara default. Algoritme AES-256 digunakan.

Dengan kata sandi yang kuat, algoritme AES-256 menyediakan enkripsi yang tahan terhadap quantum.

© Acronis International GmbH, 2003-2024

Untuk akun dalam mode Kepatuhan, Anda tidak dapat mengkonfigurasi enkripsi dalam rencana proteksi. Untuk informasi lebih lanjut tentang cara mengkonfigurasi enkripsi pada perangkat yang dilindungi, lihat "Mengonfigurasi enkripsi sebagai properti mesin" (hlm. 442).

Untuk mengonfigurasi enkripsi

1. Di rencana proteksi, perbesar modul **Cadangan**.
2. Dalam **Enkripsi**, klik **Tentukan kata sandi**.
3. Masukkan dan konfirmasi kata sandi enkripsi.
4. Klik **OK**.

Peringatan!
Tidak ada cara untuk memulihkan cadangan terenkripsi jika Anda menghilangkan atau lupa kata sandi.

Anda tidak dapat mengubah pengaturan enkripsi setelah menerapkan rencana proteksi. Untuk menggunakan pengaturan enkripsi yang berbeda, buatlah rencana baru.

Mengonfigurasi enkripsi sebagai properti mesin

Anda dapat mengonfigurasi enkripsi cadangan sebagai properti mesin. Dalam hal ini, enkripsi cadangan tidak dikonfigurasi dalam rencana proteksi, tetapi pada beban kerja yang diproteksi. Enkripsi sebagai properti mesin menggunakan algoritma AES dengan kunci 256 bit (AES-256).

Catatan
Menggunakan algoritma AES-256 dengan kata sandi yang kuat memberikan enkripsi yang tahan terhadap kuantum. Ini aman terhadap serangan analisis kriptografi yang mengandalkan komputasi kuantum.

Mengonfigurasi enkripsi sebagai properti mesin mempengaruhi rencana proteksi dengan cara berikut:

- **Rencana proteksi yang sudah diterapkan pada mesin.** Jika pengaturan enkripsi dalam rencana proteksi berbeda, pencadangan akan gagal.
- **Rencana proteksi yang akan diterapkan pada mesin nantinya.** Pengaturan enkripsi yang disimpan di mesin akan mengambil alih pengaturan enkripsi dalam rencana proteksi. Cadangan apa pun akan dienkripsi, meskipun enkripsi dinonaktifkan di Pengaturan modul pencadangan.

Untuk akun dalam mode Kepatuhan, hanya enkripsi sebagai properti mesin yang tersedia.

Jika Anda memiliki lebih dari satu Agen untuk VMware yang terhubung ke vCenter Server yang sama, dan Anda mengonfigurasi enkripsi sebagai properti mesin, Anda harus menggunakan kata sandi enkripsi yang sama di semua mesin dengan Agen untuk VMware, karena adanya penyeimbangan beban antar agen.

Anda dapat mengonfigurasi enkripsi sebagai properti mesin dengan cara berikut:

© Acronis International GmbH, 2003-2024

- Di baris perintah
- Di Cyber Protect Monitor (Tersedia untuk Windows dan macOS)

Untuk mengkonfigurasi enkripsi

Di baris perintah

1. Masuk sebagai administrator (di Windows) atau pengguna root (di Linux).
2. Pada baris perintah, jalankan perintah berikut:
   - Untuk Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
     <encryption_password>
     ```

     Secara default, jalur instalasinya adalah `%ProgramFiles%\BackupClient`.
   - Untuk Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   - Untuk alat virtual:

     ```
      /./sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   Peringatan!
   Tidak ada cara untuk memulihkan cadangan terenkripsi jika Anda menghilangkan atau lupa kata sandi.

Di Cyber Protect Monitor

1. Masuk sebagai administrator.
2. Klik ikon Cyber Protect Monitor di area notifikasi (di Windows) atau bilah menu (di macOS).
3. Klik ikon roda, lalu klik **Pengaturan** > **Enkripsi**.
4. Pilih **Tetapkan kata sandi untuk mesin ini**. Tentukan dan konfirmasi kata sandi enkripsi.
5. Klik **Simpan**.

Peringatan!
Tidak ada cara untuk memulihkan cadangan terenkripsi jika Anda menghilangkan atau lupa kata sandi.

Untuk mengatur ulang pengaturan enkripsi

1. Masuk sebagai administrator (di Windows) atau pengguna root (di Linux).
2. Pada baris perintah, jalankan perintah berikut:
   - Untuk Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
     ```


© Acronis International GmbH, 2003-2024

Secara default, jalur instalasinya adalah `%ProgramFiles%\BackupClient`.

- Untuk Linux:

```
/usr/sbin/acropsh -m manage_creds --reset
```

- Untuk alat virtual:

```
/./sbin/acropsh -m manage_creds --reset
```

Penting
Jika Anda mengatur ulang enkripsi sebagai properti mesin atau mengubah kata sandi enkripsi setelah rencana proteksi membuat cadangan, operasi pencadangan berikutnya akan gagal. Untuk melanjutkan pencadangan beban kerja, buat rencana proteksi baru.

Notarisasi

Catatan
Fitur ini tersedia dengan paket Cadangan Lanjutan.

Notarisasi memungkinkan Anda untuk membuktikan bahwa file tersebut asli dan tidak berubah sejak dicadangkan. Kami menyarankan Anda untuk mengaktifkan notarisasi ketika mencadangkan file dokumen hukum atau file lain yang membutuhkan keaslian yang terbukti.

Notarisasi hanya tersedia untuk pencadangan level file. File yang memiliki tanda tangan digital akan dilewati, karena tidak perlu dinotariskan.

Notarisasi *tidak* tersedia:

- Jika format pencadangan diatur ke **Versi 11**
- Jika tujuan cadangan adalah Secure Zone

Cara menggunakan notarisasi

Untuk mengaktifkan notarisasi semua file yang dipilih untuk pencadangan (kecuali file yang memiliki tanda tangan digital), aktifkan switch **Notarisasi** saat membuat rencana proteksi.

Saat mengonfigurasi pemulihan, file yang dinotariskan akan ditandai dengan ikon khusus, dan Anda dapat memverifikasi keaslian file.

Cara kerjanya

Selama pencadangan, agen akan menghitung kode hash dari file yang dicadangkan, membangun pohon hash (berdasarkan pada struktur folder), menyimpan pohon di cadangan, lalu mengirimkan root pohon hash ke layanan notaris. Layanan notaris menyimpan root pohon hash dalam database blockchain Ethereum untuk memastikan bahwa nilai ini tidak berubah.

© Acronis International GmbH, 2003-2024

Saat memverifikasi keaslian file, agen akan menghitung hash file, lalu membandingkannya dengan hash yang disimpan di pohon hash dalam cadangan. Jika hash tidak cocok, file tersebut akan dianggap tidak asli. Jika tidak, keaslian file dijamin oleh pohon hash.

Untuk memverifikasi bahwa pohon hash itu sendiri tidak terganggu, agen akan mengirimkan root pohon hash ke layanan notaris. Layanan notaris akan membandingkannya dengan yang disimpan dalam database blockchain. Jika hash cocok, file yang dipilih dijamin asli. Jika tidak, perangkat lunak akan menampilkan pesan bahwa file tersebut tidak asli.

Opsi cadangan default

Nilai default dari opsi pencadangan terdapat di level perusahaan, unit, dan pengguna. Jika unit atau akun pengguna dibuat dalam perusahaan atau dalam unit, ini akan mewarisi nilai default yang diatur untuk perusahaan atau untuk unit.

Administrator perusahaan, administrator unit, dan setiap pengguna tanpa hak administrator dapat mengubah nilai opsi default dari yang sudah ditentukan sebelumnya. Nilai baru akan digunakan secara default di semua rencana proteksi yang dibuat di tingkat terkait setelah perubahan dilakukan.

Saat membuat rencana proteksi, pengguna dapat mengesampingkan nilai default dengan nilai kustom yang hanya akan berlaku khusus untuk rencana ini.

Untuk mengubah nilai opsi default

1. Lakukan salah satu langkah berikut:
   - Untuk mengubah nilai default perusahaan, masuk ke konsol Cyber Protect sebagai administrator perusahaan.
   - Untuk mengubah nilai default unit, masuk ke konsol Cyber Protect sebagai administrator unit.
   - Untuk mengubah nilai default untuk Anda sendiri, masuk ke konsol Cyber Protect dengan menggunakan akun tanpa hak administrator.
2. Klik **Pengaturan** > **Pengaturan sistem**.
3. Perluas bagian **Opsi pencadangan default**.
4. Pilih opsi, lalu buat perubahan yang diperlukan.
5. Klik **Simpan**.

Opsi cadangan

Untuk mengubah opsi pencadangan rencana proteksi, dalam modul **Cadangan**, di bidang **Opsi pencadangan**, klik **Ubah**.

Ketersediaan opsi pencadangan

Set opsi pencadangan yang ada bergantung pada:

© Acronis International GmbH, 2003-2024

- Lingkungan operasi agen (Windows, Linux, macOS).
- Jenis data yang sedang dicadangkan (disk, file, mesin virtual, data aplikasi).
- Tujuan pencadangan (penyimpanan awan, folder lokal atau jaringan).

Tabel berikut merangkum ketersediaan opsi pencadangan.

	Pencadangan tingkat disk			**Pencadangan tingkat file**			**Mesin virtual**			**SQL dan Exchange**
	Windows	**Linux**	**macOS**	**Windows**	**Linux**	**macOS**	**ESXi**	**Hyper-V**	**Virtuozzo**	**Windows**
Peringatan	+	+	+	+	+	+	+	+	+	+
Konsolidasi cadangan	+	+	+	+	+	+	+	+	+	-
Nama file cadangan	+	+	+	+	+	+	+	+	+	+
Format cadangan	+	+	+	+	+	+	+	+	+	+
Validasi cadangan	+	+	+	+	+	+	+	+	+	+
Pelacakan perubahan blok (CBT)	+	-	-	-	-	-	+	+	-	-
Mode cadangan klaster	-	-	-	-	-	-	-	-	-	+
Tingkat kompresi	+	+	+	+	+	+	+	+	+	+
Penanganan eror										
Coba lagi, jika eror terjadi	+	+	+	+	+	+	+	+	+	+
Jangan menampilkan pesan dan dialog saat memproses (mode diam)	+	+	+	+	+	+	+	+	+	+
Abaikan sektor buruk	+	-	+	+	-	+	+	+	+	-
Coba lagi, jika kesalahan terjadi	-	-	-	-	-	-	+	+	+	-

© Acronis International GmbH, 2003-2024

selama pembuatan snapshot VM										
Cadangan inkremental/diferensial cepat	+	+	+	-	-	-	-	-	-	-
Snapshot pencadangan tingkat file	-	-	-	+	+	+	-	-	-	-
Filter file	+	+	+	+	+	+	+	+	+	-
Data forensik	+	-	-	-	-	-	-	-	-	-
Pemotongan log	-	-	-	-	-	-	+	+	-	Hanya SQL
Membuat snapshot LVM	-	+	-	-	-	-	-	-	-	-
Titik mount	-	-	-	+	-	-	-	-	-	-
Snapshot multivolume	+	+	-	+	+	-	-	-	-	-
Pemulihan sekali klik	+	+	-	-	-	-	-	-	-	-
Pengaturan kinerja dan cadangan jendela	+	+	+	+	+	+	+	+	+	+
Pengiriman Data Fisik	+	+	+	+	+	+	+	+	+	-
Perintah pra/pasca	+	+	+	+	+	+	+	+	+	+
Perintah pengambilan data Pra/Pasca	+	+	+	+	+	+	-	-	-	+
Penjadwalan										
Distribusikan waktu mulai dalam jendela waktu	+	+	+	+	+	+	+	+	+	+
Batasi jumlah pencadangan	-	-	-	-	-	-	+	+	+	-

© Acronis International GmbH, 2003-2024

yang berjalan secara simultan										
Pencadangan sektor demi sektor	+	+	-	-	-	-	+	+	+	-
Pembagian	+	+	+	+	+	+	+	+	+	+
Penanganan kegagalan tugas	+	+	+	+	+	+	+	+	+	+
Syarat mulai tugas	+	+	-	+	+	-	+	+	+	+
Layanan Menyalin Bayangan Volume (VSS)	+	-	-	+	-	-	-	+	-	+
Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual	-	-	-	-	-	-	+	+	-	-
Pencadangan mingguan	+	+	+	+	+	+	+	+	+	+
Log event Windows	+	-	-	+	-	-	+	+	-	+

Peringatan

Tidak ada pencadangan yang berhasil untuk jumlah hari berurutan yang ditentukan

Nilai prasetelnya adalah: **Dinonaktifkan**.

Opsi ini menentukan apakah peringatan akan dikeluarkan jika tidak ada pencadangan yang berhasil dilakukan oleh rencana proteksi selama periode yang ditentukan. Selain pencadangan yang gagal, perangkat lunak juga menghitung pencadangan yang tidak berjalan sesuai jadwal (pencadangan terlewat).

Peringatan dikeluarkan pada tiap mesin dan ditampilkan pada tab **Peringatan**.

Anda dapat menentukan jumlah hari berurutan tanpa pencadangan setelah peringatan dikeluarkan.

© Acronis International GmbH, 2003-2024

Konsolidasi cadangan

Opsi ini menentukan apakah konsolidasi cadangan akan dilakukan selama pembersihan atau menghapus keseluruhan rantai cadangan.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Konsolidasi adalah proses menggabungkan dua atau lebih cadangan berikutnya ke dalam satu cadangan.

Jika opsi ini diaktifkan, cadangan yang harus dihapus selama pembersihan akan dikonsolidasikan dengan cadangan dependen berikutnya (inkremental atau diferensial).

Jika tidak, cadangan tersebut akan dipertahankan sampai semua cadangan dependen harus dihapus. Metode ini membantu mencegah konsolidasi yang berpotensi memakan banyak waktu, namun membutuhkan ruang ekstra untuk menyimpan cadangan yang penghapusannya ditunda. Usia atau jumlah cadangan dapat melebihi nilai yang ditentukan pada aturan retensi.

Penting
Harap diperhatikan bahwa konsolidasi hanyalah metode penghapusan, bukan alternatif penghapusan. Hasil pencadangan tidak akan berisi data yang ada pada cadangan terhapus dan tidak ada pada cadangan inkremental atau diferensial yang dipertahankan.

Opsi ini *tidak* efektif jika hal-hal berikut benar:

- Tujuan pencadangan berada di penyimpanan awan.
- Skema cadangan diatur ke **Selalu inkremental (file tunggal)**.
- Format cadangan diatur ke **Versi 12**.

Cadangan yang disimpan di penyimpanan awan, seperti cadangan file tunggal (baik format versi 11 dan 12), selalu dikonsolidasi karena struktur dalamnya membuat konsolidasi cepat dan mudah.

Namun, jika format versi 12 digunakan, dan ada banyak rantai cadangan (setiap rantai disimpan pada file .tibx terpisah), konsolidasi hanya bekerja dalam rantai terakhir. Rantai lain dihapus keseluruhan, kecuali yang pertama, yang diperkecil ke ukuran minimum untuk menyimpan informasi meta (~12 KB). Informasi meta ini diperlukan untuk memastikan konsistensi data selama operasi pembacaan dan penulisan simultan. Cadangan yang disertakan dalam rantai ini akan hilang dari GUI segera setelah aturan retensi diterapkan, meskipun secara fisik cadangan tersebut tetap ada hingga keseluruhan rantai dihapus.

Dalam hal lain, cadangan yang penghapusannya ditunda akan ditandai dengan ikon tempat sampah ( ) dalam GUI. Jika Anda menghapus cadangan tersebut dengan mengklik tanda X, konsolidasi akan dilakukan.

© Acronis International GmbH, 2003-2024

Nama file cadangan

Opsi ini menentukan nama file cadangan yang dibuat oleh rencana proteksi atau rencana pencadangan aplikasi cloud.

Untuk file cadangan yang dibuat berdasarkan rencana proteksi, Anda dapat melihat nama ini di manajer file saat menelusuri lokasi pencadangan.

Apa itu file cadangan?

Setiap rencana proteksi membuat satu atau beberapa file di lokasi pencadangan, bergantung pada skema pencadangan dan format cadangan apa yang digunakan. Tabel berikut mencantumkan file yang dapat dibuat tiap mesin atau kotak surat.

	Selalu inkremental (file tunggal)	**Skema cadangan lainnya**
Format cadangan **Versi 11**	Satu file TIB dan satu file metadata XML	Beberapa file TIB dan satu file metadata XML
Format cadangan **Versi 12**	Satu file TIBX per rantai cadangan (cadangan penuh atau diferensial, dan semua cadangan bertahap yang bergantung padanya). Jika ukuran file yang disimpan di folder lokal atau folder jaringan (SMB) melebihi 200 GB, file dibagi menjadi file-file 200 GB secara default.	

Semua file memiliki nama yang sama, dengan atau tanpa penambahan stempel waktu atau nomor urut. Anda dapat menentukan nama ini (disebut sebagai nama file cadangan) saat Anda membuat atau mengedit rencana proteksi atau rencana pencadangan aplikasi cloud.

Catatan
Stempel waktu ditambahkan ke nama file cadangan hanya dalam format cadangan versi 11.

Jika Anda mengubah nama file cadangan dalam rencana proteksi atau rencana pencadangan aplikasi cloud, pencadangan berikutnya akan menjadi cadangan penuh.

Jika Anda menentukan nama file dari cadangan yang ada pada mesin yang sama, cadangan penuh, inkremental, atau diferensial akan dibuat sesuai dengan jadwal rencana.

Catatan
Jika Anda memindahkan file cadangan (.tibx) dari penyimpanan aslinya, jangan ganti namanya. File yang diganti namanya akan tampak rusak dan Anda tidak akan dapat memulihkan data darinya.

Dimungkinkan untuk mengatur nama file cadangan untuk lokasi yang tidak dapat dijelajahi oleh manajer file (seperti penyimpanan cloud). Dalam hal ini, Anda akan melihat nama kustom di tab **Penyimpanan cadangan**.

© Acronis International GmbH, 2003-2024

Di mana saya dapat melihat nama file cadangan?

Untuk rencana proteksi, pada tab **Penyimpanan cadangan**, pilih lokasi, dan kemudian pilih arsip cadangan.

- Nama file cadangan default ditampilkan di panel **Detail**.
- Jika Anda menetapkan nama file cadangan non-default, nama tersebut akan ditampilkan langsung pada tab **Penyimpanan cadangan**, di kolom **Nama**.

Untuk rencana pencadangan aplikasi cloud, pada tab **Penyimpanan cadangan**, pilih lokasi, pilih arsip cadangan, dan kemudian klik ikon roda.

Batasan untuk nama file cadangan

- Nama file cadangan tidak boleh diakhiri dengan angka.

  Di dalam nama file cadangan default, huruf "A" akan ditambahkan untuk mencegah nama diakhiri dengan angka. Saat membuat nama kustom, selalu pastikan nama tersebut tidak berakhir dengan angka. Saat menggunakan variabel, nama tidak boleh diakhiri dengan variabel, karena variabel bisa saja diakhiri dengan angka.
- Nama file cadangan tidak boleh berisi simbol berikut: **()&?*$<>":\|/#**, akhiran baris (**\n**), dan tab (**\t**).

Catatan
Pilih nama file cadangan yang mudah digunakan. Ini akan membantu Anda membedakan cadangan dengan mudah saat menjelajahi lokasi cadangan dengan manajer file.

Nama file cadangan default

Nama file cadangan default untuk pencadangan keseluruhan mesin fisik dan virtual, disk/volume, file/folder, database Microsoft SQL Server, database Microsoft Exchange Server, dan konfigurasi ESXi adalah `[Machine Name]-[Plan ID]-[Unique ID]A`.

Nama default untuk cadangan kotak surat Exchange dan cadangan kotak surat Microsoft 365 yang dibuat oleh Agen untuk Microsoft 365 lokal adalah `[Mailbox ID]_mailbox_[Plan ID]A`.

Nama default untuk cadangan Microsoft Azure diawali dengan `[Mailbox ID]_`. Awalan ini tidak dapat dihapus.

Nama default untuk pencadangan aplikasi awan yang dibuat oleh agen awan adalah `[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`.

Nama default terdiri dari variabel berikut:

- `[Machine Name]` Variabel ini diganti dengan nama mesin (nama yang sama yang ditampilkan di konsol Cyber Protect).
- `[Plan ID], [Plan Id]` Variabel-variabel ini diganti dengan pengidentifikasi unik dari rencana proteksi. Nilai ini tidak akan berubah jika nama rencana diubah.

© Acronis International GmbH, 2003-2024

- `[Unique ID]` Variabel ini diganti dengan pengidentifikasi unik dari mesin yang dipilih. Nilai ini tidak akan berubah jika nama mesin diganti.
- `[Mailbox ID]` Variabel ini diganti dengan nama utama pengguna (UPN) kotak surat.
- `[Resource Name]` Variabel ini diganti dengan nama sumber data awan, seperti nama utama pengguna (UPN), URL situs SharePoint, atau nama drive Shared.
- `[Resource Type]` Variabel ini diganti dengan jenis sumber data awan, seperti `mailbox`, `O365Mailbox`, `O365PublicFolder`, `OneDrive`, `SharePoint`, `GDrive`.
- `[Resource ID]` Variabel ini diganti dengan pengidentifikasi unik pada sumber data awan. Nilai ini tidak akan berubah jika sumber data awan diganti.
- `"A"` adalah surat perlindungan yang ditambahkan untuk mencegah nama diakhiri dengan angka.

Diagram di bawah ini menunjukkan nama file cadangan default.

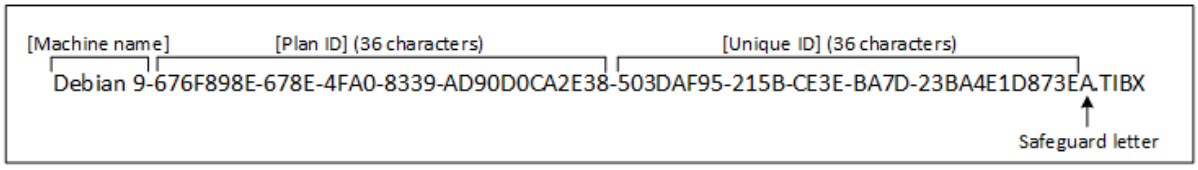
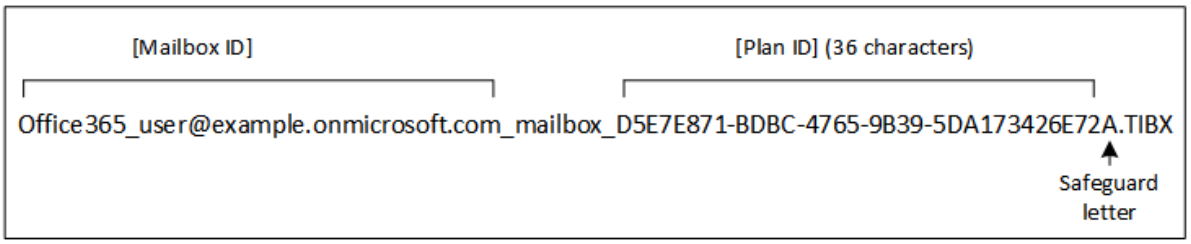


Diagram di bawah ini menunjukkan nama file cadangan default untuk cadangan kotak surat Microsoft 365 yang dijalankan oleh agen lokal.



Nama tanpa variabel

Jika Anda mengubah nama file cadangan ke `MyBackup`, file cadangan akan terlihat seperti contoh berikut. Kedua contoh menganggap pencadangan inkremental harian dijadwalkan pada 14:40, dimulai dari 13 September 2016.

Untuk format Versi 12 dengan skema pencadangan **Selalu inkremental (file tunggal)**:

```
MyBackup.tibx
```

Untuk format versi 12 dengan skema pencadangan lain:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```


© Acronis International GmbH, 2003-2024

Menggunakan variabel

Selain variabel yang digunakan secara default, Anda juga dapat menggunakan variabel berikut:

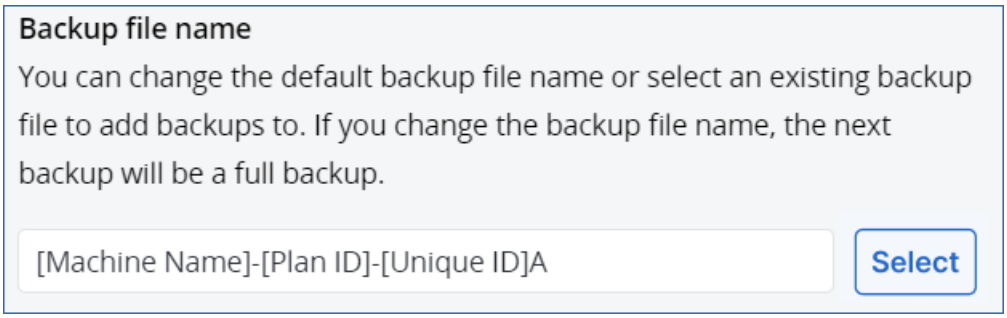
- Variabel `[Plan name]`, yang diganti dengan nama rencana proteksi.
- Variabel `[Virtualization Server Type]`, yang diganti dengan "vmwesx" jika mesin virtual dicadangkan oleh Agen untuk VMware atau dengan "mshyperv" jika mesin virtual dicadangkan oleh Agen untuk Hyper-V.

Jika beberapa mesin atau kotak surat dipilih untuk pencadangan, nama file cadangan harus berisi variabel `[Machine Name]`, `[Unique ID]`, `[Mailbox ID]`, `[Resource Name]`, atau `[Resource Id]`.

Membuat cadangan dalam arsip cadangan yang sudah ada

Anda dapat mengkonfigurasi cadangan dari beban kerja untuk ditambahkan ke arsip cadangan yang sudah ada.

Opsi ini mungkin berguna, misalnya, ketika rencana proteksi diterapkan pada satu mesin, dan Anda harus menghapus mesin ini dari konsol Cyber Protect, atau melakukan penghapusan instalasi agen beserta pengaturan konfigurasinya. Setelah Anda menambahkan mesin lagi atau menginstal ulang agen, Anda dapat menjalankan paksa rencana proteksi untuk melanjutkan pencadangan ke arsip asli.



Untuk mengkonfigurasi cadangan beban kerja agar ditambahkan ke arsip cadangan yang sudah ada

Beban kerja non-awan-ke-awan

1. Di layar **Semua perangkat**, klik beban kerja, dan kemudian klik **Lindungi**.
2. Dalam pengaturan rencana proteksi, perluas modul **Cadangan**.
3. Klik **Opsi pencadangan**, lalu klik **Ubah**.
4. Pada tab **Nama file cadangan**, klik **Pilih**.
   Tombol **Pilih** menunjukkan cadangan di lokasi yang dipilih di bagian **Kemana harus mencadangkan** dari rencana proteksi.

© Acronis International GmbH, 2003-2024

Catatan
Tombol **Pilih** hanya tersedia untuk rencana proteksi yang dibuat dan diterapkan pada satu beban kerja.

5. Pilih arsip, lalu klik **Selesai**.
6. Klik **Selesai**, dan kemudian klik **Terapkan**.

Beban kerja awan-ke-awan

1. Pada tab **Manajemen** > **Cadangan aplikasi cloud**, pilih rencananya.
2. Klik **Edit**, dan kemudian klik ikon roda di sebelah nama rencana.
3. Pada tab **Nama cadangan file**, klik **Pilih**.

Catatan
Tombol **Pilih** hanya tersedia untuk rencana pencadangan yang dibuat untuk dan diterapkan pada satu beban kerja saja.

4. Pilih arsip cadangan, lalu klik **Selesai**.
5. Klik **Selesai**, dan kemudian klik **Simpan perubahan**.

Format cadangan

Opsi **Format cadangan** menetapkan format cadangan yang dibuat oleh rencana proteksi. Opsi ini tersedia hanya untuk rencana proteksi yang sudah digunakan dalam format cadangan versi 11. Jika ini yang terjadi, Anda dapat mengubah format cadangan menjadi versi 12. Setelah mengubah format cadangan ke versi 12, opsi tersebut akan menjadi tidak tersedia.

- **Versi 11**
  Format legasi yang dipertahankan untuk kompatibilitas mundur.

  Catatan
  Anda tidak dapat mencadangkan Database Availability Group (DAG) dengan menggunakan format cadangan versi 11. Mencadangkan DAG hanya didukung dalam format versi 12.

- **Versi 12**
  Format cadangan yang diperkenalkan di Acronis Backup 12 untuk pencadangan dan pemulihan lebih cepat. Tiap rantai cadangan (cadangan penuh atau diferensial, dan semua cadangan bertahap yang bergantung padanya) disimpan dalam file TIBX tunggal.

Format cadangan dan file cadangan

Untuk lokasi cadangan yang dapat dijelajahi dengan manajer file (seperti folder lokal atau dalam jaringan), format cadangan menentukan jumlah file dan ekstensinya. Tabel berikut mencantumkan file yang dapat dibuat tiap mesin atau kotak surat.

© Acronis International GmbH, 2003-2024

	Selalu inkremental (file tunggal)	Skema cadangan lainnya
Format cadangan **Versi 11**	Satu file TIB dan satu file metadata XML	Beberapa file TIB dan satu file metadata XML
Format cadangan **Versi 12**	Satu file TIBX per rantai cadangan (cadangan penuh atau diferensial, dan semua cadangan bertahap yang bergantung padanya). Jika ukuran file yang disimpan di folder lokal atau folder jaringan (SMB) melebihi 200 GB, file dibagi menjadi file-file 200 GB secara default.	

Mengubah format cadangan ke versi 12 (TIBX)

Jika Anda mengubah format cadangan dari versi 11 (format TIB) ke versi 12 (format TIBX):

- Cadangan berikutnya akan penuh.
- Di lokasi cadangan yang dapat dijelajahi dengan manajer file (seperti folder lokal atau jaringan), file TIBX baru akan dibuat. File baru akan memiliki nama file asli, ditambah dengan akhiran _ **v12A**.
- Aturan retensi dan replikasi hanya akan diterapkan ke cadangan baru.
- Cadangan lama tidak akan dihapus dan akan tetap tersedia di tab **Penyimpanan cadangan**. Anda dapat menghapusnya secara manual.
- Cadangan awan lama tidak akan menggunakan kuota **Penyimpanan awan**.
- Cadangan lokal lama akan menggunakan kuota **Cadangan lokal** hingga Anda menghapusnya secara manual.

Deduplikasi dalam arsip

Format cadangan TIBX versi 12 mendukung deduplikasi dalam arsip yang memberi keuntungan berikut:

- Ukuran cadangan yang berkurang secara signifikan, dengan deduplikasi tingkat blok bawaan untuk semua jenis data
- Penanganan tautan keras secara efisien memastikan bahwa tidak ada duplikat penyimpanan
- Chunking berbasis hash

Catatan
Deduplikasi dalam arsip diaktifkan secara default untuk semua cadangan dalam format TIBX. Anda tidak harus mengaktifkannya dalam opsi pencadangan, dan Anda tidak dapat menonaktifkannya.

Kompatibilitas format cadangan lintas berbagai versi produk

Untuk informasi tentang kompatibilitas format cadangan, lihat Kompatibilitas arsip cadangan lintas berbagai versi produk (1689).

© Acronis International GmbH, 2003-2024

Validasi cadangan

Validasi adalah operasi untuk memeriksa kemungkinan pemulihan data dari cadangan. Jika opsi ini diaktifkan, setiap cadangan yang dibuat oleh rencana proteksi divalidasi segera setelah pembuatan, dengan menggunakan metode verifikasi checksum. Operasi ini dilakukan oleh agen perlindungan.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Untuk informasi selengkapnya tentang validasi melalui verifikasi checksum, lihat "Verifikasi checksum" (hlm. 204).

Catatan
Tergantung pengaturan yang dipilih oleh penyedia layanan Anda, validasi mungkin tidak tersedia saat mencadangkan ke penyimpanan awan. Validasi juga tidak tersedia untuk lokasi pencadangan di cloud publik.

Pelacakan perubahan blok (CBT)

Opsi ini efektif untuk cadangan berikut:

- Cadangan tingkat disk mesin virtual
- Cadangan tingkat disk mesin fisik yang menjalankan Windows
- Cadangan dari database Microsoft SQL Server
- Cadangan dari database Microsoft Exchange Server

Nilai prasetelnya adalah: **Diaktifkan**.

Opsi ini menentukan apakah Pelacakan Perubahan Blok (CBT) akan digunakan saat melakukan pencadangan inkremental atau diferensial.

Teknologi CBT mempercepat proses pencadangan. Perubahan pada konten disk atau database terus dilacak di level blok. Saat pencadangan dimulai, perubahan dapat secara langsung disimpan ke cadangan.

Mode cadangan klaster

Catatan
Fitur ini tersedia dengan paket Cadangan Lanjutan.

Opsi ini efektif untuk pencadangan level database Microsoft SQL Server dan Microsoft Exchange Server.

Opsi ini hanya efektif jika klaster (Microsoft SQL Server Always On Availability Group (AAG) atau Microsoft Exchange Server Database Availability Group (DAG)) dipilih untuk pencadangan, bukan simpul individu atau database di dalamnya. Jika Anda memilih masing-masing item di dalam klaster,

© Acronis International GmbH, 2003-2024

cadangan tidak akan menyertakan klaster dan hanya salinan item yang dipilih yang akan dicadangkan.

Microsoft SQL Server

Opsi ini menentukan mode pencadangan untuk SQL Server Always On Availability Group (AAG). Agar opsi ini efektif, Agen untuk SQL harus diinstal pada semua simpul AAG. Untuk informasi lebih lanjut tentang mencadangkan Always On Availability Groups, lihat "Melindungi Always On Availability Group (AAG)".

Nilai prasetelnya adalah: **Replika sekunder jika memungkinkan.**

Anda dapat memilih salah satu dari pilihan berikut:

- **Replika sekunder jika memungkinkan**
  Jika semua replika sekunder luring, replika primer dicadangkan. Mencadangkan replika utama dapat memperlambat operasi SQL Server, tetapi data akan dicadangkan dalam keadaan terbaru.
- **Replika sekunder**
  Jika semua replika sekunder luring, cadangan akan gagal. Mencadangkan replika sekunder tidak memengaruhi performa SQL server dan memungkinkan Anda untuk memperpanjang jendela cadangan. Namun, replika pasif dapat berisi informasi yang tidak terbarui, karena replika semacam itu sering diatur untuk diperbarui secara tidak sinkron (tertinggal).
- **Replika primer**
  Jika replika primer luring, cadangan akan gagal. Mencadangkan replika utama dapat memperlambat operasi SQL Server, tetapi data akan dicadangkan dalam keadaan terbaru.

Terlepas dari nilai opsi ini, untuk memastikan konsistensi database, perangkat lunak akan melompati database yang *bukan* dalam status **SYNCHRONIZED** atau **SYNCHRONIZING** ketika pencadangan dimulai. Jika semua database dilewati, pencadangan akan gagal.

Server Microsoft Exchange

Opsi ini menentukan mode pencadangan untuk Exchange Server Database Availability Groups (DAG). Agar opsi ini efektif, Agen untuk Exchange harus diinstal pada semua simpul DAG. Untuk informasi lebih lanjut tentang mencadangkan Database Availability Groups, lihat "Melindungi Database Availability Groups (DAG)".

Nilai prasetelnya adalah: **Salinan pasif jika memungkinkan.**

Anda dapat memilih salah satu dari pilihan berikut:

- **Salinan pasif jika memungkinkan**
  Jika semua salinan pasif sedang offline, salinan yang aktif dicadangkan. Mencadangkan salinan aktif dapat memperlambat operasi Exchange Server, tetapi data akan dicadangkan dalam kondisi terbaru.
- **Salinan pasif**

© Acronis International GmbH, 2003-2024

Jika semua salinan pasif sedang offline, cadangan akan gagal. Mencadangkan salinan pasif tidak memengaruhi performa Exchange Server dan memungkinkan Anda untuk memperluas jendela cadangan. Namun, salinan pasif dapat berisi informasi yang tidak terbarui, karena salinan semacam itu sering diatur untuk diperbarui secara tidak sinkron (tertinggal).

- **Salinan aktif**

  Jika salinan aktif sedang luring, cadangan akan gagal. Mencadangkan salinan aktif dapat memperlambat operasi Exchange Server, tetapi data akan dicadangkan dalam kondisi terbaru.

Terlepas dari nilai opsi ini, untuk memastikan konsistensi database, perangkat lunak akan melompati database yang *bukan* dalam status **HEALTHY** atau **ACTIVE** ketika pencadangan dimulai. Jika semua database dilewati, pencadangan akan gagal.

Tingkat kompresi

Catatan
Opsi ini tidak tersedia untuk cadangan awan-ke-awan. Kompresi untuk cadangan ini diaktifkan secara default dengan level tetap yang sesuai dengan level **Normal** di bawah.

Opsi ini menentukan tingkat kompresi yang diterapkan pada data yang sedang dicadangkan. Tingkat yang tersedia adalah: **Tidak ada**, **Normal**, **Tinggi**, **Maksimum**.

Nilai prasetelnya adalah: **Normal**.

Tingkat kompresi yang lebih tinggi berarti proses pencadangan memerlukan waktu lebih lama, tetapi hasilnya memakan lebih sedikit ruang. Saat ini, level **Tinggi** dan **Maksimum** berfungsi secara serupa.

Tingkat kompresi data yang optimal bergantung pada jenis data yang dicadangkan. Misalnya, kompresi maksimum tidak akan mengurangi ukuran cadangan secara signifikan jika cadangan berisi file yang sudah terkompresi seperti .jpg, .pdf, atau .mp3. Namun, format seperti .doc atau .xls akan dikompres dengan baik.

Penanganan eror

Opsi ini memungkinkan Anda untuk menentukan cara penanganan eror yang mungkin terjadi selama pencadangan.

Coba lagi, jika eror terjadi

Nilai prasetelnya adalah: **Diaktifkan. Jumlah percobaan: 10. Interval di antara percobaan: 30 detik.**

Ketika terjadi eror yang dapat dipulihkan, program akan mencoba untuk melakukan operasi yang tidak berhasil. Anda dapat mengatur interval waktu dan jumlah percobaan. Percobaan akan dihentikan begitu operasi berhasil atau jumlah percobaan yang ditentukan sudah habis, mana pun yang terlebih dahulu tercapai.

© Acronis International GmbH, 2003-2024

Misalnya, jika tujuan cadangan di jaringan tidak tersedia atau tidak dapat dijangkau selama pencadangan berjalan, perangkat lunak akan berusaha mencapai tujuan setiap 30 detik, tetapi tidak lebih dari 30 kali. Percobaan akan dihentikan begitu koneksi dilanjutkan atau jumlah percobaan yang ditentukan sudah habis, mana pun yang terlebih dahulu tercapai.

Namun, jika tujuan cadangan tidak tersedia saat pencadangan dimulai, hanya 10 percobaan yang akan dilakukan.

Jangan menampilkan pesan dan dialog saat memproses (mode diam)

Nilai prasetelnya adalah: **Diaktifkan**.

Dengan mode diam yang diaktifkan, program akan secara otomatis menangani situasi yang membutuhkan interaksi pengguna (kecuali dalam penanganan sektor buruk, yang dianggap sebagai opsi terpisah). Jika operasi tidak dapat dilanjutkan tanpa interaksi pengguna, operasi akan gagal. Detail operasi, termasuk eror, jika ada, dapat ditemukan pada log operasi.

Abaikan sektor buruk

Nilai prasetelnya adalah: **Dinonaktifkan**.

Ketika opsi ini dinonaktifkan, setiap kali program menemukan sektor buruk, aktivitas pencadangan akan diberi status **Interaksi diperlukan**. Agar dapat mencadangkan informasi yang valid pada hard disk yang mengalami kerusakan dengan cepat, aktifkan opsi abaikan sektor buruk. Sisa data akan dicadangkan dan Anda akan bisa melakukan mounting hasil cadangan disk serta mengekstrak file valid ke disk lain.

Catatan
Melewati sektor buruk tidak didukung di Linux. Anda dapat mencadangkan sistem Linux dengan sektor buruk dalam mode offline, dengan menggunakan pembuat media yang dapat di-boot di versi lokal Cyber Protect. Menggunakan pembuat media yang dapat di-boot lokal memerlukan lisensi terpisah. Hubungi dukungan untuk bantuan.

Coba lagi, jika kesalahan terjadi selama pembuatan snapshot VM

Nilai prasetelnya adalah: **Diaktifkan. Jumlah percobaan: 3. Interval di antara percobaan: 5 menit.**

Ketika gagal mengambil snapshot mesin virtual, program akan mencoba lagi operasi yang belum berhasil. Anda dapat mengatur interval waktu dan jumlah percobaan. Upaya percobaan akan dihentikan begitu operasi berhasil ATAU jumlah percobaan yang ditentukan sudah habis, mana pun yang terlebih dahulu tercapai.

Cadangan inkremental/diferensial cepat

Opsi ini efektif untuk cadangan tingkat disk inkremental atau diferensial.

© Acronis International GmbH, 2003-2024

Opsi ini tidak efektif (selalu dinonaktifkan) untuk volume yang diformat dengan sistem file JFS, ReiserFS3, ReiserFS4, ReFS, atau XFS.

Nilai prasetelnya adalah: **Diaktifkan**.

Cadangan inkremental atau diferensial hanya menangkap perubahan data. Untuk mempercepat proses pencadangan, program akan menentukan apakah file telah diubah atau tidak dengan melihat ukuran file dan tanggal/waktu file terakhir dimodifikasi. Menonaktifkan fitur ini akan membuat program membandingkan seluruh konten file dengan yang disimpan dalam cadangan.

Filter file (Penyertaan/Pengecualian)

Gunakan filter file untuk menyertakan hanya file dan folder tertentu dalam cadangan, atau untuk mengecualikan file dan folder tertentu dari cadangan.

Filter tersedia untuk cadangan keseluruhan mesin, cadangan tingkat disk, dan cadangan tingkat file, kecuali dinyatakan lain.

Filter file tidak tersedia dengan sistem file XFS, JFS, exFAT, dan ReiserFS4. Untuk informasi lebih lanjut, lihat "Sistem file yang didukung" (hlm. 53).

Filter file tidak berlaku untuk disk dinamis (volume LVM atau LDM) mesin virtual yang dicadangkan dalam mode tanpa agen, misalnya, oleh Agen untuk VMware, Agen untuk Hyper-V, atau Agen untuk Scale Computing.

Untuk mengaktifkan filter file

1. Di rencana proteksi, perbesar modul **Cadangan**.
2. Dalam **Opsi cadangan**, klik **Ubah**.
3. Pilih **Filter file (Penyertaan/Pengecualian)**.
4. Gunakan opsi mana saja yang dijelaskan di bawah ini.

Filter penyertaan dan pengecualian

Ada dua filter – filter penyertaan dan filter pengecualian.

- **Sertakan hanya file yang sesuai dengan kriteria di bawah ini**
  Jika Anda menentukan `C:\File.exe` di filter penyertaan, hanya file ini yang akan dicadangkan, meskipun Anda memilih Cadangan keseluruhan mesin.

  Catatan
  Filter ini tidak didukung untuk pencadangan tingkat file jika format pencadangan adalah **Versi 11**, dan tujuan cadangan bukan penyimpanan awan.

- **Kecualikan file yang sesuai dengan kriteria di bawah ini**
  Jika Anda menentukan `C:\File.exe` di filter pengecualian, file ini akan dilewati selama pencadangan, meskipun Anda memilih Cadangan keseluruhan mesin.

© Acronis International GmbH, 2003-2024

Anda dapat menggunakan kedua filter secara bersamaan. Filter pengecualian lebih diutamakan daripada filter penyertaan – yaitu, jika Anda menentukan `C:\File.exe` di kedua bidang, file akan dilewati selama pencadangan.

Kriteria filter

Sebagai kriteria filter, Anda dapat menggunakan nama file dan folder, jalur lengkap ke file dan folder, dan mask dengan simbol wildcard.

Kriteria filter tidak peka huruf besar/kecil. Misalnya, dengan menentukan `C:\Temp`, Anda akan memilih `C:\TEMP`, `C:\temp`.

- Nama

  Tentukan nama file atau folder, seperti `Document.txt`. Semua file dan folder dengan nama tersebut akan dipilih.
- Jalur lengkap

  Tentukan jalur lengkap untuk file atau folder, mulai dengan huruf drive (saat mencadangkan Windows) atau direktori root (saat mencadangkan Linux atau MacOS). Di Windows, Linux, dan macOS, Anda dapat menggunakan garis miring (seperti pada `C:/Temp/File.tmp`). Di Windows, Anda juga dapat menggunakan garis miring terbalik (seperti pada `C:\Temp\File.tmp`).

  Penting

  Jika sistem operasi dari mesin yang dicadangkan tidak terdeteksi dengan benar selama pencadangan tingkat disk, filter file jalur lengkap tidak akan berfungsi. Untuk filter pengecualian, pesan peringatan akan muncul. Jika terdapat filter penyertaan, cadangan akan gagal.

  Misalnya, jalur lengkap ke file bisa jadi `C:\Temp\File.tmp`. Filter jalur lengkap yang menyertakan huruf drive atau direktori root, seperti `C:\Temp\File.tmp` atau `C:\Temp\*`, akan mengakibatkan peringatan atau kegagalan.

  Filter yang tidak menggunakan huruf drive atau direktori root (misalnya, `Temp\*` atau `Temp\File.tmp`) atau filter yang dimulai dengan tanda bintang (contohnya, `*C:\`) tidak akan mengakibatkan peringatan atau kegagalan. Namun, jika sistem operasi mesin yang dicadangkan tidak terdeteksi dengan benar, filter ini juga tidak akan berfungsi.

- Mask

  Anda dapat menggunakan wildcard berikut untuk nama dan jalur lengkap: tanda bintang (*), tanda bintang ganda (**), dan tanda tanya (?).

  Tanda bintang (*) mewakili nol atau lebih banyak karakter. Misalnya, kriteria filter **Doc*.txt** cocok dengan file `Doc.txt` dan `Document.txt`.

  Tanda bintang ganda (**) mewakili nol atau karakter lainnya, termasuk karakter garis miring. Misalnya, ****/Docs/**.txt** cocok dengan semua file .txt di semua subfolder dari semua folder bernama `Docs`. Anda dapat menggunakan wildcard tanda bintang ganda (**) hanya untuk cadangan dalam format Versi 12.

  Tanda tanya (?) hanya mewakili satu karakter. Misalnya, **Doc?.txt** cocok dengan file `Doc1.txt` dan `Docs.txt`, tetapi tidak dengan file `Doc.txt` atau `Doc11.txt`.

© Acronis International GmbH, 2003-2024

Snapshot pencadangan tingkat file

Opsi ini hanya efektif untuk pencadangan tingkat file.

Opsi ini menentukan apakah pencadangan file akan dilakukan satu per satu atau dengan mengambil snapshot data instan.

Catatan
File yang disimpan dalam jaringan bersama selalu dicadangkan satu per satu.

Nilai prasetelnya adalah:

- Jika hanya mesin yang menjalankan Linux yang dipilih untuk pencadangan: **Jangan membuat snapshot.**
- Atau: **Buat snapshot jika memungkinkan.**

Anda dapat memilih salah satu dari tindakan berikut:

- **Buat snapshot jika memungkinkan**
  Cadangkan file secara langsung jika tidak memungkinkan mengambil snapshot.
- **Selalu buat snapshot**
  Snapshot memungkinkan pencadangan semua file termasuk file yang dibuka untuk akses eksklusif. Berkas akan dicadangkan di poin yang sama pada waktunya. Pilih pengaturan ini hanya jika faktor ini bersifat kritis, yaitu, mencadangkan file tanpa snapshot tidak dimungkinkan. Jika tidak dapat mengambil snapshot, pencadangan akan gagal.
- **Jangan membuat snapshot**
  Selalu cadangkan berkas secara langsung. Berusaha mencadangkan file yang terbuka untuk akses eksklusif akan mengakibatkan eror pembacaan. File dalam cadangan mungkin tidak konsisten waktu.

Data forensik

Virus, malware, dan ransomware dapat menjalankan aktivitas berbahaya, seperti mencuri atau mengubah data. Aktivitas ini mungkin perlu diselidiki, yang hanya memungkinkan jika bukti digital tersedia. Akan tetapi, potongan bukti digital, seperti file atau jejak aktivitas, dapat dihapus atau mesin tempat terjadinya aktivitas berbahaya dapat menjadi tidak tersedia.

Pencadangan dengan data forensik memungkinkan penyelidik untuk menganalisis area disk yang biasanya tidak termasuk dalam cadangan disk biasa. Opsi pencadangan **Data forensik** memungkinkan Anda mengumpulkan potongan bukti digital berikut yang dapat digunakan dalam penyelidikan forensik: snapshot ruang disk yang tidak terpakai, sampah memori, dan snapshot proses yang sedang berlangsung.

Cadangan dengan data forensik secara otomatis dinotariskan.

Opsi **Data forensik** hanya tersedia untuk seluruh cadangan mesin Windows yang menjalankan sistem operasi berikut:

© Acronis International GmbH, 2003-2024

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

Cadangan dengan data forensik tidak tersedia untuk mesin berikut:

- Mesin yang tersambung ke jaringan Anda melalui VPN dan tidak memiliki akses langsung ke Internet
- Mesin dengan disk yang dienkripsi dengan BitLocker

Catatan
Anda tidak dapat memodifikasi pengaturan data forensik setelah menerapkan rencana proteksi dengan modul **Cadangan** yang diaktifkan ke suatu mesin. Untuk menggunakan pengaturan data forensik yang berbeda, buat rencana proteksi baru.

Anda dapat menyimpan cadangan dengan data forensik di lokasi berikut ini:

- Penyimpanan awan
- Folder lokal

  Catatan
  Lokasi folder lokal hanya didukung untuk hard disk eksternal yang terhubung melalui USB. Disk dinamis lokal tidak didukung sebagai lokasi untuk cadangan dengan data forensik.

- Folder jaringan

Proses cadangan forensik

Sistem melakukan hal berikut selama proses cadangan forensik:

1. Mengumpulkan timbunan memori mentah dan daftar proses yang berjalan.
2. Secara otomatis melakukan boot ulang mesin pada media yang dapat di-boot.
3. Membuat cadangan yang mencakup ruang yang terpakai dan yang bebas.
4. Menotariskas disk yang dicadangkan.
5. Melakukan boot ulang ke sistem operasi langsung dan melanjutkan eksekusi rencana (misalnya, replikasi, retensi, validasi, dan lainnya).

Untuk mengonfigurasi pengumpulan data forensik

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**. Jika tidak, rencana proteksi dapat dibuat dari tab **Manajemen**.
2. Pilih perangkat dan klik **Lindungi**.
3. Dalam rencana proteksi, aktifkan modul **Cadangan**.
4. Dalam **Apa yang akan dicadangkan**, pilih **Seluruh mesin**.
5. Dalam **Opsi cadangan**, klik **Ubah**.

© Acronis International GmbH, 2003-2024

6. Temukan opsi **Data forensik**.
7. Aktifkan **Kumpulkan data forensik**. Sistem akan secara otomatis mengumpulkan timbunan memori dan membuat snapshot dari proses yang sedang berjalan.

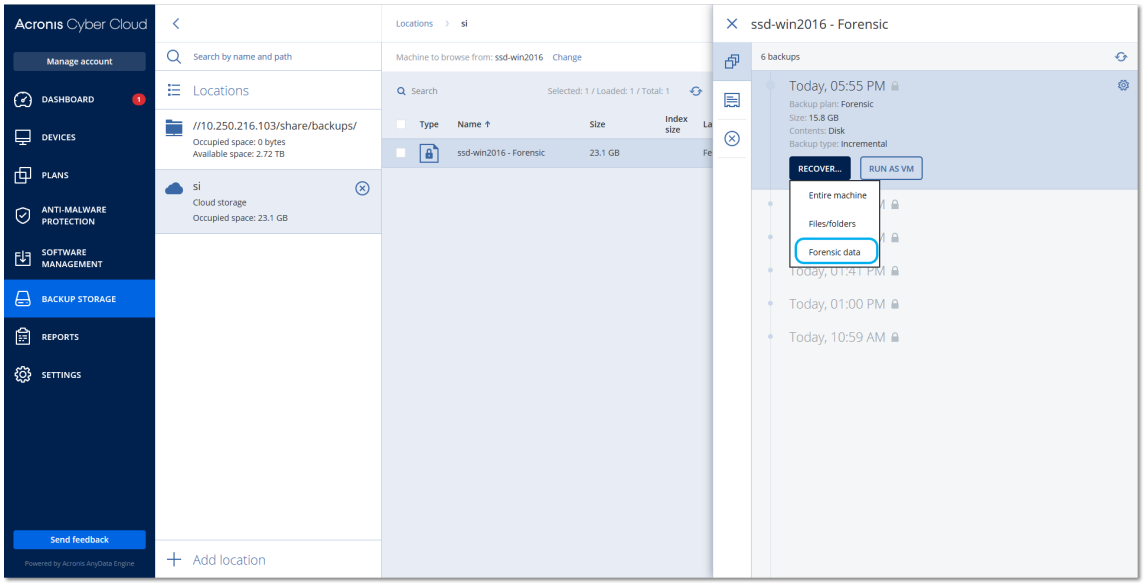
   Catatan
   Sampah memori yang penuh bisa berisi data sensitif seperti kata sandi.

8. Tentukan lokasi.
9. Klik **Jalankan Sekarang** untuk melakukan cadangan dengan data forensik segera atau tunggu hingga cadangan dibuat sesuai jadwal.
10. Buka **Pemantauan** > **Aktivitas**, verifikasi bahwa cadangan dengan data forensik telah berhasil dibuat.

Akibatnya, cadangan akan mencakup data forensik dan Anda akan bisa mendapatkannya dan menganalisis. Cadangan dengan data forensik ditandai dan dapat difilter di antara cadangan lainnya di **Penyimpanan cadangan** > **Lokasi** dengan menggunakan opsi **Hanya dengan data forensik**.

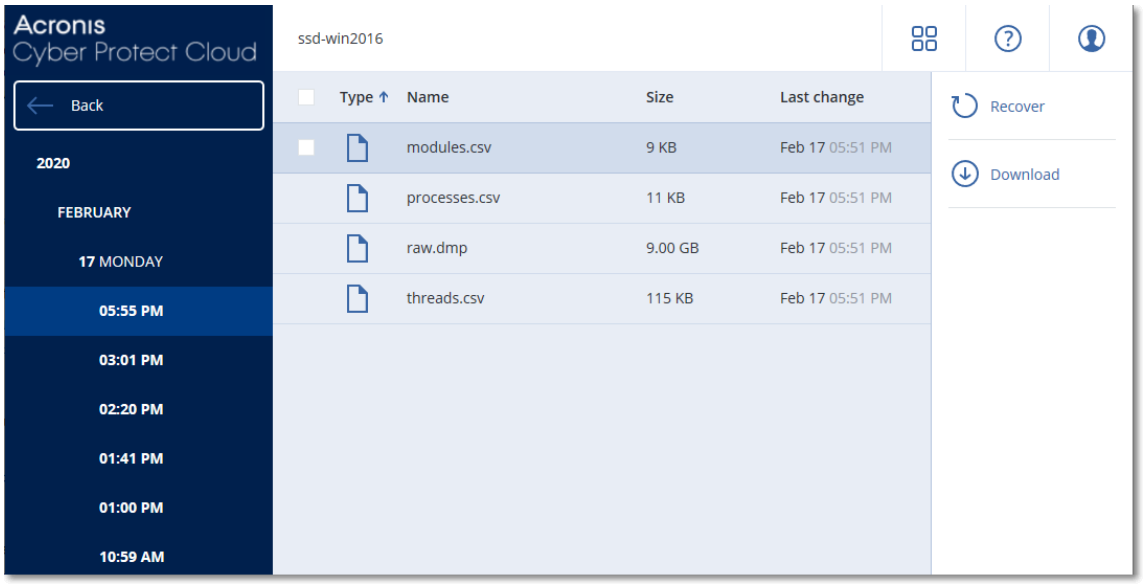
Bagaimana cara mendapatkan data forensik dari cadangan?

1. Di konsol Cyber Protect, buka **Penyimpanan cadangan**, pilih lokasi dengan cadangan yang menyertakan data forensik.
2. Pilih cadangan dengan data forensik dan klik **Tampilkan cadangan**.
3. Klik **Pulihkan** untuk cadangan dengan data forensik.
   - Untuk mendapatkan hanya data forensik, klik **Data forensik**.



   Sistem akan menampilkan folder dengan data forensik. Pilih file sampah memori atau file forensik lainnya lalu klik **Unduh**.

© Acronis International GmbH, 2003-2024



- Untuk memulihkan cadangan forensik yang penuh, klik **Seluruh mesin**. Sistem akan memulihkan cadangan tanpa mode boot. Dengan demikian, dimungkinkan untuk memeriksa apakah disk tidak diubah.

Anda dapat menggunakan timbunan memori yang disediakan dengan beberapa perangkat lunak forensik pihak ketiga, misalnya, gunakan Volatility Framework di https://www.volatilityfoundation.org/ untuk analisis memori lebih lanjut.

Notarisasi cadangan dengan data forensik

Untuk memastikan bahwa cadangan dengan data forensik tepat dengan gambar yang diambil dan tidak terganggu, modul cadangan menyediakan notarisasi cadangan dengan data forensik.

Cara kerjanya

Notarisasi memungkinkan Anda untuk membuktikan bahwa disk dengan data forensik asli dan tidak berubah sejak dicadangkan.

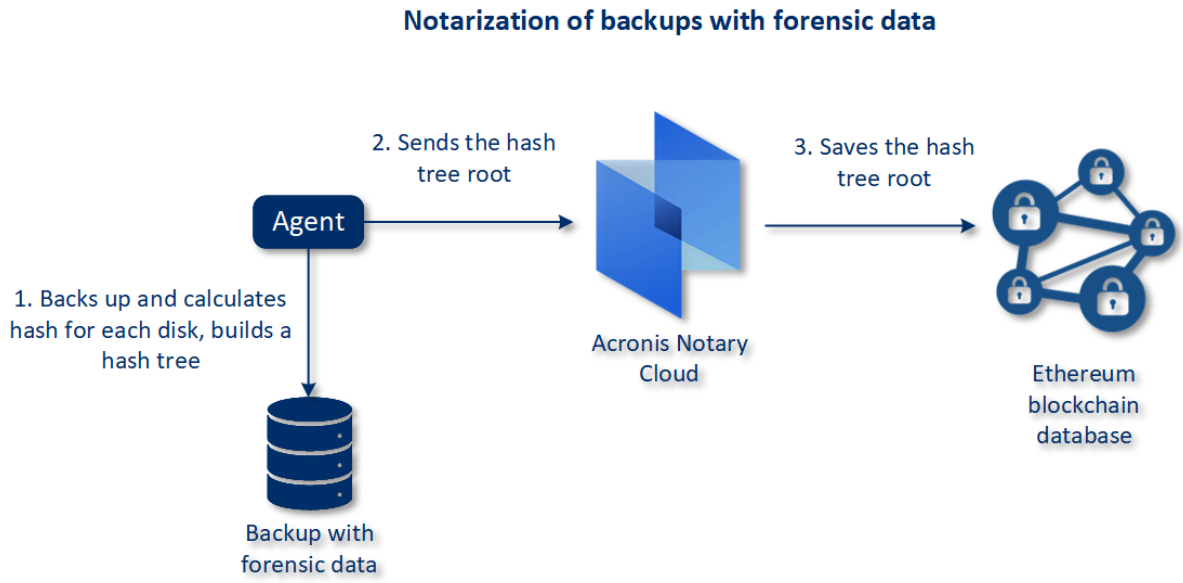
Selama pencadangan, agen akan menghitung kode hash dari disk yang dicadangkan, membangun pohon hash, menyimpan pohon di cadangan, lalu mengirimkan root pohon hash ke layanan notaris. Layanan notaris menyimpan root pohon hash dalam database blockchain Ethereum untuk memastikan bahwa nilai ini tidak berubah.

Saat memverifikasi keaslian disk dengan data forensik, agen akan menghitung hash disk, lalu membandingkannya dengan hash yang disimpan di pohon hash dalam cadangan. Jika hash tidak cocok, disk tersebut akan dianggap tidak asli. Jika tidak, keaslian disk dijamin oleh pohon hash.

Untuk memverifikasi bahwa pohon hash itu sendiri tidak terganggu, agen akan mengirimkan root pohon hash ke layanan notaris. Layanan notaris akan membandingkannya dengan yang disimpan dalam database blockchain. Jika hash cocok, disk yang dipilih dijamin asli. Jika tidak, perangkat lunak akan menampilkan pesan bahwa disk tersebut tidak asli.

© Acronis International GmbH, 2003-2024

Skema di bawah ini menunjukkan proses notarisasi dengan singkat untuk cadangan dengan data forensik.



Untuk memverifikasi cadangan disk yang dinotariskan secara manual, Anda dapat memperoleh sertifikat untuk itu dan ikuti prosedur verifikasi yang ditunjukkan dengan sertifikat dengan menggunakan alat bantu tibxread.

Mendapatkan sertifikat untuk cadangan dengan data forensik

Untuk mendapatkan sertifikat cadangan dengan data forensik dari konsol, lakukan hal berikut:

1. Masuk ke **Penyimpanan cadangan** dan pilih cadangan dengan data forensik.
2. Pulihkan keseluruhan mesin.
3. Sistem membuka tampilan **Pemetaan Disk**.
4. Klik ikon **Dapatkan sertifikat** untuk disk.
5. Sistem akan menghasilkan sertifikat dan membuka jendela baru di browser dengan sertifikat. Di bawah sertifikat, Anda akan melihat petunjuk untuk verifikasi manual cadangan disk yang dinotariskan.

Alat bantu "tibxread" untuk mendapatkan data yang dicadangkan

Cyber Protection menyediakan alat bantu, yang disebut `tibxread`, untuk pemeriksaan manual integritas disk yang dicadangkan. Alat bantu ini memungkinkan Anda untuk mendapatkan data dari cadangan dan menghitung hash dari disk yang ditentukan. Alat bantu ini diinstal secara otomatis dengan komponen berikut: Agen untuk Windows, Agen untuk Linux, dan Agen untuk Mac.

Jalur instalasi: folder yang sama dengan yang dimiliki agen (misalnya, `C:\Program Files\BackupClient\BackupAndRecovery`).

Lokasi yang didukung adalah:

© Acronis International GmbH, 2003-2024

- Disk lokal
- Folder jaringan (CIFS/SMB) yang dapat diakses tanpa kredensial.

  Dalam kasus folder jaringan yang dilindungi kata sandi, Anda dapat memasang folder jaringan ke folder lokal dengan menggunakan alat bantu OS dan kemudian folder lokal sebagai sumber untuk alat ini.
- Penyimpanan awan

  Anda harus memberikan URL, port, dan sertifikat. URL dan port dapat diperoleh dari kunci registri Windows atau file konfigurasi di mesin Linux/Mac.

  Untuk Windows:

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<tenant_login>\FesUri
  ```

  Untuk Linux:

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  Untuk macOS:

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  Sertifikat dapat ditemukan di lokasi berikut:

  Untuk Windows:

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```

  Untuk Linux:

  ```
  /var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

  Untuk macOS:

  ```
  /Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

Alat bantu ini memiliki perintah berikut:

- `list backups`
- `list content`
- `get content`
- `calculate hash`

daftarkan cadangan

Mencantumkan titik pemulihan dalam cadangan.

SINOPSIS:

© Acronis International GmbH, 2003-2024

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Opsi

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Templat keluaran:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <tanggal> <timestamp>
```

<guid> – GUID cadangan.

<tanggal> – tanggal pembuatan cadangan. Formatnya adalah "HH.BB.TTTT JJ24: MM: DD". Di zona waktu lokal secara default (dapat diubah dengan menggunakan opsi --utc).

Contoh keluaran:

```
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
```

daftarkan konten

Mendaftarkan konten dalam titik pemulihan.

SINOPSIS:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

Opsi

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

Templat keluaran:

© Acronis International GmbH, 2003-2024

```
Disk     Size   Notarization status
-------- ------ --------------------
<jumlah> <ukuran> <status_notarisasi>
```

<jumlah> – pengidentifikasi disk.

<ukuran> - ukuran dalam bit.

<status_notarisasi> - status berikut memungkinkan: Tanpa notarisasi, Dinotariskan, Cadangan selanjutnya.

Contoh keluaran:

```
Disk     Size   Notary status
-------- ------ --------------
1        123123465798 Notarized
2        123123465798 Notarized
```

dapatkan konten

Menulis konten disk yang ditentukan di titik pemulihan ke keluaran standar (stdout).

SINOPSIS:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

Opsi

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

hitung hash

Menghitung hash dari disk yang ditentukan di titik pemulihan menggunakan algoritme SHA-2 (256-bit) dan menulisnya ke stdout.

SINOPSIS:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Opsi

© Acronis International GmbH, 2003-2024

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

Deskripsi opsi

Opsi	Deskripsi
--arc=BACKUP_NAME	Nama file cadangan yang bisa Anda dapatkan dari properti cadangan di konsol Cyber Protect. File cadangan harus ditentukan dengan ekstensi .tibx.
--backup=RECOVERY_POINT_ID	Pengidentifikasi titik pemulihan
--disk=DISK_NUMBER	Nomor disk (sama seperti yang tertulis pada keluaran dari perintah "dapatkan konten")

--loc=URI	URI lokasi cadangan. Format yang memungkinkan dari opsi "--loc" adalah:
	• Nama jalur lokal (Windows)
	`c:/upload/backups`
	• Nama jalur lokal (Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• Penyimpanan awan
	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`
	`<IP_address>` – Anda dapat menemukannya di kunci registri di Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri
	`<path_to_certificate>` – jalur ke file sertifikat untuk mengakses Cyber Protect Cloud. Misalnya, di Windows sertifikat ini berlokasi di `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt`, tempat <username> – merupakan nama akun Anda untuk mengakses Cyber Protect Cloud.

--log=PATH	Memungkinkan menulis log dengan PATH yang ditentukan (hanya jalur lokal, formatnya sama dengan untuk parameter `--loc=URI`). Level logging adalah DEBUG.
--password=PASSWORD	Kata sandi enkripsi untuk cadangan Anda. Jika cadangan tidak terenkripsi, biarkan nilai ini kosong.

© Acronis International GmbH, 2003-2024

--raw	Menyembunyikan header (2 baris pertama) pada keluaran perintah. Ini digunakan ketika keluaran perintah harus diuraikan.
	
	Contoh keluaran tanpa "`--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`
	
	Keluaran dengan"`--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	Menampilkan tanggal dalam UTC

--progress	Menampilkan progres operasi.
	
	Misalnya:
	
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

Pemotongan log

Opsi ini efektif untuk cadangan database Microsoft SQL Server dan untuk cadangan tingkat disk dengan cadangan aplikasi Microsoft SQL Server yang diaktifkan.

Opsi ini menentukan apakah log transaksi SQL Server dipotong setelah pencadangan berhasil.

Nilai prasetelnya adalah: **Diaktifkan**.

Ketika opsi ini diaktifkan, database hanya dapat dipulihkan ke titik waktu pencadangan yang dibuat oleh perangkat lunak ini. Nonaktifkan opsi ini jika Anda mencadangkan log transaksi menggunakan mesin cadangan asli Microsoft SQL Server. Anda akan dapat menerapkan log transaksi setelah pemulihan agar dapat memulihkan database ke titik waktu mana pun.

Membuat snapshot LVM

Opsi ini hanya efektif untuk mesin fisik.

Opsi ini efektif untuk cadangan volume tingkat disk yang dikelola oleh Linux Logical Volume Manager (LVM). Volume tersebut juga disebut volume logis.

Opsi ini menentukan bagaimana snapshot volume logis diambil. Perangkat lunak cadangan dapat melakukannya sendiri atau mengandalkan Linux Logical Volume Manager (LVM).

© Acronis International GmbH, 2003-2024

Nilai prasetelnya adalah: **Oleh perangkat lunak pencadangan**.

- **Oleh perangkat lunak pencadangan**. Data snapshot sebagian besar disimpan dalam RAM. Pencadangan lebih cepat dan tidak memerlukan ruang tidak teralokasi pada grup volume. Oleh karena itu, kami menyarankan Anda mengubah preset hanya jika Anda mengalami masalah saat mencadangkan volume logis.
- **Oleh LVM**. Snapshot disimpan di ruang yang tidak teralokasi pada grup volume. Jika ruang yang tidak teralokasi tidak ditemukan, snapshot akan diambil oleh perangkat lunak cadangan.

Snapshot hanya digunakan selama operasi pencadangan, dan secara otomatis dihapus ketika operasi pencadangan selesai. Tidak ada file sementara yang disimpan.

Titik mount

Opsi ini hanya efektif pada Windows untuk pencadangan tingkat file dari sumber data yang menyertakan volume ter-mount atau volume klaster bersama.

Opsi ini hanya efektif jika Anda memilih mencadangkan folder yang lebih tinggi pada hierarki folder dibandingkan titik mount. (Titik mount adalah folder tempat volume tambahan ter-mount.)

- Jika folder tersebut (folder induk) dipilih untuk dicadangkan, dan opsi **Titik mount** diaktifkan, semua file yang berada pada volume ter-mount akan disertakan dalam cadangan. Jika opsi **Titik mount** diaktifkan, titik mount pada cadangan akan kosong.

  Selama pemulihan folder induk, konten titik mount akan atau tidak akan dipulihkan, tergantung apakah opsi **Titik mount** untuk pemulihan diaktifkan atau dinonaktifkan.
- Jika Anda memilih titik mount secara langsung, atau memilih folder mana pun dalam volume ter-mount, folder yang dipilih akan dianggap sebagai folder biasa. Folder tersebut akan dicadangkan apa pun status opsi **Titik mount-nya** dan dipulihkan apa pun status opsi pemulihan **Titik mount**.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Catatan
Anda dapat mencadangkan mesin virtual Hyper-V yang berada pada volume klaster bersama dengan mencadangkan file yang diperlukan atau keseluruhan volume dengan pencadangan tingkat file. Cukup matikan mesin virtual untuk memastikan bahwa mesin dicadangkan dalam status konsisten.

Contoh

Anggaplah folder **C:\Data1** merupakan titik mount untuk volume ter-mount. Volume tersebut berisi folder **Folder1** dan **Folder2**. Anda membuat rencana proteksi untuk pencadangan tingkat file data Anda.

Jika Anda memilih kotak centang untuk volume C dan mengaktifkan opsi **Titik mount**, maka folder **C:\Data1** pada cadangan Anda akan berisi **Folder1** dan **Folder2**. Ketika memulihkan data yang dicadangkan, berhati-hatilah saat menggunakan opsi pemulihan **Titik mount**.

© Acronis International GmbH, 2003-2024

Jika Anda memilih kotak centang untuk volume C dan menonaktifkan opsi **Titik mount**, folder **C:\Data1** pada cadangan Anda akan kosong.

Jika Anda memilih kotak centang untuk folder **Data1**, **Folder1** atau **Folder2**, folder yang dicentang akan dimasukkan dalam cadangan sebagai folder biasa, apa pun status opsi **Titik mount**.

Snapshot multivolume

Opsi ini efektif untuk cadangan mesin fisik yang menjalankan Windows atau Linux.

Opsi ini berlaku untuk pecadangan tingkat disk. Opsi ini juga berlaku untuk pencadangan tingkat file ketika pencadangan tingkat file dilakukan dengan mengambil snapshot. (Opsi "Snapshot pencadangan tingkat file" menentukan apakah snapshot diambil selama pencadangan tingkat file).

Opsi ini menentukan apakah perlu mengambil snapshot dari beberapa volume secara bersamaan atau satu per satu.

Nilai prasetelnya adalah:

- Jika setidaknya satu mesin yang menjalankan Windows dipilih untuk pencadangan: **Diaktifkan**.
- Atau: **Dinonaktifkan**.

Ketika opsi ini diaktifkan, snapshot dari semua volume yang sedang dicadangkan akan dibuat secara bersamaan. Gunakan opsi ini untuk membuat cadangan data konsisten waktu yang menjangkau beberapa volume; misalnya, untuk database Oracle.

Ketika opsi ini dinonaktifkan, snapshot volume akan diambil satu per satu. Hasilnya, jika data menjangkau beberapa volume, cadangan yang dihasilkan mungkin tidak konsisten.

Pemulihan sekali klik

Catatan
Fitur ini tersedia dengan paket Cadangan Lanjutan.

Dengan pemulihan Sekali klik, Anda dapat secara otomatis memulihkan cadangan disk dari mesin Windows atau Linux Anda. Cadangan ini bisa berupa cadangan dari seluruh mesin, atau cadangan dari disk atau volume tertentu pada mesin ini.

Pemulihan sekali klik mendukung operasi berikut ini:

- Pemulihan otomatis dari cadangan terbaru
- Pemulihan dari cadangan spesifik (juga dikenal sebagai titik pemulihan) dalam arsip cadangan

Pemulihan sekali klik mendukung penyimpanan cadangan berikut ini:

- Secure Zone
- Folder lokal

© Acronis International GmbH, 2003-2024

- Folder jaringan
- Penyimpanan awan

Penting
Tunda enkripsi BitLocker sampai Anda melakukan restart pada mesin di waktu berikutnya ketika Anda melakukan salah satu operasi berikut:

- Membuat, memodifikasi, atau menghapus Secure Zone.
- Mengaktifkan atau menonaktifkan Startup Recovery Manager.
- [Hanya jika Startup Recovery Manager belum diaktifkan] Menjalankan cadangan pertama setelah mengaktifkan pemulihan di rencana proteksi. Operasi ini mengaktifkan Startup Recovery Manager secara otomatis.
- Memperbarui Startup Recovery Manager, misalnya dengan memperbarui proteksi.

Jika enkripsi BitLocker tidak ditangguhkan selama operasi ini, Anda perlu menentukan PIN BitLocker Anda setelah memulai ulang mesin Anda.

Mengaktifkan pemulihan Sekali klik

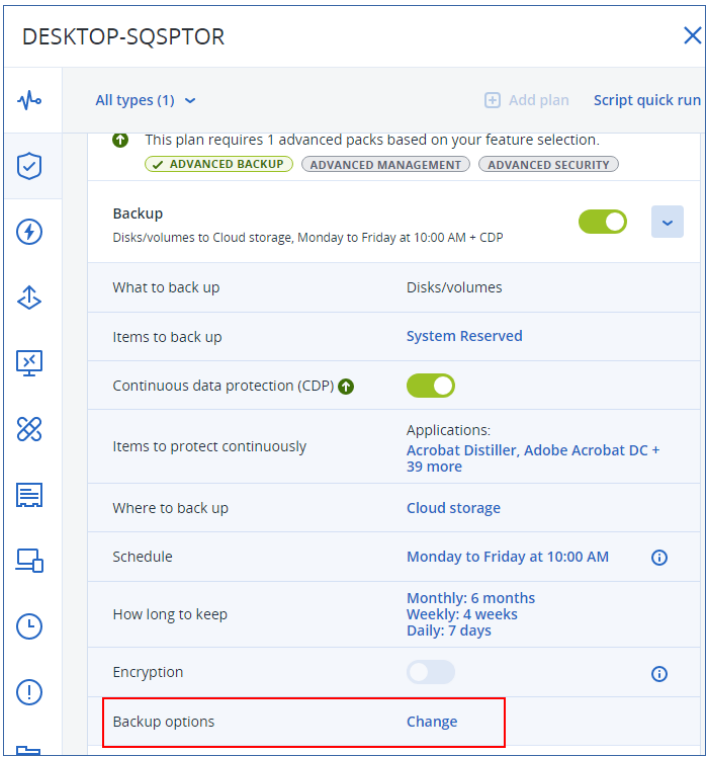
Pemulihan Sekali klik adalah opsi pencadangan dalam rencana proteksi. Untuk informasi lebih lanjut tentang cara membuat rencana, lihat "Membuat rencana proteksi" (hlm. 214).

Catatan
Mengaktifkan pemulihan Sekali klik juga mengaktifkan Startup Recovery Manager pada mesin target. Jika Startup Recovery Manager tidak dapat diaktifkan, operasi pencadangan yang menciptakan cadangan pemulihan One-click akan gagal. Untuk informasi lebih lanjut tentang Startup Recovery Manager, lihat "Startup Recovery Manager" (hlm. 727).

Untuk mengaktifkan pemulihan satu-klik

1. Dalam rencana proteksi, perbesar modul **Cadangan**.
2. Dalam **Apa yang akan dicadangkan**, pilih **Seluruh mesin** atau **Disk/volume**.
3. [Jika Anda memilih **Disk/volume**]. Di **Item yang akan dicadangkan**, tentukan disk atau volume yang akan dicadangkan.
4. Dalam **Opsi pencadangan**, klik **Ubah**, lalu pilih **Pemulihan sekali klik**.

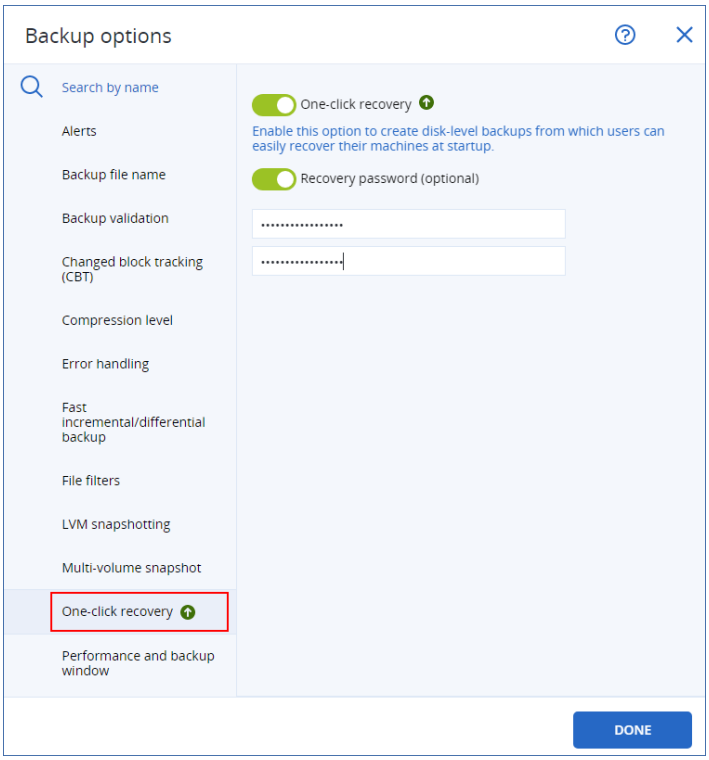
© Acronis International GmbH, 2003-2024



5. Aktifkan tombol **Pemulihan sekali klik**.
6. [Opsional] Aktifkan tombol **Pemulihan kata sandi**, lalu tentukan kata sandi.

Penting
Kami sangat menyarankan Anda menentukan kata sandi pemulihan. Pastikan bahwa pengguna yang melakukan Pemulihan sekali klik pada mesin target mengetahui kata sandi ini.

© Acronis International GmbH, 2003-2024



7. Klik **Selesai**.
8. Konfigurasikan elemen lain dari rencana proteksi menurut kebutuhan Anda, lalu simpan rencana.

Hasilnya, setelah rencana proteksi berjalan dan membuat cadangan, Pemulihan sekali klik dapat diakses oleh pengguna mesin terlindungi.

Penting
Pemulihan sekali klik menjadi tidak tersedia untuk sementara ketika Anda memperbarui agen perlindungan. Untuk mengaktifkan kembali pemulihan sekali klik, jalankan pencadangan. Ketika pencadangan selesai, Anda bisa kembali menjalankan pemulihan sekali klik.

Menonaktifkan Pemulihan Sekali klik

Anda dapat menonaktifkan pemulihan Sekali klik untuk beban kerja tertentu dengan cara berikut:

- Nonaktifkan opsi **Pemulihan Sekali klik** dalam rencana proteksi yang diterapkan pada beban kerja.
- Batalkan rencana proteksi di mana opsi **Pemulihan Sekali klik** diaktifkan.
- Hapus rencana proteksi di mana opsi **Pemulihan Sekali klik** diaktifkan.

© Acronis International GmbH, 2003-2024

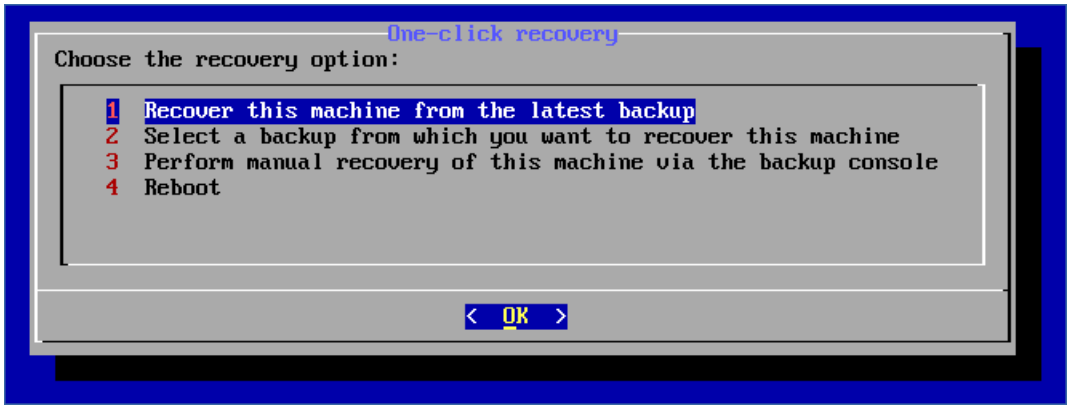
Memulihkan mesin dengan pemulihan Satu-klik

Prasyarat

- Rencana proteksi dengan opsi pencadangan **Pemulihan sekali klik** aktif diterapkan pada mesin.
- Setidaknya ada satu cadangan disk dari mesin.

Untuk memulihkan mesin

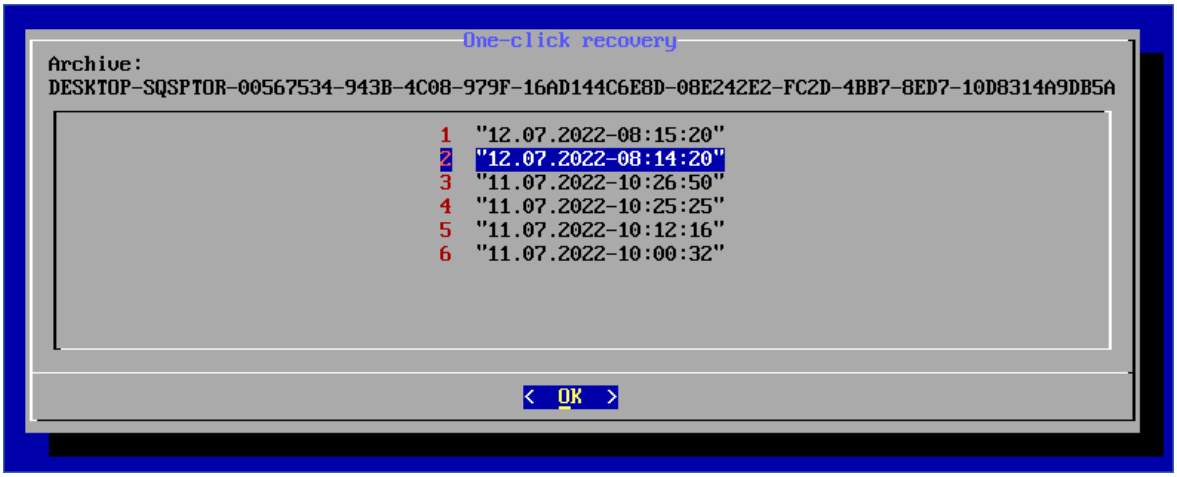
1. Nyalakan ulang mesin yang ingin Anda pulihkan.
2. Selama reboot, tekan F11 untuk masuk ke Startup Recovery Manager.
   Jendela media cadangan terbuka.
3. Pilih **Acronis Cyber Protect**.
4. [Jika kata sandi pemulihan ditentukan dalam rencana proteksi] Masukkan kata sandi pemulihan, lalu klik **OK**.
5. Pilih opsi Pemulihan sekali klik yang diinginkan.
   - Untuk memulihkan cadangan terbaru secara otomatis, pilih opsi pertama, lalu klik **OK**.
   - Untuk memulihkan cadangan lain di dalam arsip cadangan, pilih opsi kedua, lalu klik **OK**.



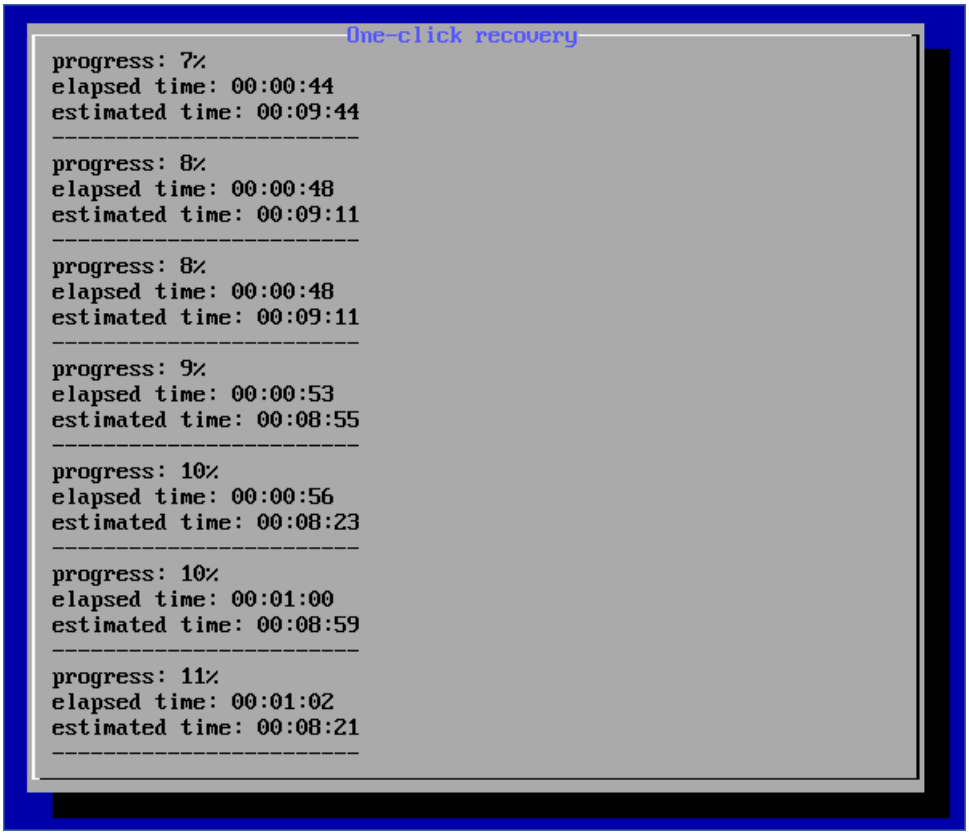
6. Konfirmasi pilihan Anda dengan mengklik **Iya**.
   Jendela media cadangan terbuka, lalu hilang. Prosedur pemulihan berlanjut tanpanya.
7. [Jika Anda memilih untuk memulihkan cadangan tertentu] Pilih cadangan yang ingin Anda

© Acronis International GmbH, 2003-2024

pulihkan, lalu klik **OK**.



Setelah beberapa saat, pemulihan dimulai dan progresnya ditampilkan. Saat pemulihan selesai, mesin Anda akan melakukan boot ulang.



Pengaturan kinerja dan cadangan jendela

Opsi ini memungkinkan Anda untuk mengatur satu dari tiga level kinerja pencadangan (tinggi, rendah, dilarang) untuk setiap jam dalam seminggu. Dengan cara ini, Anda dapat menentukan jendela waktu kapan pencadangan diizinkan untuk memulai dan berjalan. Level performa tinggi dan rendah dapat dikonfigurasi dalam hal prioritas proses dan kecepatan output.

© Acronis International GmbH, 2003-2024

Opsi ini tidak tersedia untuk pencadangan yang dijalankan oleh agen awan, seperti pencadangan situs web atau pencadangan server yang berada di situs pemulihan awan.

Opsi ini hanya efektif untuk proses pencadangan dan replikasi cadangan. Perintah pasca-pencadangan dan operasi lain yang termasuk dalam rencana proteksi (misalnya, validasi) akan berjalan, terlepas dari opsi ini.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Ketika opsi ini dinonaktifkan, pencadangan akan diizinkan untuk berjalan kapan saja, dengan parameter berikut (tidak masalah jika nilai prasetel parameter diubah):

- Prioritas CPU: **Rendah** (di Windows, ini sesuai dengan **Di bawah normal**)
- Kecepatan output: **Tidak terbatas**

Ketika opsi ini diaktifkan, pencadangan terjadwal diizinkan atau diblokir sesuai dengan parameter kinerja yang ditentukan untuk jam saat ini. Di awal jam ketika pencadangan diblokir, proses pencadangan secara otomatis dihentikan dan peringatan dihasilkan. Meskipun pencadangan terjadwal diblokir, pencadangan dapat dimulai secara manual. Ini akan menggunakan parameter kinerja dari jam terakhir ketika pencadangan diizinkan.

Catatan
Anda dapat mengonfigurasi kinerja dan jendela pencadangan untuk setiap lokasi replikasi secara individual. Untuk mengakses pengaturan lokasi replikasi, dalam rencana proteksi, klik ikon roda di sebelah nama lokasi, dan kemudian klik **Kinerja dan jendela pencadangan**.

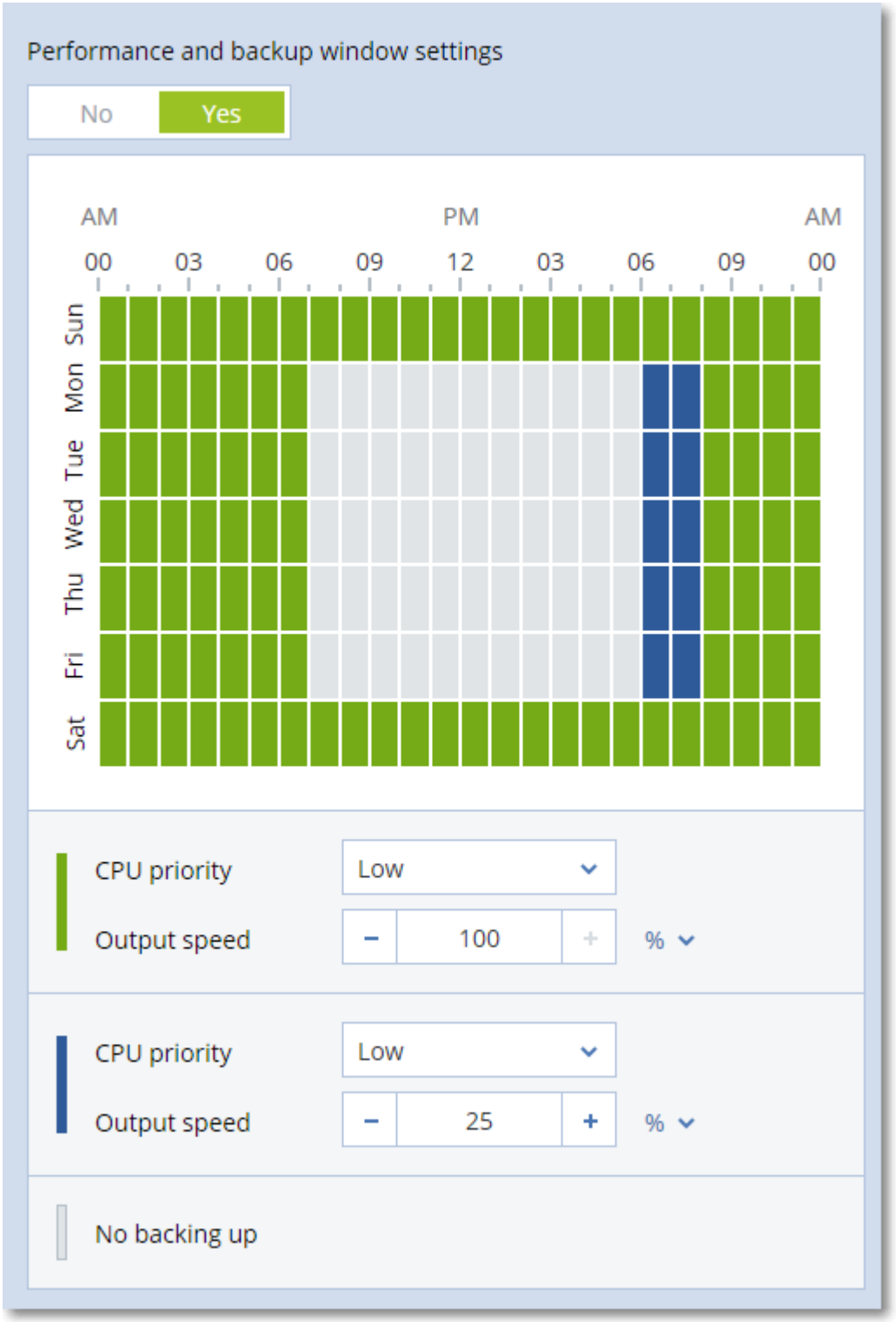
Jendela pencadangan

Setiap kotak menunjukkan satu jam dalam sehari. Klik kotak untuk memutar status berikut:

- **Hijau:** pencadangan diizinkan dengan parameter yang ditentukan di bagian hijau di bawah ini.
- **Biru:** pencadangan diizinkan dengan parameter yang ditentukan di bagian biru di bawah ini. Status ini tidak tersedia jika format cadangan diatur ke **Versi 11**.
- **Abu-abu**: pencadangan diblokir.

Anda dapat mengklik dan menariknya untuk mengubah status beberapa kotak secara bersamaan.

© Acronis International GmbH, 2003-2024



Prioritas CPU

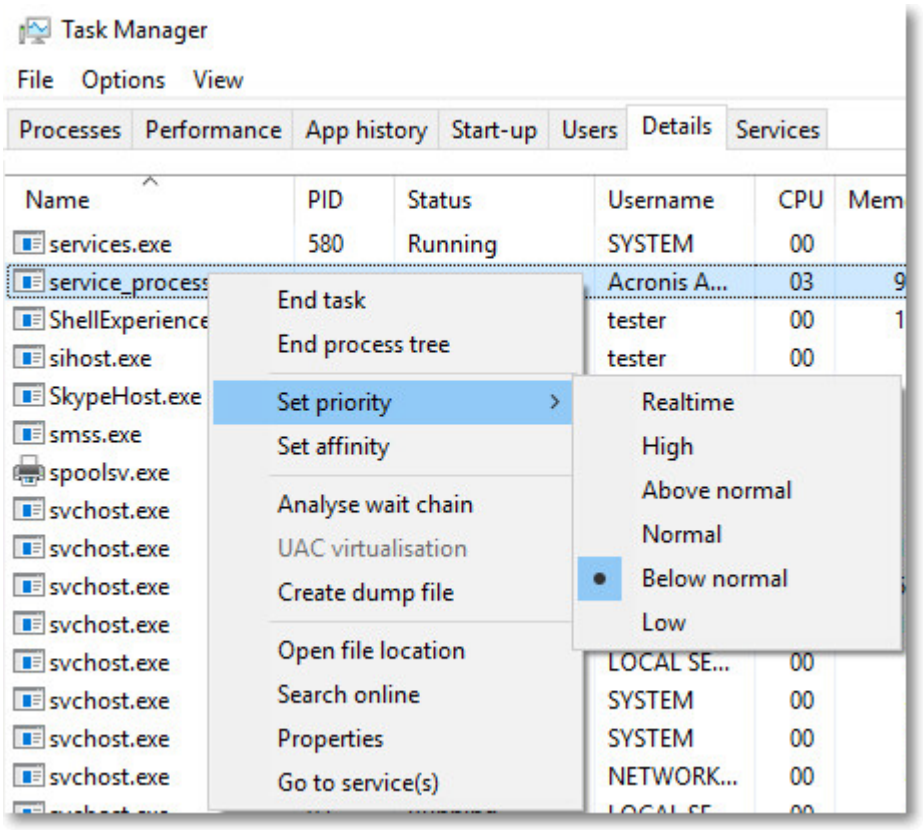
Parameter ini menentukan prioritas proses pencadangan di sistem operasi.

Pengaturan yang tersedia adalah: **Rendah**, **Normal**, **Tinggi**.

© Acronis International GmbH, 2003-2024

Prioritas proses yang berjalan dalam sebuah sistem menentukan jumlah CPU dan sumber daya sistem yang dialokasikan untuk proses tersebut. Menurunkan prioritas pencadangan akan membebaskan lebih banyak sumber daya untuk aplikasi lain. Meningkatkan prioritas pencadangan dapat mempercepat proses pencadangan dengan meminta sistem operasi mengalokasikan lebih banyak sumber daya seperti CPU ke aplikasi cadangan. Namun, efek yang dihasilkan akan bergantung pada penggunaan CPU keseluruhan dan faktor lain seperti kecepatan masuk/keluar disk atau lalu lintas jaringan.

Opsi ini mengatur prioritas proses pencadangan (**service_process.exe)** di Windows dan kelancaran proses pencadangan (**service_process)** di Linux dan macOS.



Tabel di bawah merangkum pemetaan untuk pengaturan ini di Windows, Linux, dan macOS.

Prioritas Cyber Protection	Prioritas Windows	Kelancaran Linux dan macOS
Rendah	Di bawah normal	10
Normal	Normal	0
Tinggi	Tinggi	-10

© Acronis International GmbH, 2003-2024

Kecepatan output selama pencadangan

Opsi ini memungkinkan Anda untuk membatasi kecepatan penulisan hard drive (ketika mencadangkan ke folder lokal) atau kecepatan mentransfer data cadangan melalui jaringan (ketika mencadangkan ke jaringan bersama atau penyimpanan awan).

Ketika opsi ini diaktifkan, Anda dapat menentukan kecepatan output maksimum yang diizinkan:

- Sebagai persentase dari perkiraan kecepatan penulisan hard disk tujuan (saat mencadangkan ke folder lokal) atau dari perkiraan kecepatan maksimum koneksi jaringan (saat mencadangkan ke jaringan bersama atau penyimpanan awan).

  Pengaturan ini hanya berfungsi jika agen berjalan di Windows.
- Dalam KB/detik (untuk semua tujuan).

Pengiriman Data Fisik

Opsi ini tersedia jika tujuan pencadangan atau replikasi adalah penyimpanan cloud dan format pencadangan diatur ke **Versi 12**.

Opsi ini efektif untuk pencadangan tingkat disk dan pencadangan file yang dibuat oleh Agen untuk Windows, Agen untuk Linux, Agen untuk Mac, Agen untuk VMware, Agen untuk Hyper-V, dan Agen untuk Virtuozzo.

Gunakan opsi ini untuk mengirimkan cadangan penuh pertama yang dibuat oleh rencana proteksi ke penyimpanan awan pada drive hard disk menggunakan layanan Pengiriman Data Fisik. Pencadangan bertahap berikutnya dilakukan melalui jaringan.

Untuk pencadangan lokal yang direplikasi ke penyimpanan awan, cadangan bertahap berlanjut dan disimpan secara lokal hingga cadangan awal diunggah ke penyimpanan awan. Lalu semua perubahan bertahap direplikasi ke awan dan replikasi berlanjut sesuai jadwal pencadangan.

Nilai prasetelnya adalah: **Dinonaktifkan.**

Tentang layanan Pengiriman Data Fisik

Antarmuka web layanan Pengiriman Data Fisik hanya tersedia untuk administrator.

Untuk petunjuk terperinci tentang penggunaan layanan Pengiriman Data Fisik dan alat pembuatan pesanan, lihat Panduan Administrator Pengiriman Data Fisik. Untuk mengakses dokumen ini di antarmuka web layanan Pengiriman Data Fisik, klik ikon tanda tanya.

Ikhtisar tentang proses pengiriman data fisik

1. [Untuk mengirim cadangan yang memiliki penyimpanan awan sebagai lokasi cadangan utama]
   a. Buat rencana proteksi baru dengan cadangan ke awan.
   b. Pada baris **Opsi pencadangan**, klik **Ubah**.
   c. Dalam daftar opsi yang tersedia, klik **Pengiriman Data Fisik**.

© Acronis International GmbH, 2003-2024

Anda dapat mencadangkan langsung ke drive yang dapat dilepas atau mencadangkan ke folder lokal atau folder jaringan, lalu salin/pindahkan cadangan ke drive.

2. [Untuk mengirim cadangan lokal yang direplikasi ke awan]

   Catatan
   Opsi ini didukung dengan versi agen proteksi dari rilis C21.06 atau versi yang lebih baru.

   a. Buat rencana proteksi baru dengan cadangan ke penyimpanan lokal atau jaringan.
   b. Klik **Tambah lokasi** dan pilih **Penyimpanan awan**.
   c. Pada baris lokasi **Penyimpanan awan**, klik roda gigi dan pilih **Pengiriman Data Fisik**.

3. Dalam **Gunakan Pengiriman Data Fisik**, klik **Iya** dan **Selesai**.
   Opsi Enkripsi diaktifkan secara otomatis dalam rencana proteksi karena semua cadangan yang dikirim harus dienkripsi.
4. Pada baris **Enkripsi**, klik **Tentukan kata sandi** dan masukkan kata sandi untuk enkripsi.
5. Pada baris **Pengiriman Data Fisik**, pilih drive yang dapat dilepas untuk menyimpan cadangan awal.
6. Klik **Buat** untuk menyimpan rencana proteksi.
7. Setelah pencadangan pertama selesai, gunakan antarmuka web layanan Pengiriman Data Fisik untuk mengunduh alat pembuatan pesanan dan membuat pesanan.
   Untuk mengakses antarmuka web ini, masuk ke portal manajemen, klik **Ikhtisar** > **Penggunaan**, lalu klik **Kelola layanan** pada **Pengiriman Data Fisik**.

   Penting
   Setelah pencadangan penuh awal selesai, pencadangan berikutnya harus dilakukan melalui rencana proteksi yang sama. Rencana proteksi lainnya, meskipun dengan parameter yang sama dan untuk mesin yang sama, akan memerlukan siklus Pengiriman Data Fisik lainnya.

8. Kemas drive dan kirim ke pusat data.

   Penting
   Pastikan Anda mengikuti petunjuk pengemasan yang disediakan di Panduan Administrator Pengiriman Data Fisik.

9. Lacak status pesanan menggunakan antarmuka web layanan Pengiriman Data Fisik. Perlu dicatat bahwa pencadangan berikutnya akan gagal hingga pencadangan awal diunggah ke penyimpanan awan.

Perintah pra/pasca

Opsi ini memungkinkan Anda untuk menentukan perintah yang akan dieksekusi secara otomatis sebelum dan setelah prosedur pencadangan.

Skema berikut menggambarkan kapan perintah pra/pasca dieksekusi.

© Acronis International GmbH, 2003-2024

Perintah pra-pencadangan	Cadangan	Perintah pasca-pencadangan

Contoh bagaimana Anda dapat menggunakan perintah pra/pasca:

- Hapus beberapa file sementara dari disk sebelum memulai pencadangan.
- Konfigurasikan produk antivirus pihak ketiga yang akan dimulai setiap kali sebelum pencadangan dimulai.
- Salin cadangan secara selektif ke lokasi lain. Opsi ini mungkin berguna karena replikasi yang dikonfigurasi dalam rencana proteksi akan menyalin *setiap* cadangan ke lokasi berikutnya.

Agen melakukan replikasi *setelah* mengeksekusi perintah pasca-cadangan.

Program tidak mendukung perintah interaktif, yaitu perintah yang memerlukan input pengguna (misalnya, "pause".)

Perintah pra-pencadangan

Untuk menentukan file perintah/batch yang akan dieksekusi sebelum proses pencadangan dimulai

1. Aktifkan switch **Eksekusi perintah sebelum pencadangan**.
2. Di bidang **Perintah...**, ketik perintah atau jelajahi ke file batch. Program tidak mendukung perintah interaktif, yaitu perintah yang memerlukan input pengguna (misalnya, "jeda".)
3. Di bidang **Direktori kerja**, tentukan jalur ke direktori lokasi file perintah/batch akan dieksekusi.
4. Di bidang **Argumen**, tentukan argumen eksekusi perintah, jika diperlukan.
5. Tergantung pada hasil yang ingin Anda peroleh, pilih opsi yang sesuai seperti yang dijelaskan pada tabel di bawah.
6. Klik **Selesai**.

Kotak centang	**Pemilihan**			
Gagalkan pencadangan jika eksekusi perintah gagal*	Dipilih	Dihapus	Dipilih	Dihapus
Jangan cadangkan sampai eksekusi perintah selesai	Dipilih	Dipilih	Dihapus	Dihapus
Hasil				
	Prasetel	Lakukan	N/A	Lakukan

© Acronis International GmbH, 2003-2024

	Lakukan pencadangan hanya setelah perintah berhasil dieksekusi. Gagalkan pencadangan jika eksekusi perintah gagal.	pencadangan setelah perintah dieksekusi, meskipun eksekusi gagal atau berhasil.		pencadangan bersama dengan eksekusi perintah, apa pun hasil eksekusi perintahnya.

* Perintah dianggap gagal jika mengeluarkan kode yang tidak sama dengan nol.

Catatan
Jika skrip gagal karena konflik terkait versi pustaka yang diperlukan di Linux, kecualikan variabel lingkungan `LD_LIBRARY_PATH` dan `LD_PRELOAD` dengan menambahkan baris berikut dalam skrip Anda:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Perintah pasca-pencadangan

Untuk menentukan file perintah/dapat dieksekusi yang akan dieksekusi setelah pencadangan selesai

1. Aktifkan switch **Eksekusi perintah setelah pencadangan**.
2. Di bidang **Perintah...**, ketik perintah atau jelajahi ke file batch.
3. Di bidang **Direktori kerja**, tentukan jalur ke direktori lokasi file perintah/batch akan dieksekusi.
4. Di bidang **Argumen**, tentukan argumen eksekusi perintah, jika diperlukan.
5. Pilih kotak centang **Gagalkan pencadangan jika eksekusi perintah gagal** jika keberhasilan eksekusi perintah sangat penting bagi Anda. Perintah dianggap gagal jika mengeluarkan kode yang tidak sama dengan nol. Jika eksekusi perintah gagal, status cadangan akan diatur ke **Eror**. Ketika kotak centang tidak dipilih, hasil eksekusi perintah tidak akan memengaruhi kegagalan atau keberhasilan pencadangan. Anda dapat melacak hasil eksekusi perintah dengan menjelajahi tab **Aktivitas**.
6. Klik **Selesai**.

Perintah pengambilan data pra/pasca

Opsi ini memungkinkan Anda untuk menentukan perintah yang akan dijalankan secara otomatis sebelum dan setelah pengambilan data (yaitu, mengambil snapshot data). Pengambilan data dilakukan di awal prosedur pencadangan.

Skema berikut menggambarkan kapan perintah pengambilan pra/pasca data dijalankan.

	<---------- Cadangan ---------->	

© Acronis International GmbH, 2003-2024

Perintah pra-pencadangan	Perintah pengambilan pra-data	Pengambilan data	Perintah pengambilan pasca-data	Tulis data ke set cadangan	Perintah pasca-pencadangan

Interaksi dengan opsi pencadangan lainnya

Menjalankan perintah pengambilan data pra/pasca dapat dimodifikasi oleh opsi pencadangan lainnya.

Jika opsi **Snapshot multivolume** diaktifkan, perintah pengambilan data pra/pasca akan berjalan hanya satu kali karena snapshot untuk semua volume dibuat secara bersamaan. Jika opsi **Snapshot multivolume** dinonaktifkan, perintah pengambilan data pra/pasca akan berjalan untuk setiap volume yang sedang dicadangkan karena snapshot dibuat secara berurutan, satu volume secara bergantian.

Jika opsi **Layanan Menyalin Bayangan Volume (VSS)** diaktifkan, perintah pengambilan data pra/pasca dan tindakan Microsoft VSS akan berjalan seperti berikut:

Perintah sebelum pengambilan data > *Tunda VSS* > *Pengambilan data* > *Lanjut VSS* > *Perintah setelah pengambilan data*

Dengan menggunakan perintah pengambilan pra/pasca data, Anda dapat menunda dan melanjutkan database atau aplikasi yang tidak kompatibel dengan VSS. Karena pengambilan data selesai dalam hitungan detik, waktu idle database atau aplikasi akan menjadi minimal.

Perintah pengambilan pra-data

Untuk menentukan file perintah/batch yang akan dieksekusi sebelum pengambilan data

1. Aktifkan switch **Eksekusi perintah sebelum pengambilan data**.
2. Di bidang **Perintah...**, ketik perintah atau jelajahi ke file batch. Program tidak mendukung perintah interaktif, yaitu perintah yang memerlukan input pengguna (misalnya, "jeda".)
3. Di bidang **Direktori kerja**, tentukan jalur ke direktori lokasi file perintah/batch akan dieksekusi.
4. Di bidang **Argumen**, tentukan argumen eksekusi perintah, jika diperlukan.
5. Tergantung pada hasil yang ingin Anda peroleh, pilih opsi yang sesuai seperti yang dijelaskan pada tabel di bawah.
6. Klik **Selesai**.

Kotak centang	**Pemilihan**			
Gagalkan pencadangan jika eksekusi perintah gagal*	Dipilih	Dihapus	Dipilih	Dihapus
Jangan lakukan	Dipilih	Dipilih	Dihapus	Dihapus

© Acronis International GmbH, 2003-2024

pengambilan data sampai eksekusi perintah selesai				
Hasil				
	Prasetel Lakukan pengambilan data hanya setelah perintah berhasil dieksekusi. Gagalkan pencadangan jika eksekusi perintah gagal.	Lakukan pengambilan data setelah perintah dieksekusi, meskipun eksekusi gagal atau berhasil.	N/A	Lakukan pengambilan data bersama dengan eksekusi perintah, apa pun hasil eksekusi perintahnya.

* Perintah dianggap gagal jika mengeluarkan kode yang tidak sama dengan nol.

Catatan
Jika skrip gagal karena konflik terkait versi pustaka yang diperlukan di Linux, kecualikan variabel lingkungan `LD_LIBRARY_PATH` dan `LD_PRELOAD` dengan menambahkan baris berikut dalam skrip Anda:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Perintah pengambilan pasca-data

Untuk menentukan file perintah/batch yang akan dieksekusi setelah pengambilan data

1. Aktifkan switch **Eksekusi perintah setelah pengambilan data**.
2. Di bidang **Perintah...**, ketik perintah atau jelajahi ke file batch. Program tidak mendukung perintah interaktif, yaitu perintah yang memerlukan input pengguna (misalnya, "jeda".)
3. Di bidang **Direktori kerja**, tentukan jalur ke direktori lokasi file perintah/batch akan dieksekusi.
4. Di bidang **Argumen**, tentukan argumen eksekusi perintah, jika diperlukan.
5. Tergantung pada hasil yang ingin Anda peroleh, pilih opsi yang sesuai seperti yang dijelaskan pada tabel di bawah.
6. Klik **Selesai**.

Kotak centang	**Pemilihan**			
Gagalkan pencadangan jika eksekusi perintah gagal*	Dipilih	Dihapus	Dipilih	Dihapus

© Acronis International GmbH, 2003-2024

Jangan cadangkan sampai eksekusi perintah selesai	Dipilih	Dipilih	Dihapus	Dihapus
Hasil				
	Prasetel Lanjutkan pencadangan hanya setelah perintah berhasil dieksekusi.	Lanjutkan pencadangan setelah perintah dieksekusi, meskipun eksekusi perintah gagal atau berhasil.	N/A	Lanjutkan pencadangan bersama dengan eksekusi perintah, apa pun hasil eksekusi perintahnya.

* Perintah dianggap gagal jika mengeluarkan kode yang tidak sama dengan nol.

Penjadwalan

Opsi ini menentukan apakah pencadangan dimulai tepat sesuai jadwal atau dengan penundaan, dan berapa banyak mesin virtual yang dicadangkan secara bersamaan.

Untuk informasi lebih lanjut tentang cara mengonfigurasi jadwal pencadangan, lihat "Menjalankan pencadangan sesuai jadwal" (hlm. 420).

Nilai prasetelnya adalah: **Distribusikan waktu mulai pencadangan dalam sebuah jendela waktu**. **Penundaan maksimum**: **30 menit**.

Anda dapat memilih salah satu dari tindakan berikut:

- **Mulai semua pencadangan sesuai jadwal**
  Pencadangan mesin fisik akan dimulai sesuai jadwal. Mesin virtual akan dicadangkan satu per satu.
- **Distribusikan waktu mulai dalam jendela waktu**
  Pencadangan mesin fisik akan dimulai dengan penundaan dari waktu yang dijadwalkan. Nilai penundaan untuk setiap mesin dipilih secara acak dan berkisar dari nilai nol hingga nilai maksimal yang Anda tentukan. Anda mungkin ingin menggunakan pengaturan ini ketika mencadangkan beberapa mesin ke lokasi jaringan, untuk menghindari beban jaringan yang berlebihan. Nilai penundaan untuk setiap mesin ditentukan ketika rencana proteksi diterapkan pada mesin dan tetap sama hingga Anda mengedit rencana proteksi dan mengubah nilai penundaan maksimal.
  Mesin virtual akan dicadangkan satu per satu.
- **Batasi jumlah pencadangan yang berjalan secara simultan sebanyak**
  Gunakan opsi ini untuk mengatur pencadangan paralel mesin virtual yang dicadangkan pada level hypervisor (cadangan tanpa agen).

© Acronis International GmbH, 2003-2024

Rencana proteksi dalam opsi yang dipilih ini dapat dijalankan bersamaan dengan rencana proteksi lain yang sedang dijalankan oleh agen yang sama pada waktu yang sama. Saat Anda memilih opsi ini, Anda harus menentukan jumlah cadangan paralel per rencana. Jumlah total mesin yang dicadangkan bersamaan oleh semua rencana dibatasi hingga 10 per agen. Untuk mempelajari cara mengubah batas bawaan, lihat "Membatasi jumlah total mesin virtual yang dicadangkan secara simultan" (hlm. 699).

Rencana proteksi yang dalam opsi ini tidak dipilih menjalankan operasi pencadangan secara berurutan, dari satu mesin virtual ke mesin lainnya.

Pencadangan sektor demi sektor

Opsi ini hanya efektif untuk pencadangan tingkat disk.

Opsi ini menentukan apakah salinan disk atau volume yang tepat pada tingkat fisik sudah dibuat.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Jika opsi ini diaktifkan, semua sektor disk atau volume akan dicadangkan, termasuk ruang yang tidak teralokasi dan sektor yang bebas data. Hasil pencadangan akan berukuran sama dengan disk yang dicadangkan (jika opsi "Tingkat kompresi" diatur ke **Tidak ada**). Perangkat lunak secara otomatis beralih ke mode sektor per sektor ketika mencadangkan drive dengan sistem file yang tidak dikenal atau tidak didukung.

Catatan
Tidak dimungkinkan untuk melakukan pemulihan data aplikasi dari pencadangan yang dibuat dalam mode sektor demi sektor.

Pembagian

Opsi ini memungkinkan Anda memilih metode pembagian cadangan besar ke file yang lebih kecil.

Catatan
Pemisahan tidak tersedia dalam rencana proteksi yang menggunakan penyimpanan awan sebagai lokasi cadangan.

Nilai prasetelnya adalah:

- Jika lokasi cadangan berada di folder lokal atau jaringan (SMB), dan format cadangan adalah Versi 12: **Ukuran tetap - 200 GB**

  Pengaturan ini memungkinkan perangkat lunak cadangan untuk bekerja dengan data dalam jumlah besar pada sistem file NTFS, tanpa efek negatif yang disebabkan oleh fragmentasi.
- Atau: **Otomatis**

Pengaturan berikut tersedia:

- **Otomatis**

  Cadangan akan dibagi jika melebihi ukuran file maksimum yang didukung oleh sistem file.

© Acronis International GmbH, 2003-2024

- **Ukuran tetap**
  Masukkan ukuran file yang diinginkan atau pilih dari daftar drop-down.

Penanganan kegagalan tugas

Opsi ini menentukan perilaku program ketika eksekusi rencana proteksi yang dijadwalkan gagal atau mesin Anda dimulai kembali saat cadangan sedang dijalankan. Opsi ini tidak efektif jika rencana proteksi dimulai secara manual.

Jika opsi ini diaktifkan, program akan berusaha menjalankan rencana proteksi lagi. Anda dapat menentukan jumlah percobaan dan interval waktu di antara percobaan tersebut. Program akan berhenti mencoba segera setelah percobaan berhasil atau jumlah percobaan yang ditentukan telah habis, mana pun yang terlebih dahulu tercapai.

Jika opsi ini diaktifkan dan mesin Anda dimulai kembali saat cadangan berjalan, operasi pencadangannya tidak akan gagal. Beberapa menit setelah memulai kembali, operasi pencadangan akan terus berlanjut secara otomatis dan melengkapi file cadangan dengan data yang hilang. Untuk kasus penggunaan ini, opsi **Interval di antara percobaan** tidak relevan.

Nilai prasetelnya adalah: **Diaktifkan**.

Catatan
Opsi ini tidak efektif untuk cadangan forensik.

Syarat mulai tugas

Opsi ini efektif pada sistem operasi Windows dan Linux.

Opsi ini menentukan perilaku program saat tugas akan segera dimulai (waktu yang dijadwalkan atau peristiwa yang ditentukan pada jadwal terjadi), namun syarat (atau lebih dari satu syarat) tidak terpenuhi. Untuk informasi lebih lanjut tentang kondisi lihat "Persyaratan untuk memulai" (hlm. 426).

Nilai prasetelnya adalah: **Tunggu sampai persyaratan jadwal dipenuhi.**

Tunggu sampai persyaratan jadwal dipenuhi

Dengan pengaturan ini, penjadwal mulai memantau syarat dan menjalankan tugas begitu syarat terpenuhi. Jika syarat tidak pernah terpenuhi, tugas tidak akan pernah dimulai.

Untuk menangani situasi ketika syarat tidak terpenuhi dalam waktu yang sangat lama dan penundaan tugas menjadi berisiko, Anda dapat menentukan interval waktu di mana tugas akan berjalan tanpa memperhatikan syarat. Pilih kotak centang **Tetap jalankan tugas setelahnya** dan tentukan interval waktunya. Tugas akan segera dimulai begitu syarat terpenuhi ATAU waktu tunda maksimum terlewati, mana pun yang terlebih dahulu tercapai.

© Acronis International GmbH, 2003-2024

Lewati eksekusi tugas

Menunda tugas mungkin tidak dapat diterima, misalnya, saat Anda harus mengeksekusi tugas tepat pada waktu yang telah ditentukan. Dengan demikian, lebih baik melewati tugas daripada menunggu syarat terpenuhi, khususnya jika tugas relatif sering terjadi.

Layanan Menyalin Bayangan Volume (VSS)

Opsi ini hanya berlaku untuk sistem operasi Windows.

Opsi ini menentukan apakah cadangan dapat berfungsi ketika salah satu atau beberapa penulis Layanan Menyalin Bayangan Volume (VSS) gagal berfungsi dan penyedia layanan mana yang harus memberi tahu aplikasi yang sadar VSS bahwa pencadangan akan dimulai.

Penggunaan Layanan Menyalin Bayangan Volume memastikan konsistensi status semua data yang digunakan oleh aplikasi; khususnya, penyelesaian semua transaksi database pada saat perangkat lunak pencadangan mengambil snapshot data. Konsistensi data, selanjutnya, memastikan bahwa aplikasi akan pulih dalam status yang tepat dan segera dapat beroperasi setelah pemulihan.

Snapshot hanya digunakan selama operasi pencadangan, dan secara otomatis dihapus ketika operasi pencadangan selesai. Tidak ada file sementara yang disimpan.

Anda juga dapat menggunakan Perintah pengambilan data pra/pasca untuk memastikan data dicadangkan secara konsisten. Misalnya, tentukan perintah pengambilan pra-data yang akan menunda database dan melakukan flush semua cache untuk memastikan semua transaksi selesai; dan kemudian tentukan perintah pengambilan pasca-data yang akan melanjutkan operasi database setelah snapshot diambil.

Catatan
File dan folder yang ditentukan dalam kunci registri **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** tidak akan dicadangkan. Secara khusus, File Data Outlook (.ost) offline tidak dicadangkan karena mereka ditentukan dalam nilai **OutlookOST** dari kunci ini.

Abaikan penulis VSS yang gagal

Anda dapat memilih salah satu dari tindakan berikut:

- **Abaikan penulis VSS yang gagal**
  Dengan opsi ini, Anda dapat membuat pencadangan sekalipun saat salah satu atau beberapa penulis VSS gagal berfungsi.

  Penting
  Cadangan terinformasi untuk aplikasi akan selalu gagal jika penulis aplikasi tertentu gagal. Misalnya, jika Anda membuat cadangan terinformasi untuk aplikasi untuk data SQL Server, dan **SqlServerWriter** gagal, maka operasi pencadangan juga akan gagal.

© Acronis International GmbH, 2003-2024

Saat opsi ini diaktifkan, akan ada tiga upaya berturut-turut untuk snapshot VSS.

Di upaya pertama, diperlukan semua penulis VSS. Jika upaya ini gagal, caranya akan diulangi. Jika upaya kedua gagal juga, penulis VSS yang gagal akan dikecualikan dari cakupan operasi pencadangan, dan kemudian akan berlanjut ke upaya ketiga. Jika upaya ketiga berhasil, cadangan akan diselesaikan dengan peringatan tentang penulis VSS yang gagal. Jika upaya ketiga tidak berhasil, pencadangan akan gagal.

- **Memerlukan pemrosesan yang berhasil untuk semua penulis VSS**
  Jika ada penulis VSS yang gagal, operasi pencadangan juga akan gagal.

Pilih penyedia snapshot

Anda dapat memilih salah satu dari tindakan berikut:

- **Memilih penyedia snapshot secara otomatis**
  Pilih secara otomatis di antara penyedia snapshot perangkat keras, penyedia snapshot perangkat lunak, dan penyedia Microsoft Software Shadow Copy.
- **Gunakan penyedia Microsoft Software Shadow Copy**
  Kami menyarankan Anda memilih opsi ini saat membuat cadangan server aplikasi (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint, atau Active Directory).

Aktifkan cadangan penuh VSS

Jika opsi ini diaktifkan, log dari Microsoft Exchange Server dan aplikasi lainnya yang sadar VSS (kecuali untuk Microsoft SQL Server) akan terpotong setelah setiap pencadangan tingkat disk penuh, inkremental, atau diferensial berhasil.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Biarkan opsi ini dinonaktifkan dalam kasus berikut:

- Jika Anda menggunakan Agen untuk Exchange atau perangkat lunak pihak ketiga untuk mencadangkan data Exchange Server. Karena pemotongan log akan mengganggu pencadangan log transaksi beruntun.
- Jika Anda menggunakan perangkat lunak pihak ketiga untuk mencadangkan data SQL Server. Alasannya adalah karena perangkat lunak pihak ketiga akan mengambil cadangan tingkat disk yang dihasilkan untuk pencadangan penuh mereka "sendiri". Akibatnya, cadangan diferensial berikutnya dari data SQL Server akan gagal. Pencadangan akan terus gagal hingga perangkat lunak pihak ketiga membuat cadangan penuh "sendiri" berikutnya.
- Jika aplikasi yang mendukung VSS lainnya berjalan di mesin dan Anda perlu menyimpan log mereka untuk alasan apa pun.

Penting
Mengaktifkan opsi ini tidak mengakibatkan pemotongan log Microsoft SQL Server. Untuk memotong log SQL Server setelah pencadangan, aktifkan opsi pencadangan Pemotongan Log.

© Acronis International GmbH, 2003-2024

Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual

Opsi ini menentukan apakah snapshot yang didiamkan dari mesin virtual akan diambil.

Nilai prasetelnya adalah: **Diaktifkan**.

Saat opsi ini dinonaktifkan, snapshot dengan bunyi akan diambil. Mesin virtual akan dicadangkan dalam status konsisten crash.

Saat opsi ini diaktifkan, transaksi semua aplikasi sadar VSS yang berjalan pada mesin virtual diselesaikan, kemudian snapshot yang disunyikan akan diambil.

Jika snapshot yang disunyikan tidak dapat diambil setelah sejumlah percobaan ulang yang ditentukan dalam opsi "Penanganan kesalahan", dan pencadangan aplikasi diaktifkan, pencadangan akan gagal.

Jika snapshot yang disunyikan tidak dapat diambil setelah sejumlah percobaan ulang yang ditentukan dalam opsi "Penanganan kesalahan", dan pencadangan aplikasi diaktifkan, pencadangan konsisten gagal (crash-consistent) akan dibuat. Untuk membuat pencadangan menjadi gagal alih-alih membuat pencadangan konsisten gagal (crash-consistent), pilih kotak centang **Gagalkan pencadangan apabila mengambil snapshot yang disunyikan tidak memungkinkan**.

Tabel berikut merangkum pengaturan yang tersedia serta hasilnya.

Pengaturan	Snapshot yang disunyikan berhasil diambil		Snapshot yang disunyikan tidak terambil	
	Cadangan aplikasi diaktifkan	**Cadangan aplikasi dinonaktifkan**	**Cadangan aplikasi diaktifkan**	**Cadangan aplikasi dinonaktifkan**
Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual diaktifkan **Pencadangan gagal jika mengambil snapshot yang disunyikan tidak dapat dilakukan** tidak dipilih	Snapshot yang disunyikan diambil. Cadangan konsisten aplikasi dibuat.	Snapshot yang disunyikan diambil. Cadangan konsisten aplikasi dibuat.	Pencadangan gagal.	Snapshot dengan bunyi diambil. Cadangan konsisten gangguan (crash-consistent) dibuat.
Layanan Menyalin	Snapshot yang disunyikan	Snapshot yang disunyikan diambil.	Pencadangan gagal.	Pencadangan gagal.

© Acronis International GmbH, 2003-2024

Pengaturan	Snapshot yang disunyikan berhasil diambil		Snapshot yang disunyikan tidak terambil	
	Cadangan aplikasi diaktifkan	**Cadangan aplikasi dinonaktifkan**	**Cadangan aplikasi diaktifkan**	**Cadangan aplikasi dinonaktifkan**
Bayangan Volume (VSS) untuk mesin virtual diaktifkan **Gagalkan pencadangan jika tidak dapat mengambil snapshot yang didiamkan** dipilih	diambil. Cadangan konsisten aplikasi dibuat.	Cadangan konsisten aplikasi dibuat.		
Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual dinonaktifkan	Snapshot dengan bunyi diambil. Cadangan konsisten gangguan (crash-consistent) dibuat.	Snapshot dengan bunyi diambil. Cadangan konsisten gangguan (crash-consistent) dibuat.	Snapshot dengan bunyi diambil. Cadangan konsisten gangguan (crash-consistent) dibuat.	Snapshot dengan bunyi diambil. Cadangan konsisten gangguan (crash-consistent) dibuat.

Mengaktifkan **Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual** juga memicu skrip pra-beku dan pasca-leleh yang mungkin Anda miliki di mesin virtual yang dicadangkan. Untuk informasi lebih lanjut tentang skrip ini, lihat "Menjalankan skrip pra-beku dan pasca-leleh secara otomatis" (hlm. 692).

Untuk mengambil snapshot yang didiamkan, perangkat lunak cadangan menerapkan VSS di dalam mesin virtual menggunakan VMware Tool, Hyper-V Integration Services, Virtuozzo Guest Tool, atau Red Hat Virtualization Guest Tool, atau QEMU Guest Tool, secara berurutan.

Catatan
Untuk mesin virtual Red Hat Virtualization (oVirt), kami sarankan Anda untuk menginstal QEMU Guest Tool, bukan Red Hat Virtualization Guest Tool. Beberapa versi Red Hat Virtualization Guest Tool tidak mendukung snapshot yang sesuai aplikasi.

Opsi ini tidak memengaruhi mesin virtual Scale Computing HC3. Untuk mesin virtual tersebut, pendiaman bergantung pada apakah alat bantu Scale diinstal di mesin virtual.

Pencadangan mingguan

Opsi ini menentukan apakah cadangan dianggap sebagai "mingguan" dalam aturan retensi dan skema cadangan. Pencadangan "mingguan" adalah pencadangan pertama yang dibuat setelah seminggu dimulai.

© Acronis International GmbH, 2003-2024

Nilai prasetelnya adalah: **Senin**.

Log event Windows

Opsi ini hanya efektif di sistem operasi Windows.

Opsi ini menentukan apakah agen harus mencatat peristiwa operasi pencadangan dalam Log Event Aplikasi Windows (untuk melihat log ini, jalankan eventvwr.exe atau pilih **Panel Kontrol** > **Alat Administratif** > **Event Viewer**). Anda dapat memfilter event yang akan di-log.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Pemulihan

Referensi cepat pemulihan

Tabel berikut merangkum metode pemulihan yang tersedia. Gunakan tabel untuk memilih metode pemulihan yang paling sesuai dengan kebutuhan Anda.

Catatan
Anda tidak dapat memulihkan cadangan di konsol Cyber Protect untuk penyewa dalam mode Kepatuhan. Untuk informasi lebih lanjut tentang cara memulihkan cadangan tersebut, silakan merujuk ke "Memulihkan cadangan untuk penyewa dalam mode Kepatuhan" (hlm. 1085).

Apa yang dipulihkan	Metode pemulihan
Mesin fisik (Windows atau Linux)	Menggunakan konsol Cyber Protect Menggunakan media yang dapat di-boot
Mesin fisik (Mac)	Menggunakan media yang dapat di-boot
Mesin virtual (VMware, Hyper-V, Red Hat Virtualization (oVirt), atau Scale Computing HC3)	Menggunakan konsol Cyber Protect Menggunakan media yang dapat di-boot
Mesin virtual atau kontainer (Virtuozzo, Virtuozzo Hybrid Server, atau Virtuozzo Hybrid Infrastructure)	Menggunakan konsol Cyber Protect
Konfigurasi ESXi	Menggunakan media yang dapat di-boot
File/folder	Menggunakan konsol Cyber Protect Mengunduh file dari penyimpanan awan Menggunakan media yang dapat di-boot

© Acronis International GmbH, 2003-2024

	Mengekstrak file dari pencadangan lokal
Status sistem	Menggunakan konsol Cyber Protect
Database SQL	Menggunakan konsol Cyber Protect
Basis data Exchange	Menggunakan konsol Cyber Protect
Kotak surat Exchange	Menggunakan konsol Cyber Protect
Situs web	Menggunakan konsol Cyber Protect
Microsoft 365	
Kotak surat (Agen untuk Microsoft 365 lokal)	Menggunakan konsol Cyber Protect
Kotak surat (Agen untuk Microsoft 365 awan)	Menggunakan konsol Cyber Protect
Folder publik	Menggunakan konsol Cyber Protect
File OneDrive	Menggunakan konsol Cyber Protect
Data SharePoint Online	Menggunakan konsol Cyber Protect
Google Workspace	
Kotak surat	Menggunakan konsol Cyber Protect
File Google Drive	Menggunakan konsol Cyber Protect
File drive Shared	Menggunakan konsol Cyber Protect

Pemulihan lintas platform

Pemulihan lintas platform tersedia untuk pencadangan seluruh mesin dan pencadangan disk yang berisi sistem operasi.

Pemulihan lintas platform dilakukan dalam kasus berikut:

- Cadangan dibuat oleh satu jenis agen namun dipulihkan oleh jenis agen lain.
- Cadangan berbasis agen dipulihkan pada tingkat hypervisor (pemulihan tanpa agen), atau cadangan tanpa agen dipulihkan oleh agen (pemulihan berbasis agen).
- Cadangan dipulihkan ke perangkat keras yang berbeda (termasuk perangkat keras virtual).

© Acronis International GmbH, 2003-2024

Catatan
Beberapa perangkat periferal, seperti pencetak, mungkin tidak dapat dipulihkan dengan benar saat Anda melakukan pemulihan lintas platform.

Tabel di bawah menunjukkan beberapa contoh pemulihan lintas platform.

Pemulihan lintas platform	
Cadangan tanpa agen	Pemulihan berbasis agen
Cadangan berbasis agen	Pemulihan tanpa agen
Pencadangan oleh Agen untuk Windows	Pemulihan oleh Agen untuk VMware
Pencadangan oleh Agen untuk VMware	Pemulihan oleh Agen untuk Hyper-V
Pencadangan oleh Agen untuk Windows yang diinstal pada mesin virtual VMware ESXi (berbasis agen)	Pemulihan oleh Agen untuk VMware (tanpa agen) pada host VMware ESXi yang sama
Pencadangan oleh Agen untuk Windows	Pemulihan oleh Agen untuk Windows yang diinstal pada mesin dengan perangkat keras yang berbeda
Cadangan mesin fisik	Pemulihan sebagai mesin virtual

Catatan untuk pengguna Mac

- Dimulai dengan 10.11 El Capitan, file, folder, dan proses sistem tertentu ditandai untuk perlindungan dengan perluasan atribut file com.apple.rootless. Fitur ini disebut Perlindungan Integritas Sistem (SIP). File yang dilindungi termasuk aplikasi yang telah diinstal sebelumnya dan sebagian besar folder di /system, /bin, /sbin, /usr.

  File dan folder yang dilindungi tidak dapat ditimpa selama pemulihan dalam sistem operasi. Jika Anda perlu menimpa file yang dilindungi, lakukan pemulihan dalam media yang dapat di-boot.
- Dimulai dengan macOS Sierra 10.12, file yang jarang digunakan dapat dipindahkan ke iCloud melalui fitur Penyimpanan di Awan. Jejak kecil file ini akan disimpan di sistem file. Jejak ini akan dicadangkan, bukan file asli.

  Ketika Anda memulihkan jejak ke lokasi asli, jejak tersebut disinkronkan dengan iCloud dan file asli akan tersedia. Ketika Anda memulihkan jejak ke lokasi yang berbeda, jejak tersebut tidak dapat disinkronkan dan file asli tidak akan tersedia.

Pemulihan aman

Gunakan pemulihan aman dengan pencadangan **Seluruh mesin** atau **Disk/volume** beban kerja Windows untuk memastikan bahwa Anda hanya memulihkan data bebas malware, bahkan jika cadangan mengandung file yang terinfeksi.

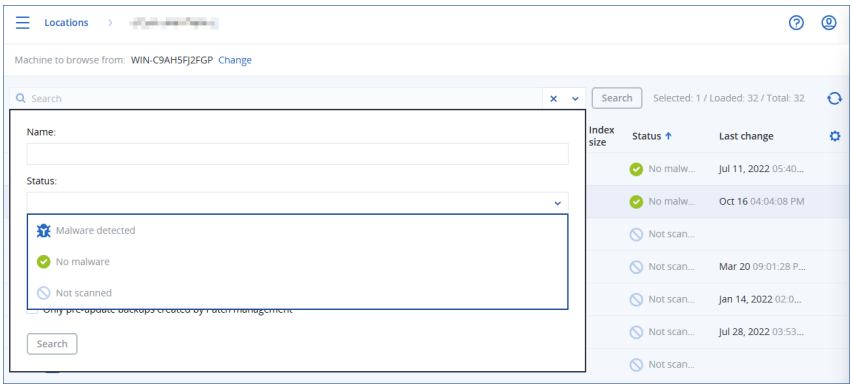
© Acronis International GmbH, 2003-2024

Saat operasi pemulihan aman, cadangan dipindai secara otomatis untuk mencari malware. Lalu, agen perlindungan memulihkan cadangan pada beban kerja target dan menghapus file yang terinfeksi. Hasilnya, cadangan bebas malware dipulihkan.

Sebagai tambahan, salah satu status berikut diberikan kepada cadangan:

- Malware terdeteksi
- Tidak ada malware
- Belum dipindai

Anda dapat memanfaatkan status untuk menyaring arsip cadangan.



Pembatasan

- Pemulihan aman didukung untuk mesin Windows fisik dan virtual di mana agen perlindungan dipasang.
- Pemulihan aman didukung untuk pencadangan **Seluruh mesin** dan **Disk/volume**.
- Hanya volume NTFS yang dipindai untuk mencari malware. Volume non-NTFS akan dipulihkan tanpa pemindaian antimalware.
- Pemulihan aman tidak didukung untuk Cadangan Perlindungan Data berkelanjutan (CDP) dalam arsip. Untuk memulihkan data dari cadangan CDP, jalankan operasi pemulihan **File/folder** tambahan. Untuk informasi lebih lanjut tentang pencadangan CDP, lihat "Perlindungan data berkelanjutan (CDP)" (hlm. 408).

Memulihkan mesin

Memulihkan mesin fisik

Bagian ini menjelaskan pemulihan mesin fisik menggunakan antarmuka web.

Gunakan media yang dapat di-boot, bukan antarmuka web jika Anda perlu memulihkan:

- Mesin yang menjalankan macOS
- Mesin dari penyewa dalam mode Kepatuhan
- Sistem operasi apa pun pada bare metal atau mesin offline

© Acronis International GmbH, 2003-2024

- Struktur volume logis (volume dibuat oleh Logical Volume Manager di Linux). Media memungkinkan Anda membuat ulang struktur volume logis secara otomatis.

Catatan
Anda tidak dapat memulihkan cadangan tingkat disk dari Mac berbasis Intel ke Mac yang menggunakan prosesor silikon Apple, dan sebaliknya. Anda dapat memulihkan file dan folder.

Pemulihan dengan mulai kembali

Pemulihan sistem operasi dan pemulihan volume yang terenkripsi dengan BitLocker memerlukan mulai kembali. Anda dapat memilih untuk memulai kembali mesin secara otomatis atau menetapkan status **Interaksi diperlukan**. Sistem operasi yang dipulihkan kembali online secara otomatis.

Penting
Volume terenkripsi yang dicadangkan dipulihkan menjadi tidak terenkripsi.

Pemulihan volume terenkripsi BitLocker memerlukan adanya volume tidak-terenkripsi di mesin yang sama, dan volume ini memiliki setidaknya ruang bebas sebesar 1 GB. Jika kondisi ini tidak terpenuhi, pemulihan gagal.

Memulihkan sistem volume terenkripsi tidak memerlukan tindakan tambahan apa pun. Untuk memulihkan bukan-sistem volume terenkripsi, Anda harus menguncinya terlebih dahulu, dengan membuka file yang ditempatkan dalam volume ini. Sebaliknya, pemulihan akan terus berlanjut tanpa mulai kembali dan volume yang dipulihkan mungkin tidak dikenali oleh Windows.

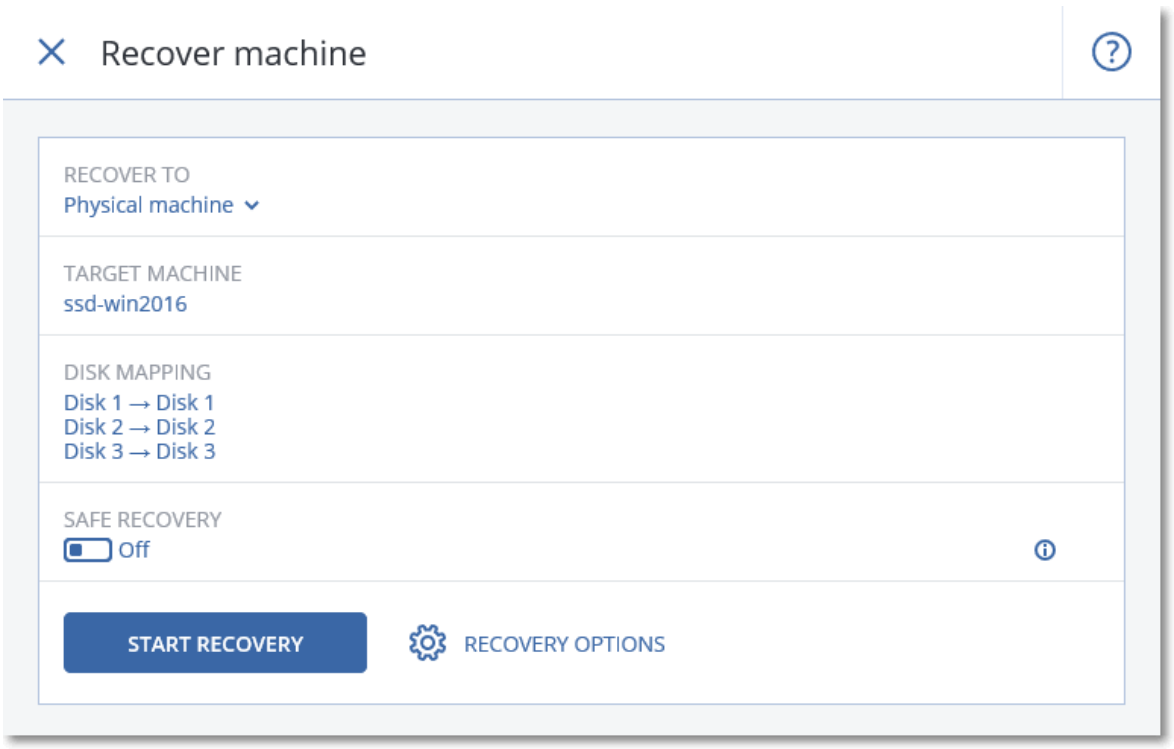
Catatan
Jika pemulihan gagal dan mesin Anda dimulai kembali dengan pesan kesalahan `Tidak dapat mendapatkan file dari partisi`, coba nonaktifkan Boot Aman. Untuk informasi lebih lanjut tentang cara melakukannya, lihat Menonaktifkan Boot Aman di dokumentasi Microsoft.

Untuk memulihkan mesin fisik

1. Pilih mesin yang dicadangkan.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Lakukan yang berikut ini:
   - Jika lokasi cadangan adalah awan atau penyimpanan bersama (yaitu agen lain dapat mengaksesnya), klik **Pilih mesin**, pilih mesin target yang online, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab Penyimpanan cadangan.
   - Pulihkan mesin seperti yang dijelaskan pada "Memulihkan disk menggunakan media yang dapat di-boot".
4. Klik **Pulihkan** > **Seluruh mesin**.
   Perangkat lunak memetakan secara otomatis disk dari cadangan ke disk mesin target.

© Acronis International GmbH, 2003-2024

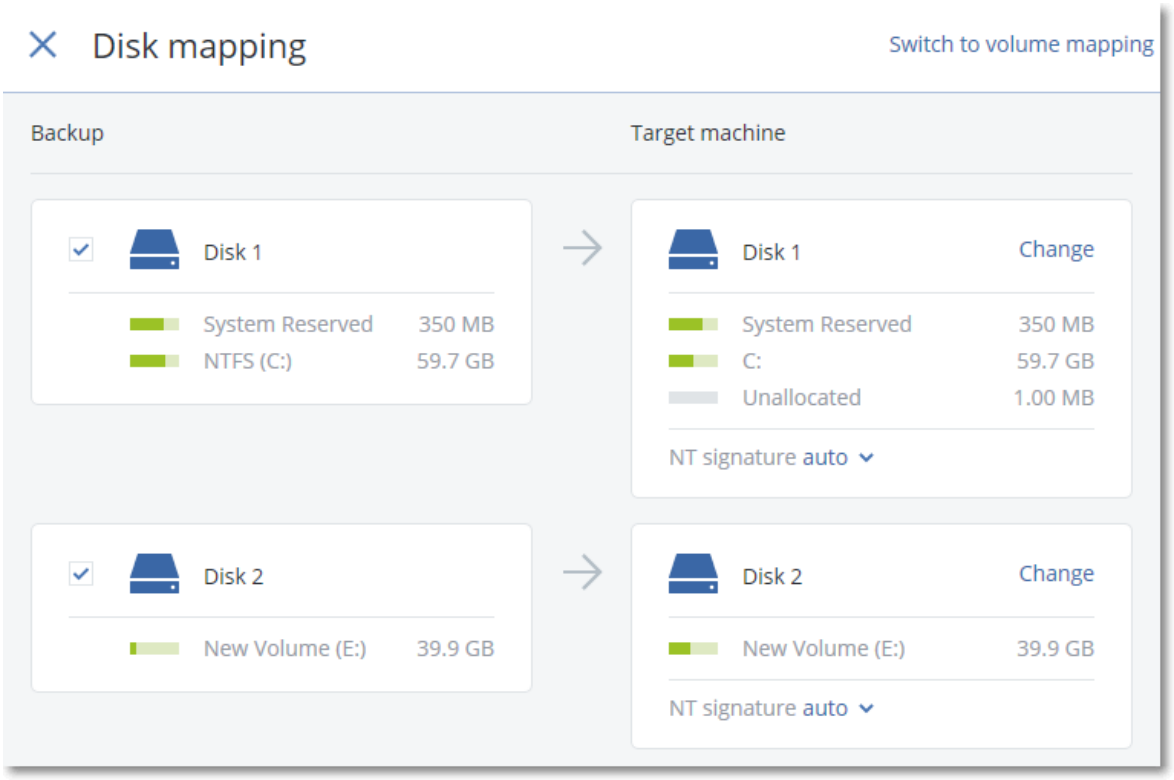
Untuk memulihkan ke mesin fisik lain, klik **Mesin target**, lalu pilih mesin target yang sedang online.



5. Jika Anda tidak puas dengan hasil pemetaan atau pemetaan disk tidak berhasil, klik **Pemetaan volume** untuk memetakan ulang disk secara manual.

   Bagian pemetaan juga memungkinkan Anda memilih disk atau volume individual untuk pemulihan. Anda dapat beralih antara memulihkan disk dan volume menggunakan tautan **Alihkan ke...** di sudut kanan atas.

© Acronis International GmbH, 2003-2024



6. [Hanya tersedia untuk mesin Windows tempat agen perlindungan diinstal.] Aktifkan tombol **pemulihan Aman** untuk memastikan bahwa data yang dipulihkan bebas malware. Untuk informasi lebih lanjut mengenai cara pemulihan aman bekerja, lihat "Pemulihan aman" (hlm. 497).
7. Klik **Mulai pemulihan**.
8. Konfirmasi bahwa Anda ingin menimpa disk dengan versi yang dicadangkannya. Pilih apakah Anda ingin mulai kembali mesin secara otomatis.

Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

Mesin fisik ke virtual

Anda dapat memulihkan mesin fisik ke mesin virtual di salah satu hypervisor yang didukung. Ini juga merupakan mekanisme untuk memigrasi mesin fisik ke mesin virtual. Untuk informasi selengkapnya tentang jalur migrasi P2V yang didukung, lihat "Migrasi mesin".

Bagian ini menjelaskan pemulihan mesin fisik sebagai mesin virtual dengan menggunakan antarmuka web. Operasi ini dapat dilakukan jika setidaknya satu agen untuk hypervisor yang relevan diinstal dan terdaftar di Server Manajemen Acronis. Misalnya, pemulihan ke VMware ESXi memerlukan setidaknya satu Agen untuk VMware, pemulihan ke Hyper-V memerlukan setidaknya satu Agen untuk Hyper-V yang diinstal dan terdaftar di lingkungan.

Pemulihan melalui antarmuka web tidak tersedia untuk penyewa dalam mode Kepatuhan.

© Acronis International GmbH, 2003-2024

Catatan
Anda tidak dapat memulihkan mesin virtual MacOS ke host Hyper-V karena Hyper-V tidak mendukung MacOS. Anda dapat memulihkan mesin virtual MacOS ke host VMware yang diinstal di perangkat keras Mac.

Selain itu, Anda tidak dapat memulihkan cadangan mesin fisik macOS sebagai mesin virtual.

Untuk memulihkan mesin fisik sebagai mesin virtual

1. Pilih mesin yang dicadangkan.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Lakukan yang berikut ini:
   - Jika lokasi cadangan adalah penyimpanan awan atau penyimpanan bersama (yang dapat diakses agen lain), klik **Pilih mesin**, pilih mesin yang online, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab Penyimpanan cadangan.
   - Pulihkan mesin seperti yang dijelaskan pada "Memulihkan disk menggunakan media yang dapat di-boot".
4. Klik **Pulihkan** > **Seluruh mesin**.
5. Pada **Pulihkan ke**, pilih **Mesin virtual**.
6. Klik **Mesin target**.
   a. Pilih hypervisor.

      Catatan
      Setidaknya satu agen untuk hypervisor tersebut harus diinstal dan terdaftar di Server Manajemen Acronis.

   b. Pilih apakah akan Anda ingin melakukan pemulihan ke mesin baru atau mesin yang sudah ada. Opsi mesin baru lebih disarankan karena tidak memerlukan konfigurasi disk dari mesin target untuk mencocokkan sama persis dengan konfigurasi disk dalam cadangan.
   c. Pilih host dan tentukan nama mesin yang baru, atau pilih mesin target yang sudah ada.
   d. Klik **OK**.
7. [Untuk Virtuozzo Hybrid Infrastructure] Klik **Pengaturan VM** untuk memilih **Cara**. Sebagai pilihan, Anda dapat mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual.

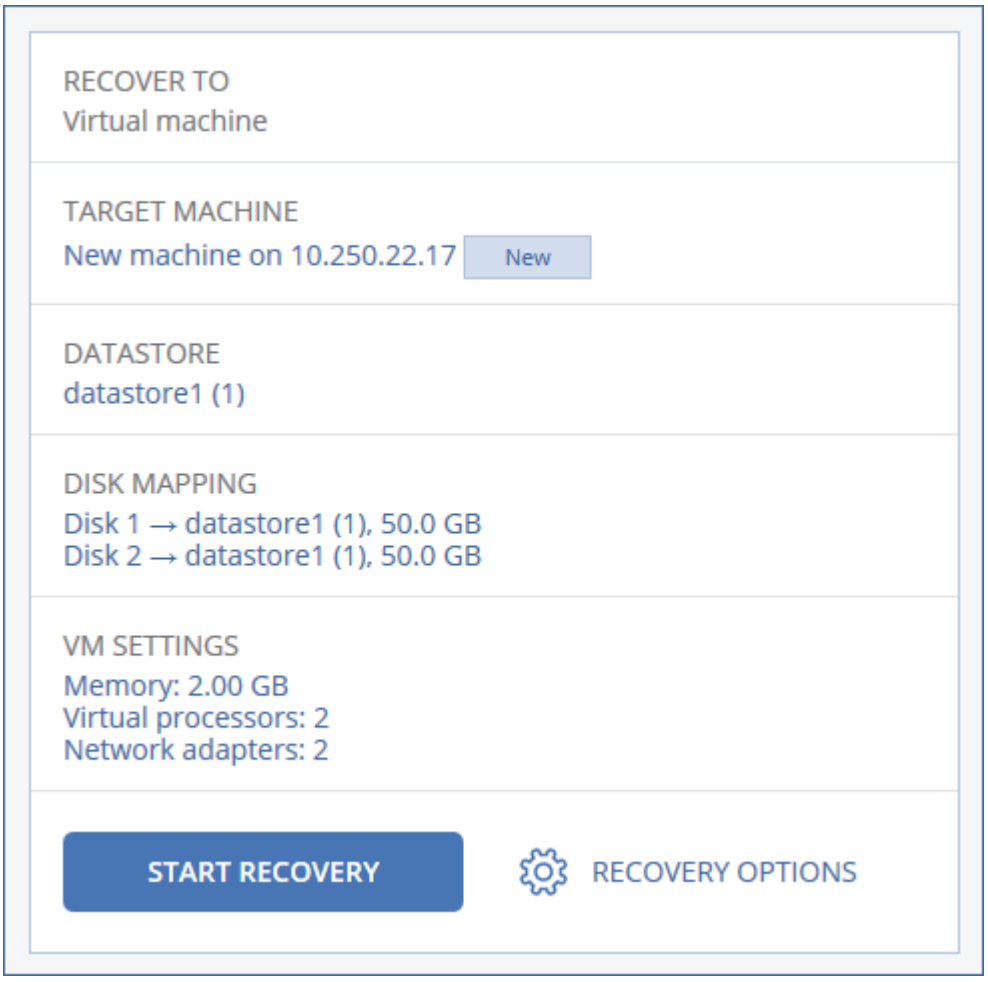
   Catatan
   Memilih cara adalah langkah wajib untuk Virtuozzo Hybrid Infrastructure.

8. [Opsional] Konfigurasi opsi pemulihan tambahan:

© Acronis International GmbH, 2003-2024

- [Tidak tersedia untuk Virtuozzo Hybrid Infrastructure] Klik **Penyimpanan data** untuk ESXi atau **Jalur** untuk Hyper-V, lalu pilih penyimpanan data (penyimpanan) untuk mesin virtual.
- Klik **Pemetaan disk** untuk memilih mode penyimpanan data (penyimpanan), antarmuka, dan penyediaan untuk setiap disk virtual. Bagian pemetaan juga memungkinkan Anda memilih disk individual untuk pemulihan.

  Untuk Virtuozzo Hybrid Infrastructure, Anda hanya dapat memilih kebijakan penyimpanan untuk disk target. Untuk melakukannya, pilih disk target yang diinginkan, lalu pilih Ubah. Di bilah yang terbuka, klik ikon roda gigi, pilih kebijakan penyimpanan, lalu klik Selesai.
- [Untuk VMware ESXi, Hyper-V, dan Red Hat Virtualization/oVirt] Klik **Pengaturan VM** untuk mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual.



9. [Hanya tersedia untuk mesin Windows tempat agen perlindungan diinstal.] Aktifkan tombol **pemulihan Aman** untuk memastikan bahwa data yang dipulihkan bebas malware. Untuk informasi lebih lanjut mengenai cara pemulihan aman bekerja, lihat "Pemulihan aman" (hlm. 497).
10. Klik **Mulai pemulihan**.
11. Ketika memulihkan ke mesin virtual yang ada, konfirmasi bahwa Anda ingin menimpa disk.

Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

© Acronis International GmbH, 2003-2024

Memulihkan mesin virtual

Anda dapat memulihkan mesin virtual dari cadangannya.

Catatan
Anda tidak dapat memulihkan cadangan di konsol Cyber Protect untuk penyewa dalam mode Kepatuhan. Untuk informasi lebih lanjut tentang cara memulihkan cadangan tersebut, silakan merujuk ke "Memulihkan cadangan untuk penyewa dalam mode Kepatuhan" (hlm. 1085).

Prasyarat

- Mesin virtual harus dihentikan selama pemulihan ke mesin ini. Secara default, perangkat lunak menghentikan mesin tanpa perintah. Ketika pemulihan selesai, Anda harus memulai mesin secara manual. Anda dapat mengubah perilaku default ini menggunakan opsi pemulihan manajemen daya VM (klik **Opsi pemulihan** > **Manajemen daya VM**).

Prosedur

1. Lakukan salah satu langkah berikut:
   - Pilih mesin yang dicadangkan, klik **Pemulihan**, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab Penyimpanan cadangan.
2. Klik **Pulihkan** > **Seluruh mesin**.
3. Jika Anda ingin memulihkan ke mesin fisik, pilih **Mesin fisik** di **Pulihkan ke**. Jika tidak, lewati langkah ini.

   Pemulihan ke mesin fisik hanya dimungkinkan jika konfigurasi disk dari mesin target sama persis dengan konfigurasi disk dalam cadangan.

   Jika hal ini terjadi, lanjutkan ke langkah 4 di "Mesin fisik". Jika tidak, kami sarankan Anda untuk melakukan migrasi V2P menggunakan media yang dapat di-boot.
4. [Opsional] Secara default, perangkat lunak akan otomatis memilih mesin asli sebagai mesin target. Untuk memulihkan ke mesin virtual lain, klik **Mesin target**, lalu lakukan hal berikut:
   a. Pilih hypervisor (**VMware ESXi**, **Hyper-V**, **Virtuozzo**, **Virtuozzo Hybrid Infrastructure**, **Scale Computing HC3**, atau **oVirt**).

      Hanya mesin virtual Virtuozzo yang dapat dipulihkan ke Virtuozzo. Untuk informasi lebih lanjut tentang migrasi V2V, lihat "Migrasi mesin".
   b. Pilih apakah akan Anda ingin melakukan pemulihan ke mesin baru atau mesin yang sudah ada.
   c. Pilih host dan tentukan nama mesin yang baru, atau pilih mesin target yang sudah ada.
   d. Klik **OK**.
5. Siapkan opsi pemulihan tambahan yang Anda perlukan.
   - [Opsional] [Tidak tersedia untuk Virtuozzo Hybrid Infrastructure dan Scale Computing HC3] Untuk memilih penyimpanan data bagi mesin virtual, klik **Penyimpanan data** untuk ESXi, **Jalur** untuk Hyper-V dan Virtuozzo, atau **Domain penyimpanan** untuk Red Hat Virtualization

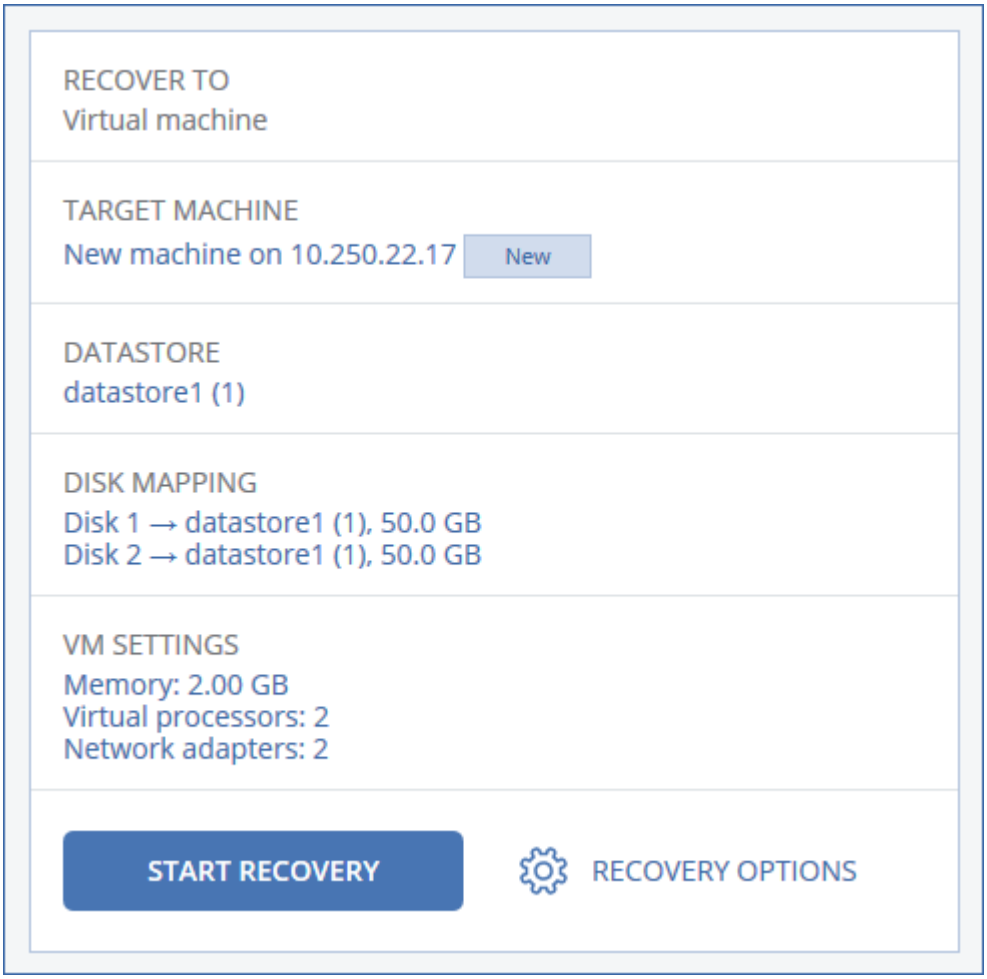
© Acronis International GmbH, 2003-2024

(oVirt), lalu pilih penyimpanan data (penyimpanan) untuk mesin virtual.

- [Opsional] Untuk melihat mode penyimpanan data (penyimpanan), antarmuka, dan provisi bagi setiap disk virtual, klik **Pemetaan disk**. Anda dapat mengubah pengaturan ini, kecuali jika Anda memulihkan kontainer Virtuozzo atau mesin virtual Virtuozzo Hybrid Infrastructure.

  Untuk Virtuozzo Hybrid Infrastructure, Anda hanya dapat memilih kebijakan penyimpanan untuk disk target. Untuk melakukannya, pilih disk target yang diinginkan, lalu pilih **Ubah**. Di bilah yang terbuka, klik ikon roda gigi, pilih kebijakan penyimpanan, lalu klik **Selesai**.

  Bagian pemetaan juga memungkinkan Anda memilih disk individual untuk pemulihan.
- [Opsional] [Tersedia untuk VMware ESXi, Hyper-V, dan Virtuozzo] Untuk mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual, klik **Pengaturan VM**.
- [Untuk Virtuozzo Hybrid Infrastructure] Untuk mengubah ukuran memori dan jumlah prosesor mesin virtual, pilih **Cara**.



6. [Hanya tersedia untuk mesin Windows tempat agen perlindungan diinstal.] Aktifkan tombol **pemulihan Aman** untuk memastikan bahwa data yang dipulihkan bebas malware. Untuk informasi lebih lanjut mengenai cara pemulihan aman bekerja, lihat "Pemulihan aman" (hlm. 497).
7. Klik **Mulai pemulihan**.
8. Ketika memulihkan ke mesin virtual yang ada, konfirmasi bahwa Anda ingin menimpa disk.

Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

© Acronis International GmbH, 2003-2024

Memulihkan disk menggunakan media yang dapat di-boot

Untuk informasi tentang cara membuat media yang dapat di-boot, lihat "Membuat media fisik yang dapat di-boot" (hlm. 706).

Catatan
Anda tidak dapat memulihkan cadangan tingkat disk dari Mac berbasis Intel ke Mac yang menggunakan prosesor silikon Apple, dan sebaliknya. Anda dapat memulihkan file dan folder.

Untuk memulihkan disk menggunakan media yang dapat di-boot

1. Boot mesin target menggunakan media yang dapat di-boot.
2. [Hanya ketika memulihkan Mac] Jika Anda memulihkan disk/volume berformat APFS ke mesin non-asli atau ke bare metal, buat kembali konfigurasi disk asli secara manual:
   a. Klik **Utilitas Disk**.
   b. Hapus dan format disk target ke APFS. Baca petunjuknya di https://support.apple.com/en-us/HT208496#erasedisk.
   c. Buat kembali konfigurasi disk asli. Baca petunjuknya di https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15.
   d. Klik **Utilitas Disk** > **Keluar dari Utiltas Disk**.
3. Klik **Kelola mesin ini secara lokal** atau klik **Selamatkan Media yang Dapat Di-Boot** dua kali, tergantung jenis media yang Anda gunakan.
4. Jika server proksi diaktifkan di jaringan Anda, klik **Alat** > **Server proksi**, lalu tentukan nama host server proksi/alamat IP, port, dan kredensial. Jika tidak, lewati langkah ini.
5. [Opsional] Ketika memulihkan Windows atau Linux, klik **Alat** > **Daftarkan media di layanan Cyber Protection**, lalu tentukan token pendaftaran yang Anda peroleh saat mengunduh media. Jika melakukan ini, Anda tidak perlu memasukkan kredensial atau kode pendaftaran untuk mengakses penyimpanan awan, seperti yang dijelaskan pada langkah 8.
6. Di layar selamat datang, klik **Pulihkan**.
7. Klik **Pilih data**, lalu klik **Jelajahi**.
8. Tentukan lokasi cadangan:
   - Untuk memulihkan dari penyimpanan awan, pilih **Penyimpanan awan**. Masukkan kredensial untuk akun yang untuknya mesin yang dicadangkan ditetapkan.
     Ketika memulihkan Windows atau Linux, Anda memiliki opsi untuk meminta kode pendaftaran dan menggunakannya sebagai ganti kredensial. Klik **Gunakan kode pendaftaran** > **Minta kode**. Perangkat lunak menampilkan tautan pendaftaran dan kode pendaftaran. Anda dapat menyalin tautan pendaftaran dan melakukan langkah pendaftaran pada mesin yang berbeda. Kode pendaftaran valid selama satu jam.
   - Untuk memulihkan dari folder lokal atau jaringan, jelajahi folder di dalam **Folder lokal** atau **Folder jaringan**.

© Acronis International GmbH, 2003-2024

- Untuk memulihkan dari lokasi cadangan pada penyimpanan cloud publik seperti Microsoft Azure, Amazon S3, Wasabi atau S3 yang kompatibel, pertama klik **Daftarkan media di layanan Cyber Protection**, kemudian konfigurasikan pemulihan menggunakan antarmuka web. Untuk informasi lebih lanjut tentang mengelola media dari jarak jauh melalui antarmuka web, lihat "Operasi jarak jauh dengan media yang dapat di-boot" (hlm. 724).

Klik **OK** untuk mengonfirmasi pilihan Anda.

9. Pilih cadangan yang berisi data yang ingin Anda pulihkan. Jika diminta, ketik kata sandi untuk cadangan.
10. Di **Konten pencadangan**, pilih disk yang ingin Anda pulihkan. Klik **OK** untuk mengonfirmasi pilihan Anda.
11. Pada **Lokasi pemulihan**, perangkat lunak secara otomatis memetakan disk yang dipilih ke disk target.

    Jika pemetaan tidak berhasil atau jika Anda tidak puas dengan hasil pemetaan, Anda dapat memetakan ulang disk secara manual.

    Catatan
    Mengubah tata letak disk dapat mempengaruhi bootabilitas sistem operasi. Gunakan tata letak disk mesin asli kecuali Anda merasa sangat yakin akan berhasil.

12. [Ketika memulihkan Linux] Jika mesin yang dicadangkan memiliki volume logis (LVM) dan Anda ingin mereproduksi struktur LVM asli:
    a. Pastikan jumlah disk mesin target dan setiap kapasitas disk sama dengan atau lebih dari yang ada pada mesin asli, lalu klik **Terapkan RAID/LVM**.
    b. Tinjau struktur volume, lalu klik **Terapkan RAID/LVM** untuk membuatnya.
13. [Opsional] Klik **Opsi pemulihan** untuk menentukan pengaturan tambahan.
14. Klik **OK** untuk memulai pemulihan.

Menggunakan Universal Restore

Sistem operasi terbaru tetap dapat di-boot ketika dipulihkan ke perangkat keras yang berbeda, termasuk platform VMware atau Hyper-V. Jika sistem operasi yang dipulihkan tidak dapat melakukan boot, gunakan alat Universal Restore untuk memperbarui driver dan modul yang sangat penting untuk mulai sistem operasi.

Universal Restore berlaku untuk Windows dan Linux.

Untuk menerapkan Universal Restore

1. Boot mesin dari media yang dapat di-boot.
2. Klik **Terapkan Universal Restore**.
3. Jika ada beberapa sistem operasi pada mesin, pilih salah satu untuk menerapkan Universal Restore.

© Acronis International GmbH, 2003-2024

4. [Hanya untuk Windows] Konfigurasikan pengaturan tambahan.
5. Klik **OK**.

Universal Restore di Windows

Persiapan

Siapkan driver

Sebelum menerapkan Universal Restore ke sistem operasi Windows, pastikan Anda memiliki driver pengontrol HDD dan chipset. Driver tersebut sangat penting untuk memulai sistem operasi. Gunakan CD atau DVD yang disediakan oleh vendor perangkat keras atau unduh driver dari situs web vendor yang bersangkutan. File driver harus berekstensi *.inf. Jika Anda mengunduh driver dengan ekstensi *.exe, *.cab, atau *.zip, ekstrak menggunakan aplikasi pihak ketiga.

Langkah terbaik adalah menyimpan semua driver perangkat keras yang digunakan organisasi Anda pada repositori tunggal yang diurutkan berdasarkan jenis perangkat atau berdasarkan konfigurasi perangkat keras. Anda dapat menyimpan salinan repositori pada DVD atau flash drive; ambil driver dan tambahkan pada media yang dapat di-boot; buat media yang dapat di-boot kustom beserta driver yang dibutuhkan (serta konfigurasi jaringan yang dibutuhkan) untuk masing-masing server Anda. Atau, Anda cukup menentukan jalur ke repositori setiap kali Universal Restore digunakan.

Cek akses ke driver pada lingkungan yang dapat di-boot

Pastikan Anda memiliki akses ke perangkat dengan driver saat bekerja dengan media yang dapat di-boot. Gunakan media berbasis WinPE jika perangkat tersedia di Windows namun media berbasis Linux tidak mendeteksinya.

Pengaturan Universal Restore

Pencarian driver otomatis

Tentukan di mana program akan mencari Hardware Abstraction Layer (HAL), driver pengontrol HDD, dan driver adaptor jaringan:

- Jika driver berada di disk vendor atau media yang dapat dilepas lainnya, aktifkan **Cari media yang dapat dilepas**.
- Jika driver berada di folder jaringan atau pada media yang dapat di-boot, tentukan jalur ke folder tersebut dengan mengklik **Tambahkan folder**.

Selain itu, Universal Restore juga akan mencari folder penyimpanan driver default Windows. Lokasinya ditentukan pada nilai registri **DevicePath**, yang dapat ditemukan pada kunci registri **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Folder penyimpanan ini biasanya terletak di WINDOWS/inf.

© Acronis International GmbH, 2003-2024

Universal Restore akan melakukan pencarian berulang di semua sub-folder dari folder yang ditentukan, mencari HAL dan driver pengontrol HDD yang paling cocok, serta menginstalnya ke dalam sistem. Universal Restore juga mencari driver adaptor jaringan; jalur ke driver yang ditemukan kemudian ditransmisikan oleh Universal Restore ke sistem operasi. Jika perangkat keras memiliki beberapa kartu antarmuka jaringan, Universal Restore akan mencoba mengonfigurasi semua driver kartu tersebut.

Driver penyimpanan massal akan tetap diinstal

Anda membutuhkan pengaturan ini jika:

- Perangkat keras memiliki pengontrol penyimpanan massal spesifik seperti RAID (khususnya NVIDIA RAID) atau adaptor kanal serat.
- Anda memigrasikan sistem ke mesin virtual yang menggunakan pengontrol hard drive SCSI. Gunakan driver SCSI yang dipaket dengan perangkat lunak virtualisasi Anda atau unduh versi driver terbaru dari situs web produsen perangkat lunak.
- Jika pencarian driver otomatis tidak membantu boot sistem.

Tentukan driver yang tepat dengan mengklik **Tambahkan driver**. Driver yang ditentukan di sini akan dipasang, dengan peringatan, meskipun program menemukan driver yang lebih baik.

Proses Universal Restore

Setelah Anda menentukan pengaturan yang diperlukan, klik **OK**.

Jika Universal Restore tidak dapat menemukan driver yang kompatibel pada lokasi yang ditentukan, peringatan tentang perangkat yang bermasalah akan ditampilkan. Lakukan salah satu langkah berikut:

- Tambahkan driver ke lokasi yang ditentukan sebelumnya dan klik **Coba lagi**.
- Jika Anda tidak ingat lokasinya, klik **Abaikan** untuk melanjutkan proses. Jika hasilnya belum sesuai, terapkan kembali Universal Restore. Saat mengonfigurasi operasi, tentukan driver yang diperlukan.

Begitu Windows melakukan boot, prosedur standar akan mulai menginstal perangkat keras baru. Driver adaptor jaringan akan dipasang secara otomatis jika driver memiliki tanda tangan Microsoft Windows. Jika tidak, Windows akan meminta konfirmasi apakah akan tetap menginstal driver tanpa tanda tangan.

Setelah itu, Anda akan dapat mengonfigurasi koneksi jaringan dan menentukan driver untuk adaptor video, USB, dan perangkat lainnya.

Universal Restore di Linux

Universal Restore dapat diterapkan pada sistem operasi Linux dengan versi kernel 2.6.8 ke atas.

© Acronis International GmbH, 2003-2024

Ketika Universal Restore diterapkan pada sistem operasi Linux, sistem file sementara yang disebut sebagai disk RAM awal (initrd) akan diperbarui. Hal ini memastikan sistem operasi dapat melakukan boot pada perangkat keras baru.

Universal Restore menambahkan modul untuk perangkat keras baru (termasuk driver perangkat) ke disk RAM awal. Aturannya, pencarian modul yang diperlukan pada direktori **/lib/modules** akan dilakukan. Jika Universal Restore tidak dapat menemukan modul yang dibutuhkan, nama file modul akan dicatat ke dalam log.

Universal Restore dapat memodifikasi konfigurasi pemuat boot GRUB. Hal ini membutuhkan, misalnya, memastikan bootabilitas sistem saat mesin baru memiliki tata letak volume yang berbeda dari mesin asli.

Universal Restore tidak pernah memodifikasi Kernel Linux.

Mengembalikan ke disk RAM awal asli

Anda dapat mengembalikan ke disk RAM awal asli jika diperlukan.

Disk RAM awal disimpan pada mesin ke dalam sebuah file. Sebelum memperbarui disk RAM awal untuk pertama kalinya, Universal Restore akan menyimpan salinannya ke direktori yang sama. Nama salinannya adalah nama file, diikuti dengan akhiran **_acronis_backup.img**. Salinan ini tidak akan ditimpa jika Anda menjalankan Universal Restore lebih dari satu kali (misalnya, setelah Anda menambahkan driver yang tidak ditemukan).

Untuk mengembalikan ke disk RAM awal asli, lakukan salah satu langkah berikut:

- Ganti nama salinan seperlunya. Misalnya, jalankan perintah yang mirip dengan perintah berikut:

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60 -default
  ```

- Tentukan salinan pada baris **initrd** pada konfigurasi pemuat boot GRUB.

Memulihkan beberapa file

Memulihkan file di konsol Cyber Protect

Catatan
Anda tidak dapat memulihkan cadangan di konsol Cyber Protect untuk penyewa dalam mode Kepatuhan. Untuk informasi lebih lanjut tentang cara memulihkan cadangan tersebut, silakan merujuk ke "Memulihkan cadangan untuk penyewa dalam mode Kepatuhan" (hlm. 1085).

1. Pilih mesin yang awalnya berisi data yang ingin Anda pulihkan.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
   Jika mesin yang dipilih adalah fisik dan sedang offline, titik pemulihan tidak akan ditampilkan. Lakukan yang berikut ini:

© Acronis International GmbH, 2003-2024

- [Disarankan] Jika lokasi cadangan adalah awan atau penyimpanan bersama (yaitu agen lain dapat mengaksesnya), klik **Pilih mesin**, pilih mesin target yang online, lalu pilih titik pemulihan.
- Pilih titik pemulihan pada tab Penyimpanan cadangan.
- Unduh file dari penyimpanan awan.
- Gunakan media yang dapat di-boot.

4. Klik **Pulihkan** > **File/folder**.
5. Jelajahi ke folder yang diperlukan atau gunakan bilah pencarian untuk mendapatkan daftar file dan folder yang diperlukan.

   Pencarian bersifat bebas bahasa.

   Anda dapat menggunakan satu atau lebih karakter wildcard (* dan ?). Untuk detail lebih lanjut tentang penggunaan wildcard, lihat "Mask" (hlm. 461).

   Catatan
   Pencarian tidak tersedia untuk cadangan tingkat disk yang disimpan dalam penyimpanan awan.

6. Pilih file yang ingin Anda pulihkan.
7. Jika Anda ingin menyimpan file sebagai file .zip, klik **Unduh**, pilih lokasi untuk menyimpan data, lalu klik **Simpan**. Jika tidak, lewati langkah ini.

   Pengunduhan tidak tersedia jika pilihan Anda berisi folder atau ukuran total file yang dipilih melebihi 100 MB. Untuk menerima jumlah data yang lebih besar dari awan, gunakan prosedur "Mengunduh file dari penyimpanan awan" (hlm. 512).
8. Klik **Pulihkan**.

   Di **Pulihkan ke**, klik untuk memilih target operasi pemulihan atau biarkan target default. Target default bervariasi sesuai dengan sumber cadangan.

   Target berikut tersedia:
   - Mesin sumber (jika agen perlindungan diinstal di perangkat).

     Ini adalah mesin yang awalnya berisi file yang ingin Anda pulihkan.
   - Mesin lain tempat agen perlindungan diinstal – mesin fisik, mesin virtual, dan host virtualisasi tempat agen perlindungan diinstal, atau alat virtual.

     Anda dapat memulihkan file ke mesin fisik, mesin virtual, dan host virtualisasi tempat agen perlindungan diinstal. Anda tidak dapat memulihkan file ke mesin virtual tempat agen perlindungan tidak diinstal (kecuali untuk mesin virtual Virtuozzo).
   - Kontainer atau mesin virtual Virtuozzo.

     Anda dapat memulihkan file ke kontainer dan mesin virtual Virtuozzo dengan beberapa batasan. Untuk informasi lebih lanjut, lihat "Batasan untuk memulihkan file di konsol Cyber Protect" (hlm. 516).
9. Di **Jalur**, pilih tujuan pemulihan. Anda dapat memilih salah satu dari tindakan berikut:
   - [Ketika memulihkan ke mesin asli] Lokasi asli.
   - Folder lokal atau penyimpanan yang terpasang secara lokal di mesin target.

© Acronis International GmbH, 2003-2024

Catatan
Tautan simbolik tidak didukung.

- Folder jaringan yang dapat diakses dari mesin target.

10. Klik **Mulai pemulihan**.
11. Pilih salah satu opsi penimpaan file:
    - **Timpa file yang ada**
    - **Timpa file yang ada jika lebih lama**
    - **Jangan timpa file yang ada**

Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

Mengunduh file dari penyimpanan awan

Di konsol Pemulihan Web, Anda dapat menjelajahi penyimpanan cloud, melihat isi cadangan, dan mengunduh file serta folder yang telah dicadangkan.

Catatan
Anda hanya dapat mengakses konsol Web Restore jika Anda adalah Administrator pelanggan Cyber Protection atau pengguna penyewa pelanggan. Peran pengguna tingkat mitra tidak diizinkan.

Pembatasan

- Anda tidak dapat mengunduh disk, volume, atau titik pemulihan keseluruhan yang telah dicadangkan.
- Ketika Anda mengeksplorasi cadangan tingkat disk, volume logis (seperti LVM dan LDM) tidak ditampilkan.
- Anda tidak dapat menjelajahi cadangan status sistem, Database SQL, dan database Exchange.

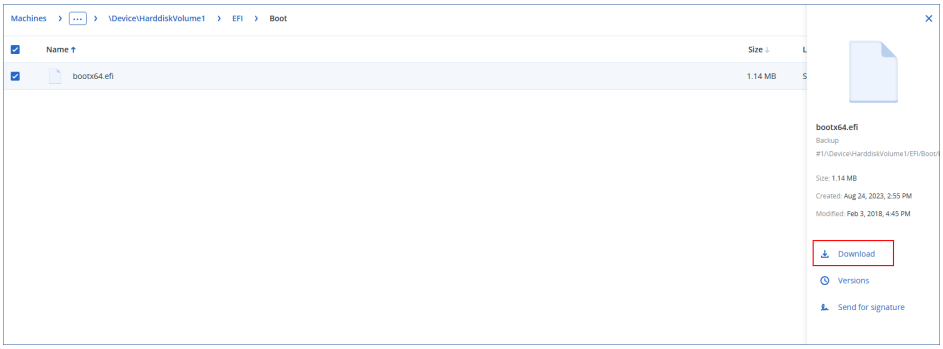
Untuk mengunduh file dan folder dari penyimpanan cloud

1. Di konsol Cyber Protection, pilih beban kerja yang diperlukan, lalu klik **Pemulihan**.
2. [Jika ada beberapa lokasi cadangan yang tersedia] Pilih lokasi cadangan, lalu klik **Cara pemulihan lain**.
3. Klik **Unduh file**.
4. Di bawah **Mesin**, klik nama beban kerja, dan kemudian klik arsip cadangan.
   Arsip cadangan berisi satu cadangan atau lebih (titik pemulihan).
5. Klik nomor cadangan (titik pemulihan) tempat asal file atau folder yang ingin Anda unduh, lalu navigasikan menuju item yang diperlukan.
6. Klik kotak centang di sebelah item yang ingin Anda unduh.

Catatan
Jika Anda memilih beberapa item, unduhan akan berbentuk file ZIP.

© Acronis International GmbH, 2003-2024

7. Klik **Unduh**.



Memverifikasi keaslian file dengan Layanan Notaris

Jika notarisisasi diaktifkan selama pencadangan, Anda dapat memverifikasi keaslian file yang dicadangkan.

Untuk memverifikasi keaslian file

1. Pilih file seperti yang dijelaskan dalam langkah 1-6 dari bagian "Memulihkan file menggunakan antarmuka web", atau langkah 1-5 dari bagian "Mengunduh file dari penyimpanan awan".
2. Pastikan bahwa file yang dipilih ditandai dengan ikon berikut: . Ini berarti bahwa file tersebut sudah dinotariskan.
3. Lakukan salah satu langkah berikut:
   - Klik **Verifikasi**.
     Perangkat lunak akan memeriksa keaslian file dan menampilkan hasilnya.
   - Klik **Dapatkan sertifikat**.
     Sertifikat yang mengonfirmasi notarisasi file dibuka di jendela browser web. Jendela ini juga berisi instruksi yang memungkinkan Anda memverifikasi keaslian file secara manual.

Menandatangani file dengan ASign

Catatan
Fitur ini tersedia dengan paket Cadangan Lanjutan.

ASign adalah layanan yang memungkinkan banyak orang untuk menandatangani file yang dicadangkan secara elektronik. Fitur ini hanya tersedia untuk pencadangan tingkat file yang disimpan di penyimpanan awan.

Hanya satu versi file yang dapat ditandatangani dalam satu waktu. Jika file dicadangkan beberapa kali, Anda harus memilih versi untuk ditandai, dan hanya versi ini yang akan ditandatangani.

Misalnya, ASign dapat digunakan untuk penandatanganan elektronik file berikut:

- Perjanjian sewa atau sewa guna
- Kontrak penjualan

© Acronis International GmbH, 2003-2024

- Perjanjian pembelian aset
- Perjanjian pinjaman
- Slip izin
- Dokumen Keuangan
- Dokumen asuransi
- Penafian kewajiban
- Dokumen layanan kesehatan
- Laporan resmi
- Sertifikat keaslian produk
- Perjanjian non-pengungkapan
- Surat penawaran
- Perjanjian kerahasiaan
- Perjanjian kontraktor independen

Untuk menandatangani versi file

1. Pilih file seperti yang dijelaskan dalam langkah 1-6 dari bagian "Memulihkan file menggunakan antarmuka web", atau langkah 1-5 dari bagian "Mengunduh file dari penyimpanan awan".
2. Pastikan memilih tanggal dan waktu yang benar di panel kiri.
3. Klik **Tandai versi file ini**.
4. Tentukan kata sandi untuk akun penyimpanan awan tempat cadangan disimpan. Log masuk akun akan ditampilkan di jendela wantian.

   Antarmuka layanan ASign dibuka di jendela browser web.
5. Tambahkan penanda tangan lain dengan menentukan alamat email mereka. Anda tidak dimungkinkan untuk menambah atau menghapus penanda tangan setelah mengirim undangan, jadi pastikan daftar tersebut berisi semua orang yang tanda tangannya diperlukan.
6. Klik **Undang untuk menandatangani** untuk mengirim undangan kepada penanda tangan.

   Setiap penanda tangan akan menerima pesan email dengan permintaan tanda tangan. Ketika semua penanda tangan yang diminta menandatangani file, file akan dinotariskan dan ditandatangani melalui layanan notaris.

   Anda akan menerima pemberitahuan setelah semua penanda tangan menandatangani file. Anda dapat mengakses halaman web ASign dengan mengklik **Lihat detail** di salah satu pesan email yang Anda terima.
7. Setelah proses selesai, buka halaman ASign dan klik **Dapatkan dokumen** untuk mengunduh konten dokumen .pdf:
   - Halaman Sertifikat Tanda Tangan berisi tanda tangan yang terkumpul.
   - Halaman Jejak Audit dengan riwayat aktivitas: ketika undangan dikirim ke penanda tangan, ketika setiap penanda tangan menandatangani file, dan seterusnya.

© Acronis International GmbH, 2003-2024

Memulihkan file menggunakan media yang dapat di-boot

Untuk informasi tentang cara membuat media yang dapat di-boot, lihat "Membuat media yang dapat di-boot".

Untuk memulihkan file menggunakan media yang dapat di-boot

1. Boot mesin target menggunakan media yang dapat di-boot.
2. Klik **Kelola mesin ini secara lokal** atau klik **Selamatkan Media yang Dapat Di-Boot** dua kali, tergantung jenis media yang Anda gunakan.
3. Jika server proksi diaktifkan di jaringan Anda, klik **Alat** > **Server proksi**, lalu tentukan nama host server proksi/alamat IP, port, dan kredensial. Jika tidak, lewati langkah ini.
4. [Opsional] Ketika memulihkan Windows atau Linux, klik **Alat** > **Daftarkan media di layanan Cyber Protection**, lalu tentukan token pendaftaran yang Anda peroleh saat mengunduh media. Jika Anda melakukan ini, Anda tidak perlu memasukkan kredensial atau kode pendaftaran untuk mengakses penyimpanan awan, seperti yang dijelaskan pada langkah 7.
5. Di layar selamat datang, klik **Pulihkan**.
6. Klik **Pilih data**, lalu klik **Jelajahi**.
7. Tentukan lokasi cadangan:
   - Untuk memulihkan dari penyimpanan awan, pilih **Penyimpanan awan**. Masukkan kredensial untuk akun yang untuknya mesin yang dicadangkan ditetapkan.

     Ketika memulihkan Windows atau Linux, Anda memiliki opsi untuk meminta kode pendaftaran dan menggunakannya sebagai ganti kredensial. Klik **Gunakan kode pendaftaran** > **Minta kode**. Perangkat lunak menampilkan tautan pendaftaran dan kode pendaftaran. Anda dapat menyalin tautan pendaftaran dan melakukan langkah pendaftaran pada mesin yang berbeda. Kode pendaftaran valid selama satu jam.
   - Untuk memulihkan dari folder lokal atau jaringan, jelajahi folder di dalam **Folder lokal** atau **Folder jaringan**.
   - Untuk memulihkan dari lokasi cadangan pada penyimpanan cloud publik seperti Microsoft Azure, Amazon S3, Wasabi atau S3 yang kompatibel, pertama klik **Daftarkan media di layanan Cyber Protection**, kemudian konfigurasikan pemulihan menggunakan antarmuka web. Untuk informasi lebih lanjut tentang mengelola media dari jarak jauh melalui antarmuka web, lihat "Operasi jarak jauh dengan media yang dapat di-boot" (hlm. 724).

   Klik **OK** untuk mengonfirmasi pilihan Anda.
8. Pilih cadangan yang berisi data yang ingin Anda pulihkan. Jika diminta, ketik kata sandi untuk cadangan.
9. Di **Konten pencadangan**, pilih **Folder/file**.
10. Pilih data yang ingin Anda pulihkan. Klik **OK** untuk mengonfirmasi pilihan Anda.
11. Pada **Lokasi pemulihan**, tentukan foldernya. Secara opsional, Anda dapat melarang penimpaan versi file yang lebih baru atau mengecualikan beberapa file dari pemulihan.

© Acronis International GmbH, 2003-2024

12. [Opsional] Klik **Opsi pemulihan** untuk menentukan pengaturan tambahan.
13. Klik **OK** untuk memulai pemulihan.

Mengekstrak file dari pencadangan lokal

Anda dapat menjelajahi konten pencadangan dan mengekstrak file yang Anda butuhkan.

Persyaratan

- Fungsi ini hanya tersedia di Windows menggunakan File Explorer.
- Sistem file yang dicadangkan harus berupa salah satu dari sistem berikut: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS, or HFS+.

Prasyarat

- Agen perlindungan harus diinstal pada mesin tempat Anda menjelajahi cadangan.
- Cadangan harus disimpan di folder lokal atau di jaringan bersama (SMB/CIFS).

Untuk mengekstrak file dari cadangan

1. Jelajahi lokasi cadangan menggunakan File Explorer.
2. Klik dua kali pada file cadangan. Nama file didasarkan pada templat berikut:
   `<nama mesin> - <GUID rencana proteksi>`
3. Jika cadangan dienkripsi, masukkan kata sandi. Jika tidak, lewati langkah ini.
   File Explorer menampilkan titik pemulihan.
4. Klik dua kali pada titik pemulihan.
   File Explorer menampilkan data yang dicadangkan.
5. Jelajahi folder yang diperlukan.
6. Salin file yang diperlukan ke folder mana pun dalam sistem file.

Batasan untuk memulihkan file di konsol Cyber Protect

Penyewa dalam mode Kepatuhan

Anda tidak dapat memulihkan cadangan di konsol Cyber Protect untuk penyewa dalam mode Kepatuhan. Untuk informasi lebih lanjut tentang cara memulihkan cadangan tersebut, silakan merujuk ke "Memulihkan cadangan untuk penyewa dalam mode Kepatuhan" (hlm. 1085).

Pemulihan ke kontainer Virtuozzo atau mesin virtual Virtuozzo

- Agen Tamu QEMU harus diinstal pada target mesin virtual.
- [Hanya berlaku saat memulihkan ke kontainer] Titik pemasangan di dalam kontainer tidak dapat digunakan sebagai target untuk pemulihan. Misalnya, Anda tidak dapat memulihkan file ke hard disk kedua atau bagian NFS yang dipasang ke kontainer.

© Acronis International GmbH, 2003-2024

- Saat memulihkan file ke mesin virtual Windows, dan jika opsi pemulihan "Keamanan tingkat file" (hlm. 522) diaktifkan, atribut bit arsip diatur ke file yang dipulihkan.
- File yang namanya tidak mengandung karakter non-ANSI dipulihkan dengan nama yang salah pada mesin yang menjalankan Windows Server 2012 atau lebih lama dan mesin yang menjalankan Windows 7 atau lebih lama.
- Untuk memulihkan file ke mesin virtual CentOS atau Red Hat Enterprise Linux yang berjalan di Virtuozzo Hybrid Server, Anda harus mengedit file `qemu-ga`, sebagai berikut:
  - Pada mesin virtual target, arahkan ke `/etc/sysconfig/`, lalu buka file `qemu-ga` untuk pengeditan.
  - Arahkan ke baris berikut, lalu hapus semuanya setelah tanda sama dengan (=):

    ```
    BLACKLIST_RPC=
    ```

  - Mulai ulang Agen Tamu QEMU dengan menjalankan perintah berikut:

    ```
    systemctl restart qemu-guest-agent
    ```

Memulihkan status sistem

Catatan
Anda tidak dapat memulihkan cadangan di konsol Cyber Protect untuk penyewa dalam mode Kepatuhan. Untuk informasi lebih lanjut tentang cara memulihkan cadangan tersebut, silakan merujuk ke "Memulihkan cadangan untuk penyewa dalam mode Kepatuhan" (hlm. 1085).

1. Pilih mesin yang ingin Anda pulihkan status sistemnya.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan status sistem. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
4. Klik **Pulihkan status sistem**.
5. Konfirmasi bahwa Anda ingin menimpa status sistem dengan versi yang dicadangkannya.

Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

Memulihkan konfigurasi ESXi

Untuk memulihkan konfigurasi ESXi, Anda perlu media yang dapat di-boot berbasis Linux. Untuk informasi tentang cara membuat media yang dapat di-boot, lihat "Membuat media fisik yang dapat di-boot" (hlm. 706).

Jika Anda memulihkan konfigurasi ESXi ke host non-asli dan host ESXi asli masih terhubung ke vCenter Server, putuskan koneksi dan hapus host ini dari vCenter Server untuk menghindari masalah yang tidak terduga selama pemulihan. Jika ingin menyimpan host asli bersama dengan yang dipulihkan, Anda dapat menambahkannya lagi setelah pemulihan selesai.

Mesin virtual yang berjalan pada host tidak dimasukkan dalam cadangan konfigurasi ESXi. Mesin virtual tersebut dapat dicadangkan dan dipulihkan secara terpisah.

© Acronis International GmbH, 2003-2024

Untuk memulihkan konfigurasi ESXi

1. Boot mesin target menggunakan media yang dapat di-boot.
2. Klik **Kelola mesin ini secara lokal**.
3. Di layar selamat datang, klik **Pulihkan**.
4. Klik **Pilih data**, lalu klik **Jelajahi**.
5. Tentukan lokasi cadangan:
   - Jelajahi folder pada **Folder lokal** atau **Folder jaringan**.

   Klik **OK** untuk mengonfirmasi pilihan Anda.
6. Di **Tampilkan**, pilih **konfigurasi ESXi**.
7. Pilih cadangan yang berisi data yang ingin Anda pulihkan. Jika diminta, ketik kata sandi untuk cadangan.
8. Klik **OK**.
9. Di **Disk yang akan digunakan untuk penyimpanan data baru**, lakukan langkah berikut:
   - Pada **Pulihkan ESXi ke**, pilih disk tempat konfigurasi host akan dipulihkan. Jika Anda memulihkan konfigurasi ke host asli, disk asli akan dipilih secara default.
   - [Opsional] Pada **Gunakan untuk penyimpanan data baru**, pilih disk tempat penyimpanan data baru akan dibuat. Berhati-hatilah karena semua data pada disk yang dipilih dapat hilang. Jika Anda ingin mempertahankan mesin virtual di penyimpanan data yang ada, jangan pilih disk apa pun.
10. Jika ada disk untuk penyimpanan data baru yang dipilih, pilih metode pembuatan penyimpanan data di **Cara membuat penyimpanan data baru**: **Buat satu penyimpanan data per disk** atau **Buat satu penyimpanan data di semua HDD yang dipilih**.
11. [Opsional] Di **Pemetaan jaringan**, ubah hasil pemetaan otomatis dari tombol virtual yang ada di cadangan ke adaptor jaringan fisik.
12. [Opsional] Klik **Opsi pemulihan** untuk menentukan pengaturan tambahan.
13. Klik **OK** untuk memulai pemulihan.

Opsi pemulihan

Untuk memodifikasi opsi pemulihan, klik **Opsi pemulihan** ketika mengonfigurasi pemulihan.

Ketersediaan opsi pemulihan

Set opsi pemulihan yang tersedia bergantung pada:

- Lingkungan agen yang melakukan pemulihan beroperasi di (Windows, Linux, macOS, atau media yang dapat di-boot).
- Jenis data yang sedang dipulihkan (disk, file, mesin virtual, data aplikasi).

Tabel berikut merangkum ketersediaan opsi pemulihan.

© Acronis International GmbH, 2003-2024

	Disk			File				Mesin virtual	SQL dan Exchange
	Windows	Linux	Media yang dapat di-boot	Windows	Linux	macOS	Media yang dapat di-boot	ESXi, Hyper-V, dan Virtuozzo	Windows
Validasi cadangan	+	+	+	+	+	+	+	+	+
Mode boot	+	-	-	-	-	-	-	+	-
Tanggal dan waktu untuk file	-	-	-	+	+	+	+	-	-
Penanganan eror	+	+	+	+	+	+	+	+	+
Pengecualian file	-	-	-	+	+	+	+	-	-
Keamanan tingkat file	-	-	-	+	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-
Pemulihan jalur lengkap	-	-	-	+	+	+	+	-	-
Titik mount	-	-	-	+	-	-	-	-	-
Performa	+	+	-	+	+	+	-	+	+
Perintah pra/pasca	+	+	-	+	+	+	-	+	+
Mengubah SID	+	-	-	-	-	-	-	-	-
Manajemen daya VM	-	-	-	-	-	-	-	+	-
Log event Windows	+	-	-	+	-	-	-	Hanya Hyper-V	+

© Acronis International GmbH, 2003-2024

Validasi cadangan

Opsi ini menentukan apakah validasi cadangan akan dilakukan untuk memastikan bahwa cadangan tidak rusak, sebelum data dipulihkan. Operasi ini dilakukan oleh agen perlindungan.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Untuk informasi selengkapnya tentang validasi melalui verifikasi checksum, lihat "Verifikasi checksum" (hlm. 204).

Catatan
Tergantung pengaturan yang dipilih oleh penyedia layanan Anda, validasi mungkin tidak tersedia saat mencadangkan ke penyimpanan awan.

Mode boot

Opsi ini efektif ketika memulihkan mesin fisik atau virtual dari pencadangan level disk yang berisi sistem operasi Windows.

Opsi ini memungkinkan Anda untuk memilih mode boot (BIOS atau UEFI) yang akan digunakan Windows setelah pemulihan. Jika mode boot mesin asli berbeda dari mode boot yang dipilih, perangkat lunak akan:

- Menginisialisasi disk tempat Anda memulihkan volume sistem, sesuai dengan mode boot yang dipilih (MBR untuk BIOS, GPT untuk UEFI).
- Sesuaikan sistem operasi Windows agar dapat memulai menggunakan mode boot yang dipilih.

Nilai prasetelnya adalah: **Sebagaimana mesin target.**

Anda dapat memilih salah satu dari pilihan berikut:

- **Sebagaimana mesin target.**
  Agen yang berjalan pada mesin target akan mendeteksi mode boot yang saat ini digunakan oleh Windows dan melakukan penyesuaian sesuai dengan mode boot yang terdeteksi.
  Ini adalah nilai teraman yang secara otomatis menghasilkan sistem yang dapat di-boot kecuali batasan yang tercantum di bawah ini berlaku. Karena opsi **Mode boot** tidak ada di bawah media yang dapat di-boot, agen pada media selalu berperilaku seolah-olah nilai ini dipilih.
- **Sebagaimana mesin yang dicadangkan**
  Agen yang berjalan pada mesin target akan membaca mode boot dari pencadangan dan membuat penyesuaian sesuai dengan mode boot ini. Hal ini dapat membantu Anda memulihkan sistem pada mesin yang berbeda, meskipun mesin ini menggunakan mode boot lain, lalu mengganti disk di mesin yang dicadangkan.
- **BIOS**
  Agen yang berjalan pada mesin target akan melakukan penyesuaian untuk menggunakan BIOS.
- **UEFI**
  Agen yang berjalan pada mesin target akan melakukan penyesuaian untuk menggunakan UEFI.

© Acronis International GmbH, 2003-2024

Setelah pengaturan diubah, prosedur pemetaan disk akan diulang. Ini akan memerlukan beberapa saat.

Rekomendasi

Jika Anda perlu mentransfer Windows antara UEFI dan BIOS:

- Pulihkan seluruh disk lokasi volume sistem. Jika Anda hanya memulihkan volume sistem di atas volume yang ada, agen tidak akan dapat menginisialisasi disk target dengan benar.
- Ingat bahwa BIOS tidak mengizinkan penggunaan lebih dari 2 TB ruang disk.

Pembatasan

- Transfer antara UEFI dan BIOS didukung untuk:
  - Sistem operasi Windows 64-bit yang dimulai dengan Windows7
  - Sistem operasi Windows Server 64-bit dimulai dengan Windows Server 2008 SP1
- Transfer antara UEFI dan BIOS tidak didukung jika pencadangan disimpan pada perangkat pita.

Ketika mentransfer sistem antara UEFI dan BIOS tidak didukung, agen akan berperilaku seolah-olah pengaturan **Sebagaimana mesin yang dicadangkan** dipilih. Jika mesin target mendukung UEFI dan BIOS, Anda harus secara manual mengaktifkan mode boot yang sesuai dengan mesin asli. Jika tidak, sistem tidak akan dapat boot.

Tanggal dan waktu untuk file

Opsi ini hanya efektif saat memulihkan file.

Opsi ini mendefinisikan apakah akan memulihkan tanggal dan waktu file dari cadangan atau menetapkan tanggal dan waktu saat ini ke file.

Jika opsi ini diaktifkan, file akan diberi tanggal dan waktu saat ini.

Nilai prasetelnya adalah: **Diaktifkan**.

Penanganan eror

Opsi ini memungkinkan Anda untuk menentukan cara menangani eror yang mungkin terjadi selama pemulihan.

Coba lagi, jika eror terjadi

Nilai prasetelnya adalah: **Diaktifkan. Jumlah percobaan: 30. Interval di antara percobaan: 30 detik.**

Ketika terjadi eror yang dapat dipulihkan, program akan mencoba untuk melakukan operasi yang tidak berhasil. Anda dapat mengatur interval waktu dan jumlah percobaan. Upaya percobaan akan dihentikan begitu operasi berhasil ATAU jumlah percobaan yang ditentukan sudah habis, mana pun yang terlebih dahulu tercapai.

© Acronis International GmbH, 2003-2024

Jangan menampilkan pesan dan dialog saat memproses (mode diam)

Nilai prasetelnya adalah: **Dinonaktifkan**.

Dengan mode diam yang aktif, program akan secara otomatis menangani situasi yang membutuhkan interaksi pengguna jika memungkinkan. Jika operasi tidak dapat dilanjutkan tanpa interaksi pengguna, operasi akan gagal. Detail operasi, termasuk eror, jika ada, dapat ditemukan pada log operasi.

Simpan informasi sistem jika pemulihan dengan reboot gagal

Opsi ini efektif untuk pemulihan disk atau volume ke mesin fisik yang menjalankan Windows atau Linux.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Ketika opsi ini diaktifkan, Anda dapat menentukan folder pada disk lokal (termasuk drive flash atau HDD yang terpasang pada mesin target) atau pada jaringan bersama di mana log, informasi sistem, dan file crash dump akan disimpan. File ini akan membantu personel dukungan teknis untuk mengidentifikasi masalah.

Pengecualian file

Opsi ini hanya efektif saat memulihkan file.

Opsi ini menentukan file dan folder mana saja yang dilewati selama proses pemulihan sehingga dapat mengecualikannya dari daftar item yang dipulihkan.

Catatan
Pengecualian mengabaikan pemilihan item data yang akan dipulihkan. Misalnya, jika Anda memilih untuk memulihkan file MyFile.tmp dan mengecualikan semua file .tmp, MyFile.tmp, file tidak akan dipulihkan.

Keamanan tingkat file

Opsi ini efektif saat memulihkan file dari cadangan tingkat disk dan file dari volume berformat NTFS.

Opsi ini menentukan apakah pemulihan izin NTFS untuk file dilakukan bersama dengan file.

Nilai prasetelnya adalah: **Diaktifkan**.

Anda dapat memilih untuk memulihkan izin atau membiarkan file menerima turunan izin NTFS-nya dari folder tujuan pemulihan file.

Flashback

Opsi ini efektif saat memulihkan disk dan volume pada mesin fisik dan virtual, kecuali untuk Mac.

Opsi ini berfungsi hanya jika tata letak volume disk yang dipulihkan sama persis dengan disk target.

© Acronis International GmbH, 2003-2024

Jika opsi ini diaktifkan, hanya perbedaan antara data dalam cadangan dan disk target yang akan dipulihkan. Hal ini akan mempercepat pemulihan mesin fisik dan virtual. Data dibandingkan pada tingkat blok.

Saat memulihkan mesin fisik, nilai prasetelnya adalah: **Dinonaktifkan**.

Saat memulihkan mesin virtual, nilai prasetelnya adalah: **Diaktifkan**.

Pemulihan jalur lengkap

Opsi ini hanya efektif saat memulihkan file data dari pencadangan tingkat file.

Jika opsi ini diaktifkan, jalur lengkap ke file akan dibuat ulang pada lokasi target.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Titik mount

Opsi ini hanya efektif untuk memulihkan file data dari pencadangan tingkat file.

Aktifkan opsi ini untuk memulihkan file dan folder yang disimpan pada volume ter-mount dan dicadangkan dengan opsi Titik Mount yang diaktifkan.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Opsi ini hanya efektif jika Anda memilih untuk memulihkan folder yang lebih tinggi pada hierarki folder dibandingkan titik mount. Jika Anda memilih folder pemulihan dalam titik mount atau titik mount itu sendiri, item yang dipilih akan dipulihkan berapa pun nilai opsi **Titik mount**.

Catatan
Perlu diperhatikan bahwa jika volume tidak terpasang pada saat pemulihan, data akan dipulihkan langsung ke folder yang telah menjadi titik pemasangan pada saat pencadangan.

Performa

Opsi ini menentukan prioritas proses pemulihan dalam sistem operasi.

Pengaturan yang tersedia adalah: **Rendah**, **Normal**, **Tinggi**.

Nilai prasetelnya adalah: **Normal**.

Prioritas proses yang berjalan dalam sebuah sistem menentukan jumlah CPU dan sumber daya sistem yang dialokasikan untuk proses tersebut. Menurunkan prioritas pemulihan akan membebaskan lebih banyak sumber daya untuk aplikasi lain. Meningkatkan prioritas pemulihan dapat mempercepat proses pemulihan dengan meminta sistem operasi mengalokasikan lebih banyak sumber daya ke aplikasi yang akan melakukan pemulihan. Namun, efek yang dihasilkan akan bergantung pada penggunaan CPU keseluruhan dan faktor lain seperti kecepatan I/O disk atau lalu lintas jaringan.

© Acronis International GmbH, 2003-2024

Perintah pra/pasca

Opsi ini memungkinkan Anda untuk menentukan perintah yang akan dieksekusi secara otomatis sebelum dan setelah pemulihan data.

Contoh bagaimana Anda dapat menggunakan perintah pra/pasca:

- Luncurkan perintah **Checkdisk** untuk menemukan dan memperbaiki eror sistem file logis, eror fisik atau sektor buruk yang harus dimulai sebelum pemulihan dimulai atau setelah pemulihan berakhir.

Program tidak mendukung perintah interaktif, yaitu perintah yang memerlukan input pengguna (misalnya, "jeda".)

Perintah setelah pemulihan tidak akan dieksekusi jika proses pemulihan dilanjutkan dengan boot ulang.

Perintah sebelum pemulihan

Untuk menentukan file perintah/batch yang akan dieksekusi sebelum proses pemulihan dimulai

1. Aktifkan switch **Eksekusi perintah sebelum pemulihan**.
2. Di bidang **Perintah...**, ketik perintah atau jelajahi ke file batch. Program tidak mendukung perintah interaktif, yaitu perintah yang memerlukan input pengguna (misalnya, "jeda".)
3. Di bidang **Direktori kerja**, tentukan jalur ke direktori lokasi file perintah/batch akan dieksekusi.
4. Di bidang **Argumen**, tentukan argumen eksekusi perintah, jika diperlukan.
5. Tergantung pada hasil yang ingin Anda peroleh, pilih opsi yang sesuai seperti yang dijelaskan pada tabel di bawah.
6. Klik **Selesai**.

Kotak centang	**Pemilihan**			
Gagalkan pemulihan jika eksekusi perintah gagal*	Dipilih	Dihapus	Dipilih	Dihapus
Jangan pulihkan sampai eksekusi perintah selesai	Dipilih	Dipilih	Dihapus	Dihapus
Hasil				

© Acronis International GmbH, 2003-2024

	Prasetel Lakukan pemulihan hanya setelah perintah berhasil dieksekusi. Gagalkan pemulihan jika eksekusi perintah gagal.	Lakukan pemulihan setelah perintah dieksekusi, meskipun eksekusi gagal atau berhasil.	N/A	Lakukan pemulihan bersama dengan eksekusi perintah, apa pun hasil eksekusi perintahnya.

* Perintah dianggap gagal jika mengeluarkan kode yang tidak sama dengan nol.

Perintah pasca-pemulihan

Untuk menentukan file perintah/dapat dieksekusi yang akan dieksekusi setelah pemulihan selesai

1. Aktifkan switch **Eksekusi perintah setelah pemulihan**.
2. Di bidang **Perintah...**, ketik perintah atau jelajahi ke file batch.
3. Di bidang **Direktori kerja**, tentukan jalur ke direktori lokasi file perintah/batch akan dieksekusi.
4. Di bidang **Argumen**, tentukan argumen eksekusi perintah, jika diperlukan.
5. Pilih kotak centang **Gagalkan pemulihan jika eksekusi perintah gagal** jika keberhasilan eksekusi perintah sangat penting bagi Anda. Perintah dianggap gagal jika mengeluarkan kode yang tidak sama dengan nol. Jika eksekusi perintah gagal, status pemulihan akan diatur ke **Eror**.
   Ketika kotak centang tidak dipilih, hasil eksekusi perintah tidak mempengaruhi kegagalan atau keberhasilan pemulihan. Anda dapat melacak hasil eksekusi perintah dengan menjelajahi tab **Aktivitas**.
6. Klik **Selesai**.

Catatan
Perintah setelah pemulihan tidak akan dieksekusi jika proses pemulihan dilanjutkan dengan boot ulang.

Mengubah SID

Opsi ini efektif saat memulihkan Windows 8.1/Windows Server 2012 R2 atau versi sebelumnya.

Opsi ini tidak efektif ketika pemulihan ke mesin virtual dilakukan oleh Agen untuk VMware, Agen untuk Hyper-V, Agen untuk Scale Computing HC3, atau Agen untuk oVirt.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Perangkat lunak tersebut dapat menghasilkan pengidentifikasi keamanan unik (SID Komputer) untuk sistem operasi yang dipulihkan. Anda hanya memerlukan opsi ini untuk memastikan operabilitas dari perangkat lunak pihak ketiga yang bergantung pada SID Komputer.

Microsoft tidak secara resmi mendukung mengubah SID pada sistem yang dikerahkan atau dipulihkan. Maka Anda menanggung sendiri risiko dari menggunakan opsi ini.

© Acronis International GmbH, 2003-2024

Manajemen daya VM

Opsi ini efektif ketika pemulihan ke mesin virtual dilakukan oleh Agen untuk VMware, Agen untuk Hyper-V, Agen untuk Virtuozzo, Agen untuk Scale Computing HC3, atau Agen untuk oVirt.

Matikan daya mesin virtual ketika memulai pemulihan

Nilai prasetelnya adalah: **Diaktifkan**.

Pemulihan ke mesin virtual yang ada tidak mungkin dilakukan jika mesin sedang online, sehingga mesin akan segera dimatikan secara otomatis setelah pemulihan dimulai. Pengguna akan diputus koneksinya dari mesin dan data yang belum disimpan akan hilang.

Kosongkan kotak centang untuk opsi ini jika Anda lebih memilih mematikan mesin virtual secara manual sebelum pemulihan.

Nyalakan mesin virtual target ketika pemulihan selesai

Nilai prasetelnya adalah: **Dinonaktifkan**.

Setelah mesin dipulihkan dari cadangan ke mesin lain, ada kemungkinan replika mesin yang ada akan muncul di jaringan. Agar tetap aman, nyalakan mesin virtual yang dipulihkan secara manual, setelah Anda melakukan pencegahan yang diperlukan.

Log event Windows

Opsi ini hanya efektif di sistem operasi Windows.

Opsi ini menentukan apakah agen harus mencatat event operasi pemulihan dalam Log Event Aplikasi Windows (untuk melihat log ini, jalankan eventvwr.exe atau pilih **Panel Kontrol** > **Alat Administratif** > **Event Viewer**). Anda dapat memfilter event yang akan di-log.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Operasi dengan pencadangan

Tab Penyimpanan cadangan

Tab **Penyimpanan cadangan** menyediakan akses ke semua cadangan, termasuk cadangan mesin offline, cadangan mesin yang tidak lagi terdaftar di layanan Cyber Protection, cadangan ke cloud publik seperti Microsoft Azure, dan cadangan tanpa induk[1].

Cadangan yang dibuat melalui `acrocmd` ditandai sebagai terlantar. Cadangan yang dibuat dalam versi 12.5 dari produk tersebut juga diidentifikasi sebagai terlantar.

[1]Cadangan tanpa induk adalah cadangan yang tidak terkait dengan rencana proteksi lagi.

© Acronis International GmbH, 2003-2024

Catatan
Harap dicatat bahwa cadangan orphaned juga dikenakan biaya.

Cadangan yang disimpan di lokasi bersama (seperti berbagi SMB atau NFS) dapat dilihat oleh semua pengguna yang memiliki izin baca untuk lokasi tersebut.

Di Windows, file cadangan mengambil izin akses dari folder induk mereka. Oleh karena itu, sebaiknya Anda membatasi izin baca untuk folder ini.

Di penyimpanan awan, pengguna hanya memiliki akses ke cadangan mereka sendiri.

Administrator dapat melihat cadangan ke awan atas nama akun mana pun yang dimiliki unit atau perusahaan tertentu dan grup turunannya, dengan memilih penyimpanan awan untuk akun tersebut. Untuk memilih perangkat yang ingin Anda gunakan untuk mendapatkan data dari awan, klik **Ubah** pada baris **Mesin untuk menelusuri**. Tab **Penyimpanan cadangan** menunjukkan cadangan dari semua mesin yang pernah terdaftar dengan akun yang dipilih.

Cadangan yang dibuat oleh Agen untuk Microsoft 365 *awan* dan cadangan data Google Workspace tidak ditampilkan di lokasi **Penyimpanan awan**, tetapi di bagian terpisah bernama **Cadangan aplikasi awan**.

Lokasi pencadangan yang digunakan dalam rencana proteksi secara otomatis ditambahkan ke tab **Penyimpanan cadangan**. Untuk menambahkan folder kustom (misalnya, perangkat USB yang dapat dilepas) ke daftar lokasi pencadangan, klik **Jelajahi** dan tentukan jalur folder.

Jika Anda menambahkan atau menghapus beberapa cadangan menggunakan manajer file, klik ikon roda gigi di samping nama lokasi, lalu klik **Menyegarkan**.

Peringatan!
Jangan mencoba mengedit file cadangan secara manual karena ini dapat mengakibatkan kerusakan file dan membuat cadangan tidak dapat digunakan. Selain itu, sebaiknya Anda menggunakan replikasi cadangan daripada memindahkan file cadangan secara manual.

Lokasi pencadangan (kecuali untuk penyimpanan awan) akan hilang dari tab **Penyimpanan cadangan** jika semua mesin yang pernah dicadangkan ke lokasi telah dihapus dari layanan Cyber Protection. Hal ini memastikan agar Anda tidak perlu membayar untuk cadangan yang disimpan di lokasi ini. Segera setelah dilakukan pencadangan ke lokasi ini, lokasi ditambahkan kembali bersama dengan semua cadangan yang disimpan di dalamnya.

Pada tab **Penyimpanan cadangan**, Anda dapat memfilter cadangan dalam daftar menggunakan kriteria berikut:

- **Hanya dengan data forensik** – hanya cadangan yang memiliki data forensik yang akan ditampilkan.
- **Hanya cadangan prapembaruan yang dibuat oleh Manajemen patch** – hanya cadangan yang dibuat selama berjalannya manajemen patch sebelum instalasi patch yang akan ditampilkan.

© Acronis International GmbH, 2003-2024

Untuk memilih titik pemulihan menggunakan tab Penyimpanan cadangan

1. Pada tab **Penyimpanan cadangan**, pilih lokasi penyimpanan cadangan.
   Perangkat lunak akan menampilkan semua cadangan yang diperbolehkan untuk dilihat oleh akun Anda dalam lokasi yang dipilih. Cadangan digabungkan ke dalam grup. Nama grup didasarkan pada templat berikut:
   `<nama mesin> - <nama rencana proteksi>`
2. Pilih grup yang berisi data yang ingin Anda pulihkan.
3. [Opsional] Klik **Ubah** di sebelah **Mesin untuk menelusuri**, lalu pilih mesin lain. Beberapa cadangan hanya dapat dilihat oleh agen spesifik. Misalnya, Anda harus memilih mesin yang menjalankan Agen untuk SQL untuk menjelajahi cadangan database Microsoft SQL Server.

   Penting
   Perlu diketahui bahwa **Mesin untuk menelusuri** adalah tujuan default untuk pemulihan dari pencadangan mesin fisik. Setelah Anda memilih titik pemulihan, klik **Pulihkan**, periksa kembali pengaturan **Mesin target** untuk memastikan bahwa Anda ingin memulihkan ke mesin spesifik ini. Untuk mengubah tujuan pemulihan, tentukan mesin lain di **Mesin untuk menelusuri**.
4. Klik **Tampilkan cadangan**.
5. Pilih titik pemulihan.

Untuk menambahkan lokasi cadangan

Catatan
Operasi ini hanya tersedia jika Anda memiliki agen online.

Di tab **Penyimpanan cadangan**, klik **Tambah lokasi**.

Pilih lokasi dari salah satu jenis lokasi berikut, lalu klik **Selesai**:

- Folder lokal
- Folder jaringan
- Secure Zone
- Folder NFS
- Cloud publik

Mounting volume dari cadangan

Mounting volume dari pencadangan tingkat disk memungkinkan Anda untuk mengakses volume seakan berupa disk fisik.

Mounting volume dalam mode baca/tulis memungkinkan Anda untuk memodifikasi konten pencadangan; yaitu, menyimpan, memindahkan, membuat, menghapus file atau folder, dan menjalankan file yang dapat dieksekusi yang terdiri dari satu file. Dalam mode ini, perangkat lunak

© Acronis International GmbH, 2003-2024

akan membuat cadangan inkremental berisi perubahan yang Anda buat pada konten pencadangan. Perhatikan bahwa tidak ada pencadangan berikutnya yang berisi perubahan ini.

Persyaratan

- Fungsi ini hanya tersedia di Windows menggunakan File Explorer.
- Agen untuk Windows harus diinstal pada mesin yang menjalankan operasi mounting.
- Sistem file yang dicadangkan harus didukung oleh versi Windows yang menjalankan mesin.
- Cadangan harus disimpan di folder lokal, di berbagi jaringan (SMB/CIFS), atau di Secure Zone.

Skenario Penggunaan

- Berbagi data
  Volume yang di-mount dapat dengan mudah dibagikan melalui jaringan.
- Solusi pemulihan database "Band aid"
  Mount volume yang berisi database SQL dari mesin yang baru saja mengalami kegagalan. Cara ini akan memberikan akses ke database sampai mesin yang mengalami kegagalan dipulihkan. Pendekatan ini juga dapat digunakan untuk pemulihan granular data Microsoft SharePoint dengan menggunakan SharePoint Explorer.
- Pembersihan virus offline
  Jika mesin terinfeksi, mount pencadangannya, bersihkan dengan program antivirus (atau temukan cadangan terbaru yang tidak terinfeksi), lalu pulihkan mesin dari cadangan ini.
- Pemeriksaan eror
  Jika pemulihan dengan pengubahan ukuran volume gagal, kemungkinan alasannya adalah eror dalam sistem file yang dicadangkan. Mount pencadangan dalam mode baca/tulis. Kemudian, periksa eror volume yang di-mount menggunakan perintah `chkdsk/r`. Setelah eror diperbaiki dan cadangan inkremental baru dibuat, pulihkan sistem dari cadangan ini.

Untuk mounting volume dari cadangan

1. Jelajahi lokasi cadangan menggunakan File Explorer.
2. Klik dua kali pada file cadangan. Nama file didasarkan pada templat berikut:
   `<nama mesin> - <GUID rencana proteksi>`
3. Jika cadangan dienkripsi, masukkan kata sandi. Jika tidak, lewati langkah ini.
   File Explorer menampilkan titik pemulihan.
4. Klik dua kali pada titik pemulihan.
   File Explorer menampilkan volume yang dicadangkan.

Catatan
Klik dua kali pada volume untuk menjelajahi kontennya. Anda dapat menyalin file dan folder dari cadangan ke folder apa pun di sistem file.

© Acronis International GmbH, 2003-2024

5. Klik kanan volume yang akan di-mount, lalu pilih salah satu opsi berikut:
   a. **Pasang**

      Catatan
      Hanya cadangan terakhir dalam arsip (rantai cadangan) yang dapat dipasang dalam mode baca-tulis.

   b. **Mount dalam mode hanya-baca**.
6. Jika cadangan disimpan di berbagi jaringan, sediakan kredensial akses. Jika tidak, lewati langkah ini.

   Perangkat lunak akan melakukan mounting volume yang dipilih. Huruf yang tidak digunakan pertama ditetapkan pada volume.

Untuk melepas volume

1. Jelajahi ke **Komputer** (**PC ini** dalam Windows 8.1 ke atas) menggunakan File Explorer.
2. Klik kanan volume ter-mount.
3. Klik **Lepas**.
4. [Opsional] Jika volume di-mount pada mode baca/tulis, dan kontennya dimodifikasi, pilih apakah akan membuat cadangan inkremental yang berisi perubahan. Jika tidak, lewati langkah ini.

Perangkat lunak akan melepas volume yang dipilih.

Memvalidasi cadangan

Dengan memvalidasi cadangan, Anda memverifikasi bahwa Anda dapat memulihkan data darinya. Untuk informasi lebih lanjut tentang operasi ini, lihat "Validasi" (hlm. 201).

Catatan
Fungsionalitas ini tersedia di penyewa pelanggan untuk yang **Cadangan Lanjutan - Server** atau **Cadangan Lanjutan - NAS** kuota diaktifkan sebagai bagian dari paket Cadangan Lanjutan.

Cara memvalidasi cadangan

1. Pilih beban kerja yang dicadangkan.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.

   Jika beban kerja sedang offline, titik pemulihan tidak ditampilkan. Lakukan yang berikut ini:
   - Jika lokasi cadangan adalah awan atau penyimpanan bersama (yaitu agen lain dapat mengaksesnya), klik **Pilih mesin**, pilih beban kerja target yang online, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab Penyimpanan cadangan. Untuk informasi lebih lanjut tentang cadangan di sana, lihat "Tab Penyimpanan cadangan" (hlm. 526).
4. Klik ikon roda gigi, lalu klik **Validasi**.

© Acronis International GmbH, 2003-2024

5. Pilih agen yang akan melakukan validasi.
6. Pilih metode validasi.
7. Jika cadangan dienkripsi, berikan kata sandi enkripsi.
8. Klik **Mulai**.

Mengekspor cadangan

Operasi ekspor membuat salinan pencadangan secara mandiri di lokasi yang Anda tentukan. Cadangan asli tetap tidak tersentuh. Mengekspor cadangan memungkinkan Anda untuk memisahkan pencadangan spesifik dari rantai pencadangan inkremental dan diferensial untuk pemulihan cepat, menulis ke media yang dapat dilepas atau dicopot, atau tujuan lain.

Catatan
Fungsionalitas ini tersedia di penyewa pelanggan untuk yang **Cadangan Lanjutan - Server** atau **Cadangan Lanjutan - NAS** kuota diaktifkan sebagai bagian dari paket Cadangan Lanjutan.

Hasil operasi ekspor selalu berupa cadangan penuh. Jika Anda ingin mereplikasi seluruh rantai cadangan ke lokasi yang berbeda dan mempertahankan beberapa titik pemulihan, gunakan rencana replikasi cadangan. Untuk informasi lebih lanjut tentang rencana ini, lihat "Replikasi cadangan" (hlm. 198).

Nama file cadangan dari cadangan yang diekspor sama dengan cadangan aslinya, kecuali nomor urutnya. Jika beberapa cadangan dari rantai cadangan yang sama diekspor ke lokasi yang sama, empat digit nomor urut akan ditambahkan ke nama file semua cadangan kecuali yang pertama.

Cadangan yang diekspor akan mewarisi pengaturan enkripsi dan kata sandi dari cadangan asli. Saat mengekspor cadangan terenkripsi, Anda harus menentukan kata sandi.

Untuk mengekspor cadangan

1. Pilih beban kerja yang dicadangkan.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
   Jika beban kerja sedang offline, titik pemulihan tidak ditampilkan. Lakukan yang berikut ini:
   - Jika lokasi cadangan adalah awan atau penyimpanan bersama (yaitu agen lain dapat mengaksesnya), klik **Pilih mesin**, pilih beban kerja target yang online, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab Penyimpanan cadangan. Untuk informasi lebih lanjut tentang cadangan di sana, lihat "Tab Penyimpanan cadangan" (hlm. 526).
4. Klik ikon roda gigi, lalu klik **Ekspor**.
5. Pilih agen yang akan melakukan ekspor.
6. Jika cadangan dienkripsi, berikan kata sandi enkripsi. Jika tidak, lewati langkah ini.

© Acronis International GmbH, 2003-2024

7. Tentukan tujuan ekspor.
8. Klik **Mulai**.

Menghapus beberapa cadangan

Arsip cadangan berisi satu atau lebih cadangan. Anda dapat menghapus cadangan tertentu (titik pemulihan) dalam arsip atau seluruh arsip.

Menghapus arsip cadangan menghapus semua cadangan di dalamnya. Menghapus semua cadangan dari beban kerja menghapus arsip cadangan yang berisi cadangan-cadangan tersebut.

Anda dapat menghapus cadangan dengan menggunakan konsol Cyber Protect – pada tab **Perangkat** dan pada tab **Penyimpanan cadangan**. Selain itu, Anda juga dapat menghapus cadangan dari penyimpanan cloud dengan menggunakan konsol Web Restore.

Peringatan!
Jika penyimpanan yang tidak dapat diubah dinonaktifkan, data yang telah dicadangkan akan dihapus secara permanen dan tidak dapat dipulihkan.

Untuk menghapus cadangan atau arsip cadangan

Di tab Perangkat

Prosedur ini hanya berlaku untuk beban kerja online.

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih cadangan beban kerja yang ingin Anda hapus.
3. Klik **Pemulihan**.
4. [Jika tersedia lebih dari satu lokasi cadangan] Pilih lokasi cadangan.
5. [Untuk menghapus semua cadangan beban kerja] Klik **Hapus semua**.
   Menghapus semua cadangan juga menghapus arsip cadangan yang berisi cadangan-cadangan ini.
6. [Untuk menghapus cadangan tertentu] Pilih cadangan (titik pemulihan) yang ingin Anda hapus, lalu klik **Aksi** > **Hapus**.
7. [Ketika menghapus semua cadangan] Pilih kotak centang, lalu klik **Hapus** untuk mengonfirmasi keputusan Anda.
8. [Ketika menghapus cadangan tertentu] Klik **Hapus** untuk mengonfirmasi keputusan Anda.

Di tab Penyimpanan cadangan

Prosedur ini berlaku untuk beban kerja online dan offline.

1. Di konsol Cyber Protect, buka **Penyimpanan cadangan**.
2. Pilih lokasi tempat ingin Anda hapus cadangannya.
3. Pilih arsip cadangan yang ingin Anda hapus cadangannya.

© Acronis International GmbH, 2003-2024

Nama arsip menggunakan templat berikut:

- Arsip cadangan non-cloud ke cloud: <nama beban kerja> - <nama rencana proteksi>
- Arsip cadangan cloud-ke-cloud: <nama pengguna> atau <nama drive> atau <nama tim> - <layanan cloud> - <nama rencana proteksi>

4. [Untuk menghapus seluruh arsip cadangan] Klik **Hapus**.
   Menghapus arsip cadangan menghapus semua cadangan di dalam arsip tersebut.
5. [Untuk menghapus cadangan tertentu di arsip cadangan] Klik **Tampilkan cadangan**.
   a. Pilih cadangan (titik pemulihan) yang ingin Anda hapus.
   b. Klik **Aksi** > **Hapus**.
6. [Ketika menghapus arsip cadangan] Pilih kotak centang, lalu klik **Hapus** untuk mengonfirmasi keputusan Anda.
7. [Ketika menghapus cadangan tertentu] Klik **Hapus** untuk mengonfirmasi keputusan Anda.

Di konsol Pemulihan Web

Prosedur ini hanya berlaku untuk arsip cadangan di penyimpanan cloud.

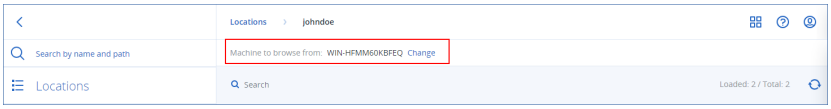
1. Di konsol Cyber Protection, buka **Perangkat** > **Semua perangkat**.
2. Pilih cadangan beban kerja yang ingin Anda hapus, lalu klik **Pemulihan**.
3. [Jika ada beberapa lokasi cadangan yang tersedia] Pilih lokasi cadangan, lalu klik **Cara pemulihan lain**.
4. Klik **Unduh file**.
   Anda dialihkan ke konsol Pemulihan Web.
5. Di konsol Web Restore, di bawah **Mesin**, klik nama beban kerja.
6. Di bawah **Versi Terakhir**, klik tanggal, dan kemudian klik **Hapus**.
   Tindakan ini hanya tersedia pada level arsip cadangan. Anda tidak dapat menelusuri arsip secara lebih dalam dan menghapus cadangan tertentu dari sana.
7. Klik **Hapus** untuk mengonfirmasi keputusan Anda.

Menghapus cadangan di luar Cyber Protect konsol

Kami merekomendasikan agar Anda menghapus cadangan dengan menggunakan konsol Cyber Protect. Jika Anda menghapus cadangan dari penyimpanan cloud dengan menggunakan konsol Web Restore atau menghapus cadangan lokal dengan menggunakan manajer file, Anda harus me-refresh lokasi cadangan untuk melakukan sinkronisasi perubahan ke konsol Cyber Protect.

Prasyarat

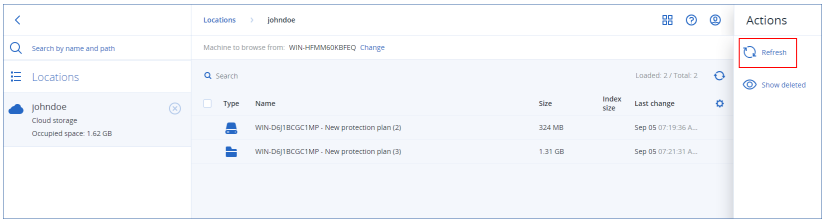
- Agen online yang dapat mengakses lokasi cadangan harus dipilih sebagai **Mesin untuk menjelajah dari** di konsol Cyber Protect.



Untuk me-refresh lokasi cadangan

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Penyimpanan cadangan**.
2. Pilih lokasi cadangan tempat cadangan yang telah dihapus disimpan.
3. Di panel **Aksi**, klik **Refresh**.



Memahami deteksi kemacetan

Fitur deteksi kemacetan membantu Anda memahami di mana Anda dapat meningkatkan kinerja dengan menyorot komponen mana di sistem Anda yang paling lambat selama proses pencadangan atau pemulihan.

Karena kemacetan *selalu* terjadi dalam peristiwa transmisi apa pun, bukan berarti setiap kemacetan harus segera ditangani. Pencadangan Anda mungkin sudah cukup cepat dan memenuhi jendela pencadangan dengan sempurna, serta memenuhi SLA Anda, jadi biasanya tidak ada yang perlu Anda tangani.

Anda dapat dengan mudah melihat dan melacak kemacetan di tab **Detail aktivitas**. Untuk melakukan ini, di konsol Cyber Protect, buka **Pemantauan > Aktivitas**, lalu klik aktivitas yang relevan. Untuk informasi lebih lanjut tentang melihat kemacetan, lihat "Melihat detail kemacetan" (hlm. 536) dan "Pada beban kerja, agen, dan lokasi pencadangan apa yang mengalami hambatan?" (hlm. 537).

Apa itu kemacetan?

Kemacetan biasanya disebabkan karena lambatnya komponen dalam rantai pemrosesan, atau dengan kata lain, ada suatu komponen yang ditunggu oleh komponen lainnya.

Fitur deteksi kemacetan memungkinkan Anda melacak laju komponen yang lambat ini selama proses pencadangan dan pemulihan, membantu Anda memahami jenis komponen mana yang paling lambat:

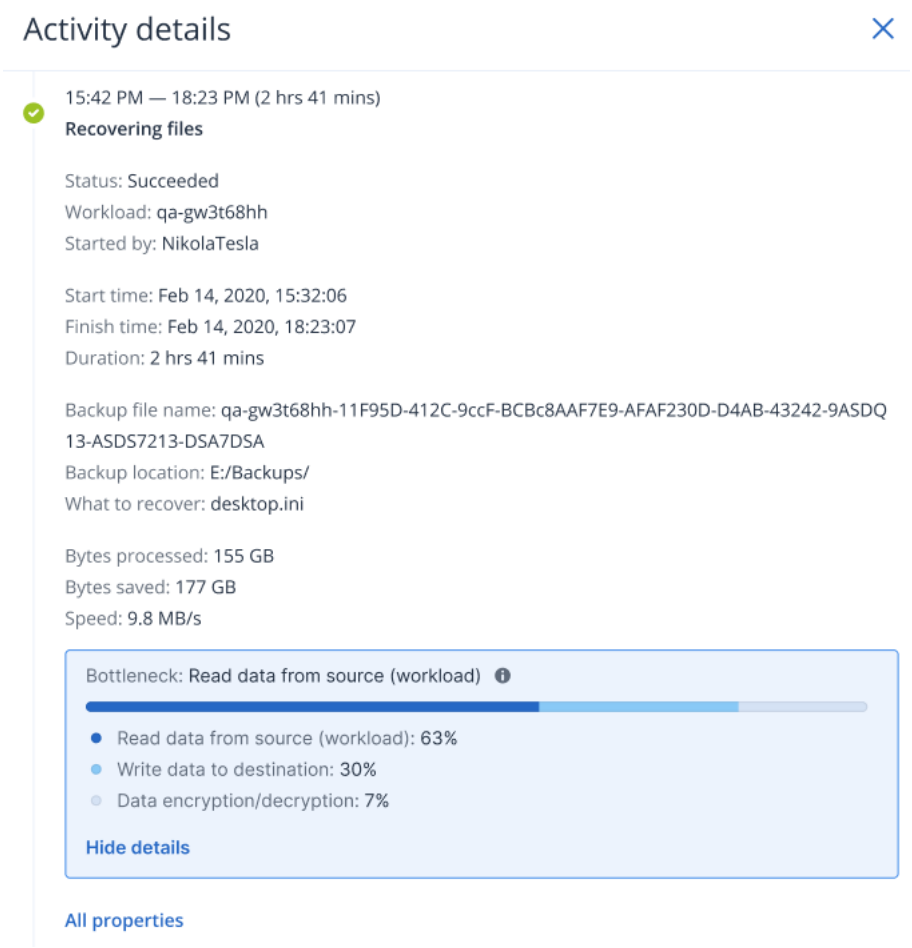
- **Sumber**: Sekilas, Anda dapat menentukan apakah kecepatan membaca dari sumber pencadangan/pemulihan menyebabkan kemacetan.
- **Tujuan**: Pahami apakah kecepatan menulis ke tujuan pencadangan/pemulihan memengaruhi kinerja.
- **Agen**: Pahami apakah agen memproses data dengan cukup cepat.

Jenis kemacetan, baik dari sumber, tujuan, atau agen, dapat berubah pada waktu yang berbeda-beda selama aktivitas pencadangan/pemulihan. Persentase yang ditampilkan di bagian **Kemacetan** dari tab **Detail aktivitas** di bawah (misalnya, **Baca data dari sumber (beban kerja): 63%**), menandakan persentase waktu ketika jenis kemacetan ini ditemui. Dalam hal ini, untuk 63% waktu

© Acronis International GmbH, 2003-2024

aktivitas pemulihan, jenis hambatannya adalah pembacaan data, dengan kata lain lambatnya kecepatan dalam membaca data dari arsip cadangan oleh agen.

Demikian pula, sebanyak 30% dari waktu tersebut, kemacetan disebabkan oleh lambatnya kecepatan penulisan data ke tujuan pemulihan (**Tulis data ke tujuan: 30%**).



Catatan
Melihat statistik kemacetan di tab **Detail aktivitas** merupakan hal yang wajar. Statistik ini hanya tersedia untuk tugas yang berdurasi lebih dari satu menit.

Bagaimana cara mengurangi kemacetan

Seperti disebutkan di atas, fitur deteksi kemacetan menyoroti aliran data *baca* dan *tulis* di antara komponen cadangan. Statistik *baca* merujuk pada aliran data dari sumber data ke agen yang melakukan operasi pencadangan/pemulihan, dan statistik *baca* merujuk pada aliran data antara agen dan arsip cadangan (tujuan).

Untuk mengurangi kemacetan dan meningkatkan kinerja aliran data baca/tulis, Anda harus menganalisis saluran antara agen dan sumber data/arsip cadangan. Misalnya, Anda dapat mencoba melakukan pengujian banding kinerja pada hard disk Anda jika agen mencadangkan beberapa file lokal.

© Acronis International GmbH, 2003-2024

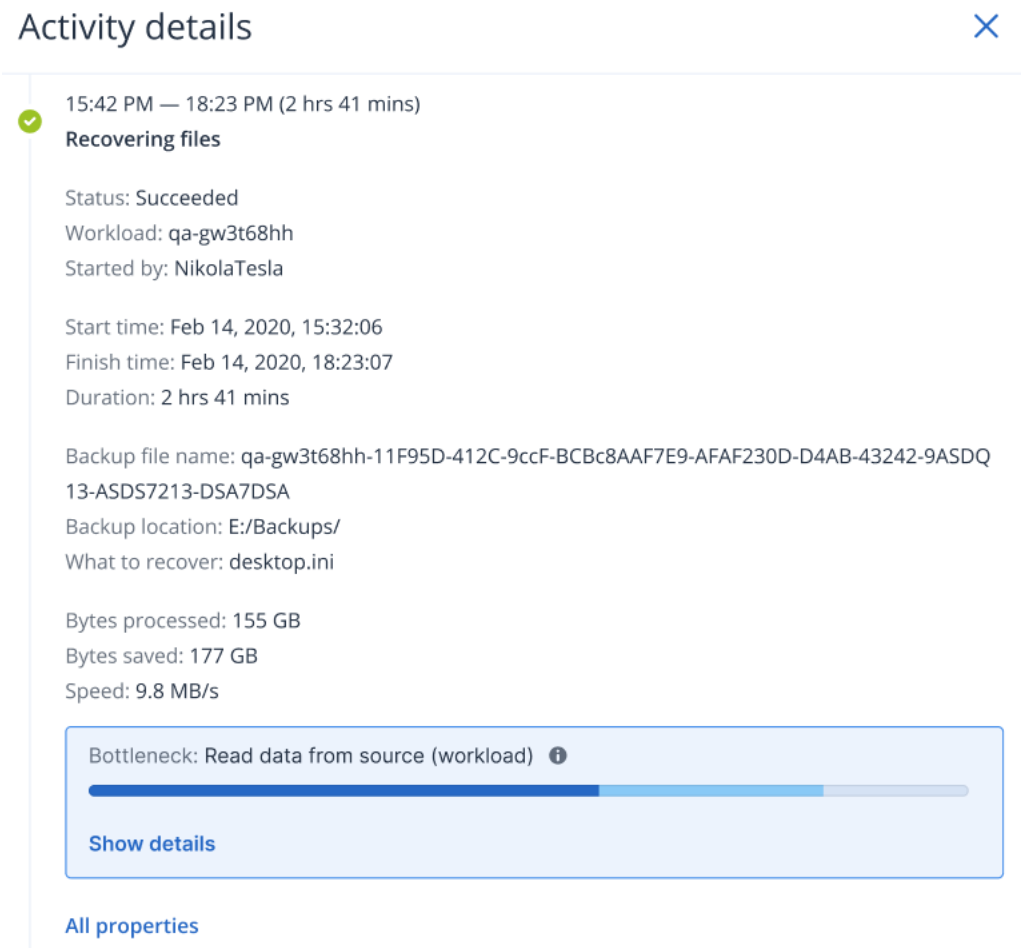
Melihat detail kemacetan

Anda dapat melihat kemacetan yang terdeteksi untuk semua jenis pencadangan, replikasi pencadangan, atau proses pemulihan (ke semua jenis folder atau lokasi tujuan), termasuk pencadangan mesin virtual, pencadangan mesin, dan pencadangan file/folder. Anda juga dapat melihat hambatan pada replikasi mesin virtual dan aktivitas failback.

Untuk informasi lebih lanjut tentang definisi dan konsep inti jenis kemacetan, lihat "Memahami deteksi kemacetan" (hlm. 534).

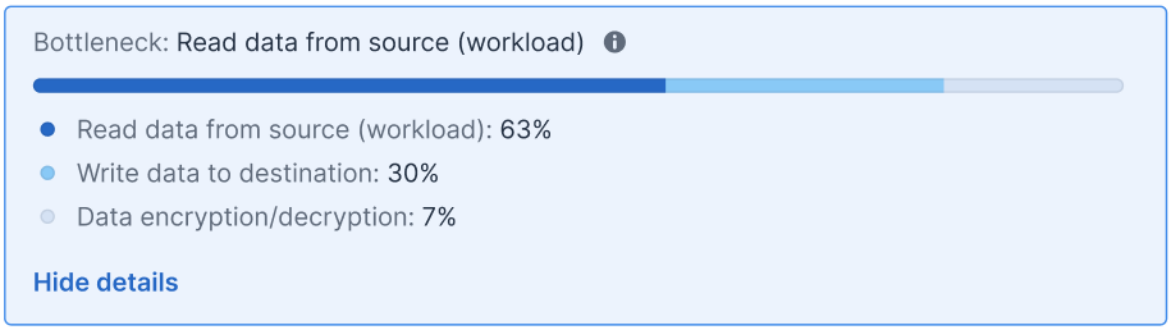
Untuk melihat detail kemacetan

1. Di konsol Cyber Protect, buka **Pemantauan > Aktivitas**.
2. Klik pada aktivitas yang relevan.
   Di tab **Detail aktivitas**, bagian **Kemacetan** ditampilkan dengan warna biru.



3. Klik **Tampilkan detail** untuk melihat hambatan yang paling sering ditemui selama operasi pencadangan/pemulihan.
   Bagian **Kemacetan** diperluas untuk menampilkan ringkasan jenis hambatan yang relevan.

© Acronis International GmbH, 2003-2024



Pada contoh di atas, kemacetan yang mencapai 63% dari keseluruhan waktu operasi disebabkan oleh operasi *Baca* (dilakukan oleh agen).

Catatan
Nilai kemacetan diperbarui secara dinamis setiap menit saat aktivitas terkait sedang berjalan.

Pada beban kerja, agen, dan lokasi pencadangan apa yang mengalami hambatan?

Deteksi kemacetan tersedia untuk jenis beban kerja, agen, dan lokasi pencadangan berikut:

- Pencadangan tingkat disk/gambar dilakukan oleh:
  - Agen untuk Azure
  - Agen untuk Windows
  - Agen untuk Linux
  - Agen untuk MAC
  - Agen untuk VMware (Peralatan Virtual dan Windows, termasuk replikasi VM dan failback dari aktivitas replika (pemulihan dari replika))
  - Agen untuk Hyper-V
  - Agen untuk Scale Computing
  - Agen untuk oVirt (KVM)
  - Agen untuk Platform Infrastruktur Virtuozzo
  - Agen untuk Virtuozzo
  - Agen untuk VMware Cloud Director (vCD-BA)
- Pencadangan tingkat file
  - Agen untuk Windows
  - Agen untuk Linux
  - Agen untuk MAC
- Pencadangan tingkat aplikasi
  - Agen untuk SQL
  - Agen untuk Exchange

© Acronis International GmbH, 2003-2024

    - Agen untuk MySQL/MariaDB
    - Agen untuk Oracle
    - Agen untuk SAP HANA
- Lokasi pencadangan
    - Penyimpanan Acronis Cloud (termasuk penyimpanan yang di-host mitra)
    - Penyimpanan Cloud Publik
    - Berbagi jaringan (SMB + NFS)
    - Folder lokal
    - Lokasi ditentukan oleh skrip
    - Zona Aman Acronis

Mencadangkan beban kerja ke cloud publik

Catatan
Fitur ini merupakan bagian dari paket Advanced Backup, yang juga merupakan bagian dari layanan Cyber Protection. Perlu diperhatikan bahwa saat Anda menambahkan fungsi ini ke rencana proteksi, Anda mungkin dikenakan biaya tambahan.

Anda dapat memilih layanan cloud publik, seperti Microsoft Azure dan Amazon S3 (Simple Storage Service), sebagai tujuan cadangan di konsol Cyber Protect.

Untuk mengkonfigurasi lokasi cadangan di cloud publik, Anda harus menjadi administrator Perusahaan atau administrator Unit, atau memiliki salah satu peran berikut sesuai ketentuan dalam layanan Perlindungan Cyber: administrator Cyber, Administrator, atau Pengguna.

Menentukan lokasi cadangan di Microsoft Azure

Catatan
Untuk mengkonfigurasi lokasi cadangan di Microsoft Azure, Anda harus memiliki salah satu peran berikut sesuai ketentuan dalam layanan Perlindungan Cyber: Administrator perusahaan, Pengguna, Administrator Cyber.

Untuk mencadangkan beban kerja ke Microsoft Azure, Anda perlu menentukan lokasi pencadangan Microsoft Azure di konsol Cyber Protect, dan membuat sambungan ke langganan Microsoft Azure yang relevan. Hal ini dapat dilakukan dengan cara berikut:

- Saat membuat atau mengedit rencana proteksi.
- Saat menentukan dan mengelola lokasi penyimpanan cadangan.

© Acronis International GmbH, 2003-2024

Penting
Pengguna administrator dan non-administrator dapat mencadangkan beban kerja ke Microsoft Azure.

Pengguna non-administrator dapat menambahkan akses ke langganan Microsoft Azure (lihat "Mengelola akses ke langganan Microsoft Azure" (hlm. 549)), namun hanya dapat menerapkan rencana proteksi jika lokasi cadangan terhubung ke langganan Microsoft Azure yang mereka tambahkan sendiri, dan untuk beban kerja yang didaftarkan di konsol Cyber Protect dengan nama mereka.

Administrator dapat menerapkan rencana proteksi ketika lokasi pencadangan terhubung ke langganan Microsoft Azure yang mereka tambahkan sendiri atau ke langganan yang ditambahkan oleh administrator lain, dan untuk beban kerja yang terdaftar di konsol Cyber Protect pada pengguna mana pun.

Untuk menentukan lokasi cadangan di Microsoft Azure

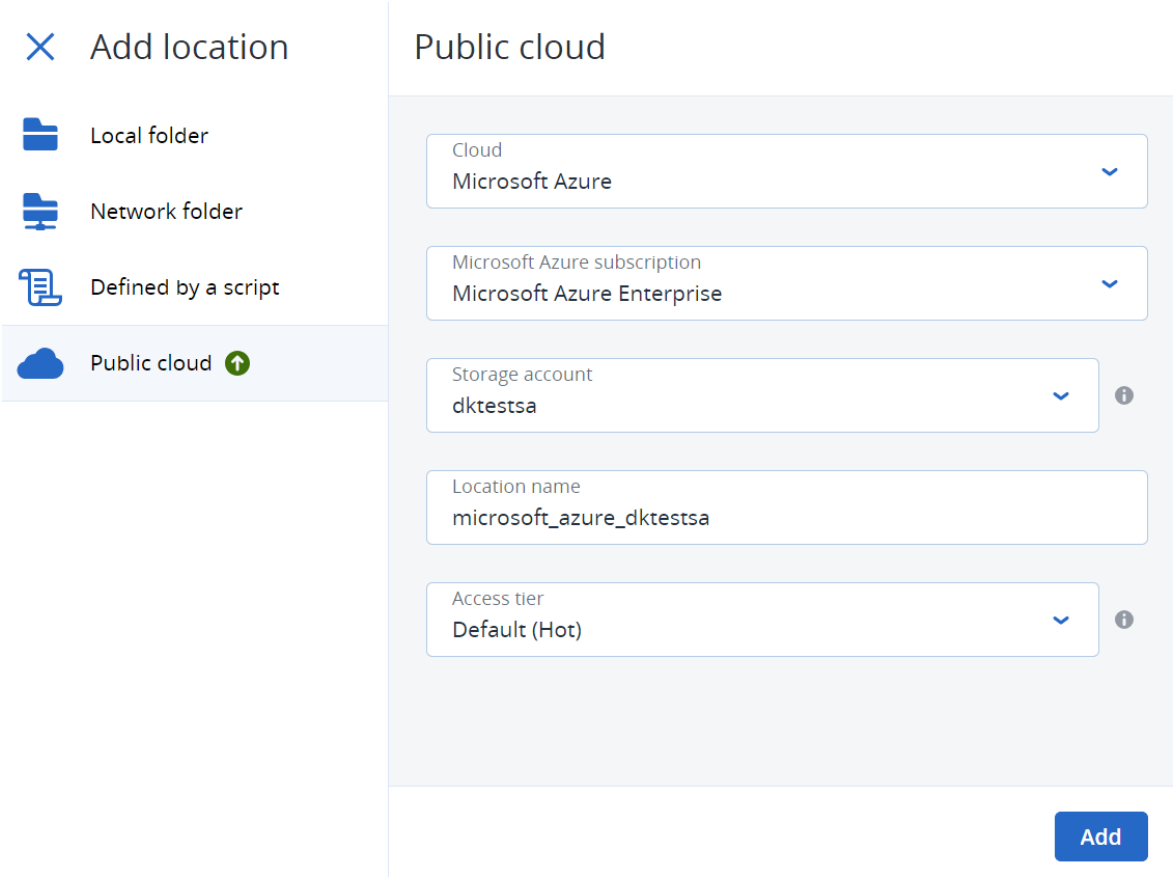
1. Di konsol Cyber Protect, lakukan salah satu hal berikut:
   - Jika Anda membuat atau mengedit rencana proteksi, buka **Perangkat** dan pilih beban kerja relevan yang ingin Anda cadangankan ke Microsoft Azure. Di bagian **Cadangan** pada rencana proteksi beban kerja yang dipilih, klik tautan di baris **Tempat menyimpan cadangan**.
     Untuk informasi lebih lanjut tentang bekerja dengan rencana proteksi, lihat "Modul dan rencana proteksi" (hlm. 213).
   - Jika Anda mengelola lokasi penyimpanan cadangan dan ingin menambahkan Microsoft Azure sebagai lokasi baru, buka **Penyimpanan cadangan**.
     Untuk informasi selengkapnya tentang mengelola lokasi penyimpanan cadangan Anda, lihat "Tab Penyimpanan cadangan" (hlm. 526).
2. Klik **Tambahkan lokasi**.
3. Dari daftar drop-down **Cloud Publik**, pilih **Microsoft Azure**.
4. Jika langganan Microsoft Azure yang relevan sudah terdaftar di konsol Cyber Protect, pilih langganan tersebut dari daftar langganan.
   Jika langganan yang relevan tidak terdaftar di konsol Cyber Protect, klik **Tambahkan** dan pada dialog yang ditampilkan, klik **Masuk**. Anda diarahkan ke halaman masuk Microsoft. Untuk informasi selengkapnya tentang menambahkan dan menentukan akses ke langganan Microsoft Azure, lihat "Menambahkan akses ke langganan Microsoft Azure" (hlm. 550).
5. Di bidang **Akun penyimpanan**, pilih akun yang relevan.

   Catatan
   Hanya akun penyimpanan Microsoft Azure dengan akhiran titik akhir reguler yang berisi `core.windows.net` yang saat ini didukung. Selain itu, akun penyimpanan yang dipilih harus berupa jenis akun StorageV2.

© Acronis International GmbH, 2003-2024

Bidang **Nama lokasi** dan **Tingkat akses** secara otomatis diisi secara default, sesuai dengan akun penyimpanan. terpilih. Nama lokasi yang ditampilkan adalah `microsoft_azure_[akun penyimpanan]` dan tingkat akses yang dipilih adalah **Default (Hot)**. Kedua bidang dapat dimodifikasi, sesuai kebutuhan.

Catatan
Saat mengubah nama lokasi, masukkan nama lokasi unik (nama harus unik untuk penyewa pelanggan). Jika nama yang Anda tambahkan sudah ada di akun penyimpanan, Acronis menambahkan nomor akhiran ke nama tersebut. Misalnya, jika **Penyimpanan Microsoft Azure** sudah tersedia, namanya otomatis diperbarui menjadi **Microsoft Azure Storage_01**.



6. Klik **Tambah**.
   Jika Anda membuat atau mengedit rencana proteksi, lokasi pencadangan Microsoft Azure ditetapkan sebagai lokasi di baris **Tempat menyimpan cadangan**. Saat pencadangan dijalankan (baik secara manual atau terjadwal), pencadangan disimpan di lokasi yang ditentukan.
   Jika Anda mengelola lokasi penyimpanan cadangan, Anda dapat melihat dan memperbarui detail lokasi sesuai kebutuhan. Lokasi Microsoft Azure juga tersedia saat mendefinisikan lokasi cadangan untuk beban kerja. Untuk informasi lebih lanjut, lihat "Melihat dan memperbarui lokasi cadangan cloud publik" (hlm. 545).

© Acronis International GmbH, 2003-2024

Mendefinisikan lokasi cadangan di Amazon S3

Catatan
Untuk mengkonfigurasi lokasi cadangan di Amazon S3, Anda harus memiliki salah satu peran berikut sesuai ketentuan dalam layanan Perlindungan Cyber: Administrator perusahaan, Pengguna, Administrator Cyber.

Untuk mencadangkan beban kerja ke Amazon S3, Anda harus menentukan lokasi cadangan Amazon S3 di konsol Cyber Protect, kemudian terhubung ke koneksi Amazon S3 yang relevan. Anda dapat melakukannya dengan cara berikut:

- Saat membuat atau mengedit rencana proteksi.
- Saat menentukan dan mengelola lokasi penyimpanan cadangan.

Penting
Baik administrator maupun pengguna non-administrator dapat mencadangkan beban kerja ke Amazon S3.

Pengguna non-administrator dapat menambahkan akses ke koneksi Amazon S3 (lihat "Mengelola akses ke layanan penyimpanan cloud publik lainnya" (hlm. 553)), tetapi hanya dapat menerapkan rencana proteksi pada saat lokasi cadangan terhubung ke koneksi Amazon S3 yang mereka tambahkan sendiri, dan untuk beban kerja yang terdaftar di konsol Cyber Protect di bawah nama mereka.

Administrator dapat menerapkan rencana proteksi pada saat lokasi cadangan terhubung ke koneksi Amazon S3 yang mereka tambahkan sendiri atau ke langganan yang ditambahkan oleh administrator lain, dan untuk beban kerja yang terdaftar di konsol Cyber Protect di bawah nama pengguna mana pun.

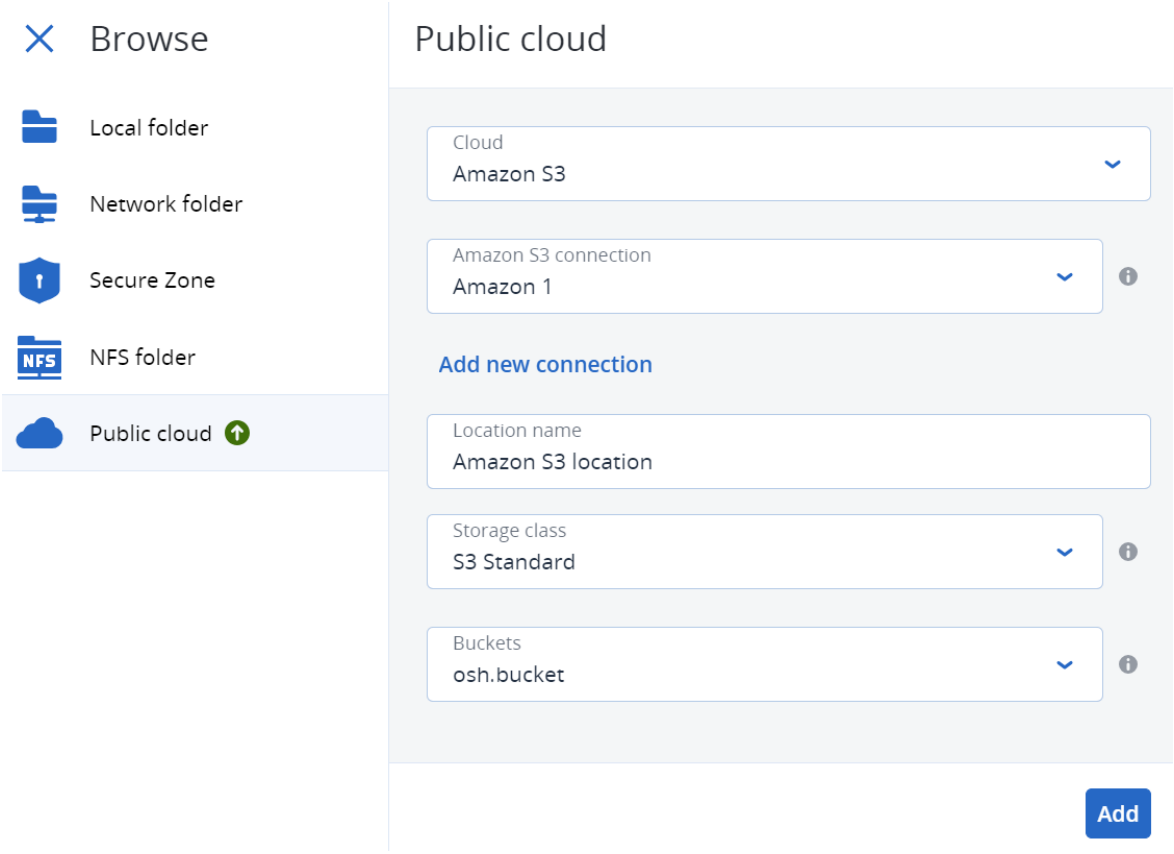
Untuk menentukan lokasi cadangan di Amazon S3

1. Di konsol Cyber Protect, lakukan salah satu hal berikut:
   - Jika Anda membuat atau mengedit rencana proteksi, buka **Perangkat**, kemudian pilih beban kerja yang ingin Anda cadangkan ke Amazon S3. Di bagian **Backup** dari rencana proteksi beban kerja yang dipilih, klik tautan di baris **Di mana harus mencadangkan**.
     Untuk informasi lebih lanjut tentang bekerja dengan rencana proteksi, lihat "Modul dan rencana proteksi" (hlm. 213).
   - Jika Anda mengelola lokasi penyimpanan cadangan Anda dan ingin menambahkan Amazon S3 sebagai lokasi baru, buka **Penyimpanan cadangan**.
     Untuk informasi selengkapnya tentang mengelola lokasi penyimpanan cadangan Anda, lihat "Tab Penyimpanan cadangan" (hlm. 526).
2. Klik **Tambahkan lokasi**.

© Acronis International GmbH, 2003-2024

3. Dari daftar drop-down **Cloud Publik**, pilih **Amazon S3**.
4. Jika koneksi Amazon S3 yang relevan sudah terdaftar di konsol Cyber Protect, pilih dari daftar tersebut.

   Jika koneksi yang relevan tidak terdaftar di konsol Cyber Protect, klik **Tambah koneksi baru**. Untuk informasi lebih lanjut tentang menambahkan dan mendefinisikan akses ke koneksi Amazon S3, lihat "Menambahkan akses ke koneksi cloud publik" (hlm. 553). Jika koneksi telah ditambahkan, lanjutkan ke langkah berikutnya.



5. Tentukan hal berikut:
   - Di bidang **Nama lokasi**, masukkan nama dari lokasi cadangan.

     Catatan
     Nama lokasi harus unik untuk penyewa pelanggan. Jika nama yang Anda tambahkan sudah ada dalam koneksi, Acronis menambahkan nomor akhiran ke nama tersebut. Sebagai contoh, jika **penyimpanan Amazon S3** sudah ada, nama akan secara otomatis diperbarui menjadi **penyimpanan Amazon S3 1**.

   - Di bidang **Kelas Penyimpanan**, pilih dari salah satu kelas penyimpanan yang didukung berikut:
     - S3 Standard
     - Standar - Akses Jarang (S3 Standard-IA)

© Acronis International GmbH, 2003-2024

- Satu Zona - Akses Jarang (S3 One Zone-IA)
- S3 Intelligent Tiering

- Di bidang **Keranjang**, pilih keranjang Amazon S3 yang relevan.

6. Klik **Tambah**.

   Jika Anda membuat atau mengedit rencana proteksi, lokasi cadangan Amazon S3 ditetapkan sebagai lokasi di baris **Di mana harus mencadangkan**. Ketika cadangan dijalankan (baik secara manual atau ketika dijadwalkan), cadangan disimpan di lokasi yang ditentukan.

   Jika Anda mengelola lokasi penyimpanan cadangan, Anda dapat melihat dan memperbarui detail lokasi sesuai kebutuhan. Lokasi Amazon S3 juga tersedia saat mendefinisikan lokasi cadangan untuk beban kerja. Untuk informasi lebih lanjut, lihat "Melihat dan memperbarui lokasi cadangan cloud publik" (hlm. 545).

Mendefinisikan lokasi cadangan di Wasabi

Catatan
Untuk mengkonfigurasi lokasi cadangan di Wasabi, Anda harus memiliki salah satu peran berikut sesuai ketentuan dalam layanan Perlindungan Cyber: Administrator perusahaan, Pengguna, Administrator Cyber.

Untuk mencadangkan beban kerja ke Wasabi, Anda harus menentukan lokasi cadangan Wasabi di konsol Cyber Protect, dan terhubung ke koneksi Wasabi yang relevan. Anda dapat melakukannya dengan cara berikut:

- Saat membuat atau mengedit rencana proteksi.
- Saat menentukan dan mengelola lokasi penyimpanan cadangan.

Penting
Baik administrator maupun pengguna non-administrator dapat mencadangkan beban kerja ke Wasabi.

Pengguna non-administrator dapat menambahkan akses ke koneksi Wasabi (lihat "Mengelola akses ke layanan penyimpanan cloud publik lainnya" (hlm. 553)), tetapi hanya dapat menerapkan rencana proteksi pada saat lokasi cadangan terhubung ke koneksi Wasabi yang mereka tambahkan sendiri, dan untuk beban kerja yang terdaftar di konsol Cyber Protect di bawah nama mereka.

Administrator dapat menerapkan rencana proteksi pada saat lokasi cadangan terhubung ke koneksi Wasabi yang mereka tambahkan sendiri atau ke langganan yang ditambahkan oleh administrator lain, dan untuk beban kerja yang terdaftar di konsol Cyber Protect di bawah nama pengguna mana pun.

Untuk menentukan lokasi cadangan di Wasabi

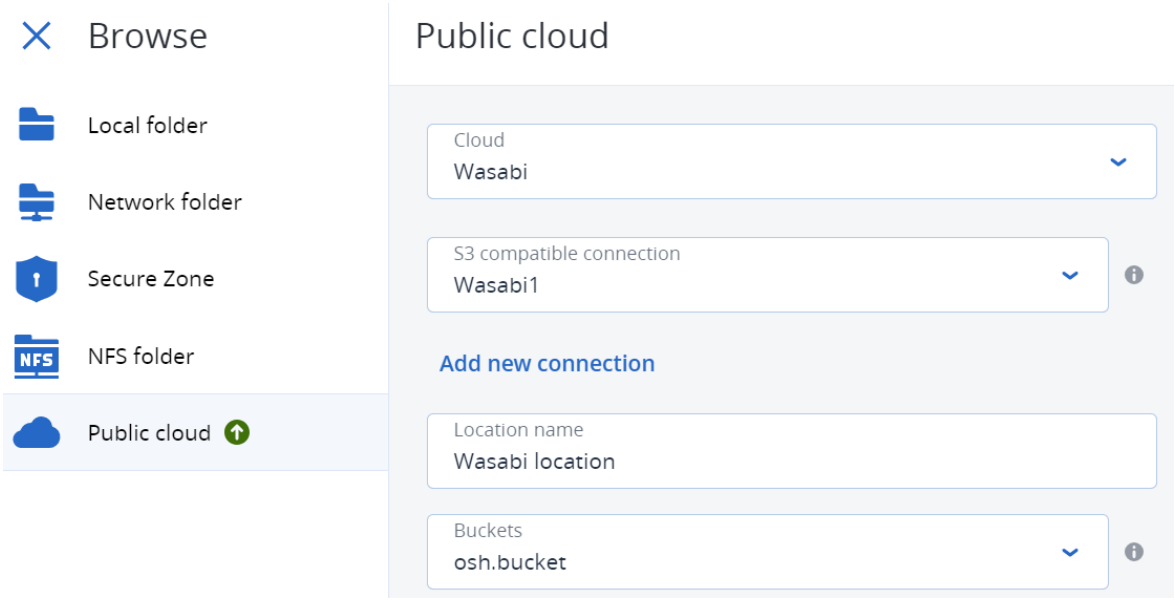
© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, lakukan salah satu hal berikut:
   - Jika Anda membuat atau mengedit rencana proteksi, buka **Perangkat**, kemudian pilih beban kerja yang ingin Anda cadangkan ke Wasabi. Di bagian **Backup** dari rencana proteksi beban kerja yang dipilih, klik tautan di baris **Di mana harus mencadangkan**.

     Untuk informasi lebih lanjut tentang bekerja dengan rencana proteksi, lihat "Modul dan rencana proteksi" (hlm. 213).
   - Jika Anda mengelola lokasi penyimpanan cadangan dan ingin menambahkan Wasabi sebagai lokasi baru, buka **Penyimpanan cadangan**.

     Untuk informasi selengkapnya tentang mengelola lokasi penyimpanan cadangan Anda, lihat "Tab Penyimpanan cadangan" (hlm. 526).
2. Klik **Tambahkan lokasi**.
3. Dari daftar drop-down **Cloud Publik**, pilih **Wasabi**.
4. Jika koneksi Wasabi yang relevan sudah terdaftar di konsol Cyber Protect, pilih dari daftar koneksi tersebut.

   Jika koneksi yang relevan tidak terdaftar di konsol Cyber Protect, klik **Tambah koneksi baru**. Untuk informasi lebih lanjut tentang menambahkan dan mendefinisikan akses ke koneksi Wasabi, lihat "Menambahkan akses ke koneksi cloud publik" (hlm. 553). Jika koneksi telah ditambahkan, lanjutkan ke langkah berikutnya.



5. Tentukan hal berikut:
   - Di bidang **Nama lokasi**, masukkan nama dari lokasi cadangan.

     Catatan
     Nama lokasi harus unik untuk penyewa pelanggan. Jika nama yang Anda tambahkan sudah ada dalam koneksi, Acronis menambahkan nomor akhiran ke nama tersebut. Sebagai contoh, jika **penyimpanan Wasabi** sudah ada, nama akan secara otomatis diperbarui menjadi **penyimpanan Wasabi 1**.
   - Di bidang **Keranjang**, pilih keranjang Wasabi yang relevan.

© Acronis International GmbH, 2003-2024

6. Klik **Tambah**.

   Jika Anda membuat atau mengedit rencana proteksi, lokasi cadangan Wasabi ditetapkan sebagai lokasi di baris **Di mana harus mencadangkan**. Ketika cadangan dijalankan (baik secara manual atau ketika dijadwalkan), cadangan disimpan di lokasi yang ditentukan.

   Jika Anda mengelola lokasi penyimpanan cadangan Anda, Anda dapat melihat dan memperbarui detail lokasi sesuai kebutuhan. Lokasi Wasabi juga tersedia saat mendefinisikan lokasi cadangan untuk beban kerja. Untuk informasi lebih lanjut, lihat "Melihat dan memperbarui lokasi cadangan cloud publik" (hlm. 545).

Melihat dan memperbarui lokasi cadangan cloud publik

Anda dapat melihat dan memperbarui lokasi cadangan Microsoft Azure, Amazon S3, dan Wasabi yang Anda tentukan dalam modul **Penyimpanan cadangan**, atau saat membuat atau mengedit rencana proteksi.

Untuk informasi tentang menghapus akses ke langganan Microsoft Azure dari konsol Cyber Protect, lihat "Menghapus akses ke langganan Microsoft Azure" (hlm. 552). Untuk informasi tentang menghapus akses ke koneksi cloud publik lainnya, lihat "Mengelola akses ke layanan penyimpanan cloud publik lainnya" (hlm. 553).

Catatan
Anda tidak dapat secara manual melakukan refresh pada atau menghapus lokasi cadangan cloud publik di modul **Penyimpanan cadangan**. Isi dari lokasi cadangan diperbarui secara otomatis setiap kali operasi cadangan atau pemulihan selesai dilakukan.

Untuk melihat lokasi cadangan cloud publik

1. Di konsol Cyber Protect, buka **Penyimpanan cadangan**.

   Daftar lokasi cadangan ditampilkan, dengan detail kapasitas penyimpanan dan jumlah cadangan yang ditentukan untuk setiap lokasi.

   Untuk informasi selengkapnya tentang bekerja dengan lokasi pencadangan yang terdaftar, lihat "Tab Penyimpanan cadangan" (hlm. 526).
2. Pilih lokasi yang relevan.

   Semua cadangan terkini untuk lokasi yang dipilih akan dicantumkan.
3. (Opsional) Klik cadangan untuk melihat perincian lebih lanjut tentang cadangan.

Untuk memperbarui lokasi cadangan cloud publik dalam rencana proteksi

1. Buka rencana proteksi yang relevan, dan pilih **Edit**.
2. Klik tautan di baris **Tempat menyimpan cadangan**.
3. Pilih dari daftar lokasi cadangan yang ada, atau klik **Tambahkan lokasi** untuk menambahkan lokasi baru.

   Jika langganan Microsoft Azure yang relevan atau koneksi cloud publik sudah terdaftar di konsol Cyber Protect, pilih dari daftar yang ditampilkan.

© Acronis International GmbH, 2003-2024

Jika Anda menambahkan langganan Microsoft Azure baru, Anda akan diminta untuk mengautentikasi detail akun Microsoft Anda (lihat "Menambahkan akses ke langganan Microsoft Azure" (hlm. 550). Untuk informasi lebih lanjut tentang izin yang diperlukan saat terhubung ke Microsoft Azure, lihat artikel Keamanan dan audit koneksi Microsoft Azure (72684).

Mengelola akses akun cloud publik

Untuk mengaktifkan layanan Acronis Cyber Protection di platform cloud publik, akses ke akun cloud publik yang relevan perlu dikonfigurasi.

Sebagai contoh, saat bekerja dengan Microsoft Azure, akses ke langganan Microsoft Azure Anda diperlukan. Setelah ditambahkan di konsol Cyber Protect, langganan dapat dipilih saat Anda mengkonfigurasi cadangan langsung ke Microsoft Azure. Demikian pula, saat bekerja dengan Amazon S3 dan Wasabi, kunci akses yang relevan yang dikaitkan dengan kebijakan tertentu yang terkait dengan cadangan diperlukan.

Akses ke cloud publik dikelola melalui menu **Infrastruktur** di konsol Cyber Protect.

Penting
Validasi cadangan dinonaktifkan untuk cadangan pada penyimpanan cloud publik, untuk menghindari biaya lalu lintas keluar yang berlebihan. Selain itu, Anda saat ini tidak dapat "menyambungkan kembali" lokasi cadangan pada cloud publik ke penyewa pelanggan yang sama atau berbeda jika lokasi sebelumnya telah dihapus. Untuk informasi lebih lanjut, hubungi tim Dukungan.

Persyaratan akses yang diperlukan untuk cadangan ke penyimpanan cloud publik

Ketika melakukan pencadangan langsung ke layanan penyimpanan cloud publik, ada sejumlah persyaratan akses yang perlu dipertimbangkan untuk setiap platform:

- MicrosoftAzure
- Amazon S3
- Wasabi

Mencadangkan ke Microsoft Azure

Agar dapat terhubung ke langganan Microsoft Azure, Anda harus memiliki beberapa izin. Terkait informasi lebih lanjut mengenai hal tersebut, lihat artikel Keamanan dan audit koneksi Microsoft Azure (72684).

Mencadangkan ke Amazon S3

Ketika Anda membuat cadangan ke Amazon S3, ada beberapa persyaratan saat menentukan lokasi cadangan Amazon S3:

© Acronis International GmbH, 2003-2024

- Kelas penyimpanan yang didukung
- Izin kebijakan
- Kunci akses
- Pengaturan keranjang

Kelas penyimpanan yang didukung

Kelas penyimpanan Amazon S3 berikut, saat ini mendapatkan dukungan:

- S3 Standard
- Standar - Akses Jarang (S3 Standard-IA)
- Satu Zona - Akses Jarang (S3 One Zone-IA)
- S3 Intelligent Tiering

Izin kebijakan

Ketika Anda membuat cadangan ke Amazon S3, akun Amazon Anda harus memiliki izin minimum yang diterapkan untuk memastikan Acronis dapat mencadangkan beban kerja yang relevan ke Amazon S3. Ini berarti bahwa pengguna yang relevan harus memiliki akses ke Konsol Manajemen AWS, dan memiliki kebijakan relevan yang diterapkan pada grup tempat mereka ditugaskan.

Contoh

Contoh kebijakan berikut menunjukkan serangkaian izin minimal untuk cakupan sumber daya yang luas. Perhatikan bahwa * menunjukkan semua sumber daya.

```
{ "Versi": "2012-10-17", "Pernyataan": [ { "Efek": "Izinkan", "Tindakan":
"s3:DaftarSemuaKeranjangSaya", "Sumber": "*" }, { "Efek": "Izinkan", "Tindakan": [
"s3:DapatkanLokasiKeranjang", "s3:DapatkanKonfigurasiKunciObjekKeranjang" ],
"Sumber": "*" }, { "Efek": "Izinkan", "Tindakan": "sts:DapatkanTokenFederasi",
"Sumber": "*" }, { "Efek": "Izinkan", "Tindakan": [ "s3:DapatkanLokasiKeranjang",
"s3:MasukkanObjek", "s3:DapatkanObjek", "s3:HapusObjek" ], "Sumber": "*" }, {
"Efek": "Izinkan", "Tindakan": [ "s3:DaftarKeranjang" ], "Sumber": "*" } ] }
```

Contoh kebijakan berikut menunjukkan izin minimum yang dibatasi pada keranjang tertentu. Perhatikan bahwa `[NAMAKERANJANG]` harus diganti dengan nama dari keranjang tersebut.

```
{ "Versi": "2012-10-17", "Pernyataan": [ { "Efek": "Izinkan", "Tindakan":
"s3:DaftarSemuaKeranjangSaya", "Sumber": "*" }, { "Efek": "Izinkan", "Tindakan": [
"s3:DapatkanLokasiKeranjang", "s3:DapatkanKonfigurasiKunciObjekKeranjang" ],
"Sumber": "arn:aws:s3:::[NAMAKERANJANG]" }, { "Efek": "Izinkan", "Tindakan":
"sts:DapatkanTokenFederasi", "Sumber": "*" }, { "Efek": "Izinkan", "Tindakan": [
"s3:DapatkanLokasiKeranjang", "s3:MasukkanObjek", "s3:DapatkanObjek",
```


© Acronis International GmbH, 2003-2024

```
"s3:HapusObjek" ], "Sumber": "arn:aws:s3:::[NAMAKERANJANG]/*" }, { "Efek":
"Izinkan", "Tindakan": [ "s3:DaftarKeranjang" ], "Sumber": "arn:aws:s3:::
[NAMAKERANJANG]" } ] }
```

Kunci akses

Kunci akses diperlukan oleh Acronis untuk setiap koneksi Amazon S3, dan digunakan saat mendefinisikan koneksi Amazon S3. Untuk informasi lebih lanjut tentang cara menghasilkan kunci akses dan ID kunci akses, lihat dokumen Amazon S3.

Pengaturan keranjang

Ketika menggunakan keranjang Amazon S3 sebagai lokasi cadangan, pastikan bahwa keranjang dikonfigurasi dengan pengaturan default, termasuk pemblokiran semua akses publik (secara default ini diatur ke **On**). Untuk informasi lebih lanjut tentang bekerja dengan keranjang, lihat dokumen Amazon S3.

Catatan
Acronis saat ini tidak mendukung versi keranjang dan penguncian objek di Amazon S3, bahkan ketika diaktifkan pada keranjang.

Mencadangkan ke Wasabi

Ketika Anda membuat cadangan ke Wasabi, ada sejumlah persyaratan yang perlu Anda pertimbangkan saat menentukan lokasi cadangan:

- Izin kebijakan
- Kunci akses
- Pengaturan keranjang

Izin kebijakan

Ketika Anda menentukan lokasi cadangan di Wasabi, pastikan bahwa kebijakan yang relevan diterapkan pada grup dan pengguna yang relevan di Wasabi.

Contoh

Contoh kebijakan berikut menunjukkan serangkaian izin minimal dengan cakupan sumber daya yang luas. Perhatikan bahwa * menunjukkan sumber daya apa pun.

```
{ "Versi": "2012-10-17", "Pernyataan": [ { "Efek": "Izinkan", "Tindakan":
"s3:DaftarSemuaKeranjangSaya", "Sumber": "*" }, { "Efek": "Izinkan", "Tindakan":
"s3:DapatkanLokasiKeranjang", "Sumber": "*" }, { "Efek": "Izinkan", "Tindakan": [
```


© Acronis International GmbH, 2003-2024

```
"iam:BuatPeran", "iam:LampirkanKebijakanPeran", "sts:DapatkanIdentitasPemanggil",
"sts:AnggapPeran" ], "Sumber": "*" }, { "Efek": "Izinkan", "Tindakan": [
"s3:TaruhObjek", "s3:DapatkanObjek", "s3:HapusObjek" ], "Sumber": "*" }, { "Efek":
"Izinkan", "Tindakan": "s3:DaftarKeranjang", "Sumber": "*" } ] }
```

Contoh kebijakan berikut menunjukkan izin terbatas dengan cakupan sumber daya yang terbatas. Perhatikan bahwa `[NAMAKERANJANG]` harus diganti dengan nama keranjang, dan `[IDAKUN]` dengan ID akun Wasabi.

```
{ "Versi": "2012-10-17", "Pernyataan": [ { "Efek": "Izinkan", "Tindakan":
"s3:DaftarSemuaKeranjangSaya", "Sumber": "*" }, { "Efek": "Izinkan", "Tindakan":
"s3:DapatkanLokasiKeranjang", "Sumber": "arn:aws:s3:::[NAMAKERANJANG]" }, { "Efek":
"Izinkan", "Tindakan": [ "iam:BuatPeran", "iam:LampirkanKebijakanPeran",
"sts:DapatkanIdentitasPemanggil", "sts:AnggapPeran" ], "Sumber": "arn:aws:iam::
[IDAKUN]:*" }, { "Efek": "Izinkan", "Tindakan": [ "s3:LetakkanObjek",
"s3:DapatkanObjek", "s3:HapusObjek" ], "Sumber": "arn:aws:s3:::[NAMAKERANJANG]/*" },
{ "Efek": "Izinkan", "Tindakan": "s3:DaftarKeranjang", "Sumber": "arn:aws:s3:::
[NAMAKERANJANG]" } ] }
```

Kunci akses

Kunci akses diperlukan oleh Acronis untuk setiap koneksi Wasabi, dan digunakan saat mendefinisikan koneksi Wasabi. Untuk informasi lebih lanjut tentang cara menghasilkan kunci akses dan ID kunci akses, lihat dokumen Wasabi.

Pengaturan keranjang

Ketika menggunakan keranjang Wasabi sebagai lokasi cadangan, pastikan bahwa keranjang dikonfigurasi dengan pengaturan default. Untuk informasi lebih lanjut tentang bekerja dengan keranjang, lihat dokumen Wasabi.

Catatan
Acronis saat ini tidak mendukung versi keranjang dan penguncian objek di Wasabi, bahkan ketika diaktifkan pada keranjang.

Mengelola akses ke langganan Microsoft Azure

Dengan menyambungkan ke langganan Microsoft Azure yang relevan di konsol Cyber Protect, Anda dapat langsung mencadangkan beban kerja yang relevan ke Microsoft Azure.

Koneksi ke langganan dapat dikonfigurasikan saat membuat lokasi cadangan melalui menu **Perangkat** atau **Penyimpanan cadangan**, seperti dijelaskan dalam "Menentukan lokasi cadangan di Microsoft Azure" (hlm. 538).

© Acronis International GmbH, 2003-2024

Cara lainnya, langganan Microsoft Azure ini dapat dikonfigurasi di layar **Cloud publik** (buka **Infrastruktur > Cloud publik**). Di sini Anda juga dapat mengelola langganan Anda, termasuk memperbarui akses ke langganan, melihat properti dan aktivitas langganan, atau menghapus langganan.

Tergantung pada peran pengguna yang ditugaskan kepada Anda, Anda mungkin dapat mengelola langganan Microsoft Azure yang ditambahkan oleh pengguna lain dalam organisasi Anda. Misalnya, jika Anda adalah Administrator Perusahaan atau Administrator Unit, atau telah menerima tugas untuk berperan sebagai Administrator Cyber atau Administrator dalam layanan Perlindungan Cyber, Anda dapat melihat dan mengelola langganan Microsoft Azure yang ditambahkan oleh administrator lain, dan langganan yang ditambahkan oleh pengguna non-administrator. Pengguna non-administrator hanya dapat melihat dan mengakses langganan Microsoft Azure yang mereka tambahkan ke konsol Cyber Protect.

Catatan
Mitra dapat mengelola langganan Microsoft Azure pelanggan di bawah level mereka dalam hierarki. Namun, bila mitra memilih **Semua pelanggan**, menu **Infrastruktur** di konsol Cyber Protect tidak tersedia.

Penting
Saat menyambungkan ke langganan Microsoft Azure, Acronis memerlukan izin minimum untuk tersambung ke langganan. Untuk informasi selengkapnya tentang izin yang diperlukan, lihat artikel Keamanan dan audit koneksi Microsoft Azure (72684).

Menambahkan akses ke langganan Microsoft Azure

Dengan menambahkan langganan Microsoft Azure di konsol Cyber Protect, Acronis dapat mengakses langganan Anda dengan aman dan langsung mencadangkan beban kerja yang relevan ke Microsoft Azure.

Untuk menambahkan akses ke langganan Microsoft Azure

1. Di konsol Cyber Protect, buka **Infrastruktur > Cloud publik**.
2. Klik **Tambah**, dan dari daftar opsi yang ditampilkan, pilih **Microsoft Azure**.
3. Dalam dialog yang ditampilkan, klik **Masuk**. Anda akan dialihkan ke halaman masuk Microsoft.

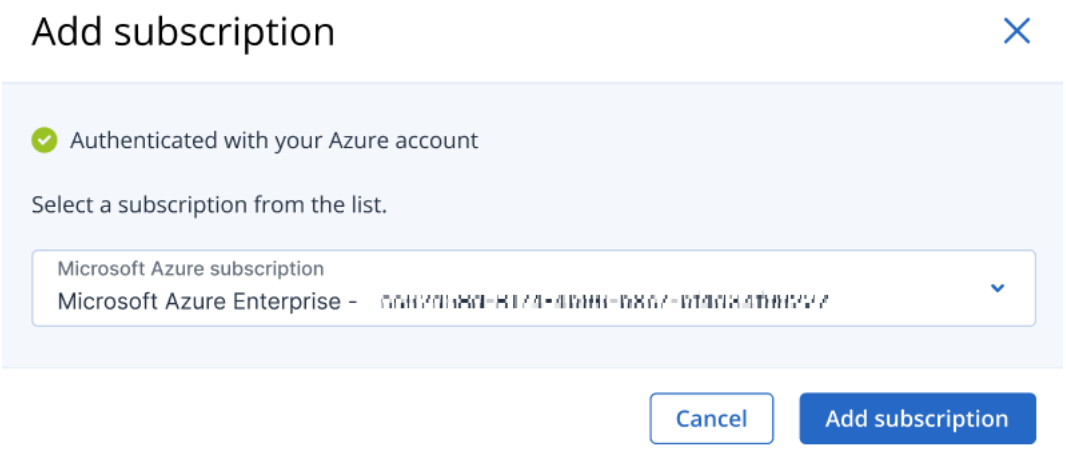
   Catatan
   Anda harus diberi salah satu peran berikut di Microsoft Azure Active Directory untuk menyelesaikan koneksi ke langganan: Administrator Aplikasi Cloud, Administrator Aplikasi, atau Administrator Global. Anda juga harus diberi peran Pemilik untuk setiap langganan yang dipilih.

4. Di layar login Microsoft, masukkan kredensial login Anda dan terima izin yang diminta. Proses koneksi dimulai, dan mungkin memakan waktu beberapa menit.

   Untuk informasi selengkapnya tentang mengakses Microsoft Azure dan langganan Anda dengan aman, lihat artikel Keamanan dan audit koneksi Microsoft Azure (72684).

© Acronis International GmbH, 2003-2024

5. Setelah koneksi selesai, pilih langganan yang relevan dari daftar drop-down pada tampilan dialog, lalu klik **Tambahkan langganan**.



Langganan ditambahkan ke daftar cloud publik.

Untuk memperbarui sertifikat akses tahunan untuk langganan, lihat "Memperbarui akses ke langganan Microsoft Azure" (hlm. 551).

Untuk menghapus akses ke langganan, lihat "Menghapus akses ke langganan Microsoft Azure" (hlm. 552).

Catatan
Jika akun Microsoft Azure yang Anda masuki menyertakan akses ke beberapa Microsoft Azure AD, termasuk AD yang Anda undang sebagai pengguna tamu, hanya direktori pengguna default yang dipilih. Jika Anda ingin menggunakan direktori tempat Anda menjadi pengguna tamu, Anda perlu membuat pengguna baru di Microsoft Azure AD spesifik tersebut. Anda kemudian dapat masuk ke akun tersebut dan terhubung ke langganan yang relevan.

Memperbarui akses ke langganan Microsoft Azure

Setelah terdaftar di konsol Cyber Protect, akses ke langganan Microsoft Azure secara otomatis ditetapkan selama satu tahun dengan Acronis menggunakan sertifikat akses gratis dan unik. Ketika sertifikat mendekati tanggal kedaluwarsa, Anda dapat memperbaruinya dengan cepat dan mudah.

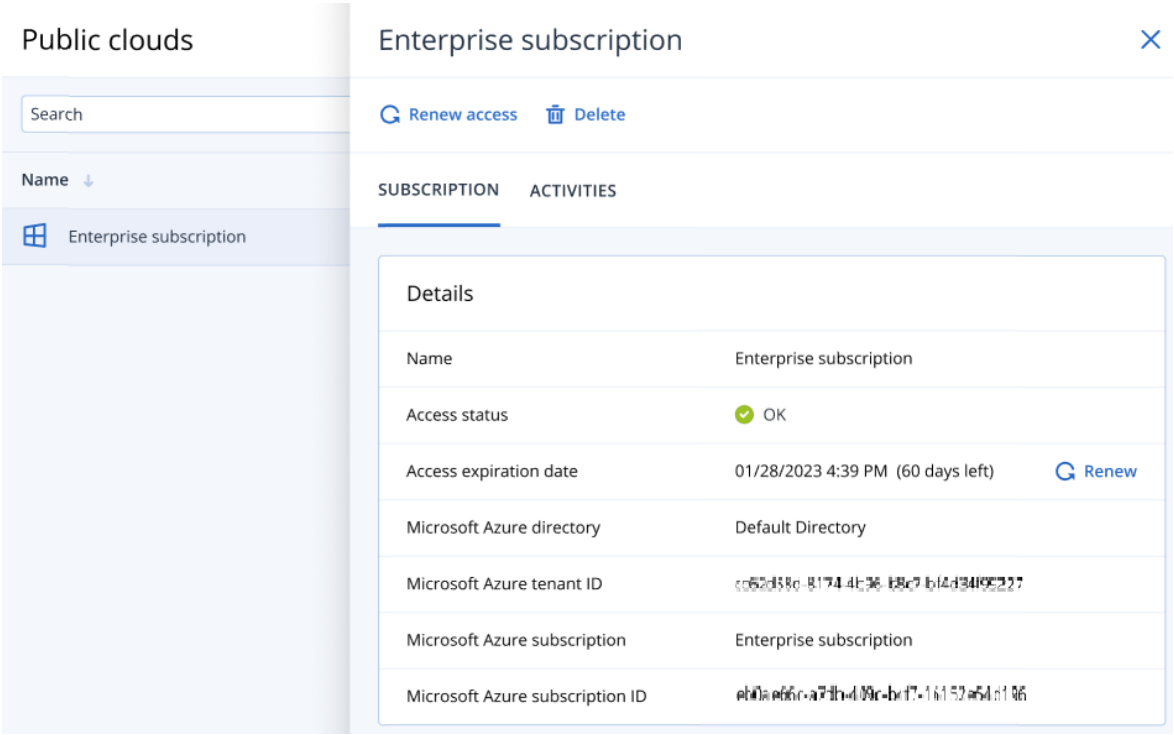
Agar dapat memperbarui sertifikat akses untuk langganan Microsoft Azure Anda

1. Di konsol Cyber Protect, buka **Infrastruktur > Cloud publik**.
2. Pilih langganan yang relevan dari daftar yang ditampilkan.

Catatan
Kolom **Status akses** menunjukkan status terkini sertifikat akses untuk setiap langganan dan menampilkan salah satu dari dua status: **OK** atau **Kedaluwarsa**.

3. Di panel kanan, klik **Perpanjang akses**.
   Cara lainnya, klik tab **Langganan**, lalu klik **Perpanjang** di bidang **Tanggal kedaluwarsa akses**.

© Acronis International GmbH, 2003-2024



4. Di layar login Microsoft, masukkan kredensial login Anda dan terima izin yang diminta. Proses koneksi dimulai, dan mungkin memakan waktu beberapa menit.

   Ketika autentikasi berhasil, akses diperpanjang secara otomatis selama satu tahun.

   Untuk informasi selengkapnya tentang izin yang diperlukan, lihat artikel Keamanan dan audit koneksi Microsoft Azure (72684).

Menghapus akses ke langganan Microsoft Azure

Anda harus menghapus akses ke langganan Microsoft Azure jika Anda tidak mencadangkan beban kerja ke Microsoft Azure.

Untuk menghapus akses ke langganan Microsoft Azure

Penting
Anda tidak dapat menghapus langganan jika sedang digunakan untuk membuat cadangan ke Microsoft Azure.

1. Di konsol Cyber Protect, buka **Infrastruktur > Cloud publik**.
2. Pilih langganan yang relevan dari daftar yang ditampilkan.
3. Di panel kanan, klik **Hapus**.

Catatan
Anda hanya dapat menghapus langganan yang Anda tambahkan. Anda juga dapat menghapus langganan jika Anda adalah administrator Perusahaan atau administrator Unit, atau diberi peran sebagai administrator Cyber atau Administrator dalam layanan Cyber Protection.

© Acronis International GmbH, 2003-2024

4. Pada pesan konfirmasi yang ditampilkan, klik **Hapus**.

Mengelola akses ke layanan penyimpanan cloud publik lainnya

Catatan
Bagian ini merujuk pada pengelolaan akses untuk semua layanan penyimpanan cloud publik selain Microsoft Azure, yang dijelaskan di "Mengelola akses ke langganan Microsoft Azure" (hlm. 549).

Dengan terhubung ke akun cloud publik yang relevan di konsol Cyber Protect, Anda dapat langsung mencadangkan beban kerja ke penyimpanan cloud publik yang relevan.

Anda dapat mengkonfigurasi koneksi ke akun penyimpanan cloud publik saat membuat lokasi cadangan melalui menu **Perangkat** atau **Penyimpanan cadangan**. Sebagai alternatif, Anda dapat mengkonfigurasi koneksi cloud publik di layar **Cloud Publik** (buka **Infrastruktur > Cloud Publik**). Di sini Anda juga dapat mengelola koneksi Anda, termasuk pembaruan akses ke koneksi, melihat properti dan aktivitas sambungan, atau menghapus sambungan.

Tergantung pada peran pengguna yang ditugaskan kepada Anda, Anda mungkin dapat mengelola koneksi cloud publik yang ditambahkan oleh pengguna lain dalam organisasi Anda. Misalnya, jika Anda adalah administrator Perusahaan atau administrator Unit, atau telah menerima tugas untuk berperan sebagai administrator Cyber atau Administrator dalam layanan Perlindungan Cyber, Anda dapat melihat dan mengelola koneksi cloud publik yang ditambahkan oleh administrator lain, serta koneksi yang ditambahkan oleh pengguna non-administrator. Pengguna non-administrator hanya dapat melihat dan mengakses koneksi cloud publik yang mereka tambahkan ke konsol Cyber Protect.

Catatan
Mitra dapat mengelola koneksi cloud publik dari pelanggan di bawah tingkat mereka dalam hierarki. Namun, ketika mitra memilih **Semua pelanggan**, menu **Infrastruktur** dalam konsol Cyber Protect tidak tersedia.

Penting
Ketika terhubung ke koneksi cloud publik, Acronis memerlukan sejumlah izin. Untuk informasi lebih lanjut, lihat "Persyaratan akses yang diperlukan untuk cadangan ke penyimpanan cloud publik" (hlm. 546).

Menambahkan akses ke koneksi cloud publik

Setelah menambahkan koneksi cloud publik (seperti Amazon S3 atau Wasabi) di konsolCyber Protect, Acronis dapat mengakses sumber daya cloud Anda dengan aman dan langsung mencadangkan beban kerja ke penyimpanan cloud publik yang relevan.

Untuk menambahkan akses ke koneksi cloud publik

1. Di konsol Cyber Protect, buka **Infrastruktur > Cloud publik**.
2. Klik **Tambah**, dan pilih salah satu dari opsi berikut:

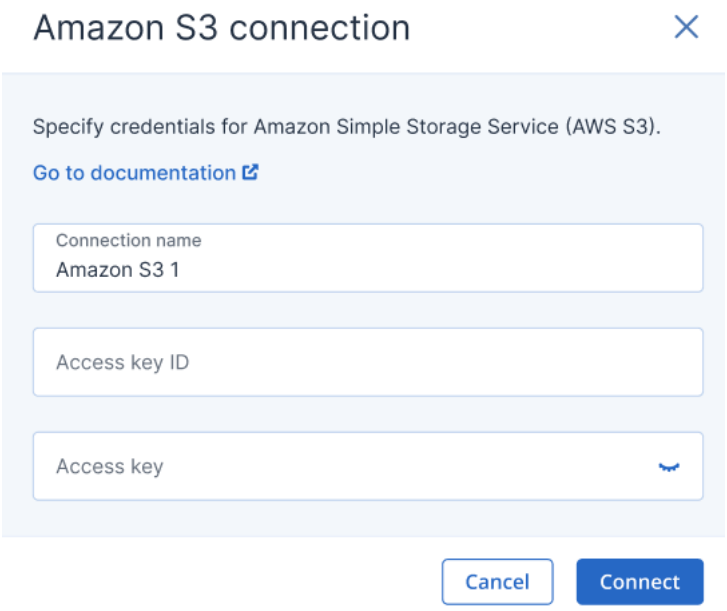
© Acronis International GmbH, 2003-2024

- **Amazon S3**

  Dalam dialog yang ditampilkan, tentukan hal-hal berikut:

  - **Nama koneksi**: Nama untuk koneksi Amazon S3.
  - **ID kunci akses**: ID kunci akses pengguna untuk layanan Amazon S3.
  - **Kunci akses**: Kunci akses pengguna untuk layanan Amazon S3.

    Dengan Kunci Akses dan ID Kunci Akses, Acronis dapat mengakses kelas penyimpanan dan keranjang untuk koneksi yang relevan. Untuk informasi lebih lanjut tentang kunci akses dan izin yang diperlukan oleh Acronis, lihat "Persyaratan akses yang diperlukan untuk cadangan ke penyimpanan cloud publik" (hlm. 546).



- **Wasabi**

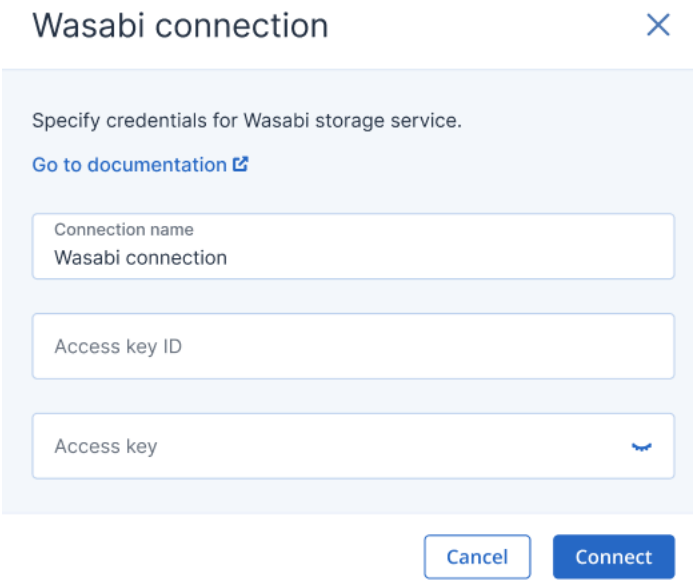
  Dalam dialog yang ditampilkan, tentukan hal-hal berikut:

  - **Nama koneksi**: Nama untuk koneksi Wasabi.
  - **ID kunci akses**: ID kunci akses pengguna untuk layanan Wasabi.
  - **Kunci akses**: Kunci akses pengguna untuk layanan Wasabi.

    Dengan Kunci Akses dan ID Kunci Akses, Acronis dapat mengakses kelas penyimpanan dan keranjang untuk koneksi yang relevan. Untuk informasi lebih lanjut tentang kunci akses dan izin yang diperlukan oleh Acronis, lihat "Persyaratan akses yang diperlukan untuk cadangan

© Acronis International GmbH, 2003-2024

ke penyimpanan cloud publik" (hlm. 546).



3. Klik **Hubungkan**.

   Proses koneksi dimulai, dan mungkin membutuhkan beberapa menit. Ketika selesai, koneksi ditambahkan ke daftar cloud publik.

   Untuk memperbarui sertifikat akses tahunan untuk koneksi, lihat "Memperbarui akses ke koneksi cloud publik" (hlm. 555).

   Untuk menghapus akses ke koneksi, lihat "Menghapus akses ke koneksi cloud publik" (hlm. 556).

Memperbarui akses ke koneksi cloud publik

Setelah koneksi cloud publik terdaftar di konsol Cyber Protect, Acronis secara otomatis menetapkan sertifikat akses gratis dan unik yang mengaktifkan akses ke koneksi cloud publik. Sertifikat ini berlaku selama satu tahun. Ketika sertifikat mendekati tanggal kedaluwarsanya, Anda dapat memperbaruinya.

Untuk memperbarui sertifikat akses pada koneksi cloud publik Anda

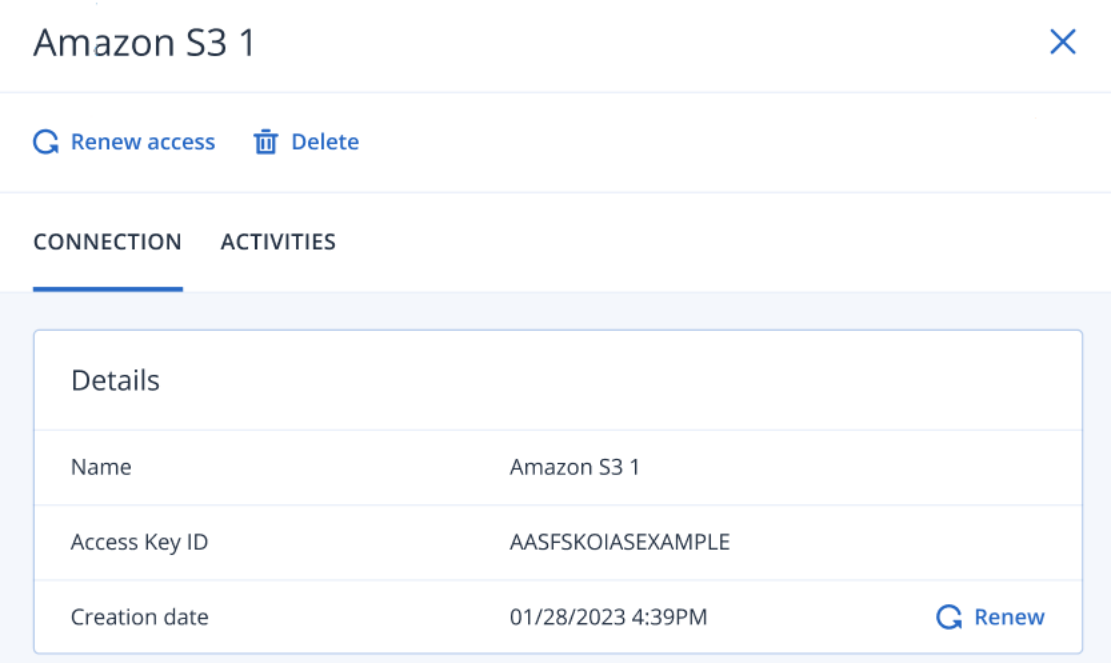
1. Di konsol Cyber Protect, buka **Infrastruktur > Cloud publik**.
2. Pilih koneksi yang relevan dari daftar.

   Catatan
   Kolom **Status akses** menunjukkan status saat ini dari sertifikat akses untuk setiap koneksi dan menunjukkan salah satu dari dua status: **OK** atau **Kedaluwarsa**.

3. Di panel kanan, klik **Perpanjang akses**.

   Sebagai alternatif, klik tab **Koneksi**, kemudian klik **Pembaruan** di baris **Tanggal pembuatan**.

© Acronis International GmbH, 2003-2024



Ketika autentikasi berhasil, akses diperpanjang secara otomatis selama satu tahun.

Menghapus akses ke koneksi cloud publik

Anda harus menghapus akses ke koneksi cloud publik jika Anda tidak mencadangkan beban kerja ke cloud publik.

Untuk menghapus akses ke koneksi cloud publik

Penting
Anda tidak dapat menghapus koneksi jika saat ini digunakan untuk cadangan ke cloud publik.

1. Di konsol Cyber Protect, buka **Infrastruktur > Cloud publik**.
2. Pilih koneksi dari daftar.
3. Di panel kanan, klik **Hapus**.

   Catatan
   Anda hanya dapat menghapus koneksi yang Anda tambahkan. Anda juga dapat menghapus koneksi jika Anda adalah administrator Perusahaan atau administrator Unit, atau jika Anda menerima tugas untuk berperan sebagai administrator Cyber atau Administrator dalam layanan Perlindungan Cyber.

4. Dalam pesan konfirmasi yang ditampilkan, klik **Hapus**.

© Acronis International GmbH, 2003-2024

Melindungi aplikasi Microsoft

Melindungi Microsoft SQL Server dan Microsoft Exchange Server

Catatan
Cadangan Microsoft SQL hanya didukung untuk database yang berjalan pada sistem file NFTS, REFS, dan FAT32. ExFat tidak didukung.

Ada dua metode untuk melindungi aplikasi Microsoft:

- **Cadangan database**
  Ini adalah pencadangan tingkat file dari database dan metadata yang terkait dengannya. Database dapat dipulihkan ke aplikasi langsung atau sebagai file.
- **Cadangan keberadaan aplikasi**
  Ini adalah pencadangan tingkat disk yang juga mengumpulkan metadata aplikasi. Metadata ini memungkinkan penjelajahan dan pemulihan data aplikasi tanpa memulihkan keseluruhan disk atau volume. Disk atau volume juga dapat dipulihkan secara keseluruhan. Ini berarti bahwa solusi tunggal dan rencana proteksi tunggal dapat digunakan untuk tujuan pemulihan bencana dan perlindungan data.

Untuk Microsoft Exchange Server, Anda dapat memilih **Pencadangan kotak surat**. Ini adalah pencadangan kotak surat individual melalui protokol Layanan Exchange Web. Kotak surat atau item kotak surat dapat dipulihkan ke Exchange Server langsung atau ke Microsoft 365. Pencadangan kotak surat didukung untuk Microsoft Exchange Server 2010 Service Pack 1 (SP1) ke atas.

Melindungi Microsoft SharePoint

Farm Microsoft SharePoint terdiri dari server ujung depan yang menjalankan layanan SharePoint, server database yang menjalankan Microsoft SQL Server, dan server aplikasi (opsional) yang memberikan beberapa layanan SharePoint dari server ujung depan. Beberapa server ujung depan dan aplikasi mungkin identik satu sama lain.

Untuk melindungi seluruh farm SharePoint:

- Cadangkan semua server database dengan cadangan keberadaan aplikasi.
- Cadangkan semua server ujung depan dan server aplikasi unik dengan pencadangan tingkat disk biasa.

Pencadangan semua server harus dilakukan pada jadwal yang sama.

Untuk hanya melindungi konten, Anda dapat mencadangkan database konten secara terpisah.

© Acronis International GmbH, 2003-2024

Melindungi pengontrol domain

Mesin yang menjalankan Active Directory Domain Services dapat dilindungi oleh cadangan keberadaan aplikasi. Jika domain berisi lebih dari satu pengontrol, dan Anda memulihkan salah satu di antaranya, pemulihan nonotoritatif akan dilakukan dan USN rollback tidak akan terjadi setelah pemulihan.

Memulihkan aplikasi

Tabel berikut meringkas metode yang tersedia untuk pemulihan aplikasi.

	Dari cadangan database	**Dari cadangan keberadaan aplikasi**	**Dari cadangan disk**
Microsoft SQL Server	Database ke instans SQL Server langsung Database sebagai file	Seluruh mesin Database ke instans SQL Server langsung Database sebagai file	Seluruh mesin
Server Microsoft Exchange	Database ke Exchange langsung Database sebagai file Pemulihan granular ke Exchange langsung atau ke Microsoft 365*	Seluruh mesin Database ke Exchange langsung Database sebagai file Pemulihan granular ke Exchange langsung atau ke Microsoft 365*	Seluruh mesin
Server database Microsoft SharePoint	Database ke instans SQL Server langsung Database sebagai file Pemulihan granular menggunakan SharePoint Explorer	Seluruh mesin Database ke instans SQL Server langsung Database sebagai file Pemulihan granular menggunakan SharePoint Explorer	Seluruh mesin
Server web ujung depan Microsoft SharePoint	-	-	Seluruh mesin
Active Directory Domain Services	-	Seluruh mesin	-

© Acronis International GmbH, 2003-2024

* Pemulihan granular juga tersedia dari pencadangan kotak surat. Pemulihan item data Exchange ke Microsoft 365, dan sebaliknya, didukung dengan ketentuan bahwa Agen untuk Microsoft 365 telah diinstal secara lokal.

Prasyarat

Sebelum mengonfigurasi pencadangan aplikasi, pastikan persyaratan yang tercantum di bawah ini telah terpenuhi.

Untuk memeriksa status VSS writer, gunakan perintah `vssadmin list writers`.

Persyaratan umum

Untuk Microsoft SQL Server, pastikan:

- Setidaknya satu instans Microsoft SQL Server dimulai.
- SQL writer untuk VSS dihidupkan.

Untuk Microsoft Exchange Server, pastikan:

- Layanan Microsoft Exchange Information Store dimulai.
- Windows PowerShell diinstal. Untuk Exchange 2010 ke atas, versi Windows PowerShell setidaknya harus 2.0.
- Microsoft .NET Framework diinstal.
  Untuk Exchange 2007, versi Microsoft .NET Framework setidaknya harus 2.0.
  Untuk Exchange 2010 ke atas, versi Microsoft .NET Framework setidaknya harus 3.5.
- Exchange writer untuk VSS dihidupkan.

Catatan
Agen untuk Exchange memerlukan penyimpanan sementara agar dapat beroperasi. Secara default, file sementara terletak di `%ProgramData%\Acronis\Temp`. Pastikan bahwa Anda memiliki ruang bebas pada volume di mana folder `% PROGRAMDATA%` ditempatkan sebagai minimal 15 persen dari ukuran database Exchange. Atau, Anda dapat mengubah lokasi file sementara sebelum membuat cadangan Exchange seperti yang dijelaskan dalam Mengubah Lokasi File dan Folder Sementara (40040).

Pada pengontrol domain, pastikan:

- Active Directory writer untuk VSS dihidupkan.

Saat membuat rencana proteksi, pastikan bahwa:

- Untuk mesin fisik dan mesin dengan agen yang diinstal di dalam, opsi cadangan Layanan Menyalin Bayangan Volume (VSS) diaktifkan.
- Untuk mesin virtual, opsi pencadangan Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual diaktifkan.

© Acronis International GmbH, 2003-2024

Persyaratan tambahan untuk pencadangan keberadaan aplikasi

Saat membuat rencana proteksi, pastikan **Keseluruhan mesin** dipilih untuk cadangan. Opsi pencadangan **Sektor-per-sektor** harus dinonaktifkan dalam rencana proteksi, atau pemulihan data aplikasi dari cadangan tersebut tidak akan dimungkinkan. Jika rencana dijalankan dalam mode **Sektor demi sektor** karena peralihan otomatis ke mode ini, maka pemulihan data aplikasi juga tidak akan mungkin terjadi.

Persyaratan untuk mesin virtual ESXi

Jika aplikasi dijalankan pada mesin virtual yang dicadangkan oleh Agen untuk VMware, pastikan:

- Mesin virtual yang sedang dicadangkan memenuhi persyaratan untuk cadangan sesuai aplikasi dan pemulihan yang tercantum dalam artikel "Implementasi Pencadangan Windows" dalam dokumentasi VMware: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html.
- VMware Tools telah diinstal dan terbarui pada mesin.
- User Account Control (UAC) dinonaktifkan pada mesin. Jika tidak ingin menonaktifkan UAC, Anda harus menyediakan kredensial dari administrator domain bawaan (DOMAIN\Administrator) ketika mengaktifkan pencadangan aplikasi.
  Jika tidak ingin menonaktifkan UAC, Anda harus menyediakan kredensial dari administrator domain bawaan (DOMAIN\Administrator) ketika mengaktifkan pencadangan aplikasi.

  Catatan
  Gunakan akun administrator domain bawaan yang dikonfigurasi sebagai bagian dari pembuatan domain. Akun yang dibuat setelahnya tidak didukung.

Persyaratan untuk mesin virtual Hyper-V

Jika aplikasi dijalankan pada mesin virtual yang dicadangkan oleh Agen untuk Hyper-V, pastikan:

- Sistem operasi tamu adalah Windows Server 2008 atau versi setelahnya.
- Untuk Hyper-V 2008 R2: sistem operasi tamu adalah Windows Server 2008/2008 R2/2012.
- Mesin virtual tidak memiliki disk dinamis.
- Koneksi jaringan ada antara host Hyper-V dan sistem operasi tamu. Ini diperlukan untuk mengeksekusi kueri WMI jarak jauh di dalam mesin virtual.
- User Account Control (UAC) dinonaktifkan pada mesin. Jika tidak ingin menonaktifkan UAC, Anda harus menyediakan kredensial dari administrator domain bawaan (DOMAIN\Administrator) ketika mengaktifkan pencadangan aplikasi.
  Jika tidak ingin menonaktifkan UAC, Anda harus menyediakan kredensial dari administrator domain bawaan (DOMAIN\Administrator) ketika mengaktifkan pencadangan aplikasi.

© Acronis International GmbH, 2003-2024

Catatan
Gunakan akun administrator domain bawaan yang dikonfigurasi sebagai bagian dari pembuatan domain. Akun yang dibuat setelahnya tidak didukung.

- Konfigurasi mesin virtual cocok dengan kriteria berikut:
  - Layanan Hyper-V Integration telah diinstal dan terbarui. Pembaruan penting terdapat di https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - Di pengaturan mesin virtual, opsi **Manajemen** > **Layanan Integrasi** > **Pencadangan (titik pemeriksaan volume)** diaktifkan.
  - Untuk Hyper-V 2012 dan versi setelahnya: mesin virtual tidak memiliki titik pemeriksaan.
  - Untuk Hyper-V 2012 R2 dan versi setelahnya: mesin virtual memiliki kontroler SCSI (periksa **Pengaturan** > **Perangkat Keras**).

Cadangan database

Sebelum mencadangkan database, pastikan persyaratan yang tercantum di "Prasyarat" terpenuhi.

Pilih database seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Memilih database SQL

Cadangan database SQL berisi file database (.mdf, .ndf), file log (.ldf), dan file terkait lainnya. File tersebut dicadangkan dengan bantuan layanan SQL Writer. Layanan harus berjalan pada saat Layanan Menyalin Bayangan Volume (VSS) meminta cadangan atau pemulihan.

Log transaksi SQL akan terpotong setelah tiap pencadangan yang berhasil. Pemotongan log SQL dapat dinonaktifkan di opsi rencana proteksi.

Untuk memilih database SQL

1. Klik **Perangkat** > **Microsoft SQL**.
   Perangkat lunak ini memperlihatkan pohon dari SQL Server Always On Availability Group (AAG), mesin yang menjalankan Microsoft SQL Server, instans SQL Server, dan database.
2. Jelajahi data yang ingin Anda cadangkan.
   Perluas simpul pohon atau klik dua kali pada item dalam daftar di sebelah kanan pohon.
3. Pilih data yang ingin Anda cadangkan. Anda dapat memilih AAG, mesin yang menjalankan SQL Server, instans SQL Server, atau database individual.
   - Jika Anda memilih AAG, semua database yang dimasukkan ke dalam AAG yang dipilih akan dicadangkan. Untuk informasi selengkapnya tentang mencadangkan AAG atau database AAG individu, lihat "Melindungi Always On Availability Group (AAG)".
   - Jika Anda memilih mesin yang menjalankan SQL Server, semua database yang dilampirkan ke semua instance SQL Server yang berjalan di mesin yang dipilih akan dicadangkan.

© Acronis International GmbH, 2003-2024

- Jika Anda memilih instans SQL Server, semua database yang terpasang ke instans yang dipilih akan dicadangkan.
- Jika Anda memilih database secara langsung, hanya database yang dipilih yang akan dicadangkan.

4. Klik **Lindungi**. Jika diminta, berikan kredensial untuk mengakses data SQL Server.

   Jika Anda menggunakan autentikasi Windows, akun harus merupakan anggota grup **Operator Pencadangan** atau **Administrator** pada mesin dan anggota peran **sysadmin** pada setiap instans yang akan Anda cadangkan.

   Jika Anda menggunakan autentikasi SQL Server, akun harus merupakan anggota peran **sysadmin** pada setiap instans yang akan Anda cadangkan.

Memilih data Exchange Server

Tabel berikut merangkum data Microsoft Exchange Server yang dapat Anda pilih untuk pencadangan dan hak pengguna minimal yang diperlukan untuk mencadangkan data.

Versi Exchange	Item data	Hak pengguna
2007	Grup penyimpanan	Keanggotaan dalam grup peran **Administrator Organisasi Exchange**
2010/2013/2016/2019	Database, Database Availability Groups (DAG)	Keanggotaan dalam grup peran **Manajemen Server**.

Pencadangan penuh berisi semua data Exchange Server yang dipilih.

Pencadangan inkremental berisi blok yang diubah dari file database, file titik pemeriksaan, dan sejumlah kecil file log yang lebih baru dari titik pemeriksaan database yang sesuai. Karena perubahan pada file database termasuk dalam cadangan, tidak perlu mencadangkan semua rekaman log transaksi sejak pencadangan sebelumnya. Hanya log yang lebih baru dari titik pemeriksaan yang perlu diputar ulang setelah pemulihan. Cara ini akan menjadikan pemulihan lebih cepat dan memastikan keberhasilan pencadangan database, meskipun logging sirkuler aktif.

File log transaksi akan terpotong setelah setiap pencadangan berhasil.

Untuk memilih data Exchange Server

1. Klik **Perangkat** > **Microsoft Exchange**.

   Perangkat lunak ini memperlihatkan pohon Exchange Server Database Availability Groups (DAG), mesin yang menjalankan Microsoft Exchange Server, dan database Exchange Server. Jika Anda mengonfigurasi Agen untuk Exchange seperti dijelaskan dalam "Pencadangan kotak surat" (hlm. 569), kotak surat juga akan ditampilkan di pohon ini.
2. Jelajahi data yang ingin Anda cadangkan.

   Perluas simpul pohon atau klik dua kali pada item dalam daftar di sebelah kanan pohon.
3. Pilih data yang ingin Anda cadangkan.
   - Jika Anda memilih DAG, satu salinan dari setiap database yang diklaster akan dicadangkan. Untuk informasi lebih lanjut tentang mencadangkan DAG, lihat "Melindungi Database

 © Acronis International GmbH, 2003-2024

Availability Group (DAG)" (hlm. 565).

- Jika Anda memilih mesin yang menjalankan Microsoft Exchange Server, semua database yang di-mount ke Exchange Server yang berjalan pada mesin yang dipilih akan dicadangkan.
- Jika Anda memilih database secara langsung, hanya database yang dipilih yang akan dicadangkan.
- Jika Anda mengonfigurasi Agen untuk Exchange seperti yang dijelaskan dalam "Pencadangan kotak surat" (hlm. 569), Anda dapat memilih kotak surat untuk pencadangan.

Jika mencakup beberapa basis data, pilihan Anda akan diproses dua sekaligus. Ketika cadangan grup pertama selesai, cadangan grup berikutnya akan dimulai.

4. Jika diminta, berikan kredensial untuk mengakses data.
5. Klik **Lindungi**.

Melindungi Always On Availability Group (AAG)

Catatan
Fitur ini tersedia dengan paket Cadangan Lanjutan.

Ikhtisar solusi ketersediaan tinggi SQL Server

Fungsionalitas Windows Server Failover Clustering (WSFC) memungkinkan Anda untuk mengonfigurasi SQL Server dengan ketersediaan tinggi melalui redundansi pada level instans (Failover Cluster instans, FCI) atau pada level database (AlwaysOn Availability Group, AAG). Anda juga dapat menggabungkan kedua metode tersebut.

Dalam instans Failover Cluster, database SQL berada di penyimpanan bersama. Penyimpanan ini hanya dapat diakses dari simpul klaster aktif. Jika simpul aktif gagal, failover akan terjadi dan simpul yang berbeda akan aktif.

Di grup ketersediaan, setiap replika database akan berada pada simpul yang berbeda. Jika replika primer menjadi tidak tersedia, peran utama akan ditetapkan ke replika sekunder yang berada pada simpul yang berbeda.

Dengan demikian, klaster tersebut sendiri sudah berfungsi sebagai solusi pemulihan bencana. Namun, mungkin akan ada kasus ketika klaster tidak dapat memberikan perlindungan data: misalnya, apabila terjadi kerusakan logis database, atau ketika seluruh klaster down. Selain itu, solusi klaster juga tidak melindungi dari perubahan konten berbahaya, karena perubahan tersebut biasanya langsung mereplikasi ke semua simpul klaster.

Konfigurasi klaster yang didukung

Perangkat lunak pencadangan ini *hanya* mendukung Always On Availability Group (AAG) untuk SQL Server 2012 atau versi setelahnya. Konfigurasi klaster lainnya, seperti Instans Klaster Failover, mirroring database, dan pengiriman log *tidak* didukung.

© Acronis International GmbH, 2003-2024

Berapa banyak agen yang diperlukan untuk pencadangan dan pemulihan data klaster?

Agar pencadangan dan pemulihan data klaster berhasil, Agen untuk SQL harus diinstal pada setiap simpul klaster WSFC.

Mencadangkan database yang termasuk dalam AAG

1. Instal Agen untuk SQL pada setiap simpul klaster WSFC.
2. Pilih AAG yang akan dicadangkan seperti yang dijelaskan dalam "Memilih database SQL".

   Anda harus memilih AAG itu sendiri untuk membuat cadangan semua database AAG. Untuk mencadangkan set database, tentukan set database ini di semua simpul AAG.

   Peringatan!
   Set database harus persis sama di semua simpul. Jika satu set saja berbeda, atau tidak ditentukan pada semua simpul, klaster cadangan tidak akan bekerja dengan benar.

3. Konfigurasikan opsi pencadangan "Mode cadangan klaster".

Pemulihan database yang termasuk dalam AAG

1. Pilih database yang ingin Anda pulihkan, lalu pilih titik pemulihan dari mana Anda ingin memulihkan database.

   Ketika Anda memilih database terklaster pada **Perangkat** > **Microsoft SQL** > **Database**, lalu mengklik **Pulihkan**, perangkat lunak hanya akan menunjukkan titik pemulihan yang sesuai dengan waktu ketika salinan yang dipilih dari database dicadangkan.

   Cara termudah untuk melihat semua titik pemulihan pada database terklaster adalah dengan memilih cadangan keseluruhan AAG di tab Penyimpanan cadangan. Nama-nama cadangan AAG didasarkan pada templat berikut: `<Nama AAG> - <nama rencana proteksi>` dan memiliki ikon khusus.
2. Untuk mengonfigurasi pemulihan, ikuti langkah-langkah yang dijelaskan dalam "Memulihkan database SQL", mulai dari langkah 5.

   Perangkat lunak secara otomatis menentukan simpul klaster yang untuknya data akan dipulihkan. Nama simpul ditampilkan di bidang **Pulihkan ke**. Anda dapat secara manual mengubah simpul target.

   Penting
   Database yang termasuk dalam Always On Availability Group tidak dapat ditimpa selama pemulihan karena Microsoft SQL Server melarangnya. Anda harus mengecualikan database target dari AAG sebelum pemulihan. Atau, cukup pulihkan database sebagai non-AAG baru. Ketika pemulihan selesai, Anda dapat merekonstruksi konfigurasi AAG asli.

© Acronis International GmbH, 2003-2024

Melindungi Database Availability Group (DAG)

Catatan
Fitur ini tersedia dengan paket Cadangan Lanjutan.

Ikhtisar klaster Exchange Server

Ide utama dari kluster Exchange adalah untuk menyediakan ketersediaan database yang tinggi dengan failover cepat dan tanpa hilangnya data. Biasanya, hal ini dicapai dengan memiliki satu atau lebih salinan database atau grup penyimpanan pada anggota klaster (simpul klaster). Jika simpul klaster yang meng-host salinan database aktif atau salinan database aktif itu sendiri gagal, simpul lain yang menampung salinan pasif akan secara otomatis mengambil alih operasi dari simpul yang gagal serta menyediakan akses ke layanan Exchange dengan downtime yang minimal. Dengan demikian, klaster tersebut sendiri sudah berfungsi sebagai solusi pemulihan bencana.

Namun, mungkin ada kasus ketika solusi failover klaster tidak dapat memberikan perlindungan data: misalnya, apabila terjadi kerusakan logis database, atau ketika database tertentu dalam sebuah klaster tidak memiliki salinan (replika), atau ketika seluruh klaster down. Selain itu, solusi klaster juga tidak melindungi dari perubahan konten berbahaya, karena perubahan tersebut biasanya langsung mereplikasi ke semua simpul klaster.

Pencadangan keberadaan klaster

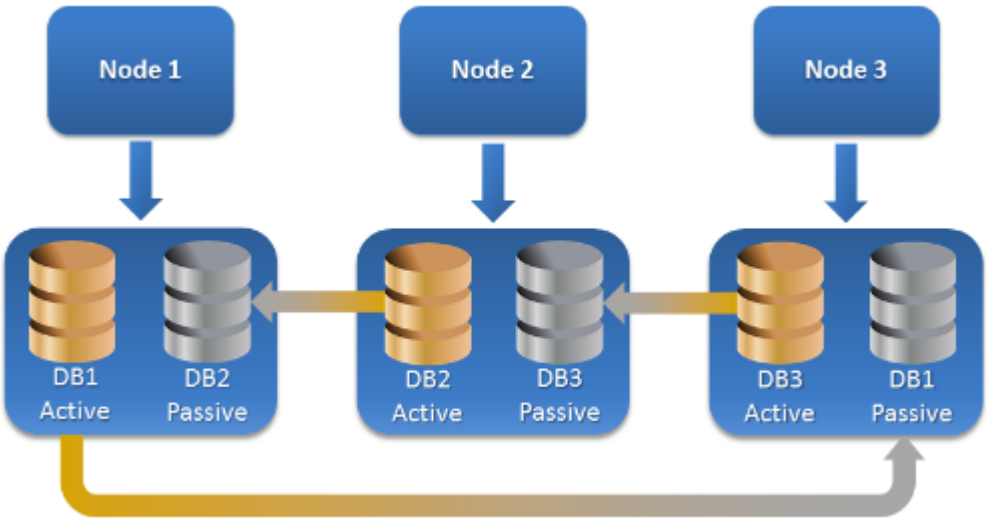
Dengan pencadangan keberadaan-klaster, Anda hanya dapat mencadangkan satu salinan data terklaster. Jika data mengubah lokasinya di dalam kluster (karena peralihan atau failover), perangkat lunak akan melacak semua relokasi data ini dan dengan aman mencadangkannya.

Konfigurasi klaster yang didukung

Pencadangan keberadaan-klaster *hanya* didukung untuk Database Availability Group (DAG) di Exchange Server 2010 ke atas. Konfigurasi klaster lainnya, seperti Single Copy Cluster (SCC) dan Continuous Replication Cluster (CCR) untuk Exchange 2007, *tidak* didukung.

DAG adalah grup yang terdiri dari maksimum 16 server Exchange Mailbox. Setiap simpul dapat meng-host salinan database kotak surat dari simpul lain mana pun. Setiap simpul dapat menyimpan salinan database pasif dan aktif. Hingga 16 salinan dari setiap database dapat dibuat.

© Acronis International GmbH, 2003-2024



Berapa banyak agen yang diperlukan untuk pencadangan dan pemulihan keberadaan-klaster?

Agar pencadangan dan pemulihan database terklaster berhasil, Agen untuk Exchange harus diinstal pada setiap simpul dari klaster Exchange.

Catatan
Setelah Anda menginstal agen di salah satu node, file konsol Cyber Protect menampilkan DAG dan simpulnya di bawah **Perangkat** > **Microsoft Exchange** > **Database**. Untuk menginstal Agen untuk Exchange di seluruh simpul, pilih DAG, klik **Detail**, lalu klik **Instal agen** di sebelah masing-masing simpul.

Mencadangkan data klaster Exchange

1. Saat membuat rencana proteksi, pilih DAG seperti yang dijelaskan dalam "Memilih data Exchange Server" (hlm. 562).
2. Konfigurasikan opsi pencadangan "Mode cadangan klaster" (hlm. 456).
3. Tentukan pengaturan lain dari rencana proteksi yang sesuai.

Penting
Untuk pencadangan keberadaan-klaster, pastikan untuk memilih DAG itu sendiri. Jika Anda memilih masing-masing simpul atau database di dalam DAG, hanya item yang dipilih yang akan dicadangkan, dan opsi **Mode cadangan klaster** akan diabaikan.

Memulihkan data klaster Exchange

1. Pilih titik pemulihan untuk database yang ingin Anda pulihkan. Memilih seluruh klaster untuk pemulihan tidak dimungkinkan.

© Acronis International GmbH, 2003-2024

Ketika Anda memilih salinan database terklaster pada **Perangkat** > **Microsoft Exchange** > **Database** > <nama klaster> > <nama simpul>, lalu mengklik **Pulihkan**, perangkat lunak hanya akan menunjukkan titik pemulihan yang sesuai dengan waktu ketika salinan ini dicadangkan.

Cara termudah untuk melihat semua titik pemulihan pada database terklaster adalah dengan memilih cadangannya di tab Penyimpanan cadangan.

2. Ikuti langkah-langkah yang dijelaskan dalam "Memulihkan database Exchange" (hlm. 579), mulai dari langkah 5.

   Perangkat lunak secara otomatis menentukan simpul klaster yang untuknya data akan dipulihkan. Nama simpul ditampilkan di bidang **Pulihkan ke**. Anda dapat secara manual mengubah simpul target.

Cadangan keberadaan aplikasi

Pencadangan level disk yang tanggap aplikasi tersedia untuk mesin fisik, mesin virtual ESXi, dan mesin virtual Hyper-V.

Ketika Anda mencadangkan mesin yang menjalankan Microsoft SQL Server, Microsoft Exchange Server, atau Active Directory Domain Services, aktifkan **Cadangan aplikasi** untuk perlindungan tambahan data aplikasi tersebut.

Mengapa menggunakan pencadangan keberadaan aplikasi?

Dengan menggunakan pencadangan keberadaan aplikasi, artinya Anda memastikan bahwa:

- Aplikasi dicadangkan dalam status konsisten, sehingga aplikasi dapat segera tersedia setelah mesin dipulihkan.
- Anda dapat memulihkan database SQL dan Exchange, kotak surat, dan item kotak surat tanpa memulihkan keseluruhan mesin.
- Log transaksi SQL akan terpotong setelah tiap pencadangan yang berhasil. Pemotongan log SQL dapat dinonaktifkan di opsi rencana proteksi. Log transaksi Exchange dipotong hanya pada mesin virtual. Anda dapat mengaktifkan opsi pencadangan penuh VSS jika Anda ingin memotong log transaksi Exchange pada mesin fisik.
- Jika domain berisi lebih dari satu pengontrol, dan Anda memulihkan salah satu di antaranya, pemulihan nonotoritatif akan dilakukan dan USN rollback tidak akan terjadi setelah pemulihan.

Apa yang saya perlukan untuk menggunakan pencadangan keberadaan aplikasi?

Pada mesin fisik, Agen untuk SQL dan/atau Agen untuk Exchange harus diinstal, selain Agen untuk Windows.

© Acronis International GmbH, 2003-2024

Pada mesin virtual, instalasi agen tidak diperlukan; karena mesin dianggap dicadangkan oleh Agen untuk VMware (Windows) atau Agen untuk Hyper-V.

Catatan
Untuk mesin virtual Hyper-V dan VMware ESXi yang menjalankan Windows Server 2022, pencadangan yang sadar aplikasi tidak didukung dalam mode tanpa agen - yaitu, ketika pencadangan dilakukan oleh Agen untuk Hyper-V atau Agen untuk VMware. Untuk melindungi berbagai aplikasi Microsoft dalam mesin-mesin ini, instal Agen untuk Windows di dalam sistem operasi tamu.

Agen untuk VMware (Alat Virtual) dapat membuat cadangan keberadaan aplikasi, namun tidak dapat memulihkan data aplikasi dari cadangan. Untuk memulihkan data aplikasi dari cadangan yang dibuat oleh agen ini, Anda membutuhkan Agen untuk VMware (Windows), Agen untuk SQL, atau Agen untuk Exchange pada mesin yang memiliki akses ke lokasi penyimpanan cadangan. Saat mengonfigurasi pemulihan data aplikasi, pilih titik pemulihan pada tab **Penyimpanan cadangan**, lalu pilih mesin ini di **Mesin untuk menelusuri**.

Persyaratan lain terdapat pada bagian "Prasyarat" dan "Hak pengguna yang diperlukan".

Catatan
Pencadangan yang sadar aplikasi dari mesin virtual Hyper-V mungkin gagal dengan kesalahan "WMI 'ExecQuery' gagal mengeksekusi kueri." atau "Gagal membuat proses baru melalui WMI" jika pencadangan dilakukan pada host dengan beban tinggi, karena tidak ada atau penundaan respons dari Instrumentasi Manajemen Windows. Coba lagi pencadangan ini dalam slot waktu ketika beban pada host lebih rendah.

Hak pengguna yang diperlukan untuk pencadangan keberadaan aplikasi

Pencadangan keberadaan aplikasi berisi metadata aplikasi keberadaan VSS yang ada pada disk. Untuk mengakses metadata ini, agen memerlukan akun dengan hak yang sesuai, yang tercantum di bawah ini. Anda diminta untuk menentukan akun ini ketika mengaktifkan cadangan aplikasi.

- Untuk SQL Server:
  Akun harus menjadi anggota dari grup **Operator pencadangan** atau **Administrator** pada mesin dan anggota dari peran **sysadmin** pada setiap instans yang akan Anda cadangkan.

  Catatan
  Hanya autentikasi Windows yang didukung.

- Untuk Server Exchange:
  Exchange 2007: Akun harus merupakan anggota grup **Administrator** pada mesin, dan anggota grup peran **Pertukaran Administrator Organisasi**.
  Exchange 2010 ke atas: Akun harus merupakan anggota grup **Administrator** pada mesin, dan anggota grup peran **Manajemen Organisasi**.

© Acronis International GmbH, 2003-2024

- Untuk Active Directory:
  Akun harus menjadi administrator domain.

Menambahkan persyaratan untuk mesin virtual

Jika aplikasi dijalankan pada mesin virtual yang dicadangkan oleh Agen untuk VMware atau Agen untuk Hyper-V, pastikan User Account Control (UAC) dinonaktifkan pada mesin.

Jika tidak ingin menonaktifkan UAC, Anda harus menyediakan kredensial dari administrator domain bawaan (DOMAIN\Administrator) ketika mengaktifkan pencadangan aplikasi.

Catatan
Gunakan akun administrator domain bawaan yang dikonfigurasi sebagai bagian dari pembuatan domain. Akun yang dibuat setelahnya tidak didukung.

Persyaratan tambahan untuk mesin yang menjalankan Windows

Untuk semua versi Windows, Anda harus menonaktifkan kebijakan Kontrol Akun Pengguna (UAC) untuk mengizinkan pencadangan terinformasi untuk aplikasi.

Jika tidak ingin menonaktifkan UAC, Anda harus menyediakan kredensial dari administrator domain bawaan (DOMAIN\Administrator) ketika mengaktifkan pencadangan aplikasi.

Catatan
Gunakan akun administrator domain bawaan yang dikonfigurasi sebagai bagian dari pembuatan domain. Akun yang dibuat setelahnya tidak didukung.

Untuk menonaktifkan kebijakan UAC di Windows

1. Di Editor Registri, temukan kunci registri berikut:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. Ubah nilai **EnableLUA** ke **0**.
3. Mulai ulang mesin.

Pencadangan kotak surat

Pencadangan kotak surat didukung untuk Microsoft Exchange Server 2010 Service Pack 1 (SP1) ke atas.

Pencadangan kotak surat tersedia jika setidaknya satu Agen untuk Exchange yang terdaftar di server manajemen. Agen harus diinstal pada mesin yang dimiliki oleh forest Active Directory yang sama dengan Microsoft Exchange Server.

Sebelum mencadangkan kotak surat, Anda harus menghubungkan Agen untuk Exchange ke mesin yang menjalankan peran server **Akses Klien** (CAS) pada Microsoft Exchange Server. Di Exchange 2016 dan yang lebih baru, peran CAS tidak tersedia sebagai opsi instalasi terpisah. Ini diinstal secara otomatis sebagai bagian dari peran server Kotak surat. Jadi, Anda dapat menghubungkan agen ke setiap server yang menjalankan **Peran kotak surat**.

© Acronis International GmbH, 2003-2024

Catatan
Anda dapat memulihkan kotak surat dan juga item kotak surat dari cadangan database dan cadangan application-aware. Untuk informasi lebih lanjut, lihat "Memulihkan kotak surat Exchange dan item kotak surat" (hlm. 581). Dengan pencadangan database dan application-aware, Anda tidak bisa membuat rencana proteksi untuk kotak surat individu.

Untuk menghubungkan Agen untuk Exchange ke CAS

1. Klik **Perangkat** > **Tambah**.
2. Klik **Microsoft Exchange Server**.
3. Klik **Kotak surat Exchange**.
   Jika tidak ada Agen untuk Exchange yang terdaftar di server manajemen, perangkat lunak akan menyarankan Anda untuk menginstal agen. Setelah instalasi, ulangi prosedur ini dari langkah 1.
4. [Opsional] Jika beberapa Agen untuk Exchange terdaftar di server manajemen, klik **Agen**, lalu ubah agen yang akan melakukan pencadangan.
5. Pada **Server Akses Klien**, tentukan nama domain yang memenuhi syarat (FQDN) dari mesin tempat peran **Akses Klien** Microsoft Exchange Server diaktifkan.
   Di Exchange 2016 dan yang lebih baru, layanan Akses Klien diinstal secara otomatis sebagai bagian dari peran server Kotak surat. Jadi, Anda dapat menentukan setiap server yang menjalankan **Peran kotak surat**. Kami merujuk ke server ini sebagai CAS nantinya dalam bagian ini.
6. Pada **Jenis otentikasi**, pilih jenis autentikasi yang digunakan oleh CAS. Anda dapat memilih **Kerberos** (default) atau **Dasar**.
7. [Hanya untuk autentikasi basic] Pilih protokol mana yang akan digunakan. Anda dapat memilih **HTTPS** (default) atau **HTTP**.
8. [Hanya untuk autentikasi basic dengan protokol HTTPS] Jika CAS menggunakan sertifikat SSL yang diperoleh dari otoritas sertifikasi, dan Anda ingin perangkat lunak memeriksa sertifikat ketika terhubung ke CAS, pilih kotak centang **Periksa sertifikat SSL**. Jika tidak, lewati langkah ini.
9. Berikan kredensial akun yang akan digunakan untuk mengakses CAS. Persyaratan untuk akun ini terdaftar pada "Hak pengguna yang diperlukan".
10. Klik **Tambah**.

Hasilnya, kotak surat akan muncul pada **Perangkat** > **Microsoft Exchange** > **Kotak Surat**.

Memilih kotak surat Exchange Server

Pilih kotak surat seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Untuk memilih kotak surat Exchange

1. Klik **Perangkat** > **Microsoft Exchange**.
   Perangkat lunak ini menampilkan pohon database dan kotak surat Exchange.

© Acronis International GmbH, 2003-2024

2. Klik **Kotak Surat**, lalu pilih kotak surat yang ingin Anda buat cadangannya.
3. Klik **Lindungi**.

Hak pengguna yang diperlukan

Untuk mengakses kotak surat, Agen untuk Exchange memerlukan akun dengan hak yang sesuai. Anda diminta untuk menentukan akun ini ketika mengonfigurasi berbagai operasi dengan kotak surat.

Keanggotaan akun di grup peran **Manajemen Organisasi** memungkinkan akses ke kotak surat apa pun, termasuk kotak surat yang akan dibuat di waktu mendatang.

Hak pengguna minimum yang diperlukan adalah sebagai berikut:

- Akun harus menjadi anggota grup peran **Manajemen Server** dan **Manajemen Penerima**.
- Akun harus memiliki peran manajemen **ApplicationImpersonation** yang diaktifkan untuk semua pengguna atau grup pengguna yang kotak suratnya akan diakses agen.
  Untuk informasi tentang mengonfigurasi peran manajemen **ApplicationImpersonation**, lihat artikel basis pengetahuan Microsoft berikut: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

Memulihkan database SQL

Anda dapat memulihkan database SQL dari cadangan database dan cadangan terinformasi untuk aplikasi. Untuk informasi lebih lanjut tentang kedua jenis cadangan, lihat "Melindungi Microsoft SQL Server dan Microsoft Exchange Server" (hlm. 557).

Anda dapat memulihkan database SQL ke instans orisinal, ke instans berbeda pada mesin orisinal, atau ke instans pada mesin non-orisinal. Saat Anda melakukan pemulihan ke mesin non-orisinal, Agen untuk SQL harus diinstal pada mesin target.

Selain itu, Anda dapat memulihkan database sebagai file.

Jika menggunakan autentikasi Windows untuk instans SQL, Anda perlu memberikan kredensial untuk akun yang merupakan anggota grup **Operator Pencadangan** atau **Administrator** pada mesin serta merupakan anggota peran **sysadmin** pada instans target. Jika menggunakan autentikasi SQL Server, Anda perlu memberikan kredensial untuk akun yang merupakan anggota peran **sysadmin** pada instans target.

Database sistem dipulihkan sebagai database pengguna, dengan beberapa perbedaan. Untuk mempelajari lebih lanjut tentang perbedaannya, lihat "Memulihkan database sistem" (hlm. 578).

Selama pemulihan, Anda dapat memeriksa progres operasi di konsol Cyber Protect, pada tab **Pemantauan** > **Aktivitas**.

© Acronis International GmbH, 2003-2024

Memulihkan database SQL ke mesin orisinal

Anda dapat memulihkan database SQL ke instans orisinal, ke instans berbeda pada mesin orisinal, atau ke instans pada mesin target non-orisinal.

Untuk memulihkan database SQL ke mesin orisinal

Dari cadangan database

1. Di konsol Cyber Protect, buka **Perangkat** > **Microsoft SQL**.
2. Pilih instans SQL Server atau klik nama instans untuk memilih database spesifik yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Untuk memulihkan data ke mesin non-orisinal, lihat "Memulihkan database SQL ke mesin non-orisinal" (hlm. 574).
3. Pilih titik pemulihan.
   Titik pemulihan difilter berdasarkan lokasi.
4. Klik **Pulihkan** > **Database ke instans**.
   Secara default, instans dan database dipulihkan ke yang orisinal. Anda juga dapat memulihkan database orisinal sebagai database baru.
5. [Saat memulihkan ke instans non-orisinal pada mesin yang sama] Klik **Instans SQL Server Target**, pilih instans target, lalu klik **Selesai**.
6. [Saat memulihkan database sebagai database baru] Klik nama database, lalu di **Pulihkan ke**, pilih **Database baru**.
   - Tentukan nama database baru.
   - Tentukan jalur database baru.
   - Tentukan jalur log.
7. [Opsional] [Tidak tersedia saat memulihkan database sebagai database baru] Untuk mengubah status database setelah pemulihan, klik nama database, pilih salah satu status berikut, lalu klik **Selesai**.
   - **Siap digunakan (KEMBALIKAN DENGAN MEMULIHKAN)** (default)
     Setelah pemulihan selesai, database akan siap digunakan. Pengguna akan memiliki akses penuh ke sana. Perangkat lunak akan mengembalikan semua transaksi tidak terikat dari database yang dipulihkan yang disimpan di dalam log transaksi. Anda tidak akan dapat memulihkan log transaksi tambahan dari cadangan Microsoft SQL asli.
   - **Non-operasional (KEMBALIKAN TANPA MEMULIHKAN)**
     Setelah pemulihan selesai, database akan menjadi non-operasional. Pengguna tidak akan memiliki akses ke sana. Perangkat lunak akan menyimpan semua transaksi yang tidak terikat dari database yang dipulihkan. Anda akan dapat memulihkan log transaksi tambahan dari cadangan Microsoft SQL asli sehingga titik pemulihan yang diperlukan akan tercapai.
   - **Hanya dibaca saja (KEMBALIKAN DENGAN STANDBY)**
     Setelah pemulihan selesai, pengguna akan memiliki akses hanya baca ke database. Perangkat lunak ini akan membatalkan transaksi yang tidak terikat. Namun, perangkat lunak akan

© Acronis International GmbH, 2003-2024

menyimpan tindakan pembatalan dalam file siaga sementara sehingga efek pemulihan dapat dikembalikan.

Nilai ini terutama digunakan untuk mendeteksi titik waktu ketika eror SQL Server terjadi.

8. Klik **Mulai pemulihan**.

Dari cadangan keberadaan aplikasi

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih mesin yang awalnya berisi data yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Untuk memulihkan data ke mesin non-orisinal, lihat "Memulihkan database SQL ke mesin non-orisinal" (hlm. 574).
3. Pilih titik pemulihan.
   Titik pemulihan difilter berdasarkan lokasi.
4. Klik **Pulihkan** > **Database SQL**.
5. Pilih instans SQL Server atau klik nama instans untuk memilih database spesifik yang ingin Anda pulihkan, lalu klik **Pulihkan**.
   Secara default, instans dan database dipulihkan ke yang orisinal. Anda juga dapat memulihkan database orisinal sebagai database baru.
6. [Saat memulihkan ke instans non-orisinal pada mesin yang sama] Klik **Instans SQL Server Target**, pilih instans target, lalu klik **Selesai**.
7. [Saat memulihkan database sebagai database baru] Klik nama database, lalu di **Pulihkan ke**, pilih **Database baru**.
   - Tentukan nama database baru.
   - Tentukan jalur database baru.
   - Tentukan jalur log.
8. [Opsional] [Tidak tersedia saat memulihkan database sebagai database baru] Untuk mengubah status database setelah pemulihan, klik nama database, pilih salah satu status berikut, lalu klik **Selesai**.
   - **Siap digunakan (KEMBALIKAN DENGAN MEMULIHKAN)** (default)
     Setelah pemulihan selesai, database akan siap digunakan. Pengguna akan memiliki akses penuh ke sana. Perangkat lunak akan mengembalikan semua transaksi tidak terikat dari database yang dipulihkan yang disimpan di dalam log transaksi. Anda tidak akan dapat memulihkan log transaksi tambahan dari cadangan Microsoft SQL asli.
   - **Non-operasional (KEMBALIKAN TANPA MEMULIHKAN)**
     Setelah pemulihan selesai, database akan menjadi non-operasional. Pengguna tidak akan memiliki akses ke sana. Perangkat lunak akan menyimpan semua transaksi yang tidak terikat dari database yang dipulihkan. Anda akan dapat memulihkan log transaksi tambahan dari cadangan Microsoft SQL asli sehingga titik pemulihan yang diperlukan akan tercapai.
   - **Hanya dibaca saja (KEMBALIKAN DENGAN STANDBY)**
     Setelah pemulihan selesai, pengguna akan memiliki akses hanya baca ke database. Perangkat lunak ini akan membatalkan transaksi yang tidak terikat. Namun, perangkat lunak akan

© Acronis International GmbH, 2003-2024

menyimpan tindakan pembatalan dalam file siaga sementara sehingga efek pemulihan dapat dikembalikan.

Nilai ini terutama digunakan untuk mendeteksi titik waktu ketika eror SQL Server terjadi.

9. Klik **Mulai pemulihan**.

Memulihkan database SQL ke mesin non-orisinal

Anda dapat memulihkan cadangan terinformasi untuk aplikasi dan cadangan database ke instans SQL Server pada mesin target non-orisinal tempat Agen untuk SQL diinstal. Cadangan harus berada di penyimpanan awan atau di penyimpanan bersama yang dapat diakses mesin target.

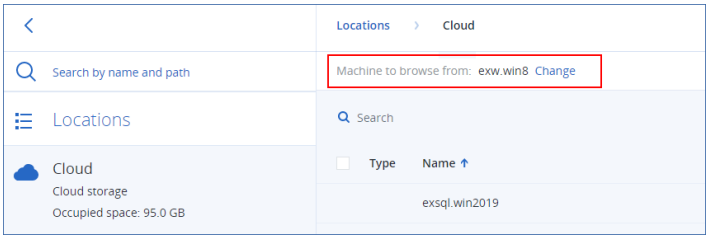
Versi SQL Server pada mesin target harus sama dengan versi pada mesin sumber, atau lebih baru.

Untuk memulihkan database SQL ke mesin non-orisinal

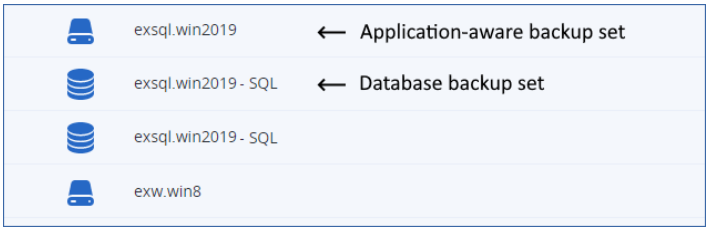
Dari Penyimpanan cadangan

Prosedur ini berlaku bagi cadangan terinformasi untuk aplikasi dan cadangan database.

1. Di konsol Cyber Protect, buka **Penyimpanan cadangan**.
2. Pilih lokasi set cadangan yang datanya ingin Anda pulihkan.
3. Di **Mesin untuk menelusuri**, pilih mesin target.
   Inilah mesin tempat Anda memulihkan data. Mesin target harus online.



4. Pilih set cadangan, lalu di panel **Tindakan**, klik **Tampilkan cadangan**.
   Set cadangan terinformasi untuk aplikasi dan set cadangan database memiliki ikon berbeda.



5. Pilih titik pemulihan yang datanya ingin Anda pulihkan.
6. [Untuk cadangan database] Klik **Pulihkan database SQL**.
7. [Untuk cadangan terinformasi untuk aplikasi] Klik **Pulihkan** > **Database SQL**.
8. Pilih instans SQL Server atau klik nama instans untuk memilih database spesifik yang ingin Anda pulihkan, lalu klik **Pulihkan**.
9. [Jika ada lebih dari satu instans SQL pada mesin target] Klik **Instans SQL Server Target**, pilih instans target, lalu klik **Selesai**.

© Acronis International GmbH, 2003-2024

10. Klik nama database, tentukan jalur database dan jalur log baru, lalu klik **Selesai**.
    Anda dapat menentukan jalur yang sama pada kedua bidang, misal:

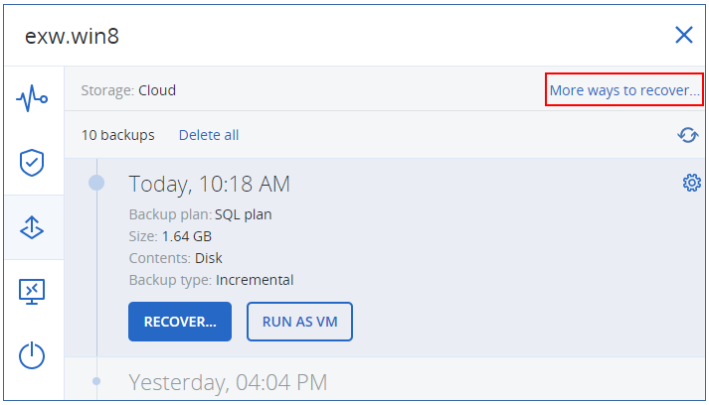
    ```
    C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
    ```

11. Klik **Mulai pemulihan**.

Dari Perangkat

Prosedur ini hanya berlaku bagi cadangan terinformasi untuk aplikasi.

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih mesin yang awalnya berisi data yang ingin Anda pulihkan, lalu klik **Pemulihan**.
3. [Jika mesin sumber sedang online] Klik **Cara lain untuk memulihkan**.



4. Klik **Pilih mesin** untuk memilih mesin target, lalu klik **OK**.
   Inilah mesin tempat Anda memulihkan data. Mesin target harus online.
5. Pilih titik pemulihan.
   Titik pemulihan difilter berdasarkan lokasi.
6. Klik **Pulihkan** > **Database SQL**.
7. Pilih instans SQL Server atau klik nama instans untuk memilih database spesifik yang ingin Anda pulihkan, lalu klik **Pulihkan**.
8. [Jika ada lebih dari satu instans SQL pada mesin target] Klik **Instans SQL Server Target**, pilih instans target, lalu klik **Selesai**.
9. Klik nama database, tentukan jalur database dan jalur log baru, lalu klik **Selesai**.
   Anda dapat menentukan jalur yang sama pada kedua bidang, misal:

   ```
   C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
   ```

10. Klik **Mulai pemulihan**.

Memulihkan database SQL sebagai file

Anda dapat memulihkan database sebagai file. Opsi ini dapat berguna jika Anda perlu mengekstrak data untuk penambangan data, audit, atau pemrosesan lebih lanjut dari alat bantu pihak ketiga.

© Acronis International GmbH, 2003-2024

Untuk mempelajari cara melampirkan file database SQL ke instans SQL Server, lihat "Menyertakan database SQL Server" (hlm. 578).

Anda dapat memulihkan database sebagai file ke mesin orisinal atau ke mesin target non-orisinal, tempat Agen untuk SQL diinstal. Saat Anda memulihkan data ke mesin non-orisinal, cadangan harus berada di penyimpanan awan atau di penyimpanan bersama yang dapat diakses mesin target.

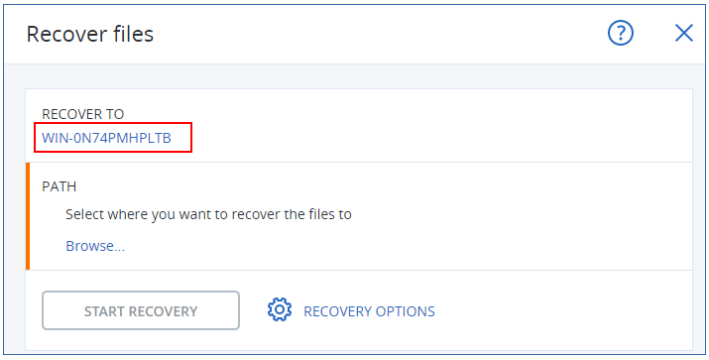
Catatan
Memulihkan database sebagai file adalah satu-satunya metode pemulihan jika Anda menggunakan Agen untuk VMware (Windows). Memulihkan database menggunakan Agen untuk VMware (Alat Virtual) adalah tidak mungkin.

Untuk memulihkan database SQL sebagai file

Dari cadangan database

Prosedur ini berlaku pada mesin sumber online.

1. Di konsol Cyber Protect, buka **Perangkat** > **Microsoft SQL**.
2. Pilih database yang ingin Anda pulihkan, lalu klik **Pulihkan**.
3. Pilih titik pemulihan.
   Titik pemulihan difilter berdasarkan lokasi.
4. Klik **Pulihkan** > **Database sebagai file**.
5. [Saat memulihkan ke mesin non-orisinal] Di **Pulihkan ke**, pilih mesin target.
   Inilah mesin tempat Anda memulihkan data. Mesin target harus online.
   Untuk mengubah pilihan, klik nama mesin, pilih mesin lain, lalu klik **OK**.



6. Di **Jalur**, klik **Telusuri**, pilih folder lokal atau folder jaringan untuk menyimpan file, lalu klik **Selesai**.
7. Klik **Mulai pemulihan**.

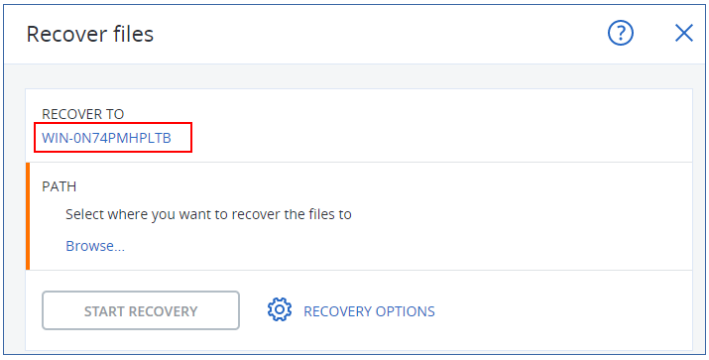
Dari cadangan keberadaan aplikasi

Prosedur ini berlaku pada mesin sumber online.

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih mesin yang awalnya berisi data yang ingin Anda pulihkan, lalu klik **Pemulihan**.

© Acronis International GmbH, 2003-2024

3. Pilih titik pemulihan.
   Titik pemulihan difilter berdasarkan lokasi.
4. Klik **Pulihkan** > **Database SQL**, pilih database yang ingin Anda pulihkan, lalu klik **Pulihkan sebagai file**.
5. [Saat memulihkan ke mesin non-orisinal] Di **Pulihkan ke**, pilih mesin target.
   Inilah mesin tempat Anda memulihkan data. Mesin target harus online.
   Untuk mengubah pilihan, klik nama mesin, pilih mesin lain, lalu klik **OK**.

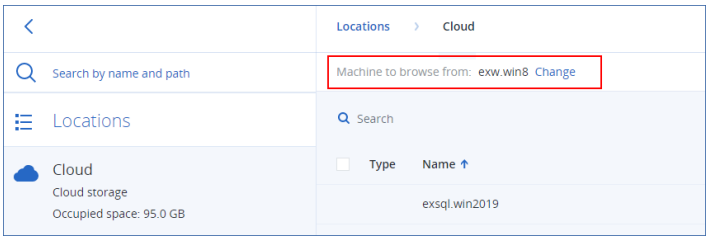


6. Di **Jalur**, klik **Telusuri**, pilih folder lokal atau folder jaringan untuk menyimpan file, lalu klik **Selesai**.
7. Klik **Mulai pemulihan**.

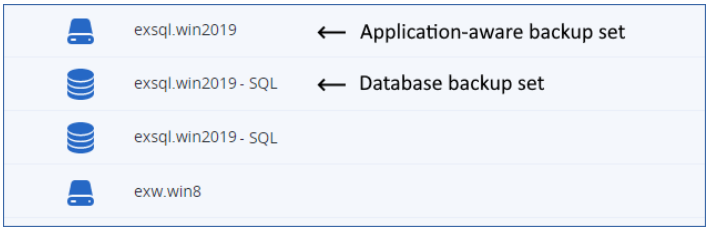
Dari cadangan atau mesin offline

Prosedur ini berlaku bagi cadangan terinformasi untuk aplikasi dan cadangan database pada mesin sumber yang sedang offline.

1. Di konsol Cyber Protect, buka **Penyimpanan cadangan**.
2. Pilih lokasi set cadangan yang datanya ingin Anda pulihkan.
3. Di **Mesin untuk menelusuri**, pilih mesin target.
   Inilah mesin tempat Anda memulihkan data. Mesin target harus online.



4. Pilih set cadangan, lalu di panel **Tindakan**, klik **Tampilkan cadangan**.
   Set cadangan terinformasi untuk aplikasi dan set cadangan database memiliki ikon berbeda.



© Acronis International GmbH, 2003-2024

5. Pilih titik pemulihan yang datanya ingin Anda pulihkan.
6. [Untuk cadangan database] Klik **Pulihkan database SQL**.
7. [Untuk cadangan terinformasi untuk aplikasi] Klik **Pulihkan** > **Database SQL**.
8. Pilih instans SQL Server atau klik nama instans untuk memilih database spesifik yang ingin Anda pulihkan, lalu klik **Pulihkan sebagai file**.
9. Di **Jalur**, klik **Telusuri**, pilih folder lokal atau folder jaringan untuk menyimpan file, lalu klik **Selesai**.
10. Klik **Mulai pemulihan**.

Memulihkan database sistem

Semua database sistem dari instans dipulihkan sekaligus. Ketika memulihkan database sistem, perangkat lunak akan secara otomatis memulai ulang instans tujuan dalam mode pengguna tunggal. Setelah pemulihan selesai, perangkat lunak akan memulai ulang instans dan memulihkan database lainnya (jika ada).

Hal lain yang perlu dipertimbangkan ketika memulihkan database sistem:

- Database sistem hanya dapat dipulihkan ke instans dengan versi yang sama seperti instans asli.
- Database sistem selalu dipulihkan dalam status "siap digunakan".

Memulihkan database master

Database sistem termasuk database **master**. Database **master** merekam informasi tentang semua database instans. Sehingga, database **master** dalam cadangan berisi informasi tentang database yang ada dalam instans pada saat pencadangan. Setelah memulihkan database **master**, Anda mungkin perlu melakukan hal berikut:

- Database yang telah muncul di dalam instans setelah pencadangan selesai tidak akan terlihat oleh instans. Untuk mengembalikan database ini ke produksi, sertakan database ke instans secara manual menggunakan SQL Server Management Studio.
- Database yang telah dihapus setelah pencadangan selesai akan ditampilkan secara offline dalam instans. Hapus database ini menggunakan SQL Server Management Studio.

Menyertakan database SQL Server

Bagian ini menjelaskan cara menyertakan database pada SQL Server menggunakan SQL Server Management Studio. Hanya satu database yang dapat disertakan dalam satu waktu.

Menyertakan database membutuhkan izin berikut: **CREATE DATABASE**, **CREATE ANY DATABASE**, atau **ALTER ANY DATABASE**. Normalnya, izin ini diberikan kepada peran **sysadmin** instans.

Untuk menyertakan database

1. Jalankan Microsoft SQL Server Management Studio.
2. Hubungkan ke instans SQL Server yang diperlukan, lalu perluas instans.

© Acronis International GmbH, 2003-2024

3. Klik kanan **Database** dan klik **Pasang**.
4. Klik **Tambah**.
5. Pada kotak dialog **Temukan File Database**, cari dan pilih file .mdf database.
6. Pada bagian **Detail Database**, pastikan seluruh file database (file .ndf dan .ldf) ditemukan.
   Detail. File database SQL Server mungkin tidak ditemukan secara otomatis jika:
   - Tidak ada di lokasi default, atau tidak ada di folder yang sama dengan file database utama (.mdf). Solusi: Tentukan jalur ke file yang diperlukan secara manual pada kolom **Jalur File Saat Ini**.
   - Anda telah memulihkan set file tidak lengkap yang membangun sebuah database. Solusi: Pulihkan file database SQL Server yang tidak ditemukan dari cadangan.
7. Ketika semua file ditemukan, klik **OK**.

Memulihkan database Exchange

Bagian ini menjelaskan pemulihan dari pencadangan database dan pencadangan keberadaan aplikasi.

Anda dapat memulihkan data Exchange Server ke Exchange Server langsung. Ini mungkin berupa Exchange Server asli atau Exchange Server dengan versi sama yang berjalan pada mesin dengan nama domain yang sepenuhnya memenuhi syarat (FQDN). Agen untuk Exchange harus diinstal pada mesin target.

Tabel berikut merangkum data Exchange Server yang dapat Anda pilih untuk pemulihan dan hak pengguna minimal yang diperlukan untuk memulihkan data.

Versi Exchange	Item data	Hak pengguna
2007	Grup penyimpanan	Keanggotaan dalam grup peran **Administrator Organisasi Exchange**.
2010/2013/2016/2019	Basis data	Keanggotaan dalam grup peran **Manajemen Server**.

Selain itu, Anda dapat memulihkan database (grup penyimpanan) sebagai file. File database, bersama dengan file log transaksi, akan diekstraksi dari cadangan ke folder yang Anda tentukan. Cara ini dapat berguna jika Anda perlu mengekstrak data untuk audit atau pemrosesan lebih lanjut dari alat pihak ketiga, atau ketika pemulihan gagal karena beberapa sebab dan Anda mencari solusi untuk mounting database secara manual.

Jika Anda hanya menggunakan Agen untuk VMware (Windows), memulihkan database sebagai file adalah satu-satunya metode pemulihan yang tersedia. Memulihkan database menggunakan Agen untuk VMware (Alat Virtual) adalah tidak mungkin.

Kami akan merujuk ke database dan grup penyimpanan sebagai "database" di seluruh prosedur di bawah ini.

Untuk memulihkan database Exchange ke Exchange Server langsung

© Acronis International GmbH, 2003-2024

1. Lakukan salah satu langkah berikut:
   - Saat memulihkan dari cadangan keberadaan aplikasi, pada **Perangkat**, pilih mesin yang awalnya berisi data yang ingin Anda pulihkan.
   - Saat memulihkan dari cadangan database, klik **Perangkat** > **Microsoft Exchange** > **Database**, lalu pilih database yang ingin Anda pulihkan.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.

   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Lakukan salah satu langkah berikut:
   - [Hanya jika memulihkan dari cadangan tanggap aplikasi] Jika lokasi cadangan adalah penyimpanan awan atau penyimpanan bersama (yang dapat diakses agen lain), klik **Pilih mesin**, pilih mesin online yang memiliki Agen untuk Exchange, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab Penyimpanan cadangan.

   Mesin yang dipilih untuk menjelajahi dalam tindakan di atas menjadi mesin target untuk pemulihan data Exchange.
4. Lakukan salah satu langkah berikut:
   - Saat memulihkan dari cadangan keberadaan aplikasi, klik **Pulihkan** > **Database Exchange**, pilih database yang ingin Anda pulihkan, lalu klik **Pulihkan**.
   - Saat memulihkan dari cadangan database, klik **Pulihkan** > **Database ke server Exchange**.
5. Secara default, database dipulihkan ke yang asli. Jika database asli tidak ada, database akan dibuat kembali.

   Untuk memulihkan database sebagai jenis yang lain:
   a. Klik nama database.
   b. Di **Pulihkan ke**, pilih **Database baru**.
   c. Tentukan nama database baru.
   d. Tentukan jalur database dan jalur log baru. Folder yang Anda tentukan tidak boleh berisi file database dan log asli.
6. Klik **Mulai pemulihan**.

Progres pemulihan akan ditampilkan pada tab Aktivitas.

Untuk memulihkan database Exchange sebagai file

1. Lakukan salah satu langkah berikut:
   - Saat memulihkan dari cadangan keberadaan aplikasi, pada **Perangkat**, pilih mesin yang awalnya berisi data yang ingin Anda pulihkan.
   - Saat memulihkan dari cadangan database, klik **Perangkat** > **Microsoft Exchange** > **Database**, lalu pilih database yang ingin Anda pulihkan.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.

   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Lakukan salah satu langkah berikut:

© Acronis International GmbH, 2003-2024

- [Hanya jika memulihkan dari cadangan tanggap aplikasi] Jika lokasi cadangan adalah penyimpanan awan atau penyimpanan bersama (yang dapat diakses agen lain), klik **Pilih mesin**, pilih mesin online yang memiliki Agen untuk Exchange atau Agen untuk VMware, lalu pilih titik pemulihan.
- Pilih titik pemulihan pada tab Penyimpanan cadangan.

Mesin yang dipilih untuk menjelajahi dalam tindakan di atas menjadi mesin target untuk pemulihan data Exchange.

4. Lakukan salah satu langkah berikut:
   - Saat memulihkan dari cadangan keberadaan aplikasi, klik **Pulihkan** > **Database Exchange**, pilih database yang ingin Anda pulihkan, lalu klik **Pulihkan sebagai file**.
   - Saat memulihkan dari cadangan database, klik **Pulihkan** > **Database sebagai file**.
5. Klik **Jelajahi**, lalu pilih folder lokal atau folder jaringan untuk menyimpan file.
6. Klik **Mulai pemulihan**.

Progres pemulihan akan ditampilkan pada tab Aktivitas.

Memasang database Server Exchange

Setelah memulihkan file database, Anda dapat mengambil database secara online dengan cara mounting. Mounting dilakukan menggunakan Exchange Management Console, Exchange System Manager, atau Exchange Management Shell.

Database yang dipulihkan akan berada dalam status Dirty Shutdown. Database yang berada dalam status Dirty Shutdown dapat di-mount oleh sistem jika dipulihkan ke lokasi aslinya (yaitu, informasi tentang database asli ada dalam Active Directory). Ketika memulihkan database ke lokasi alternatif (seperti database baru atau sebagai database pemulihan), database tidak dapat dipasang hingga Anda mengembalikannya ke status Clean Shutdown menggunakan perintah `Eseutil /r <Enn>`. `<Enn>` menentukan prefiks file log untuk database (atau grup penyimpanan yang berisi database) ke lokasi yang perlu diterapkan file log transaksi oleh Anda.

Akun yang Anda gunakan untuk menyertakan database harus didelegasikan dengan peran Administrator Server Exchange dan grup Administrator lokal untuk server target.

Untuk detail tentang cara mounting database, lihat artikel berikut:

- Exchange 2010 ke atas: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

Memulihkan kotak surat Exchange dan item kotak surat

Anda dapat memulihkan kotak surat Exchange dan item kotak surat dari cadangan berikut:

- Cadangan database
- Cadangan keberadaan aplikasi
- Cadangan kotak surat

© Acronis International GmbH, 2003-2024

Anda dapat memulihkan item berikut:

- Kotak surat (kecuali untuk kotak surat arsip)
- Folder publik

Catatan
Tersedia hanya dari cadangan database. Lihat "Memilih data Exchange Server" (hlm. 562).

- Item folder publik
- Folder Email
- Pesan email
- Acara kalender
- Tugas
- Kontak
- Entri jurnal
- Catatan

Anda dapat menggunakan pencarian untuk menemukan item.

Kotak surat atau item kotak surat dapat dipulihkan ke Exchange Server langsung atau ke Microsoft 365.

Pemulihan ke Server Exchange

Pemulihan granular dapat dilakukan untuk Microsoft Exchange Server 2010 Service Pack 1 (SP1) dan yang lebih baru. Pemulihan granular dapat dilakukan oleh Agen untuk Exchange atau Agen untuk VMware (Windows).

Pemulihan granular dapat dilakukan oleh Agen untuk Exchange atau Agen untuk VMware (Windows). Target Exchange Server dan mesin yang menjalankan agen harus menjadi bagian dari forest Active Directory yang sama.

Ketika kotak surat dipulihkan ke kotak surat yang ada, item yang ada dengan ID yang sama akan ditimpa.

Pemulihan item kotak surat tidak menimpa apa pun. Sebaliknya, jalur lengkap ke item kotak surat dibuat kembali di folder target.

Persyaratan pada akun pengguna

Kotak surat yang dipulihkan dari cadangan harus memiliki akun pengguna yang terkait di Active Directory.

Kotak surat pengguna dan kontennya dapat dipulihkan hanya jika akun pengguna terkait mereka *diaktifkan*. Kotak surat bersama, ruang, dan peralatan dapat dipulihkan hanya jika akun pengguna terkait mereka *dinonaktifkan*.

Kotak surat yang tidak memenuhi syarat di atas akan dilewati selama pemulihan.

© Acronis International GmbH, 2003-2024

Jika beberapa kotak surat dilewati, pemulihan akan berhasil namun disertai peringatan. Jika semua kotak surat dilewati, pemulihan akan gagal.

Pemulihan ke Microsoft 365

Pemulihan item data Exchange ke Microsoft 365, dan sebaliknya, didukung dengan ketentuan bahwa Agen untuk Microsoft 365 telah diinstal secara lokal.

Pemulihan dapat dilakukan dari cadangan Microsoft Exchange Server 2010 ke atas.

Ketika kotak surat dipulihkan ke kotak surat Microsoft 365 yang sudah ada, item yang ada akan tetap utuh, dan item yang dipulihkan akan ditempatkan di sebelahnya.

Saat memulihkan kotak surat tunggal, Anda harus memilih kotak surat Microsoft 365 target. Saat memulihkan beberapa kotak surat dalam satu operasi pemulihan, perangkat lunak akan mencoba memulihkan setiap kotak surat ke kotak surat pengguna dengan nama yang sama. Jika pengguna tidak ditemukan, kotak surat akan dilewati. Jika beberapa kotak surat dilewati, pemulihan akan berhasil namun disertai peringatan. Jika semua kotak surat dilewati, pemulihan akan gagal.

Untuk informasi lebih lanjut tentang pemulihan ke Microsoft 365, lihat "Melindungi data Microsoft 365" (hlm. 596).

Memulihkan kotak surat

Untuk memulihkan kotak surat dari cadangan keberadaan aplikasi atau cadangan database

1. [Hanya ketika memulihkan dari cadangan database ke Microsoft 365] Jika Agen untuk Microsoft 365 tidak diinstal pada mesin yang menjalankan Exchange Server yang dicadangkan, lakukan salah satu langkah berikut:
   - Jika tidak ada Agen untuk Microsoft 365 di organisasi Anda, instal Agen untuk Microsoft 365 pada mesin yang dicadangkan (atau pada mesin lain dengan versi Microsoft Exchange Server yang sama).
   - Jika sudah memiliki Agen untuk Microsoft 365 di organisasi Anda, salin pustaka dari mesin yang dicadangkan (atau dari mesin lain dengan versi Microsoft Exchange Server yang sama) ke mesin yang memiliki Agen untuk Microsoft 365, seperti yang dijelaskan dalam "Menyalin pustaka Microsoft Exchange".
2. Lakukan salah satu langkah berikut:
   - Saat memulihkan dari cadangan keberadaan aplikasi: pada **Perangkat**, pilih mesin yang awalnya berisi data yang ingin Anda pulihkan.
   - Saat memulihkan dari cadangan database, klik **Perangkat** > **Microsoft Exchange** > **Database**, lalu pilih database yang awalnya berisi data yang ingin Anda pulihkan.
3. Klik **Pemulihan**.
4. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.

   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Gunakan cara lain untuk memulihkan:

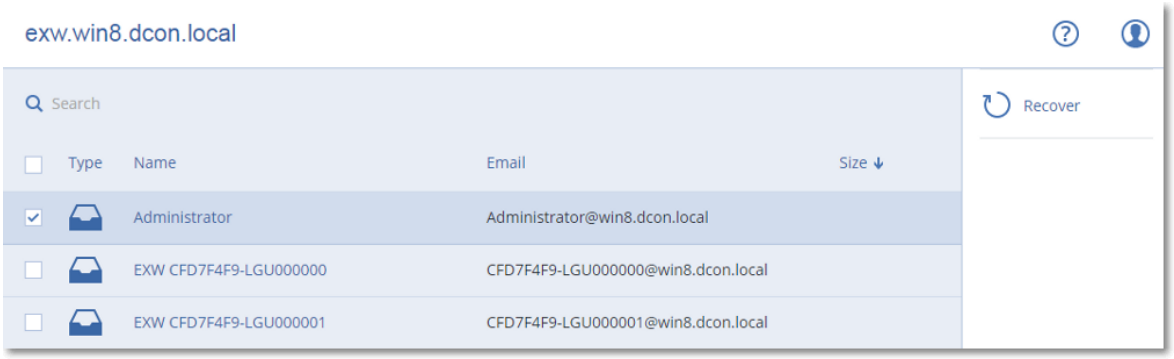
© Acronis International GmbH, 2003-2024

- [Hanya jika memulihkan dari cadangan tanggap aplikasi] Jika lokasi cadangan adalah penyimpanan awan atau penyimpanan bersama (yang dapat diakses agen lain), klik **Pilih mesin**, pilih mesin online yang memiliki Agen untuk Exchange atau Agen untuk VMware, lalu pilih titik pemulihan.
- Pilih titik pemulihan pada tab Penyimpanan cadangan.

Mesin yang dipilih untuk menjelajahi dalam tindakan di atas akan melakukan pemulihan, bukan dalam mesin asli yang sedang offline.

5. Klik **Pulihkan** > **Kotak surat Exchange**.
6. Pilih kotak surat yang ingin Anda pulihkan.

   Anda dapat mencari kotak surat berdasarkan nama. Wildcard tidak didukung.



7. Klik **Pulihkan**.
8. [Hanya ketika memulihkan ke Microsoft 365]:
   a. Pada **Pulihkan ke**, pilih **Microsoft 365**.
   b. [Jika Anda hanya memilih satu kotak surat di langkah 6] Pada **Kotak surat target**, tentukan kotak surat target.
   c. Klik **Mulai pemulihan**.

   Langkah lebih lanjut dari prosedur ini tidak diperlukan.

   Klik **mesin Target dengan Microsoft Exchange Server** untuk memilih atau mengubah mesin target. Langkah ini memungkinkan pemulihan ke mesin yang tidak menjalankan Agen untuk Exchange.

   Tentukan nama domain yang sepenuhnya memenuhi syarat (FQDN) dari mesin tempat peran **Akses Klien** (di Microsoft Exchange Server 2010/2013) atau **Peran kotak surat** (di Microsoft Exchange Server 2016 atau setelahnya) dimungkinkan. Mesin harus dimiliki oleh forest Active Directory yang sama dengan mesin yang melakukan pemulihan.
9. Jika diminta, berikan kredensial akun yang akan digunakan untuk mengakses mesin. Persyaratan untuk akun ini terdaftar pada "Hak pengguna yang diperlukan".
10. [Opsional] Klik **Database untuk membuat ulang kotak surat yang tertinggal** untuk mengubah database yang dipilih secara otomatis.
11. Klik **Mulai pemulihan**.

Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

Untuk memulihkan kotak surat dari cadangan kotak surat

© Acronis International GmbH, 2003-2024

1. Klik **Perangkat** > **Microsoft Exchange** > **Kotak surat**.
2. Pilih kotak surat untuk memulihkan, lalu klik **Pemulihan**.

   Anda dapat mencari kotak surat berdasarkan nama. Wildcard tidak didukung.

   Jika kotak surat dihapus, pilih kotak surat pada tab Penyimpanan cadangan, lalu klik **Tampilkan cadangan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
4. Klik **Pulihkan** > **Kotak surat**.
5. Lakukan langkah 8-11 dari prosedur di atas.

Memulihkan item kotak surat

Untuk memulihkan item kotak surat dari cadangan keberadaan aplikasi atau cadangan database

1. [Hanya ketika memulihkan dari cadangan database ke Microsoft 365] Jika Agen untuk Microsoft 365 tidak diinstal pada mesin yang menjalankan Exchange Server yang dicadangkan, lakukan salah satu langkah berikut:
   - Jika tidak ada Agen untuk Microsoft 365 di organisasi Anda, instal Agen untuk Microsoft 365 pada mesin yang dicadangkan (atau pada mesin lain dengan versi Microsoft Exchange Server yang sama).
   - Jika sudah memiliki Agen untuk Microsoft 365 di organisasi Anda, salin pustaka dari mesin yang dicadangkan (atau dari mesin lain dengan versi Microsoft Exchange Server yang sama) ke mesin yang memiliki Agen untuk Microsoft 365, seperti yang dijelaskan dalam "Menyalin pustaka Microsoft Exchange".
2. Lakukan salah satu langkah berikut:
   - Saat memulihkan dari cadangan keberadaan aplikasi: pada **Perangkat**, pilih mesin yang awalnya berisi data yang ingin Anda pulihkan.
   - Saat memulihkan dari cadangan database, klik **Perangkat** > **Microsoft Exchange** > **Database**, lalu pilih database yang awalnya berisi data yang ingin Anda pulihkan.
3. Klik **Pemulihan**.
4. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.

   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Gunakan cara lain untuk memulihkan:
   - [Hanya jika memulihkan dari cadangan tanggap aplikasi] Jika lokasi cadangan adalah penyimpanan awan atau penyimpanan bersama (yang dapat diakses agen lain), klik **Pilih mesin**, pilih mesin online yang memiliki Agen untuk Exchange atau Agen untuk VMware, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab Penyimpanan cadangan.

   Mesin yang dipilih untuk menjelajahi dalam tindakan di atas akan melakukan pemulihan, bukan dalam mesin asli yang sedang offline.
5. Klik **Pulihkan** > **Kotak surat Exchange**.

© Acronis International GmbH, 2003-2024

6. Klik kotak surat yang awalnya berisi item yang ingin Anda pulihkan.
7. Pilih item yang ingin Anda pulihkan.

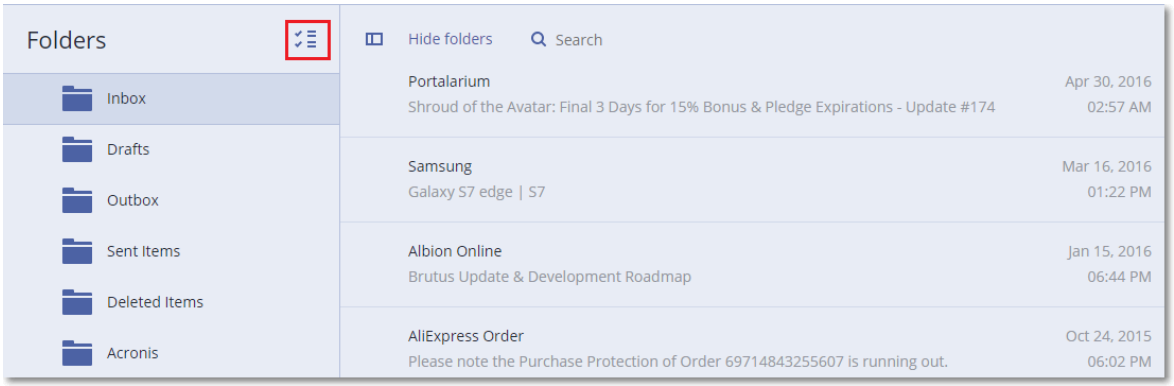
   Opsi pencarian berikut tersedia. Wildcard tidak didukung.

   - Untuk pesan email: cari berdasarkan subjek, pengirim, penerima, dan tanggal.
   - Untuk acara: cari berdasarkan judul dan tanggal.
   - Untuk tugas: cari berdasarkan subjek dan tanggal.
   - Untuk kontak: cari berdasarkan nama, alamat email, dan nomor telepon.

   Ketika pesan email dipilih, Anda dapat mengklik **Tampilkan konten** untuk melihat kontennya, termasuk lampiran.

   Catatan
   Klik nama file terlampir untuk mengunduhnya.

   Untuk dapat memilih folder, klik ikon folder pemulihan.



8. Klik **Pulihkan**.
9. Untuk memulihkan ke Microsoft 365, pilih **Microsoft 365** di **Pulihkan ke**.

   Untuk memulihkan ke Exchange Server, pertahankan nilai default **Microsoft Exchange** di **Pulihkan ke**.

   [Hanya ketika memulihkan ke Exchange Server] Klik **Mesin target dengan Microsoft Exchange Server** untuk memilih atau mengubah mesin target. Langkah ini memungkinkan pemulihan ke mesin yang tidak menjalankan Agen untuk Exchange.

   Tentukan nama domain yang sepenuhnya memenuhi syarat (FQDN) dari mesin tempat peran **Akses Klien** (di Microsoft Exchange Server 2010/2013) atau **Peran kotak surat** (di Microsoft Exchange Server 2016 atau setelahnya) dimungkinkan. Mesin harus dimiliki oleh forest Active Directory yang sama dengan mesin yang melakukan pemulihan.
10. Jika diminta, berikan kredensial akun yang akan digunakan untuk mengakses mesin. Persyaratan untuk akun ini terdaftar pada "Hak pengguna yang diperlukan".
11. Di **Kotak surat target**, lihat, ubah, atau tentukan kotak surat target.

    Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada atau mesin target non-asli dipilih, Anda harus menentukan kotak surat target.

© Acronis International GmbH, 2003-2024

12. [Hanya ketika memulihkan pesan email] Di **Folder target**, lihat atau ubah folder target di kotak surat target. Secara default, folder **Pulihkan item** dipilih. Karena pembatasan, acara, tugas, catatan, dan kontak Microsoft Exchange dipulihkan ke lokasi aslinya terlepas dari **Folder Target** yang ditentukan.
13. Klik **Mulai pemulihan**.

Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

Untuk memulihkan item kotak surat dari cadangan kotak surat

1. Klik **Perangkat** > **Microsoft Exchange** > **Kotak surat**.
2. Pilih kotak surat yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   Anda dapat mencari kotak surat berdasarkan nama. Wildcard tidak didukung.
   Jika kotak surat dihapus, pilih kotak surat pada tab Penyimpanan cadangan, lalu klik **Tampilkan cadangan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
4. Klik **Pulihkan** > **Pesan Email**.
5. Pilih item yang ingin Anda pulihkan.
   Opsi pencarian berikut tersedia. Wildcard tidak didukung.
   - Untuk pesan email: cari berdasarkan subjek, pengirim, penerima, dan tanggal.
   - Untuk acara: cari berdasarkan judul dan tanggal.
   - Untuk tugas: cari berdasarkan subjek dan tanggal.
   - Untuk kontak: cari berdasarkan nama, alamat email, dan nomor telepon.

   Ketika pesan email dipilih, Anda dapat mengklik **Tampilkan konten** untuk melihat kontennya, termasuk lampiran.

   Catatan
   Klik nama file terlampir untuk mengunduhnya.

   Ketika pesan email dipilih, Anda dapat mengklik **Kirim sebagai surel** untuk mengirim pesan ke alamat email. Pesan dikirim dari alamat email akun administrator Anda.

   Untuk dapat memilih folder, klik ikon pulihkan folder:
6. Klik **Pulihkan**.
7. Lakukan langkah 9-13 dari prosedur di atas.

Menyalin pustaka Microsoft Exchange Server

Saat memulihkan kotak surat atau item kotak surat Exchange ke Microsoft 365, Anda mungkin perlu menyalin pustaka berikut ini dari mesin yang dicadangkan (atau dari mesin lain dengan versi Microsoft Exchange Server yang sama) ke mesin yang memiliki Agen untuk Microsoft 365.

Salin file berikut, sesuai dengan versi Microsoft Exchange Server yang didukung.

© Acronis International GmbH, 2003-2024

Versi Microsoft Exchange Server	Pustaka	Lokasi default

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`

Pustaka harus ditempatkan di folder `%ProgramData%\Acronis\ese`. Jika folder ini tidak ada, buat secara manual.

Mengubah kredensial akses SQL Server atau Exchange Server

Anda dapat mengubah kredensial akses untuk SQL Server atau Exchange Server tanpa menginstal ulang agen.

Untuk mengubah kredensial akses SQL Server atau Exchange Server

1. Klik **Perangkat**, lalu klik **Microsoft SQL** atau **Microsoft Exchange**.
2. Pilih Always On Availability Group, Database Availability Group, SQL Server instance, atau Exchange Server yang Anda ingin ubah kredensial aksesnya.
3. Klik **Tentukan kredensial**.
4. Tentukan kredensial akses baru, lalu klik **OK**.

Untuk mengubah kredensial akses Exchange Server untuk pencadangan kotak pesan

1. Klik **Perangkat** > **Microsoft Exchange**, lalu perluas **Kotak surat**.
2. Pilih Exchange Server yang ingin Anda ubah kredensial aksesnya.
3. Klik **Pengaturan**.
4. Pada **akun administrator Exchange**, tentukan kredensial akses baru, lalu klik **Simpan**.

Melindungi perangkat seluler

Aplikasi Cyber Protect memungkinkan untuk mencadangkan data seluler Anda ke Penyimpanan awan, lalu memulihkannya apabila hilang atau rusak. Perhatikan bahwa pencadangan ke penyimpanan awan memerlukan akun dan langganan Cloud.

© Acronis International GmbH, 2003-2024

Perangkat seluler yang didukung

Anda dapat menginstal aplikasi Cyber Protect di perangkat seluler yang menjalankan sistem operasi berikut:

- iOS 14 hingga iOS 16 (iPhone, iPod, iPad)
- Android 9 hingga Android 13

Apa yang dapat Anda cadangkan

- Kontak (nama, nomor telepon, and email)
- Foto (ukuran dan format asli foto Anda dipertahankan)
- Video
- Kalender
- Pengingat (hanya di perangkat iOS)

Apa yang perlu Anda ketahui

- Anda hanya dapat mencadangkan data ke penyimpanan awan.
- Setiap kali Anda membuka aplikasi, Anda akan melihat ringkasan perubahan data dan pencadangan dapat dimulai secara manual.
- Fungsionalitas **Pencadangan kontinu** diaktifkan secara default. Jika pengaturan ini diaktifkan, aplikasi Cyber Protect secara otomatis mendeteksi data baru yang sedang diproses dan mengunggahnya ke Awan.
- Opsi **Hanya gunakan Wi-Fi** diaktifkan secara standar di pengaturan aplikasi. Jika pengaturan ini diaktifkan, aplikasi Cyber Protect akan mencadangkan data Anda hanya saat terdapat koneksi Wi-Fi. Jika koneksi Wi-Fi hilang, proses pencadangan tidak akan dimulai. Agar aplikasi juga dapat menggunakan koneksi seluler, nonaktifkan opsi ini.
- Optimalisasi baterai pada perangkat Anda bisa mencegah aplikasi Cyber Protect dari pengoperasian yang benar. Untuk menjalankan pencadangan tepat waktu, Anda harus menghentikan optimalisasi baterai untuk aplikasi tersebut.
- Anda memiliki dua cara untuk menghemat energi:
  - Fungsi **Cadangkan selama mengisi daya** dinonaktifkan secara standar. Jika pengaturan ini diaktifkan, aplikasi Cyber Protect akan mencadangkan data Anda hanya saat perangkat tersambung ke sumber daya. Jika perangkat terputus dari sumber daya selama proses pencadangan kontinu, pencadangan akan dijeda.
  - **Mode hemat daya** yang diaktifkan secara standar. Jika pengaturan ini diaktifkan, aplikasi Cyber Protect akan mencadangkan data Anda hanya saat baterai perangkat tidak lemah. Jika baterai perangkat melemah, pencadangan kontinu akan dijeda.
- Anda dapat mengakses data yang dicadangkan dari perangkat seluler apa pun yang terdaftar dengan akun Anda. Hal ini membantu Anda mentransfer data dari perangkat seluler lama ke

© Acronis International GmbH, 2003-2024

yang baru. Anda dapat memulihkan kontak dan foto dari perangkat Android ke perangkat iOS dan sebaliknya. Anda juga dapat mengunduh foto, video, atau kontak ke perangkat apa pun dengan menggunakan konsol Cyber Protect.

- Data yang dicadangkan dari perangkat seluler yang terdaftar dengan akun Anda hanya tersedia dengan akun tersebut. Tidak seorang pun dapat melihat atau memulihkan data Anda.
- Di aplikasi Cyber Protect, Anda hanya dapat memulihkan versi data terakhir. Jika Anda perlu memulihkan dari versi cadangan tertentu, gunakan konsol Cyber Protect di tablet atau komputer.
- Aturan retensi tidak diterapkan terhadap pencadangan perangkat seluler.
- [Hanya untuk perangkat Android] Jika terdapat kartu SD saat pencadangan, data yang disimpan di kartu ini juga akan dicadangkan. Data akan dipulihkan ke kartu SD, ke folder **Dipulihkan oleh Pencadangan** jika ini ada selama pemulihan, atau aplikasi akan meminta lokasi yang berbeda untuk memulihkan data tersebut.

Tempat untuk mendapatkan aplikasi Cyber Protect

Tergantung pada perangkat seluler Anda, instal aplikasi dari App Store atau Google Play.

Cara memulai pencadangan data Anda

1. Buka aplikasi.
2. Masuk dengan akun Anda.
3. Sentuh **Atur** untuk membuat cadangan Anda. Perhatikan bahwa tombol ini muncul hanya saat Anda tidak memiliki cadangan perangkat seluler Anda.
4. Pilih kategori data yang ingin Anda cadangkan. Secara default, semua kategori dipilih.
5. [langkah opsional] Aktifkan **Enkripsi Cadangkan** untuk melindungi cadangan Anda dengan enkripsi. Dalam hal ini, Anda juga akan perlu:
   a. Masukkan kata sandi enkripsi dua kali.

      Catatan
      Pastikan Anda mengingat kata sandi, karena kata sandi yang dilupakan dapat tidak pernah dipulihkan atau diubah.

   b. Sentuh **Enkripsi**.
6. Ketuk **Cadangkan**.
7. Izinkan akses aplikasi ke data pribadi Anda. Jika Anda menolak akses ke beberapa kategori data, data tidak akan dicadangkan.

Mulai mencadangkan.

Cara memulihkan data ke perangkat seluler

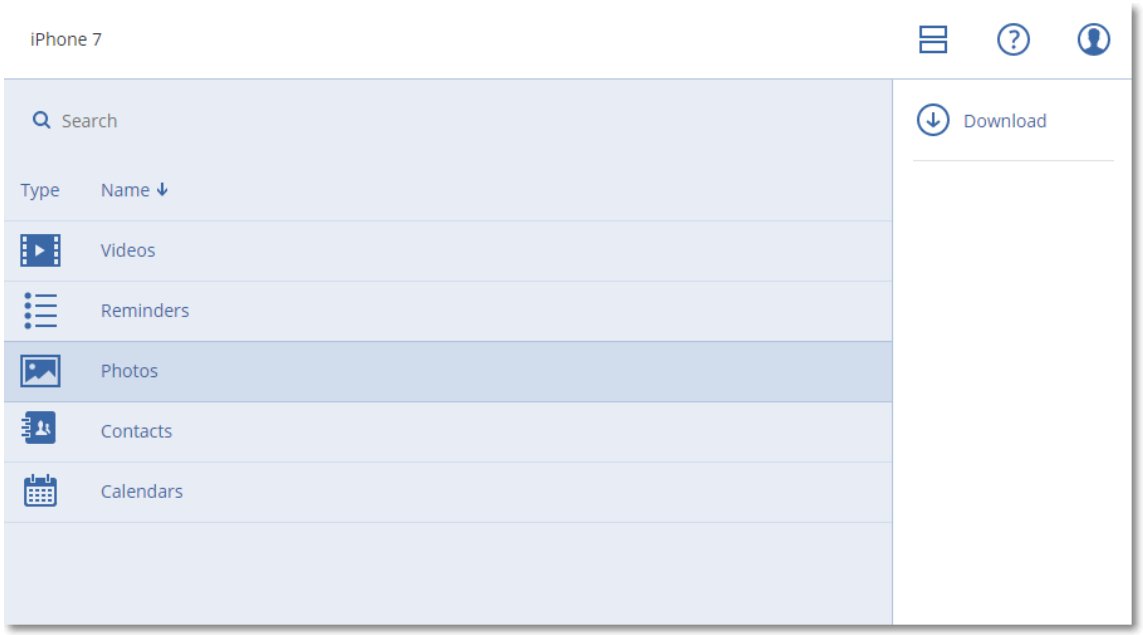
Peringatan!
Untuk memulihkan data seluler, Anda harus menggunakan akun pengguna akhir.

© Acronis International GmbH, 2003-2024

1. Buka aplikasi Cyber Protect.
2. Sentuh **Jelajahi**.
3. Ketuk nama perangkat.
4. Lakukan salah satu langkah berikut:
   - Untuk memulihkan semua data yang dicadangkan, ketuk **Pulihkan semua**. Tidak diperlukan tindakan lainnya.
   - Untuk memulihkan satu atau beberapa kategori data, ketuk **Pilih**, lalu ketuk kotak centang untuk kategori data yang diperlukan. Ketuk **Pulihkan**. Tidak diperlukan tindakan lainnya.
   - Untuk memulihkan satu atau beberapa item data yang masuk dalam kategori data yang sama, ketuk kategori data. Proses ke langkah selanjutnya.
5. Lakukan salah satu langkah berikut:
   - Untuk memulihkan satu item data, ketuk itemnya.
   - Untuk memulihkan beberapa item data, ketuk **Pilih**, lalu ketuk kotak centang untuk item data yang diperlukan.
6. Ketuk **Pulihkan**.

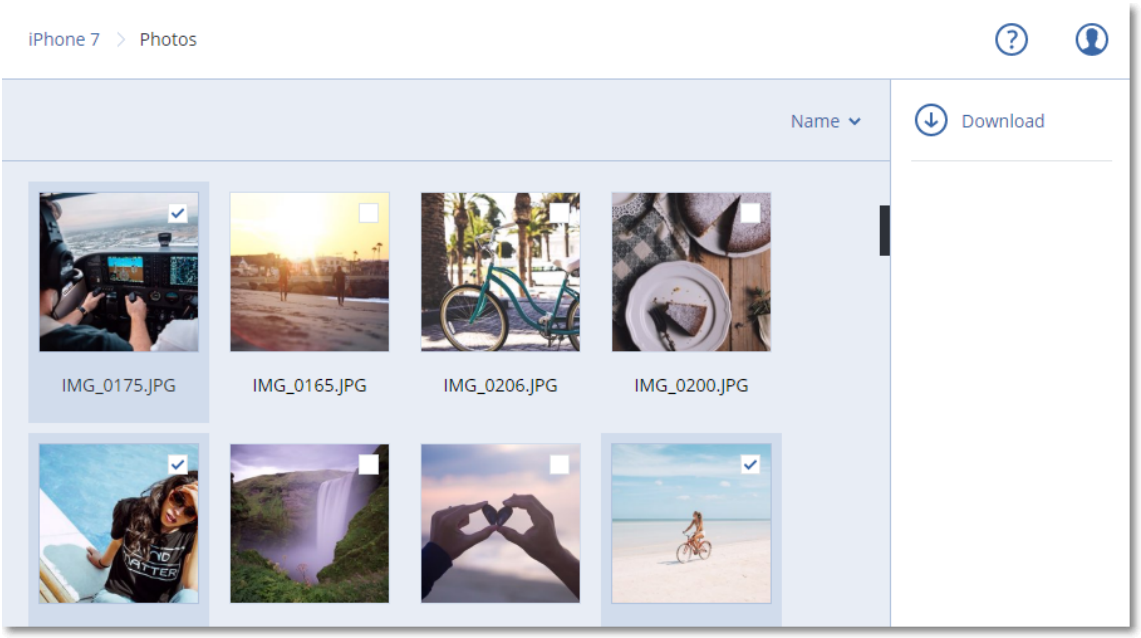
Cara meninjau data melalui konsol Cyber Protect

1. Di komputer, buka browser dan ketik konsol Cyber Protect URL.
2. Masuk dengan akun Anda.
3. Di **Semua perangkat**, klik **Pulihkan** pada nama perangkat seluler Anda.
4. Lakukan yang berikut ini:
   - Untuk mengunduh semua foto, video, kontak, kalender, atau pengingat, pilih masing-masing kategori data. Klik **Unduh**.



© Acronis International GmbH, 2003-2024

- Untuk mengunduh setiap foto, video, kontak, kalender, atau pengingat, klik nama kategori data masing-masing, lalu pilih kotak centang untuk butir data yang diperlukan. Klik **Unduh**.



- Untuk meninjau foto atau kontak, klik nama kategori data masing-masing, lalu klik item data yang diperlukan.

Melindungi data Exchange yang Dihosting

Apa saja item yang dapat dicadangkan?

Anda dapat mencadangkan kotak surat pengguna, kotak surat bersama, dan kotak surat grup. Secara opsional, Anda dapat memilih untuk mencadangkan kotak surat arsip (**Arsip Di Tempat**) dari kotak surat yang dipilih.

Apa saja item yang dapat dipulihkan?

Item berikut dapat dipulihkan dari cadangan kotak surat:

- Kotak surat
- Folder Email
- Pesan email
- Acara kalender
- Tugas
- Kontak
- Entri jurnal
- Catatan

Anda dapat menggunakan pencarian untuk menemukan item.

© Acronis International GmbH, 2003-2024

Ketika memulihkan kotak surat, item kotak surat, folder umum, dan item folder umum, Anda dapat memilih apakah item di lokasi target akan ditimpa atau tidak.

Ketika kotak surat dipulihkan ke kotak surat yang ada, item yang ada dengan ID yang sama akan ditimpa.

Pemulihan item kotak surat tidak menimpa apa pun. Sebaliknya, jalur lengkap ke item kotak surat dibuat kembali di folder target.

Memilih kotak surat Exchange Online

Pilih kotak surat seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Untuk memilih kotak surat Exchange Online

1. Klik **Perangkat > Exchange yang Dihosting**.
2. Jika beberapa organisasi Exchange yang Dihosting ditambahkan ke layanan Cyber Protection, pilih organisasi yang data penggunanya ingin Anda cadangkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk mencadangkan kotak surat semua pengguna dan semua kotak surat bersama (termasuk kotak surat yang akan dibuat di waktu mendatang), perluas simpul **Pengguna**, pilih **Semua pengguna**, lalu klik **Cadangan grup**.
   - Untuk mencadangkan pengguna individual atau kotak surat bersama, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang kotak suratnya ingin Anda cadangkan, lalu klik **Cadangkan**.
   - Untuk mencadangkan semua kotak surat grup (termasuk kotak surat grup yang akan dibuat di waktu mendatang), perluas simpul **Grup**, pilih **Semua grup**, lalu klik **Cadangan grup**.
   - Untuk mencadangkan kotak surat grup individual, perluas simpul **Grup**, pilih **Semua grup**, pilih grup yang kotak suratnya ingin Anda cadangkan, lalu klik **Cadangkan**.

Memulihkan kotak surat dan item kotak surat

Memulihkan kotak surat

1. Klik **Perangkat > Exchange yang Dihosting**.
2. Jika beberapa organisasi Exchange yang Dihosting ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk memulihkan kotak surat pengguna, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang kotak suratnya ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Untuk memulihkan kotak surat bersama, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih kotak surat bersama yang ingin Anda pulihkan, lalu klik **Pemulihan**.

© Acronis International GmbH, 2003-2024

- Untuk memulihkan kotak surat grup, perluas simpul **Grup**, pilih **Semua grup**, pilih kotak surat grup yang ingin Anda pulihkan, lalu klik **Pemulihan**.
- Jika pengguna, grup, atau kotak surat bersama dihapus, pilih item tersebut di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.

Anda dapat mencari pengguna dan grup berdasarkan nama. Wildcard tidak didukung.

4. Pilih titik pemulihan.
5. Klik **Pulihkan** > **Keseluruhan kotak surat**.
6. Jika beberapa organisasi Exchange yang Dihosting ditambahkan ke layanan Cyber Protection, klik **Organisasi Exchange yang Dihosting** untuk melihat, mengubah, atau menentukan organisasi target.

   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
7. Di **Pulihkan ke kotak surat**, lihat, ubah, atau tentukan kotak surat target.

   Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan kotak surat target.
8. Klik **Mulai pemulihan**.
9. Pilih salah satu opsi penimpaan:
   - **Timpa item yang ada**
   - **Jangan timpa item yang ada**
10. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Memulihkan item kotak surat

1. Klik **Perangkat > Exchange yang Dihosting**.
2. Jika beberapa organisasi Exchange yang Dihosting ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk memulihkan item dari kotak surat pengguna, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna dengan kotak surat yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Untuk memulihkan item dari kotak surat bersama, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih kotak surat bersama yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Untuk memulihkan item dari kotak surat grup, perluas simpul **Grup**, pilih **Semua grup**, pilih grup dengan kotak surat yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Jika pengguna, grup, atau kotak surat bersama dihapus, pilih item tersebut di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.

   Anda dapat mencari pengguna dan grup berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.

© Acronis International GmbH, 2003-2024

5. Klik **Pulihkan** > **Pesan Email**.
6. Jelajahi ke folder yang diperlukan atau gunakan pencarian untuk mendapatkan daftar item yang diperlukan.

   Opsi pencarian berikut tersedia. Wildcard tidak didukung.
   - Untuk pesan email: cari berdasarkan subjek, pengirim, penerima, nama lampiran, dan tanggal.
   - Untuk acara: cari berdasarkan judul dan tanggal.
   - Untuk tugas: cari berdasarkan subjek dan tanggal.
   - Untuk kontak: cari berdasarkan nama, alamat email, dan nomor telepon.
7. Pilih item yang ingin Anda pulihkan. Untuk dapat memilih folder, klik ikon "pulihkan folder":

   Selain itu, Anda dapat melakukan hal-hal berikut:
   - Ketika item dipilih, klik **Tampilkan konten** untuk melihat kontennya, termasuk lampiran. Klik nama file terlampir untuk mengunduhnya.
   - Ketika pesan email atau item kalender dipilih, klik **Kirim sebagai surel** untuk mengirim item ke alamat email yang ditentukan. Anda dapat memilih pengirim dan menulis teks yang akan ditambahkan ke item yang diteruskan.
   - Hanya jika cadangan tidak dienkripsi, gunakan pencarian, dan pilih satu item pada hasil pencarian: klik **Tampilkan versi** untuk memilih versi item yang akan dipulihkan. Anda dapat memilih versi yang dicadangkan, yang lebih baru atau lebih lama dari titik pemulihan yang dipilih.
8. Klik **Pulihkan**.
9. Jika beberapa organisasi Exchange yang Dihosting ditambahkan ke layanan Cyber Protection, klik **organisasi Exchange yang Dihosting** untuk melihat, mengubah, atau menentukan organisasi target.

   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
10. Di **Pulihkan ke kotak surat**, lihat, ubah, atau tentukan kotak surat target.

    Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan kotak surat target.
11. [Hanya ketika memulihkan ke pengguna atau kotak surat bersama] Di **Jalur**, lihat atau ubah folder target di kotak surat target. Secara default, folder **Pulihkan item** dipilih.

    Item kotak surat grup selalu dipulihkan ke folder **Kotak masuk**.
12. Klik **Mulai pemulihan**.
13. Pilih salah satu opsi penimpaan:
    - **Timpa item yang ada**
    - **Jangan timpa item yang ada**
14. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

© Acronis International GmbH, 2003-2024

Melindungi data Microsoft 365

Mengapa perlu mencadangkan data Microsoft 365?

Meskipun Microsoft 365 merupakan serangkaian layanan awan, pencadangan rutin memberikan lapisan perlindungan tambahan terhadap kesalahan pengguna dan tindakan membahayakan yang disengaja. Anda dapat memulihkan item yang dihapus dari cadangan bahkan setelah periode penyimpanan Microsoft 365 berakhir. Anda juga dapat menyimpan salinan lokal kotak surat Exchange Online jika diperlukan untuk kepatuhan peraturan.

Data yang dicadangkan dikompres secara otomatis dan menggunakan lebih sedikit ruang di lokasi pencadangan dibandingkan lokasi aslinya. Tingkat kompresi untuk pencadangan awan-ke-awan telah diperbaiki dan sesuai dengan level **Normal** pada pencadangan non-awan-ke-awan. Untuk informasi lebih lanjut tentang level ini, lihat "Tingkat kompresi" (hlm. 458).

Agen cloud dan agen lokal

Untuk beban kerja Microsoft 365, terdapat dua agen tersedia:

- Agen cloud

  Agen cloud menyediakan fungsi cadangan yang diperluas, yang mana dapat diakses secara langsung dalam konsol Cyber Protect. Pemasangan tidak diperlukan. Untuk informasi lebih lanjut, lihat "Menggunakan versi awan Agen untuk Microsoft 365" (hlm. 605).
- Agen lokal

  Agen lokal hanya menyediakan cadangan kotak surat Exchange online. Agen ini harus diinstal pada mesin Windows yang terhubung ke Internet. Untuk informasi lebih lanjut, lihat "Menggunakan Agen untuk Office 365 yang diinstal secara lokal" (hlm. 601).

Azure Information Protection (AIP) didukung oleh kedua agen.

Catatan
Untuk penyewa dalam mode Kepatuhan, hanya agen lokal yang tersedia. Penyewa ini hanya dapat mencadangkan kotak surat Microsoft 365 saja. Mereka tidak dapat menggunakan fungsi tambahan yang disediakan oleh agen cloud.

Tabel berikut meringkas fungsionalitas dari para agen.

	Agen lokal	Agen cloud
Item data yang dapat dicadangkan	**Exchange Online:** kotak surat pengguna dan kotak surat bersama (termasuk kotak surat pengguna pada rencana Kios dan kotak surat dalam penangguhan litigasi)	• **Exchange Online**: ◦ kotak surat pengguna dan kotak surat bersama (termasuk kotak surat pengguna pada rencana Kios dan kotak surat dalam

© Acronis International GmbH, 2003-2024

	Agen lokal	Agen cloud
		penangguhan litigasi) ◦ kotak surat grup ◦ folder umum • **OneDrive**: file dan folder pengguna • **SharePoint Online**: ◦ pengumpulan situs klasik ◦ situs grup (tim) ◦ situs komunikasi ◦ item data individual • **Microsoft 365 Teams**: ◦ seluruh tim ◦ saluran tim ◦ file saluran ◦ kotak surat tim ◦ file dan pesan surel dalam kotak surat tim ◦ pertemuan ◦ situs tim • **Notebook OneNote**: sebagai bagian dari cadangan OneDrive, SharePoint Online, dan Microsoft 365 Teams
Pencadangan kotak surat arsip (**Arsip Di Tempat**)	Tidak	Iya
Jadwal pencadangan	Ditentukan pengguna	Hingga enam kali per hari*
Lokasi pencadangan	Penyimpanan awan, folder lokal atau folder jaringan	Hanya Penyimpanan awan (termasuk penyimpanan yang dihosting oleh mitra)
Perlindungan otomatis pengguna, grup, situs, dan tim baru Microsoft 365	Tidak	Ya, dengan menerapkan rencana proteksi ke grup **Semua pengguna**, **Semua grup**, **Semua situs**, dan **Semua tim**
Melindungi lebih dari satu organisasi Microsoft 365	Tidak	Iya
Pemulihan granular	Iya	Iya
Pemulihan untuk pengguna lain dalam satu organisasi	Iya	Iya

© Acronis International GmbH, 2003-2024

	Agen lokal	Agen cloud
Pemulihan untuk organisasi lain	Tidak	Iya
Pemulihan untuk Microsoft Exchange Server di fasilitas	Tidak	Tidak
Jumlah maksimal item yang dapat dicadangkan tanpa penurunan kinerja	Saat mencadangkan ke penyimpanan awan: 5000 kotak surat per perusahaan Saat mencadangkan ke tujuan lain: 2.000 kotak surat per rencana proteksi (tidak ada batasan jumlah kotak surat per perusahaan)	10.000 item terlindungi (kotak surat, OneDrive, atau situs) per perusahaan**
Jumlah maksimum operasi cadangan manual	Tidak	10 operasi manual selama satu jam
Jumlah maksimum operasi pemulihan serentak	Tidak	10 operasi, termasuk operasi pemulihan Google Workspace

Opsi default adalah **Sekali sehari**. Dengan paket Cadangan Tingkat Lanjut, Anda dapat menjadwalkan hingga enam cadangan per hari. Pencadangan dimulai pada interval perkiraan yang bergantung pada beban saat ini dari agen awan, yang melayani banyak pelanggan di pusat data. Ini memastikan pemuatan yang merata di siang hari dan kualitas layanan yang sama untuk semua pelanggan.*

Catatan
Jadwal perlindungan dapat terdampak oleh operasi layanan pihak ketiga, misalnya aksesibilitas server Microsoft 365, pembatasan pengaturan pada server Microsoft, dan sebagainya. Lihat juga https://docs.microsoft.com/en-us/graph/throttling.

** Kami menyarankan Anda mencadangkan item yang dilindungi secara bertahap dan dalam urutan ini:

1. Kotak surat.
2. Setelah semua kotak surat dicadangkan, lanjutkan dengan OneDrive.
3. Setelah pencadangan OneDrive selesai, lanjutkan dengan situs SharePoint Online.

Pencadangan penuh pertama mungkin berlangsung beberapa hari, bergantung pada jumlah item yang dilindungi dan ukurannya.

© Acronis International GmbH, 2003-2024

Hak pengguna yang diperlukan

Dalam Cyber Protection

Agen lokal harus terdaftar dalam akun administrator perusahaan dan digunakan di tingkat penyewa pelanggan. Administrator perusahaan yang bertindak pada tingkat unit, administrator unit, dan pengguna tidak dapat mencadangkan atau memulihkan data Microsoft 365.

Agen cloud dapat digunakan baik di tingkat penyewa pelanggan dan di tingkat unit. Untuk informasi lebih lanjut tentang tingkat ini dan masing-masing administratornya, lihat "Pengelolaan organisasi Microsoft 365 yang ditambahkan pada tingkat berbeda" (hlm. 606).

Di Microsoft 365

Akun Anda harus diberi peran administrator global di Microsoft 365.

Untuk menemukan, mencadangkan dan memulihkan folder umum Microsoft 365, setidaknya salah satu akun administrator Microsoft 365 harus memiliki kotak surat dan hak baca/tulis ke folder publik yang ingin Anda cadangkan.

- Agen lokal akan masuk ke Microsoft 365 menggunakan akun ini. Untuk mengaktifkan agen untuk mengakses konten semua kotak surat, akun ini akan diberi peran manajemen **ApplicationImpersonation**. Jika Anda mengubah kata sandi akun, perbarui kata sandi di konsol Cyber Protect, seperti yang dijelaskan dalam "Mengubah kredensial akses Microsoft 365" (hlm. 603).
- Agen awan tidak masuk ke Microsoft 365. Anda perlu masuk ke dalam Microsoft 365 sebagai administrator global satu kali, untuk memberi izin yang diperlukan kepada agen cloud untuk melaksanakan operasinya.

  Izin berikut dalam Microsoft 365 diperlukan:
  - Masuk dan membaca profil pengguna
  - Membaca dan menulis file di semua kumpulan situs
  - Membaca dan menulis semua profil lengkap pengguna
  - Membaca dan menulis semua grup
  - Membaca data direktori
  - Membaca semua pesan saluran
  - Membaca dan menulis metadata yang dikelola
  - Membaca dan menulis item serta daftar di semua kumpulan situs
  - Memiliki kontrol penuh atas semua kumpulan situs
  - Membaca dan menulis item di semua kumpulan situs
  - Menggunakan Layanan Web Exchange dengan akses penuh menuju semua kotak surat

© Acronis International GmbH, 2003-2024

- Agen cloud tidak menyimpan kredensial akun Anda dan tidak menggunakannya untuk melakukan pencadangan dan pemulihan. Mengubah kredensial, menonaktifkan akun, atau menghapus akun tidak memengaruhi operasi dari agen cloud.

Pembatasan

- Dengan agen lokal, Anda dapat melindungi maksimum 5000 beban kerja. Dengan agen cloud, Anda dapat melindungi maksimum 50000 beban kerja.
- Semua pengguna dengan kotak surat atau OneDrive diperlihatkan di konsol Cyber Protect, termasuk pengguna tanpa lisensi Microsoft 365 dan pengguna yang diblokir untuk masuk ke layanan Microsoft 365.
- Pencadangan kotak surat hanya mencakup folder yang dapat dilihat pengguna. Folder **Item yang dapat dipulihkan** dan subfoldernya (**Penghapusan**, **Versi**, **Pembersihan**, **Audit**, **DiscoveryHold**, **Pencatatan Kalender**) tidak termasuk dalam pencadangan kotak surat.
- Selama pemulihan berlangsung, pembuatan pengguna, folder umum, grup, atau situs secara otomatis tidak dimungkinkan. Misalnya, jika Anda ingin memulihkan situs SharePoint Online yang telah dihapus, buat situs baru secara manual terlebih dahulu, lalu tentukan situs baru tersebut sebagai situs target selama pemulihan.
- Anda tidak dapat memulihkan item secara bersamaan dari titik pemulihan yang berbeda, meskipun Anda dapat memilih item tersebut dari hasil pencarian.
- Selama cadangan, setiap label sensitif yang diterapkan ke konten akan dijaga. Oleh karena itu, konten sensitif mungkin tidak ditampilkan jika dipulihkan ke lokasi non-asli dan penggunanya memiliki izin akses yang berbeda.
- Anda tidak dapat menerapkan lebih dari satu rencana pencadangan individual untuk beban kerja yang sama.
- Ketika rencana pencadangan individual dan rencana pencadangan grup diterapkan pada beban kerja yang sama, pengaturan dalam rencana individual akan diutamakan.

Laporan pelisensian kursi Microsoft 365

Administrator perusahaan dapat mengunduh laporan tentang kursi Microsoft 365 yang terlindungi dan pelisensiannya. Laporan tersebut dalam format CSV dan mencakup informasi tentang status pelisensian kursi dan alasan penggunaan lisensi. Laporan itu juga mencakup nama kursi yang terlindungi, email, grup, organisasi Microsoft 365 terkait, serta nama dan tipe beban kerja yang dilindungi.

Laporan ini tersedia hanya untuk penyewa dengan Organisasi Microsoft 365 yang terdaftar.

Untuk mengunduh laporan pelisensian kursi Microsoft 365

1. Masuk ke konsol Cyber Protect sebagai administrator perusahaan.
2. Klik ikon akun di sudut kanan atas.
3. Klik **Laporan pelisensian kursi Microsoft 365**.

© Acronis International GmbH, 2003-2024

Pencatatan

Tindakan dengan sumber daya awan-ke-awan, seperti menampilkan konten surel yang dicadangkan, mengunduh lampiran atau file, memulihkan surel ke kotak surat non-asli, atau mengirimkannya sebagai surel dapat melanggar kebijakan privasi pengguna. Tindakan ini dicatat di **Pemantauan** > **Log audit** di Portal Manajemen.

Menggunakan Agen untuk Office 365 yang diinstal secara lokal

Menambahkan organisasi Microsoft 365

Untuk menambahkan organisasi Microsoft 365

1. Masuk ke konsol Cyber Protect sebagai administrator perusahaan.
2. Klik ikon akun di sudut kanan atas, lalu klik **Unduhan** > **Agen untuk Office 365**.
3. Unduh agen dan instal pada mesin Windows yang terhubung dengan internet.
4. Di konsol Cyber Protect, buka **Perangkat** > **Microsoft Office 365 (Agen lokal)**.
5. Di jendela yang terbuka, masukkan ID aplikasi, rahasia aplikasi, dan ID penyewa Microsoft 365 Anda. Untuk informasi lebih lanjut tentang cara menemukannya, lihat "Mendapatkan ID aplikasi dan rahasia aplikasi" (hlm. 601).
6. Klik **OK**.

Hasilnya, item data organisasi Anda akan muncul di konsol Cyber Protect, pada tab **Microsoft Office 365 (Agen lokal)**.

Penting
Hanya diperbolehkan satu Agen untuk Office 365 yang terinstal secara lokal pada sebuah organisasi (grup perusahaan).

Mendapatkan ID aplikasi dan rahasia aplikasi

Untuk menggunakan autentikasi modern untuk Office 365, Anda perlu membuat aplikasi kustom di pusat admin Entra dan memberikannya izin API khusus. Dengan demikian, Anda akan mendapatkan **ID aplikasi**, **rahasia aplikasi**, dan **ID direktori (tenant)** yang Anda butuhkan untuk dimasukkan di Cyber Protect konsol.

Catatan
Di mesin tempat Agen untuk Office 365 diinstal, pastikan Anda mengizinkan akses ke graph.microsoft.com melalui port 443.

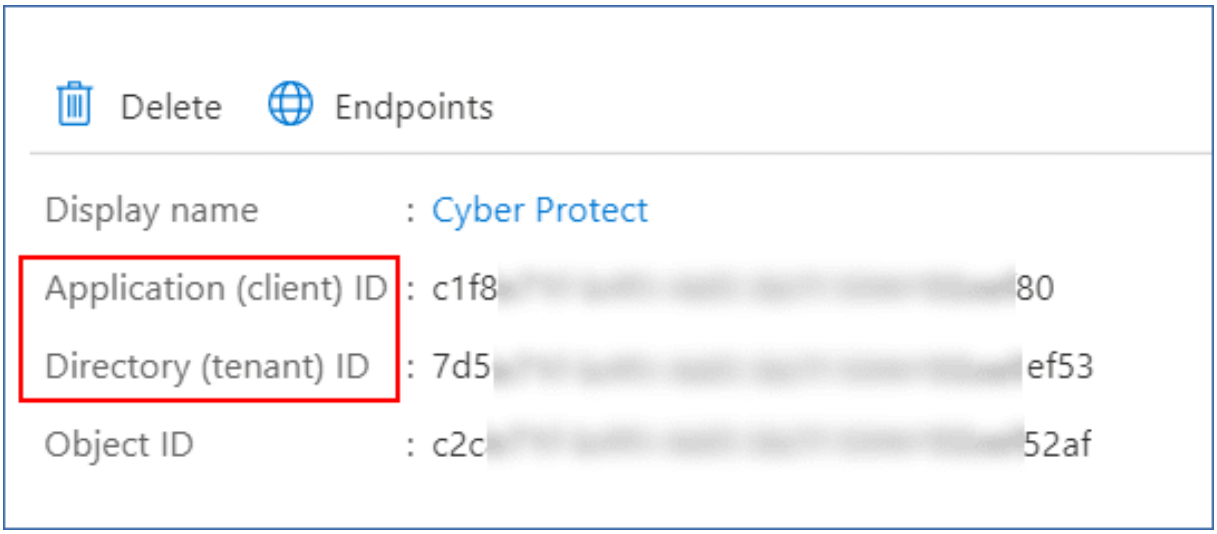
Untuk membuat aplikasi di pusat admin Entra

1. Masuk ke Pusat admin Entra sebagai Administrator.
2. Navigasi ke **Azure Active Directory** > **Registrasi apl**, kemudian klik **Registrasi baru**.

© Acronis International GmbH, 2003-2024

3. Tentukan nama untuk aplikasi kustom Anda, misalnya, Cyber Protection.
4. Dalam **jenis Dukungan Akun**, pilih **Akun di direktori organisasi ini saja**.
5. Klik **Daftar**.

Aplikasi Anda sekarang sedang dibuat. Di pusat admin Entra, navigasikan ke halaman **Ikhtisar** aplikasi dan periksa ID aplikasi (klien) dan direktori ID (penyewa) Anda.



Untuk informasi lebih lanjut mengenai cara membuat aplikasi di pusat admin Entra, lihat dokumentasi Microsoft.

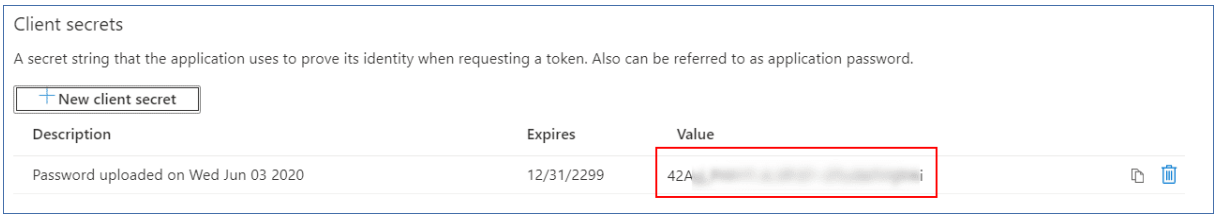
Untuk memberi aplikasi Anda izin API yang dibutuhkan

1. Di pusat admin Entra, navigasi ke **izin API** aplikasi, kemudian klik **Tambah izin**.
2. Pilih tab **API yang digunakan organisasi saya**, lalu cari **Office 365 Exchange Online**.
3. Klik **Office 365 Exchange Online**, lalu klik **Izin aplikasi**.
4. Pilih kotak centang **full_access_as_app**, dan klik **Tambah izin**.
5. Di **Izin API**, klik **Tambah izin**.
6. Pilih **Microsoft Graph**.
7. Pilih **Izin Aplikasi**.
8. Perluas tab **Direktori**, kemudian pilih kotak centang **Directory.Read.All**. Klik **Tambah izin**.
9. Periksa semua izin, kemudian klik **Berikan persetujuan admin untuk <nama aplikasi Anda>**.
10. Konfirmasi pilihan Anda dengan mengklik **Iya**.

Untuk membuat rahasia aplikasi

1. Di pusat admin Entra, navigasi ke **Sertifikat & rahasia** aplikasi Anda > **Rahasia klien baru**.
2. Dalam kotak dialog yang terbuka, pilih Kedaluwarsa: **Jangan pernah**, kemudian klik **Tambah**.
3. Periksa rahasia aplikasi dalam bidang **Nilai** dan pastikan Anda mengingatnya.

© Acronis International GmbH, 2003-2024



Untuk informasi lebih lanjut mengenai rahasia aplikasi, lihat dokumentasi Microsoft.

Mengubah kredensial akses Microsoft 365

Anda dapat mengubah kredensial akses untuk Microsoft 365 tanpa menginstal ulang agen.

Untuk mengubah kredensial akses Microsoft 365

1. Klik **Perangkat** > **Microsoft Office 365 (Agen lokal)**.
2. Pilih organisasi Microsoft 365.
3. Klik **Tentukan kredensial**.
4. Masukkan ID aplikasi, rahasia aplikasi, dan ID penyewa Microsoft 365 Anda. Untuk informasi lebih lanjut tentang cara menemukannya, lihat "Mendapatkan ID aplikasi dan rahasia aplikasi" (hlm. 601).
5. Klik **OK**.

Melindungi kotak surat Exchange Online

Apa saja item yang dapat dicadangkan?

Anda dapat mencadangkan kotak surat pengguna dan kotak surat bersama. Kotak surat grup dan kotak surat arsip (**Arsip Di Tempat**) tidak dapat dicadangkan.

Apa saja item yang dapat dipulihkan?

Item berikut dapat dipulihkan dari cadangan kotak surat:

- Kotak surat
- Folder Email
- Pesan email
- Acara kalender
- Tugas
- Kontak
- Entri jurnal
- Catatan

Anda dapat menggunakan pencarian untuk menemukan item.

© Acronis International GmbH, 2003-2024

Ketika kotak surat dipulihkan ke kotak surat yang ada, item yang ada dengan ID yang sama akan ditimpa.

Pemulihan item kotak surat tidak menimpa apa pun. Sebaliknya, jalur lengkap ke item kotak surat dibuat kembali di folder target.

Memilih kotak surat Microsoft 365

Pilih kotak surat seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Untuk memilih kotak surat

1. Klik **Microsoft Office 365 (Agen lokal)**.
2. Pilih kotak surat yang ingin Anda cadangkan.
3. Klik **Cadangkan**.

Memulihkan kotak surat dan item kotak surat

Memulihkan kotak surat

1. Klik **Microsoft Office 365 (Agen lokal)**.
2. Pilih kotak surat untuk memulihkan, lalu klik **Pemulihan**.
   Anda dapat mencari kotak surat berdasarkan nama. Wildcard tidak didukung.
   Jika kotak surat dihapus, pilih kotak surat pada tab Penyimpanan cadangan, lalu klik **Tampilkan cadangan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
4. Klik **Pulihkan** > **Kotak surat**.
5. Di **Kotak surat target**, lihat, ubah, atau tentukan kotak surat target.
   Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada, Anda harus menentukan kotak surat target.
6. Klik **Mulai pemulihan**.

Memulihkan item kotak surat

1. Klik **Microsoft Office 365 (Agen lokal)**.
2. Pilih kotak surat yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   Anda dapat mencari kotak surat berdasarkan nama. Wildcard tidak didukung.
   Jika kotak surat dihapus, pilih kotak surat pada tab Penyimpanan cadangan, lalu klik **Tampilkan cadangan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
4. Klik **Pulihkan** > **Pesan Email**.
5. Pilih item yang ingin Anda pulihkan.

© Acronis International GmbH, 2003-2024

Opsi pencarian berikut tersedia. Wildcard tidak didukung.

- Untuk pesan email: cari berdasarkan subjek, pengirim, penerima, nama lampiran, dan tanggal.
- Untuk acara: cari berdasarkan judul dan tanggal.
- Untuk tugas: cari berdasarkan subjek dan tanggal.
- Untuk kontak: cari berdasarkan nama, alamat email, dan nomor telepon.

Ketika pesan email dipilih, Anda dapat mengklik **Tampilkan konten** untuk melihat kontennya, termasuk lampiran.

Catatan
Klik nama file terlampir untuk mengunduhnya.

Ketika pesan email dipilih, Anda dapat mengklik **Kirim sebagai surel** untuk mengirim pesan ke alamat email. Pesan dikirim dari alamat email akun administrator Anda.

Untuk dapat memilih folder, klik ikon "pulihkan folder":

6. Klik **Pulihkan**.
7. Di **Kotak surat target**, lihat, ubah, atau tentukan kotak surat target.
   Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada, Anda harus menentukan kotak surat target.
8. Klik **Mulai pemulihan**.
9. Konfirmasi keputusan Anda.

Item kotak surat selalu dipulihkan ke folder **Item yang dipulihkan** dari kotak surat target.

Menggunakan versi awan Agen untuk Microsoft 365

Menambahkan organisasi Microsoft 365

Administrator dapat menambahkan satu atau beberapa organisasi Microsoft 365 ke penyewa pelanggan atau unit.

Administrator perusahaan menambahkan organisasi ke penyewa pelanggan. Administrator unit dan administrator pelanggan yang menjabat di tingkat unit menambahkan organisasi ke unit.

Untuk menambahkan organisasi Microsoft 365

1. Tergantung di mana Anda perlu menambahkan organisasi, masuk ke konsol Cyber Protect sebagai administrator perusahaan atau administrator unit.
2. [Untuk administrator perusahaan yang menjabat di tingkat unit] Di portal manajemen, navigasikan ke unit yang diinginkan.
3. Klik **Perangkat** > **Tambah** > **Microsoft 365 Business**.
   Perangkat lunak mengarahkan Anda ke halaman masuk Microsoft 365.
4. Masuk dengan kredensial administrator global Office 365.

© Acronis International GmbH, 2003-2024

Microsoft 365 menampilkan daftar izin yang diperlukan untuk mencadangkan dan memulihkan data organisasi Anda.

5. Konfirmasi bahwa Anda memberi izin ini untuk layanan Cyber Protection.

Akibatnya, organisasi Microsoft 365 Anda muncul di bawah tab **Perangkat** di konsol Cyber Protect.

Tips berguna

- Agen awan melakukan sinkronisasi dengan Microsoft 365 setiap 24 jam, dimulai sejak organisasi ditambahkan ke layanan Cyber Protection. Jika Anda menambah atau menghapus pengguna, grup, atau situs, Anda tidak akan melihat perubahan ini di konsol Cyber Protect dengan segera. Untuk segera menyinkronkan perubahan, pilih organisasi pada halaman **Microsoft 365**, lalu klik **Menyegarkan**.

  Untuk informasi lebih lanjut tentang menyinkronkan sumber daya organisasi Microsoft 365 dan konsol Cyber Protect, lihat "Menemukan sumber daya Microsoft 365" (hlm. 608).
- Jika Anda menerapkan rencana proteksi pada **Semua pengguna**, **Semua grup**, atau grup **Semua situs**, item yang baru ditambahkan akan disertakan dalam cadangan hanya setelah sinkronisasi.
- Berdasarkan kebijakan Microsoft, ketika pengguna, grup, atau situs dihapus dari antarmuka pengguna grafis Microsoft 365, semuanya akan tetap tersedia melalui API selama beberapa hari. Selama periode ini, item yang dihapus tidak aktif (berwarna abu-abu) di konsol Cyber Protect dan tidak dicadangkan. Saat item yang dihapus menjadi tidak tersedia melalui API, item tersebut menghilang dari konsol Cyber Protect. Cadangannya (jika ada) dapat ditemukan di **Penyimpanan cadangan** > **Cadangan aplikasi awan**.

Pengelolaan organisasi Microsoft 365 yang ditambahkan pada tingkat berbeda

Administrator perusahaan memiliki akses penuh ke organisasi Microsoft 365 yang ditambahkan ke tingkat penyewa pelanggan.

Administrator perusahaan memiliki akses terbatas ke organisasi yang ditambahkan ke suatu unit. Di organisasi tersebut, ditunjukkan dengan nama unit di dalam kurung, administrator perusahaan dapat melakukan hal berikut:

- Memulihkan data dari cadangan.

  Administrator perusahaan dapat memulihkan data ke semua organisasi dalam penyewa, terlepas dari tingkat organisasi tersebut ditambahkan.
- Menelusuri cadangan dan titik pemulihan di cadangan.
- Menghapus cadangan dan titik pemulihan di cadangan.
- Melihat peringatan dan aktivitas.

Administrator perusahaan, saat bekerja di tingkat penyewa pelanggan, tidak dapat melakukan hal berikut:

© Acronis International GmbH, 2003-2024

- Menambahkan organisasi Microsoft 365 ke unit.
- Menghapus organisasi Microsoft 365 dari unit.
- Menyinkronkan organisasi Microsoft 365 yang ditambahkan ke suatu unit.
- Melihat, membuat, mengedit, menghapus, menerapkan, menjalankan, atau membatalkan rencana proteksi untuk item data di organisasi Microsoft 365 yang ditambahkan ke suatu unit.

Administrator unit dan administrator perusahaan yang bekerja di tingkat unit memiliki akses penuh ke organisasi yang ditambahkan ke suatu unit. Namun, mereka tidak memiliki akses ke sumber daya dari penyewa pelanggan induk, termasuk rencana proteksi yang dibuat di dalamnya.

Menghapus organisasi Microsoft 365

Menghapus organisasi Microsoft 365 tidak memengaruhi cadangan data organisasi yang ada. Jika Anda tidak membutuhkan cadangan ini lagi, hapus terlebih dahulu, lalu hapus organisasi Microsoft 365. Jika tidak, cadangan masih akan menggunakan ruang penyimpanan awan yang mungkin dikenai biaya.

Untuk informasi lebih lanjut tentang cara menghapus cadangan, lihat "Untuk menghapus cadangan atau arsip cadangan" (hlm. 532).

Untuk menghapus organisasi Microsoft 365

1. Bergantung pada tempat organisasi ditambahkan, masuk ke konsol Cyber Protect sebagai administrator perusahaan atau administrator unit.
2. [Untuk administrator perusahaan yang menjabat di tingkat unit] Di portal manajemen, navigasikan ke unit yang diinginkan.
3. Buka **Perangkat** > **Microsoft 365.**
4. Pilih organisasi, lalu klik **Hapus grup**.

Akibatnya, rencana pencadangan yang diterapkan pada grup ini akan dicabut.

Namun, Anda juga harus mencabut hak akses aplikasi Layanan Pencadangan ke data organisasi Microsoft 365 secara manual.

Untuk mencabut hak akses

1. Masuk ke Microsoft 365 dalam administrator global.
2. Buka **Pusat Admin** > **Azure Active Directory** > **Aplikasi perusahaan** > **Semua aplikasi**.
3. Pilih aplikasi **Layanan Pencadangan** dan telusuri lebih lanjut.
4. Buka tab **Properti**, lalu klik **Hapus** pada panel tindakan.
5. Konfirmasi operasi penghapusan.

Akibatnya, hak akses ke data organisasi Microsoft 365 akan dicabut dari aplikasi Layanan Pencadangan.

© Acronis International GmbH, 2003-2024

Menemukan sumber daya Microsoft 365

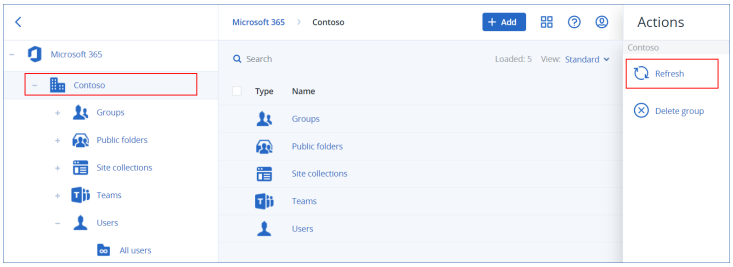
Saat Anda menambahkan organisasi Microsoft 365 ke layanan Cyber Protection, sumber daya di organisasi ini, seperti kotak surat, penyimpanan OneDrive, Microsoft Teams, dan situs SharePoint, akan disinkronkan ke konsol Cyber Protect. Operasi ini disebut penemuan dan dicatat di **Pemantauan** > **Aktivitas**.

Setelah operasi penemuan selesai, Anda dapat melihat sumber daya organisasi Microsoft 365 pada tab **Perangkat** > **Microsoft 365** di konsol Cyber Protect, dan Anda dapat menerapkan rencana pencadangan di sana.

Operasi penemuan otomatis berjalan sekali sehari untuk menjaga agar daftar sumber daya di konsol Cyber Protect tetap mutakhir. Anda juga dapat menyinkronkan daftar ini sesuai permintaan, dengan menjalankan kembali operasi penemuan secara manual.

Untuk menjalankan kembali operasi penemuan secara manual

1. Di konsol Cyber Protect, buka **Perangkat** > **Microsoft 365**.
2. Pilih organisasi Microsoft 365 Anda, lalu, di panel **Tindakan**, klik **Menyegarkan**.



Catatan
Anda dapat menjalankan operasi penemuan secara manual hingga 10 kali per jam. Ketika jumlah ini tercapai, operasi yang diizinkan diatur ulang menjadi satu kali per jam, dan kemudian setiap jam proses tambahan tersedia, hingga total 10 proses per jam tercapai lagi.

Mengatur frekuensi pencadangan Microsoft 365

Secara default, pencadangan Microsoft 365 berjalan sekali sehari dan tidak ada opsi penjadwalan tambahan yang tersedia.

Jika paket Cadangan Tingkat Lanjut diaktifkan di penyewa Anda, Anda dapat mengonfigurasi pencadangan yang lebih sering. Anda dapat memilih jumlah cadangan per hari, namun Anda tidak dapat mengonfigurasi waktu mulai pencadangan. Pencadangan dimulai secara otomatis pada interval perkiraan yang bergantung pada beban saat ini dari agen awan, yang melayani banyak pelanggan di pusat data. Ini memastikan pemuatan yang merata di siang hari, dan kualitas layanan yang sama untuk semua pelanggan.

Opsi berikut tersedia.

© Acronis International GmbH, 2003-2024

Opsi penjadwalan	Perkiraan interval antara setiap pencadangan
Sekali sehari	24 jam
Dua kali sehari (default)	12 jam
3 kali sehari	8 jam
6 kali sehari	4 jam

Catatan
Bergantung pada beban pada agen awan dan kemungkinan pelambatan di sisi Microsoft 365, pencadangan mungkin akan dimulai lebih lambat dari yang dijadwalkan atau memerlukan waktu lebih lama untuk menyelesaikannya. Jika pencadangan memerlukan waktu lebih lama dari interval rata-rata antara dua pencadangan, pencadangan berikutnya akan dijadwalkan ulang, yang mungkin akan menghasilkan lebih sedikit cadangan per hari daripada yang dipilih. Sebagai contoh, hanya dua cadangan per hari yang mungkin dapat diselesaikan, meskipun Anda memilih enam cadangan per hari.

Pencadangan kotak surat grup hanya dapat dilakukan sekali sehari.

Melindungi data Exchange Online

Apa saja item yang dapat dicadangkan?

Anda dapat mencadangkan kotak surat pengguna, kotak surat bersama, dan kotak surat grup. Secara opsional, Anda dapat memilih untuk mencadangkan kotak surat arsip online (**Arsip Di Tempat**) dari kotak surat yang dipilih.

Mulai versi 8.0 layanan Cyber Protection, Anda dapat mencadangkan folder umum. Jika organisasi Anda ditambahkan ke layanan Cyber Protection sebelum rilis versi 8.0, Anda perlu menambahkan kembali organisasi untuk mendapatkan fungsi ini. Jangan hapus organisasi, cukup ulangi langkah-langkah yang dijelaskan dalam "Menambahkan organisasi Microsoft 365" (hlm. 605). Hasilnya, layanan Cyber Protection mendapatkan izin untuk menggunakan API yang sesuai.

Apa saja item yang dapat dipulihkan?

Item berikut dapat dipulihkan dari cadangan kotak surat:

- Kotak surat
- Folder Email
- Pesan email
- Acara kalender
- Tugas
- Kontak

© Acronis International GmbH, 2003-2024

- Entri jurnal
- Catatan

Item berikut dapat dipulihkan dari cadangan folder umum:

- Subfolder
- Kiriman
- Pesan email

Anda dapat menggunakan pencarian untuk menemukan item.

Ketika memulihkan kotak surat, item kotak surat, folder umum, dan item folder umum, Anda dapat memilih apakah item di lokasi target akan ditimpa atau tidak.

Memilih kotak surat

Pilih kotak surat seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Untuk memilih kotak surat Exchange Online

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data penggunanya ingin Anda cadangkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk mencadangkan kotak surat semua pengguna dan semua kotak surat bersama (termasuk kotak surat yang akan dibuat di waktu mendatang), perluas simpul **Pengguna**, pilih **Semua pengguna**, lalu klik **Cadangan grup**.
   - Untuk mencadangkan pengguna individual atau kotak surat bersama, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang kotak suratnya ingin Anda cadangkan, lalu klik **Cadangkan**.
   - Untuk mencadangkan semua kotak surat grup (termasuk kotak surat grup yang akan dibuat di waktu mendatang), perluas simpul **Grup**, pilih **Semua grup**, lalu klik **Cadangan grup**.
   - Untuk mencadangkan kotak surat grup individual, perluas simpul **Grup**, pilih **Semua grup**, pilih grup yang kotak suratnya ingin Anda cadangkan, lalu klik **Cadangkan**.

     Catatan
     Agen untuk Microsoft 365 awan menggunakan akun dengan hak yang sesuai untuk mengakses kotak surat grup. Jadi, untuk mencadangkan kotak surat grup, setidaknya salah satu pemilik grup harus merupakan pengguna Microsoft 365 berlisensi dengan kotak surat. Jika grup bersifat pribadi atau dengan keanggotaan tersembunyi, pemilik juga harus menjadi anggota grup.
4. Pada panel rencana proteksi:

© Acronis International GmbH, 2003-2024

- Pastikan item **Kotak surat Microsoft 365** dipilih pada **Untuk dicadangkan**.

  Jika beberapa pengguna yang dipilih secara individual tidak memiliki layanan Exchange yang disertakan dalam paket Microsoft 365 mereka, Anda tidak dapat memilih opsi ini.

  Jika beberapa pengguna yang dipilih untuk cadangan grup tidak memiliki layanan Exchange yang disertakan dalam paket Microsoft 365 mereka, Anda dapat memilih opsi ini, tetapi rencana proteksi tidak akan diterapkan ke pengguna tersebut.
- Jika Anda tidak ingin mencadangkan kotak surat arsip, nonaktifkan tombol **Kotak surat arsip**.

Memilih folder umum

Pilih folder umum seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang tepat.

Catatan
Folder umum menggunakan lisensi dari kuota cadangan Anda untuk kursi Microsoft 365.

Untuk memilih folder umum Exchange Online

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, perluas organisasi yang datanya ingin Anda cadangkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Folder umum**, lalu pilih **Semua folder umum**.
4. Lakukan salah satu langkah berikut:
   - Untuk mencadangkan semua folder umum (termasuk folder umum yang akan dibuat di masa mendatang), klik **Cadangan grup**.
   - Untuk mencadangkan folder umum individual, pilih folder umum yang ingin Anda cadangkan, lalu klik **Cadangkan**.
5. Pada panel rencana proteksi, pastikan item **kotak surat Microsoft 365** dipilih di **Apa yang harus dicadangkan**.

Memulihkan kotak surat dan item kotak surat

Memulihkan kotak surat

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk memulihkan kotak surat pengguna, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang kotak suratnya ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Untuk memulihkan kotak surat bersama, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih kotak surat bersama yang ingin Anda pulihkan, lalu klik **Pemulihan**.

© Acronis International GmbH, 2003-2024

- Untuk memulihkan kotak surat grup, perluas simpul **Grup**, pilih **Semua grup**, pilih kotak surat grup yang ingin Anda pulihkan, lalu klik **Pemulihan**.
- Jika pengguna, grup, atau kotak surat bersama dihapus, pilih item tersebut di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.

Anda dapat mencari pengguna dan grup berdasarkan nama. Wildcard tidak didukung.

4. Pilih titik pemulihan.

Catatan
Untuk hanya melihat titik pemulihan yang berisi kotak surat, pilih **Kotak Surat** di **Filter berdasarkan konten**.

5. Klik **Pulihkan** > **Keseluruhan kotak surat**.
6. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target.
   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
7. Di **Pulihkan ke kotak surat**, lihat, ubah, atau tentukan kotak surat target.
   Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan kotak surat target.
   Anda tidak dapat membuat kotak surat target baru selama pemulihan. Untuk memulihkan kotak surat ke yang baru, pertama-tama Anda perlu membuat kotak surat target di organisasi Microsoft 365 yang diinginkan, dan kemudian biarkan agen cloud melakukan sinkronisasi perubahan. Agen cloud secara otomatis melakukan sinkronisasi dengan Microsoft 365 setiap 24 jam. Untuk mensinkronkan perubahan dengan segera, di konsol Cyber Protect, pilih organisasi di halaman **Microsoft 365**, dan kemudian klik **Refresh**.
8. Klik **Mulai pemulihan**.
9. Pilih salah satu opsi penimpaan:
   - **Timpa item yang ada**
   - **Jangan timpa item yang ada**
10. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Memulihkan item kotak surat

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk memulihkan item dari kotak surat pengguna, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna dengan kotak surat yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.

© Acronis International GmbH, 2003-2024

- Untuk memulihkan item dari kotak surat bersama, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih kotak surat bersama yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
- Untuk memulihkan item dari kotak surat grup, perluas simpul **Grup**, pilih **Semua grup**, pilih grup dengan kotak surat yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
- Jika pengguna, grup, atau kotak surat bersama dihapus, pilih item tersebut di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.

Anda dapat mencari pengguna dan grup berdasarkan nama. Wildcard tidak didukung.

4. Pilih titik pemulihan.

   Catatan
   Untuk hanya melihat titik pemulihan yang berisi kotak surat, pilih **Kotak Surat** di **Filter berdasarkan konten**.

5. Klik **Pulihkan** > **Pesan Email**.
6. Jelajahi ke folder yang diperlukan atau gunakan pencarian untuk mendapatkan daftar item yang diperlukan.

   Opsi pencarian berikut tersedia. Wildcard tidak didukung.
   - Untuk pesan email: cari berdasarkan subjek, pengirim, penerima, nama lampiran, dan tanggal. Anda dapat memilih tanggal mulai atau tanggal berakhir (keduanya bersifat inklusif), atau kedua tanggal untuk melakukan pencarian dalam suatu rentang waktu.
   - Untuk acara: cari berdasarkan judul dan tanggal.
   - Untuk tugas: cari berdasarkan subjek dan tanggal.
   - Untuk kontak: cari berdasarkan nama, alamat email, dan nomor telepon.
7. Pilih item yang ingin Anda pulihkan. Untuk dapat memilih folder, klik ikon "pulihkan folder":

   Anda tidak dapat membuat kotak surat target baru selama pemulihan. Untuk memulihkan item kotak surat baru ke kotak surat baru, pertama-tama Anda perlu membuat item kotak surat target baru di organisasi Microsoft 365, dan kemudian membiarkan agen cloud mensinkronisasikan perubahan tersebut. Agen cloud secara otomatis melakukan sinkronisasi dengan Microsoft 365 setiap 24 jam. Untuk mensinkronkan perubahan dengan segera, di konsol Cyber Protect, pilih organisasi di halaman **Microsoft 365**, dan kemudian klik **Refresh**.

   Selain itu, Anda dapat melakukan hal-hal berikut:
   - Ketika sebuah item dipilih, klik **Tampilkan konten** untuk melihat kontennya, termasuk lampiran. Klik nama file yang dilampirkan untuk mengunduhnya.
   - Ketika pesan email atau item kalender dipilih, klik **Kirim sebagai surel** untuk mengirim item ke alamat email yang ditentukan. Anda dapat memilih pengirim dan menulis teks yang akan ditambahkan ke item yang diteruskan.
   - Hanya jika cadangan tidak dienkripsi, gunakan pencarian, dan pilih satu item pada hasil pencarian: klik **Tampilkan versi** untuk memilih versi item yang akan dipulihkan. Anda dapat

© Acronis International GmbH, 2003-2024

memilih versi yang dicadangkan, yang lebih baru atau lebih lama dari titik pemulihan yang dipilih.

8. Klik **Pulihkan**.
9. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target.
   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
10. Di **Pulihkan ke kotak surat**, lihat, ubah, atau tentukan kotak surat target.
    Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan kotak surat target.
11. [Hanya ketika memulihkan ke pengguna atau kotak surat bersama] Di **Jalur**, lihat atau ubah folder target di kotak surat target. Secara default, folder **Pulihkan item** dipilih.
    Item kotak surat grup selalu dipulihkan ke folder **Kotak masuk**.
12. Klik **Mulai pemulihan**.
13. Pilih salah satu opsi penimpaan:
    - **Timpa item yang ada**
    - **Jangan timpa item yang ada**
14. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Memulihkan seluruh kotak surat ke file data PST

Catatan
Arsip di tempat tidak dapat dipulihkan sebagai bagian dari pemulihan ke file PST. Untuk memulihkan arsip di tempat bersama dengan kotak surat, lihat "Memulihkan kotak surat" (hlm. 611).

Untuk memulihkan kotak surat

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk memulihkan kotak surat pengguna ke file data PST, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih kotak surat yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Untuk memulihkan kotak surat bersama ke file data PST, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih kotak surat yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Untuk memulihkan kotak surat grup ke file data PST, perluas simpul **Grup**, pilih **Semua grup**, pilih grup yang kotak suratnya ingin Anda pulihkan, lalu klik **Pemulihan**.

   Anda dapat mencari pengguna dan grup berdasarkan nama. Wildcard tidak didukung.
   Jika pengguna, grup, atau file data Outlook bersama telah dihapus, pilih item di bagian **Pencadangan aplikasi Awan** pada tab Penyimpanan cadangan, lalu klik **Tampilkan cadangan**.

© Acronis International GmbH, 2003-2024

4. Klik **Pulihkan** > **Sebagai file PST**.
5. Atur kata sandi untuk mengenkripsi arsip dengan file PST.
   Kata sandi harus berisi setidaknya satu simbol.
6. Konfirmasi kata sandi dan klik **Selesai**.
7. Item kotak surat yang dipilih akan dipulihkan sebagai file data PST dan diarsipkan dalam format ZIP. Ukuran maksimum satu file PST dibatasi hingga 2 GB, jika data yang Anda pulihkan melebihi 2 GB, maka akan dibagi menjadi beberapa file PST. Arsip ZIP akan dilindungi dengan kata sandi yang Anda atur.
8. Anda akan menerima surel dengan tautan ke arsip ZIP yang berisi file PST yang dibuat.
9. Administrator akan menerima surel pemberitahuan bahwa Anda telah melakukan prosedur pemulihan.

Catatan
Pemulihan kotak surat ke file PST dapat memakan banyak waktu, karena tidak hanya melibatkan transfer data, tetapi juga transformasi data menggunakan algoritme kompleks.

Untuk mengunduh arsip dengan file PST dan menyelesaikan pemulihan

1. Lakukan salah satu langkah berikut:
   - Untuk mengunduh arsip dari surel, ikuti tautan **Unduh file**.
     Arsip tersedia untuk diunduh dalam waktu 24 jam. Jika tautan kedaluwarsa, ulangi prosedur pemulihan.
   - Untuk mengunduh arsip dari konsol Cyber Protect:
     a. Buka **Penyimpanan Cadangan** > **file PST**.
     b. Pilih arsip terbaru yang disorot.
     c. Klik **Unduh** di panel kanan.

   Arsip akan diunduh ke direktori unduhan default di komputer Anda.
2. Ekstraksi file PST dari arsip menggunakan kata sandi yang Anda atur untuk mengenkripsi arsip.
3. Buka file PST dengan Microsoft Outlook.
   File PST hasilnya bisa jauh lebih kecil ukurannya dibandingkan kotak surat asli. Itu adalah hal yang normal.

   Penting
   Jangan mengimpor file ini ke Microsoft Outlook menggunakan **Wizard Impor dan Ekspor**.
   Buka file dengan mengeklik ganda atau klik kanan dan pilih **Buka dengan...** > **Microsoft Outlook** di menu konteks.

© Acronis International GmbH, 2003-2024

Memulihkan item kotak surat ke file PST

Catatan
Arsip di tempat tidak dapat dipulihkan sebagai bagian dari pemulihan ke file PST. Untuk memulihkan arsip di tempat bersama dengan kotak surat, lihat "Memulihkan kotak surat" (hlm. 611).

Untuk memulihkan item kotak surat

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk memulihkan item dari kotak surat pengguna, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna dengan kotak surat yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Untuk memulihkan item dari kotak surat bersama, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih kotak surat bersama yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Untuk memulihkan item dari kotak surat grup, perluas simpul **Grup**, pilih **Semua grup**, pilih grup dengan kotak surat yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Jika pengguna, grup, atau kotak surat bersama dihapus, pilih item tersebut di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.

   Anda dapat mencari pengguna dan grup berdasarkan nama. Wildcard tidak didukung.
4. Klik **Pulihkan** > **Pesan Email**.
5. Jelajahi ke folder yang diperlukan atau gunakan pencarian untuk mendapatkan daftar item yang diperlukan.

   Opsi pencarian berikut tersedia. Wildcard tidak didukung.
   - Untuk pesan email: cari berdasarkan subjek, pengirim, penerima, nama lampiran, dan tanggal.
   - Untuk acara: cari berdasarkan judul dan tanggal.
   - Untuk tugas: cari berdasarkan subjek dan tanggal.
   - Untuk kontak: cari berdasarkan nama, alamat email, dan nomor telepon.
6. Pilih item yang ingin Anda pulihkan. Untuk dapat memilih folder, klik ikon "pulihkan folder":

   Selain itu, Anda dapat melakukan hal-hal berikut:
   - Ketika item dipilih, klik **Tampilkan konten** untuk melihat kontennya, termasuk lampiran. Klik nama file terlampir untuk mengunduhnya.

© Acronis International GmbH, 2003-2024

- Ketika pesan email atau item kalender dipilih, klik **Kirim sebagai surel** untuk mengirim item ke alamat email yang ditentukan. Anda dapat memilih pengirim dan menulis teks yang akan ditambahkan ke item yang diteruskan.
- Hanya jika cadangan tidak dienkripsi, gunakan pencarian, dan pilih satu item pada hasil pencarian: klik **Tampilkan versi** untuk memilih versi item yang akan dipulihkan. Anda dapat memilih versi yang dicadangkan, yang lebih baru atau lebih lama dari titik pemulihan yang dipilih.

7. Klik **Pulihkan sebagai file PST**.
8. Atur kata sandi untuk mengenkripsi arsip dengan file PST.
   Kata sandi harus berisi setidaknya satu simbol.
9. Konfirmasi kata sandi dan klik **SELESAI**.

Item kotak surat yang dipilih akan dipulihkan sebagai file data PST dan diarsipkan dalam format ZIP. Ukuran maksimum satu file PST dibatasi hingga 2 GB, jika data yang Anda pulihkan melebihi 2 GB, maka akan dibagi menjadi beberapa file PST. Arsip ZIP akan dilindungi dengan kata sandi yang Anda atur.

Anda akan menerima surel dengan tautan ke arsip ZIP yang berisi file PST yang dibuat.

Administrator akan menerima surel pemberitahuan bahwa Anda telah melakukan prosedur pemulihan.

Untuk mengunduh arsip dengan file PST dan menyelesaikan pemulihan

1. Lakukan salah satu langkah berikut:
   - Untuk mengunduh arsip dari surel, ikuti tautan **Unduh file**.
     Arsip tersedia untuk diunduh dalam waktu 24 jam. Jika tautan kedaluwarsa, ulangi prosedur pemulihan.
   - Untuk mengunduh arsip dari konsol Cyber Protect:
     a. Buka **Penyimpanan Cadangan** > **file PST**.
     b. Pilih arsip terbaru yang disorot.
     c. Klik **Unduh** di panel kanan.

   Arsip akan diunduh ke direktori unduhan default di komputer Anda.
2. Ekstraksi file PST dari arsip menggunakan kata sandi yang Anda atur untuk mengenkripsi arsip.
3. Buka file PST dengan Microsoft Outlook.
   File PST hasilnya bisa jauh lebih kecil ukurannya dibandingkan kotak surat asli. Itu adalah hal yang normal.

Penting
Jangan mengimpor file ini ke Microsoft Outlook menggunakan **Wizard Impor dan Ekspor**.
Buka file dengan mengeklik ganda atau klik kanan dan pilih **Buka dengan...** > **Microsoft Outlook** di menu konteks.

© Acronis International GmbH, 2003-2024

Memulihkan folder umum dan item folder

Untuk memulihkan folder umum atau item folder umum, setidaknya satu administrator organisasi Microsoft 365 target harus memiliki hak **Pemilik** untuk folder umum target. Jika pemulihan gagal dengan kesalahan tentang akses ditolak, tetapkan hak ini di properti folder target, pilih organisasi target di konsol Cyber Protect, klik **Menyegarkan**, lalu ulangi pemulihan.

Untuk memulihkan folder umum atau item folder

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, perluas organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Perluas simpul **Folder umum**, pilih **Semua folder umum**, pilih folder umum yang ingin Anda pulihkan atau yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Jika folder umum dihapus, pilih di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tampilkan cadangan**.

   Anda dapat mencari folder umum berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.
5. Klik **Pulihkan data**.
6. Jelajahi ke folder yang diperlukan atau gunakan pencarian untuk mendapatkan daftar item yang diperlukan.

   Anda dapat mencari pesan email dan postingan berdasarkan subjek, pengirim, penerima, dan tanggal. Wildcard tidak didukung.
7. Pilih item yang ingin Anda pulihkan. Untuk dapat memilih folder, klik ikon "pulihkan folder":

   Selain itu, Anda dapat melakukan hal-hal berikut:
   - Ketika pesan email atau postingan dipilih, klik **Tampilkan konten** untuk melihat kontennya, termasuk lampiran. Klik nama file terlampir untuk mengunduhnya.
   - Ketika pesan email atau postingan dipilih, klik **Kirim sebagai email** to untuk mengirim item ke alamat email yang ditentukan. Anda dapat memilih pengirim dan menulis teks yang akan ditambahkan ke item yang diteruskan.
   - Hanya jika cadangan tidak dienkripsi, gunakan pencarian, dan pilih satu item pada hasil pencarian: klik **Tampilkan versi** untuk memilih versi item yang akan dipulihkan. Anda dapat memilih versi yang dicadangkan, yang lebih baru atau lebih lama dari titik pemulihan yang dipilih.
8. Klik **Pulihkan**.
9. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target.

   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
10. Di **Pulihkan ke folder umum**, lihat, ubah, atau tentukan folder umum target.

© Acronis International GmbH, 2003-2024

Secara default, folder asli dipilih. Jika folder ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan folder target.

Anda tidak dapat membuat folder umum baru selama pemulihan. Untuk memulihkan folder umum ke yang baru, pertama-tama Anda perlu membuat folder umum target di organisasi Microsoft 365 yang diinginkan, dan kemudian membiarkan agen cloud mensinkronisasikan perubahan tersebut. Agen cloud secara otomatis melakukan sinkronisasi dengan Microsoft 365 setiap 24 jam. Untuk mensinkronkan perubahan dengan segera, di konsol Cyber Protect, pilih organisasi di halaman **Microsoft 365**, dan kemudian klik **Refresh**.

11. Di **Jalur**, lihat atau ubah subfolder target dalam folder umum target. Secara default, jalur asli akan dibuat kembali.
12. Klik **Mulai pemulihan**.
13. Pilih salah satu opsi penimpaan:

Opsi	Deskripsi
Timpa item yang ada	Semua file yang ada di lokasi tujuan akan ditimpa.
Jangan timpa item yang ada	Jika lokasi tujuan berisi file dengan nama yang sama, file tersebut tidak ditimpa dan file sumber tidak disimpan ke lokasi tujuan.

14. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Melindungi file OneDrive

Apa saja item yang dapat dicadangkan?

Anda dapat mencadangkan keseluruhan OneDrive, atau file dan folder individual.

Opsi terpisah dalam rencana pencadangan memungkinkan pencadangan buku catatan OneNote.

File dicadangkan bersama dengan izin berbaginya. Tingkat izin lanjutan (**Desain**, **Penuh**, **Kontribusi**) tidak dicadangkan.

Beberapa file mungkin berisi informasi sensitif dan aksesnya mungkin diblokir oleh aturan pencegahan kehilangan data (data loss prevention atau DLP) di Microsoft 365. File-file ini tidak dicadangkan dan tidak ada peringatan yang ditampilkan setelah operasi pencadangan selesai.

Pembatasan

Mencadangkan konten OneDrive tidak didukung untuk kotak surat bersama. Untuk mencadangkan konten ini, ubah kotak surat bersama menjadi akun pengguna biasa dan pastikan OneDrive diaktifkan untuk akun tersebut.

Apa saja item yang dapat dipulihkan?

Anda dapat memulihkan keseluruhan OneDrive maupun file atau folder apa pun yang dicadangkan.

© Acronis International GmbH, 2003-2024

Anda dapat menggunakan pencarian untuk menemukan item.

Anda dapat memilih untuk memulihkan izin atau membiarkan file menerima turunan izin dari folder tujuan pemulihan file.

Berbagi tautan untuk file dan folder tidak dapat dipulihkan.

Memilih file OneDrive

Pilih file seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Untuk memilih file OneDrive

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data penggunanya ingin Anda cadangkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk mencadangkan file semua pengguna (termasuk pengguna yang akan dibuat di waktu mendatang), perluas simpul **Pengguna**, pilih **Semua pengguna**, lalu klik **Cadangan grup**.
   - Untuk mencadangkan file pengguna individual, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang filenya ingin Anda cadangkan, lalu klik **Cadangkan**.
4. Pada panel rencana proteksi:
   - Pastikan item **OneDrive** dipilih di **Apa yang akan dicadangkan**.

     Jika beberapa pengguna yang dipilih secara individual tidak memiliki layanan OneDrive yang disertakan dalam paket Microsoft 365 mereka, Anda tidak dapat memilih opsi ini.

     Jika beberapa pengguna yang dipilih untuk cadangan grup tidak memiliki layanan OneDrive yang disertakan dalam paket Microsoft 365 mereka, Anda akan dapat memilih opsi ini, tetapi rencana proteksi tidak akan diterapkan ke pengguna tersebut.
   - Di **Item untuk dicadangkan**, lakukan salah satu hal berikut:
     - Simpan pengaturan default **[Semua]** (semua file).
     - Tentukan file dan folder untuk mencadangkan dengan menambahkan nama atau jalur mereka.

       Anda dapat menggunakan karakter wildcard (*, **, dan ?). Untuk informasi lebih lanjut tentang menentukan jalur dan menggunakan wildcard, lihat "Filter file".
     - Tentukan file dan folder yang akan dicadangkan dengan menjelajahi.

       Tautan **Jelajahi** hanya tersedia saat membuat rencana proteksi untuk pengguna tunggal.
   - [Opsional] Di **Item untuk dicadangkan**, klik **Tampilkan pengecualian** untuk menentukan file dan folder yang akan dilewati selama pencadangan.

     Pengecualian file akan mengesampingkan pemilihan file tersebut; yaitu jika Anda menentukan file yang sama di kedua bidang, file ini akan dilewati selama pencadangan.
   - [Opsional] Untuk mencadangkan buku catatan OneNote, aktifkan tombol **Sertakan OneNote**.

© Acronis International GmbH, 2003-2024

Memulihkan OneDrive dan file OneDrive

Memulihkan keseluruhan OneDrive

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang OneDrive-nya ingin Anda pulihkan, lalu klik **Pemulihan**.

   Jika pengguna dihapus, pilih pengguna di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.

   Anda dapat mencari pengguna berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.

   Catatan
   Untuk hanya melihat titik pemulihan yang berisi file OneDrive, pilih **OneDrive** di **Filter berdasarkan konten**.
5. Klik **Pulihkan** > **Keseluruhan OneDrive**.
6. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target.

   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.

   Anda tidak dapat membuat target OneDrive baru selama pemulihan. Untuk memulihkan OneDrive ke yang baru, pertama-tama Anda perlu membuat target OneDrive di organisasi Microsoft 365, dan kemudian membiarkan agen cloud melakukan sinkronisasi perubahan. Agen cloud secara otomatis melakukan sinkronisasi dengan Microsoft 365 setiap 24 jam. Untuk mensinkronkan perubahan dengan segera, di konsol Cyber Protect, pilih organisasi di halaman **Microsoft 365**, dan kemudian klik **Refresh**.
7. Di bagian **Pulihkan ke drive**, lihat, ubah, atau tentukan pengguna target.

   Secara default, pengguna asli dipilih. Jika pengguna ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan pengguna target.
8. Pilih apakah akan memulihkan izin berbagi untuk file.
9. Klik **Mulai pemulihan**.
10. Pilih salah satu opsi penimpaan:

Opsi	Deskripsi
Timpa file yang ada jika lebih lama	Jika ada file dengan nama yang sama di lokasi tujuan, dan lebih lama dari file sumber, file sumber akan disimpan di lokasi tujuan, menggantikan versi yang lebih lama.

© Acronis International GmbH, 2003-2024

Opsi	Deskripsi
Timpa file yang ada	Semua file yang ada di lokasi tujuan akan ditimpa, terlepas dari tanggal terakhir diubah.
Jangan timpa file yang ada	Jika ada file dengan nama yang sama di lokasi tujuan, tidak ada perubahan yang diterapkan padanya, dan file sumber tidak disimpan ke lokasi tujuan.

Catatan
Ketika memulihkan buku catatan OneNote, opsi **Timpa file yang ada jika lebih lama** dan **Timpa file yang ada** akan mengakibatkan penimpaan buku catatan OneNote yang ada.

11. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Memulihkan file OneDrive

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang file OneDrive-nya ingin Anda pulihkan, lalu klik **Pemulihan**.
   Jika pengguna dihapus, pilih pengguna di bagian **Cadangan Aplikasi Awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.
   Anda dapat mencari pengguna berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.

Catatan
Untuk hanya melihat titik pemulihan yang berisi file OneDrive, pilih **OneDrive** di **Filter berdasarkan konten**.

5. Klik **Pulihkan** > **File/folder**.
6. Jelajahi ke folder yang diperlukan atau gunakan pencarian untuk mendapatkan daftar file dan folder yang diperlukan.
7. Pilih file yang ingin Anda pulihkan.
   Jika cadangan tidak dienkripsi dan Anda memilih satu file, Anda dapat mengklik **Tampilkan versi** untuk memilih versi file yang akan dipulihkan. Anda dapat memilih versi yang dicadangkan, yang lebih baru atau lebih lama dari titik pemulihan yang dipilih.
8. Jika Anda ingin mengunduh suatu file, pilih file tersebut, klik **Unduh**, pilih lokasi untuk menyimpan file, lalu klik **Simpan**. Jika tidak, lewati langkah ini.
9. Klik **Pulihkan**.
10. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target.

© Acronis International GmbH, 2003-2024

Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.

Anda tidak dapat membuat OneDrive baru selama pemulihan. Untuk memulihkan file ke OneDrive baru, pertama-tama Anda perlu membuat target OneDrive di organisasi Microsoft 365 yang diinginkan, dan kemudian membiarkan agen cloud melakukan sinkronisasi perubahan. Agen cloud secara otomatis melakukan sinkronisasi dengan Microsoft 365 setiap 24 jam. Untuk mensinkronkan perubahan dengan segera, di konsol Cyber Protect, pilih organisasi di halaman **Microsoft 365**, dan kemudian klik **Refresh**.

11. Di bagian **Pulihkan ke drive**, lihat, ubah, atau tentukan pengguna target.

    Secara default, pengguna asli dipilih. Jika pengguna ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan pengguna target.
12. Di **Jalur**, lihat atau ubah folder target di pengguna target. Secara default, lokasi asli dipilih.
13. Pilih apakah akan memulihkan izin berbagi untuk file.
14. Klik **Mulai pemulihan**.
15. Pilih salah satu opsi penimpaan file:

Opsi	Deskripsi
Timpa file yang ada jika lebih lama	Jika ada file dengan nama yang sama di lokasi tujuan, dan lebih lama dari file sumber, file sumber akan disimpan di lokasi tujuan, menggantikan versi yang lebih lama.
Timpa file yang ada	Semua file yang ada di lokasi tujuan akan ditimpa, terlepas dari tanggal terakhir diubah.
Jangan timpa file yang ada	Jika ada file dengan nama yang sama di lokasi tujuan, tidak ada perubahan yang diterapkan padanya, dan file sumber tidak disimpan ke lokasi tujuan.

Catatan
Ketika memulihkan buku catatan OneNote, opsi **Timpa file yang ada jika lebih lama** dan **Timpa file yang ada** akan mengakibatkan penimpaan buku catatan OneNote yang ada.

16. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Melindungi situs SharePoint Online

Apa saja item yang dapat dicadangkan?

Anda dapat mencadangkan kumpulan situs klasik, situs grup (tim modern), dan situs komunikasi SharePoint. Selain itu, Anda dapat memilih masing-masing subsitus, daftar, dan pustaka untuk pencadangan.

Opsi terpisah dalam rencana pencadangan memungkinkan pencadangan buku catatan OneNote.

Item berikut *dilewati* selama pencadangan:

© Acronis International GmbH, 2003-2024

- Pengaturan situs **Tampilan dan Nuansa** (kecuali untuk **Judul, deskripsi, dan logo**).
- Komentar halaman situs dan pengaturan komentar halaman (komentar **Nyala**/**Mati**).
- Pengaturan situs **Fitur situs**.
- Halaman bagian web dan bagian web disematkan di halaman wiki (karena pembatasan API SharePoint Online).
- File yang diperiksa—file yang diperiksa secara manual untuk diedit dan semua file yang dibuat atau diunggah di perpustakaan, yang untuknya opsi **Memerlukan Pemeriksaan** diaktifkan. Untuk mencadangkan file-file ini, periksa dulu semuanya.
- Jenis kolom Data eksternal dan Metadata Terkelola.
- Kumpulan situs default "domain-my.sharepoint.com". Ini adalah kumpulan yang merupakan tempat semua file OneDrive pengguna situs.
- Isi kotak sampah.

Pembatasan

- Judul dan deskripsi situs/subsitus/daftar/kolom akan terpotong selama pencadangan jika ukuran judul/deskripsi lebih besar dari 10000 byte.
- Anda tidak dapat mencadangkan versi file sebelumnya yang dibuat di SharePoint Online. Hanya versi file terbaru yang dilindungi.
- Anda tidak dapat mencadangkan pustaka Preservation Hold.
- Anda tidak dapat mencadangkan situs yang dibuat di Business Productivity Online Suite (BPOS), pendahulu Microsoft 365.
- Anda tidak dapat mencadangkan pengaturan untuk situs yang menggunakan jalur `/portals` yang dikelola (misalnya, `https://<tenant>.sharepoint.com/portals/...`).
- Pengaturan Manajemen Hak Informasi (IRM) dari daftar atau pustaka dapat dipulihkan hanya jika IRM diaktifkan di organisasi Microsoft 365 target.

Apa saja item yang dapat dipulihkan?

Item berikut dapat dipulihkan dari cadangan situs:

- Keseluruhan mesin
- Subsitus
- Daftar
- Item daftar
- Pustaka dokumen
- Dokumen
- Lampiran item daftar
- Halaman situs dan halaman wiki

Anda dapat menggunakan pencarian untuk menemukan item.

© Acronis International GmbH, 2003-2024

Item dapat dipulihkan ke situs asli atau non-asli. Jalur ke item yang dipulihkan sama dengan aslinya. Jika tidak ada, jalur akan dibuat.

Anda dapat memilih untuk memulihkan izin berbagi atau membiarkan item menerima turunan izin dari objek induk setelah pemulihan.

Apa saja item yang tidak dapat dipulihkan?

- Subsitus yang didasarkan pada templat **Visio Process Repository**.
- Daftar jenis berikut: **Daftar survei**, **Daftar tugas**, **Pustaka gambar**, **Tautan**, **Kalender**, **Papan Diskusi**, **Eksternal**, dan **Spreadsheet Impor**.
- Daftar untuk beberapa jenis konten diaktifkan.

Memilih data SharePoint Online

Pilih data seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Untuk memilih data SharePoint Online

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data penggunanya ingin Anda cadangkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk mencadangkan semua situs SharePoint klasik di organisasi, termasuk situs yang akan dibuat di masa mendatang, perluas simpul **Kumpulan situs**, pilih **Semua kumpulan situs**, lalu klik **Pencadangan grup**.
   - Untuk mencadangkan situs klasik, perluas simpul **Kumpulan situs**, pilih **Semua koleksi situs**, pilih situs yang ingin Anda cadangkan, lalu klik **Cadangkan**.
   - Untuk mencadangkan semua situs grup (tim modern), termasuk situs yang akan dibuat di masa mendatang, perluas simpul **Grup**, pilih **Semua grup**, lalu klik **Pencadangan grup**.
   - Untuk mencadangkan situs grup (tim modern) individual, perluas simpul **Grup**, pilih **Semua grup**, pilih grup yang situsnya ingin Anda cadangkan, lalu klik **Cadangkan**.
4. Pada panel rencana proteksi:
   - Pastikan item **Situs SharePoint** dipilih di **Apa yang akan dicadangkan**.
   - Di **Item untuk dicadangkan**, lakukan salah satu hal berikut:
     - Simpan pengaturan default **[Semua]** (semua item dari situs yang dipilih).
     - Tentukan subsitus, daftar, dan pustaka untuk mencadangkan dengan menambahkan nama atau jalur mereka.

       Untuk mencadangkan subsitus atau daftar/pustaka situs tingkat teratas, tentukan nama tampilannya dalam format berikut: `/display name/**`

       Untuk mencadangkan daftar/pustaka subsitus, tentukan nama tampilannya dalam format berikut: `/subsite display name/list display name/**`

© Acronis International GmbH, 2003-2024

Nama tampilan subsitus, daftar, dan pustaka ditampilkan di halaman **Konten situs** dari situs atau subsitus SharePoint.

- Tentukan subsitus yang akan dicadangkan dengan menjelajahi.

  Tautan **Jelajahi** hanya tersedia saat membuat rencana proteksi untuk situs tunggal.

- [Opsional] Di **Item untuk dicadangkan**, klik **Tampilkan pengecualian** untuk menentukan subsitus, daftar, dan pustaka yang akan dilewati selama pencadangan.

  Pengecualian item akan mengesampingkan pemilihan item tersebut; yaitu jika Anda menentukan subsitus yang sama di kedua bidang, subsitus ini akan dilewati selama pencadangan.
- [Opsional] Untuk mencadangkan buku catatan OneNote, aktifkan tombol **Sertakan OneNote**.

Memulihkan data SharePoint Online

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk memulihkan data dari situs grup (tim modern), perluas simpul **Grup**, pilih **Semua grup**, pilih grup dengan situs yang pada awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Untuk memulihkan data dari situs klasik, perluas simpul **Kumpulan Situs**, pilih **Semua koleksi situs**, pilih situs yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
   - Jika situs dihapus, pilih situs tersebut di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tampilkan cadangan**.

   Anda dapat mencari grup dan situs berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.

   Catatan
   Untuk hanya melihat titik pemulihan yang berisi situs SharePoint, pilih **situs SharePoint** di **Filter berdasarkan konten**.
5. Klik **Pulihkan file SharePoint**.
6. Jelajahi ke folder yang diperlukan atau gunakan pencarian untuk mendapatkan daftar item data yang diperlukan.
7. Pilih item yang ingin Anda pulihkan.

   Jika cadangan tidak dienkripsi, gunakan pencarian, dan pilih satu item pada hasil pencarian, Anda dapat mengklik **Tampilkan versi** untuk memilih versi item yang akan dipulihkan. Anda dapat memilih versi yang dicadangkan, yang lebih baru atau lebih lama dari titik pemulihan yang dipilih.
8. [Opsional] Untuk mengunduh item, pilih item, klik **Unduh**, pilih lokasi di mana Anda ingin menyimpan item tersebut, lalu klik **Simpan**.

© Acronis International GmbH, 2003-2024

9. Klik **Pulihkan**.
10. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target.
    Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
11. Di **Pulihkan ke situs**, lihat, ubah, atau tentukan situs target.
    Anda tidak dapat membuat situs SharePoint baru selama pemulihan. Untuk memulihkan situs SharePoint ke yang baru, pertama-tama Anda perlu membuat situs target di organisasi Microsoft 365 yang diinginkan, dan kemudian membiarkan agen cloud melakukan sinkronisasi perubahan. Agen cloud secara otomatis melakukan sinkronisasi dengan Microsoft 365 setiap 24 jam. Untuk mensinkronkan perubahan dengan segera, di konsol Cyber Protect, pilih organisasi di halaman **Microsoft 365**, dan kemudian klik **Refresh**.
12. Pilih apakah akan memulihkan izin berbagi untuk item yang dipulihkan.
13. Klik **Mulai pemulihan**.
14. Pilih salah satu opsi penimpaan:

Opsi	Deskripsi
Timpa file yang ada jika lebih lama	Jika ada file dengan nama yang sama di lokasi tujuan, dan lebih lama dari file sumber, file sumber akan disimpan di lokasi tujuan, menggantikan versi yang lebih lama.
Timpa file yang ada	Semua file yang ada di lokasi tujuan akan ditimpa, terlepas dari tanggal terakhir diubah.
Jangan timpa file yang ada	Jika ada file dengan nama yang sama di lokasi tujuan, tidak ada perubahan yang diterapkan padanya, dan file sumber tidak disimpan ke lokasi tujuan.

Catatan
Ketika memulihkan buku catatan OneNote, opsi **Timpa file yang ada jika lebih lama** dan **Timpa file yang ada** akan mengakibatkan penimpaan buku catatan OneNote yang ada.

15. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Melindungi Tim Microsoft 365

Apa saja item yang dapat dicadangkan?

Anda dapat mencadangkan seluruh tim. Ini mencakup nama tim, daftar anggota tim, saluran tim dan kontennya, kotak surat tim dan pertemuan, dan situs tim.

Opsi terpisah dalam rencana pencadangan memungkinkan pencadangan buku catatan OneNote.

© Acronis International GmbH, 2003-2024

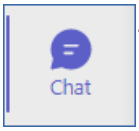
Apa saja item yang dapat dipulihkan?

- Seluruh tim
- Saluran tim
- File saluran
- Kotak surat tim
- Folder email dalam kotak surat tim
- Pesan email dalam kotak surat tim
- Pertemuan
- Situs tim

Anda tidak dapat memulihkan percakapan dalam saluran tim, tapi Anda dapat mengunduhnya sebagai file html tunggal.

Pembatasan

Item berikut ini tidak dicadangkan:

- Pengaturan saluran umum (preferensi moderasi) – karena pembatasan API beta Microsoft Teams.
- Pengaturan saluran umum (preferensi moderasi) – karena pembatasan API beta Microsoft Teams.
- Catatan pertemuan.
- Pesan di bagian chat 

. Bagian ini berisi obrolan pribadi satu lawan satu dan obrolan grup.
- Stiker dan pujian.

Pencadangan dan pemulihan didukung untuk tab saluran berikut:

- Word
- Excel
- PowerPoint
- PDF
- Pustaka Dokumen

Memilih tim

Pilih tim seperti dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Untuk memilih tim

© Acronis International GmbH, 2003-2024

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang timnya ingin Anda cadangkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk mencadangkan semua tim dalam organisasi (termasuk tim yang akan dibuat di waktu mendatang), perluas simpul **Tim**, pilih **Semua tim**, lalu klik **Cadangan grup**.
   - Untuk mencadangkan tim individual, perluas simpul **Tim**, pilih **Semua tim**, pilih tim yang ingin Anda cadangkan, lalu klik **Cadangkan**.

   Anda dapat mencari tim berdasarkan nama. Wildcard tidak didukung.
4. Pada panel rencana proteksi:
   - Pastikan item **Microsoft Teams** dipilih di **Apa yang akan dicadangkan**.
   - [Opsional] Dalam fitur **Berapa lama akan disimpan**, atur opsi pembersihan.
   - [Opsional] Jika Anda ingin mengenkripsi cadangan, aktifkan switch **Enkripsi**, lalu atur kata sandi Anda dan pilih algoritme enkripsi.
   - [Opsional] Untuk mencadangkan buku catatan OneNote, aktifkan tombol **Sertakan OneNote**.

Memulihkan keseluruhan tim

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang tim cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Tim**, pilih **Semua tim**, pilih tim yang ingin Anda pulihkan, lalu pilih **Pemulihan**.

   Anda dapat mencari tim berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.
5. Klik **Pulihkan** > **Seluruh Tim**.

   Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target. Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
6. Di bagian **Pulihkan ke tim**, lihat tim target atau pilih lainnya.

   Secara default, tim asli dipilih. Jika tim ini tidak ada (misalnya, dihapus) atau Anda memilih organisasi yang tidak memiliki tim asli, Anda harus memilih tim target dari daftar drop-down.

   Anda hanya dapat memulihkan tim ke dalam tim yang sudah ada. Anda tidak dapat membuat tim selama operasi pemulihan.
7. Klik **Mulai pemulihan**.
8. Pilih salah satu opsi penimpaan:
   - **Timpa konten yang ada jika sudah lebih lama**
   - **Timpa konten yang ada**
   - **Jangan timpa konten yang ada**

© Acronis International GmbH, 2003-2024

Catatan
Ketika memulihkan buku catatan OneNote, opsi **Timpa konten yang ada jika sudah lebih lama** dan **Timpa konten yang ada** akan mengakibatkan penimpaan buku catatan OneNote yang ada.

9. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Saat Anda menghapus saluran dalam antarmuka grafis Microsoft Teams, antarmuka tersebut tidak langsung dihapus dari sistem. Maka, saat Anda memulihkan keseluruhan tim, nama saluran ini tidak dapat digunakan dan akan ditambahkan postfix.

Percakapan dipulihkan sebagai file html tunggal dalam tab **File** pada saluran. Anda dapat menemukan file ini dalam folder yang dinamai sesuai pola berikut: `<Nama tim>_<Nama saluran>_cadangan_percakapan_<tanggal pemulihan>T<waktu pemulihan>Z`.

Catatan
Setelah memulihkan tim atau saluran tim, buka Microsoft Teams, pilih saluran yang dipulihkan, lalu klik tab **File** saluran tersebut. Jika tidak, cadangan selanjutnya dari saluran ini tidak akan termasuk isi tab ini – karena pembatasan API beta Microsoft Teams.

Memulihkan saluran atau file tim dalam saluran tim

Untuk memulihkan saluran tim

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang tim cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Tim**, pilih **Semua tim**, pilih tim yang salurannya ingin Anda pulihkan, lalu pilih **Pemulihan**.
4. Pilih titik pemulihan.
5. Klik **Pulihkan** > **Saluran**.
6. Pilih saluran yang ingin Anda pulihkan, lalu klik **Pulihkan**. Untuk memilih saluran di panel utama, pilih kotak centang di depan namanya.

   Tersedia opsi pencarian berikut:
   - Untuk **Percakapan**: pengirim, subjek, konten, bahasa, nama lampiran, tanggal, atau rentang tanggal.
   - Untuk **File**: nama file atau nama folder, tipe file, ukuran, tanggal atau rentang tanggal perubahan terakhir.

   Catatan
   Anda juga dapat mengunduh file secara lokal, alih-alih memulihkannya.
7. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target.

© Acronis International GmbH, 2003-2024

Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.

8. Di bagian **Pulihkan ke tim**, lihat, ubah, atau tentukan tim target.
   Secara default, tim asli dipilih. Jika tim ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan tim target.
9. Di bagian **Pulihkan ke saluran**, lihat, ubah, atau tentukan saluran target.
10. Klik **Mulai pemulihan**.
11. Pilih salah satu opsi penimpaan:
    - **Timpa konten yang ada jika sudah lebih lama**
    - **Timpa konten yang ada**
    - **Jangan timpa konten yang ada**

    Catatan
    Ketika memulihkan buku catatan OneNote, opsi **Timpa konten yang ada jika sudah lebih lama** dan **Timpa konten yang ada** akan mengakibatkan penimpaan buku catatan OneNote yang ada.
12. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Percakapan dipulihkan sebagai file html tunggal dalam tab **File** pada saluran. Anda dapat menemukan file ini dalam folder yang dinamai sesuai pola berikut: `<Nama tim>_<Nama saluran>_cadangan_percakapan_<tanggal pemulihan>T<waktu pemulihan>Z`.

Catatan
Setelah memulihkan tim atau saluran tim, buka Microsoft Teams, pilih saluran yang dipulihkan, lalu klik tab **File** saluran tersebut. Jika tidak, cadangan selanjutnya dari saluran ini tidak akan termasuk isi tab ini – karena pembatasan API beta Microsoft Teams.

Untuk memulihkan file di saluran tim

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang tim cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Tim**, pilih **Semua tim**, pilih tim yang salurannya ingin Anda pulihkan, lalu pilih **Pemulihan**.
4. Pilih titik pemulihan.
5. Klik **Pulihkan** > **Saluran**.
6. Pilih saluran yang diinginkan, lalu buka folder **File**.
   Jelajahi ke item yang diperlukan atau gunakan pencarian untuk mendapatkan daftar item yang diperlukan. Opsi pencarian berikut tersedia: nama file atau nama folder, jenis file, ukuran, tanggal atau rentang tanggal perubahan terakhir.

© Acronis International GmbH, 2003-2024

7. [Opsional] Untuk mengunduh item, pilih item, klik **Unduh**, pilih lokasi di mana Anda ingin menyimpan item tersebut, lalu klik **Simpan**.
8. Pilih item yang ingin Anda pulihkan, lalu klik **Pulihkan**
9. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik organisasi Microsoft 365 untuk melihat, mengubah, atau menentukan organisasi target.
   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
10. Di bagian **Pulihkan ke tim**, lihat, ubah, atau tentukan tim target.
    Secara default, tim asli dipilih. Jika tim ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan tim target.
11. Di bagian **Pulihkan ke saluran**, lihat, ubah, atau tentukan saluran target.
12. Pilih apakah akan memulihkan izin berbagi untuk item yang dipulihkan.
13. Klik **Mulai pemulihan**.
14. Pilih salah satu opsi penimpaan:
    - **Timpa konten yang ada jika sudah lebih lama**
    - **Timpa konten yang ada**
    - **Jangan timpa konten yang ada**

    Catatan
    Ketika memulihkan buku catatan OneNote, opsi **Timpa konten yang ada jika sudah lebih lama** dan **Timpa konten yang ada** akan mengakibatkan penimpaan buku catatan OneNote yang ada.
15. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Anda tidak dapat memulihkan percakapan individual. Di panel utama, Anda hanya dapat menjelajahi folder **Percakapan** atau mengunduh kontennya sebagai file html tunggal. Untuk melakukannya, klik ikon "pulihkan folder" , pilih folder **Percakapan** yang diinginkan, lalu klik **Unduh**.

Anda dapat mencari pesan dalam folder **Percakapan** berdasarkan:

- Pengirim
- Konten
- Nama lampiran
- Tanggal

© Acronis International GmbH, 2003-2024

Memulihkan kotak surat tim

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang tim cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Tim**, pilih **Semua tim**, pilih tim yang kotak suratnya ingin Anda pulihkan, lalu pilih **Pemulihan**.

   Anda dapat mencari tim berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.
5. Klik **Pulihkan** > **Pesan email**.
6. Klik ikon "pulihkan folder" , pilih folder kotak surat akar, lalu klik **Pulihkan**.

   Catatan
   Anda juga dapat memulihkan folder individual dari kotak surat yang dipilih.
7. Klik **Pulihkan**.
8. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target.

   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
9. Di **Pulihkan ke kotak surat**, lihat, ubah, atau tentukan kotak surat target.

   Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan kotak surat target.
10. Klik **Mulai pemulihan**.
11. Pilih salah satu opsi penimpaan:
    - **Timpa item yang ada**
    - **Jangan timpa item yang ada**
12. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Memulihkan item kotak surat tim ke file PST

Untuk memulihkan item kotak surat tim

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Anda dapat mencari pengguna dan grup berdasarkan nama. Wildcard tidak didukung.
4. Perluas simpul **Tim**, pilih **Semua tim**, pilih tim yang kotak suratnya awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.
5. Klik **Pulihkan** > **Pesan Email**.

© Acronis International GmbH, 2003-2024

6. Jelajahi ke folder yang diperlukan atau gunakan pencarian untuk mendapatkan daftar item yang diperlukan.

   Opsi pencarian berikut tersedia. Wildcard tidak didukung.

   - Untuk pesan email: cari berdasarkan subjek, pengirim, penerima, nama lampiran, dan tanggal.
   - Untuk acara: cari berdasarkan judul dan tanggal.
   - Untuk tugas: cari berdasarkan subjek dan tanggal.
   - Untuk kontak: cari berdasarkan nama, alamat email, dan nomor telepon.

7. Pilih item yang ingin Anda pulihkan. Untuk dapat memilih folder, klik ikon "pulihkan folder":

   Selain itu, Anda dapat melakukan hal-hal berikut:

   - Ketika item dipilih, klik **Tampilkan konten** untuk melihat kontennya, termasuk lampiran. Klik nama file terlampir untuk mengunduhnya.
   - Ketika pesan email atau item kalender dipilih, klik **Kirim sebagai surel** untuk mengirim item ke alamat email yang ditentukan. Anda dapat memilih pengirim dan menulis teks yang akan ditambahkan ke item yang diteruskan.
   - Saat cadangan tidak dienkripsi, Anda menggunakan pencarian, dan memilih satu item dari hasil pencarian: klik **Tampilkan versi** untuk melihat versi item. Anda dapat memilih versi yang dicadangkan, baik yang lebih baru atau lebih lama dari titik pemulihan yang dipilih.

8. Klik **Pulihkan sebagai file PST**.
9. Atur kata sandi untuk mengenkripsi arsip dengan file PST.

   Kata sandi harus berisi setidaknya satu simbol.
10. Konfirmasi kata sandi dan klik **SELESAI**.

Item kotak surat yang dipilih akan dipulihkan sebagai file data PST dan diarsipkan dalam format ZIP. Ukuran maksimum satu file PST dibatasi hingga 2 GB, jika data yang Anda pulihkan melebihi 2 GB, maka akan dibagi menjadi beberapa file PST. Arsip ZIP akan dilindungi dengan kata sandi yang Anda atur.

Anda akan menerima surel dengan tautan ke arsip ZIP yang berisi file PST yang dibuat.

Administrator akan menerima surel pemberitahuan bahwa Anda telah melakukan prosedur pemulihan.

Untuk mengunduh arsip dengan file PST dan menyelesaikan pemulihan

1. Lakukan salah satu langkah berikut:
   - Untuk mengunduh arsip dari surel, ikuti tautan **Unduh file**.
     Arsip tersedia untuk diunduh dalam waktu 24 jam. Jika tautan kedaluwarsa, ulangi prosedur pemulihan.
   - Untuk mengunduh arsip dari konsol Cyber Protect:
     a. Buka **Penyimpanan Cadangan** > **file PST**.

© Acronis International GmbH, 2003-2024

b. Pilih arsip terbaru yang disorot.

c. Klik **Unduh** di panel kanan.

Arsip akan diunduh ke direktori unduhan default di komputer Anda.

2. Ekstraksi file PST dari arsip menggunakan kata sandi yang Anda atur untuk mengenkripsi arsip.
3. Di Microsoft Outlook, buka atau impor file PST. Untuk mempelajari cara melakukannya, lihat dokumentasi Microsoft.

Memulihkan pesan email dan pertemuan

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang tim cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Tim**, pilih **Semua tim**, pilih tim yang pesan email atau pertemuannya ingin Anda pulihkan, lalu klik **Pemulihan**.

   Anda dapat mencari tim berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.
5. Klik **Pulihkan** > **Pesan email**.
6. Jelajahi ke item yang diperlukan atau gunakan pencarian untuk mendapatkan daftar item yang diperlukan.

   Tersedia opsi pencarian berikut:
   - Untuk pesan email: cari berdasarkan subjek, pengirim, penerima, dan tanggal.
   - Untuk pertemuan: cari berdasarkan nama dan tanggal peristiwa.
7. Pilih item yang ingin Anda pulihkan, lalu klik **Pulihkan**.

   Catatan
   Anda dapat menemukan pertemuan di folder **Kalender**.

   Selain itu, Anda dapat melakukan hal-hal berikut:
   - Ketika item dipilih, klik **Tampilkan konten** untuk melihat kontennya, termasuk lampiran. Klik nama file terlampir untuk mengunduhnya.
   - Ketika pesan email atau pertemuan dipilih, klik **Kirim sebagai email** untuk mengirim item ke alamat email yang ditentukan. Anda dapat memilih pengirim dan menulis teks yang akan ditambahkan ke item yang diteruskan.
8. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target.

   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
9. Di **Pulihkan ke kotak surat**, lihat, ubah, atau tentukan kotak surat target.

   Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan kotak surat target.

© Acronis International GmbH, 2003-2024

10. Klik **Mulai pemulihan**.
11. Pilih salah satu opsi penimpaan:
    - **Timpa item yang ada**
    - **Jangan timpa item yang ada**
12. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Memulihkan situs tim atau item spesifik dalam suatu situs

1. Klik **Microsoft 365**.
2. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, pilih organisasi yang tim cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Tim**, pilih **Semua tim**, pilih tim yang situsnya ingin Anda pulihkan, lalu pilih **Pemulihan**.
   Anda dapat mencari tim berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.
5. Klik **Pulihkan** > **Situs tim**.
6. Jelajahi ke item yang diperlukan atau gunakan pencarian untuk mendapatkan daftar item yang diperlukan.
7. [Opsional] Untuk mengunduh item, pilih item, klik **Unduh**, pilih lokasi di mana Anda ingin menyimpan item tersebut, lalu klik **Simpan**.
8. Pilih item yang ingin Anda pulihkan, lalu klik **Pulihkan**.
9. Jika beberapa organisasi Microsoft 365 ditambahkan ke layanan Cyber Protection, klik **organisasi Microsoft 365** untuk melihat, mengubah, atau menentukan organisasi target.
   Secara default, organisasi dan tim asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus menentukan organisasi target.
10. Di bagian **Pulihkan ke tim**, lihat, ubah, atau tentukan tim target.
    Secara default, tim asli dipilih. Jika tim ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan situs target.
11. Pilih apakah akan memulihkan izin berbagi untuk item yang dipulihkan.
12. Klik **Mulai pemulihan**.
13. Pilih salah satu opsi penimpaan:
    - **Timpa konten yang ada jika sudah lebih lama**
    - **Timpa konten yang ada**
    - **Jangan timpa konten yang ada**

Catatan
Ketika memulihkan buku catatan OneNote, opsi **Timpa konten yang ada jika sudah lebih lama** dan **Timpa konten yang ada** akan mengakibatkan penimpaan buku catatan OneNote

© Acronis International GmbH, 2003-2024

yang ada.

14. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Melindungi buku catatan OneNote

Secara default, buku catatan OneNote disertakan dalam cadangan file OneDrive, Microsoft Teams, dan situs SharePoint.

Untuk mengecualikan buku catatan OneNote dari cadangan ini, nonaktifkan tombol **Sertakan OneNote** dalam rencana pencadangan masing-masing.

Memulihkan buku catatan OneNote yang dicadangkan

Untuk mempelajari cara memulihkan buku catatan OneNote yang dicadangkan, lihat topik terkait:

- Untuk pencadangan OneDrive, lihat "Memulihkan keseluruhan OneDrive" (hlm. 621) atau "Memulihkan file OneDrive" (hlm. 622).
- Untuk pencadangan Teams, lihat "Memulihkan keseluruhan tim" (hlm. 629), "Memulihkan saluran atau file tim dalam saluran tim" (hlm. 630), atau "Memulihkan situs tim atau item spesifik dalam suatu situs" (hlm. 636).
- Untuk pencadangan situs SharePoint, lihat "Memulihkan data SharePoint Online" (hlm. 626).

Versi yang didukung

- OneNote (OneNote 2016 dan yang lebih baru)
- OneNote untuk Windows 10

Pembatasan dan masalah yang diketahui

- Buku catatan OneNote yang disimpan di OneDrive atau SharePoint dibatasi hingga 2 GB. Anda tidak dapat memulihkan buku catatan OneNote yang lebih besar ke target OneDrive atau SharePoint.
- Buku catatan OneNote dengan grup bagian tidak didukung.
- Dalam buku catatan OneNote yang dicadangkan yang berisi bagian dengan nama non-default, bagian pertama diperlihatkan dengan nama default (seperti `Bagian baru` atau `Bagian tanpa judul`). Ini mungkin memengaruhi urutan bagian di buku catatan dengan beberapa bagian.
- Ketika memulihkan buku catatan OneNote, opsi **Timpa konten yang ada jika sudah lebih lama** dan **Timpa konten yang ada** akan mengakibatkan penimpaan buku catatan OneNote yang ada.
- Ketika Anda memulihkan seluruh tim, situs tim, atau folder `Aset Situs` dari situs tim, dan Anda memilih opsi **Timpa konten yang ada jika sudah lebih lama** atau **Timpa konten yang ada**, buku catatan OneNote default tim tersebut tidak akan ditimpa. Pemulihan berhasil dengan peringatan *Gagal memperbarui properti file '/sites/<Nama tim>/SiteAssets/<Nama buku catatan OneNote>'*.

© Acronis International GmbH, 2003-2024

Melindungi akun apl kolaborasi Microsoft 365

Anda dapat menggunakan paket Advanced Email Security, yang memberikan proteksi real-time untuk kotak surat Microsoft 365, Google Workspace, atau Open-Xchange Anda:

- Antimalware dan anti-spam
- Pindaian URL dalam email
- Analisis DMARC
- Antiphishing
- Perlindungan penyamaran
- Pindaian lampiran
- Pelucutan dan rekonstruksi konten
- Grafik kepercayaan

Anda juga dapat mengaktifkan kursi aplikasi kolaborasi Microsoft 365, yang memungkinkan perlindungan aplikasi kolaborasi cloud Microsoft 365 dari ancaman keamanan bawaan konten. Aplikasi ini mencakup OneDrive, SharePoint, dan Teams.

Advanced Email Security dapat diaktifkan per beban kerja atau per gigabyte dan akan memengaruhi model pelisensian Anda.

Untuk mendapatkan orientasi Advanced Email Security dari konsol Cyber Protect Cloud

1. Klik **Perangkat** > **Microsoft 365**.
2. Klik simpul **Pengguna** dan kemudian klik tautan **Buka Keamanan Email** di pojok kanan atas.

Pelajari selengkapnya tentang Advanced Email Security di Lembar data Advanced Email Security.

Untuk instruksi konfigurasi, lihat Advanced Email Security dengan Titik Persepsi.

Melindungi data Google Workspace

Catatan
Fitur ini tidak tersedia untuk penyewa dalam mode Kepatuhan. Untuk informasi lebih lanjut, silakan lihat "Mode kepatuhan" (hlm. 1083).

Apa definisi perlindungan Google Workspace?

- Pencadangan awan ke awan dan pemulihan data pengguna Google Workspace (kotak surat Gmail, Kalender, Kontak, Google Drive) dan drive Google Workspace Shared.
- Pemulihan granular email, file, kontak, dan item lainnya.
- Dukungan untuk organisasi Google Workspace dan pemulihan lintas organisasi.

© Acronis International GmbH, 2003-2024

- Notarisasi opsional untuk file yang dicadangkan menggunakan database blockchain Ethereum. Saat diaktifkan, Anda dapat membuktikan bahwa file tersebut asli dan tidak berubah sejak dicadangkan.
- Pencarian teks lengkap opsional. Saat diaktifkan, Anda dapat mencari surel berdasarkan kontennya.
- Mencapai 5000 item (kotak surat, Google Drive, dan drive Shared) per perusahaan yang dapat dilindungi tanpa penurunan kinerja.
- Data yang dicadangkan dikompres secara otomatis dan menggunakan lebih sedikit ruang di lokasi pencadangan dibandingkan lokasi aslinya. Tingkat kompresi untuk pencadangan awan-ke-awan telah diperbaiki dan sesuai dengan level **Normal** pada pencadangan non-awan-ke-awan. Untuk informasi lebih lanjut tentang level ini, lihat "Tingkat kompresi" (hlm. 458).

Hak pengguna yang diperlukan

Dalam Cyber Protection

Dalam Cyber Protection, Anda harus menjadi administrator perusahaan yang bertindak pada tingkat penyewa pelanggan. Administrator perusahaan yang bertindak pada tingkat unit, administrator unit, dan pengguna tidak dapat mencadangkan atau memulihkan data Google Workspace.

Di Google Workspace

Untuk menambahkan organisasi Google Workspace Anda ke layanan Cyber Protection, Anda harus masuk sebagai Super Admin dengan akses API yang diaktifkan (**Keamanan** > **Referensi API** > **Aktifkan akses API** di konsol Admin Google).

Kata sandi Super Admin tidak disimpan di mana pun dan tidak digunakan untuk melakukan pencadangan dan pemulihan. Mengganti kata sandi ini di Google Workspace tidak memengaruhi operasi layanan Cyber Protection.

Jika Admin Super yang menambahkan organisasi Google Workspace dihapus dari Google Workspace atau diberi peran dengan hak istimewa yang lebih sedikit, pencadangan akan gagal dengan pesan kesalahan seperti 'Akses ditolak'. Dalam hal ini, ulangi prosedur yang dijelaskan dalam "Menambahkan organisasi Google Workspace" (hlm. 640) dan tentukan kredensial Admin Super yang valid. Untuk menghindari hal ini, kami menyarankan Anda membuat pengguna Admin Super khusus untuk tujuan pencadangan dan pemulihan.

Tentang jadwal pencadangan

Karena melayani banyak pelanggan, agen awan akan menentukan sendiri waktu mulai untuk setiap rencana proteksi, guna memastikan pemuatan yang merata selama satu hari dan kualitas layanan yang sama bagi semua pelanggan.

Setiap rencana proteksi berjalan setiap hari pada waktu yang sama.

© Acronis International GmbH, 2003-2024

Opsi default adalah **Sekali sehari**. Dengan paket Cadangan Tingkat Lanjut, Anda dapat menjadwalkan hingga enam cadangan per hari. Pencadangan dimulai pada interval perkiraan yang bergantung pada beban saat ini dari agen awan, yang melayani banyak pelanggan di pusat data. Ini memastikan pemuatan yang merata di siang hari dan kualitas layanan yang sama untuk semua pelanggan.

Pembatasan

- Konsol hanya menampilkan pengguna yang memiliki lisensi Google Workspace yang ditetapkan dan kotak surat atau Google Drive.
- Dokumen dalam format asli Google dicadangkan sebagai dokumen kantor umum dan ditampilkan dengan ekstensi berbeda di konsol Cyber Protect– seperti .docx atau .pptx. Dokumen tersebut diubah kembali ke format aslinya selama pemulihan.
- Tidak lebih dari 10 cadangan manual selama satu jam.
- Tidak lebih dari 10 operasi pemulihan serentak (jumlah ini mencakup pemulihan Microsoft 365 dan Google Workspace).
- Anda tidak dapat memulihkan item secara bersamaan dari titik pemulihan yang berbeda, meskipun Anda dapat memilih item tersebut dari hasil pencarian.
- Cadangan akun pengguna Google Workspace yang dihapus tidak otomatis dihapus dari penyimpanan awan. Cadangan ini dikenakan tagihan untuk penyimpanan awan yang digunakan.
- Anda tidak dapat menerapkan lebih dari satu rencana pencadangan individual untuk beban kerja yang sama.
- Ketika rencana pencadangan individual dan rencana pencadangan grup diterapkan pada beban kerja yang sama, pengaturan dalam rencana individual akan diutamakan.

Pencatatan

Tindakan dengan sumber daya awan-ke-awan, seperti menampilkan konten surel yang dicadangkan, mengunduh lampiran atau file, memulihkan surel ke kotak surat non-asli, atau mengirimkannya sebagai surel dapat melanggar kebijakan privasi pengguna. Tindakan ini dicatat di **Pemantauan** > **Log audit** di Portal Manajemen.

Menambahkan organisasi Google Workspace

Untuk menambahkan organisasi Google Workspace ke layanan Cyber Protection, Anda memerlukan proyek Google Cloud pribadi khusus. Untuk informasi lebih lanjut mengenai cara membuat dan mengonfigurasi proyek ini, lihatlah "Membuat proyek Google Cloud pribadi." (hlm. 641).

Untuk menambahkan organisasi Google Workspace menggunakan proyek Google Cloud pribadi khusus

1. Masuk ke konsol Cyber Protect sebagai administrator perusahaan.
2. Klik **Perangkat** > **Tambah** > **Google Workspace**.

© Acronis International GmbH, 2003-2024

3. Masukkan alamat email Administrator Super dari akun Google Workspace.
   Untuk prosedur ini, apakah Verifikasi 2 Langkah diaktifkan untuk akun email Administrator Super tidaklah relevan.
4. Cari file JSON yang berisi kode pribadi akun layanan yang dibuat di proyek Google Cloud Anda.
   Anda juga dapat menempelkan isi file sebagai teks.

5. Klik **Konfirmasi**.

Akibatnya, organisasi Google Workspace Anda muncul di bawah tab **Perangkat** di konsol Cyber Protect.

Tips berguna

- Setelah menambah organisasi Google Workspace, data pengguna dan drive Shared di domain utama dan semua domain sekunder, jika ada, akan dicadangkan. Sumber daya yang dicadangkan akan ditampilkan dalam satu daftar, dan tidak akan dikelompokkan berdasarkan domainnya.
- Agen cloud melakukan sinkronisasi dengan Google Workspace setiap 24 jam, mulai dari saat organisasi ditambahkan ke layanan Cyber Protection. Jika Anda menambahkan atau menghapus pengguna atau Drive bersama, Anda tidak akan melihat perubahan ini di konsol Cyber Protect dengan segera. Untuk segera menyinkronkan perubahan, pilih organisasi di halaman **Google Workspace**, lalu klik **Menyegarkan**.
  Untuk informasi lebih lanjut tentang menyinkronkan sumber daya organisasi Google Workspace dan konsol Cyber Protect, lihat "Menemukan sumber daya Google Workspace" (hlm. 645).
- Jika Anda menerapkan rencana proteksi untuk grup **Semua pengguna** atau **Semua drive Shared**, item yang baru ditambahkan akan disertakan dalam pencadangan setelah sinkronisasi.
- Menurut kebijakan Google, saat pengguna atau Drive bersama dihapus dari antarmuka pengguna grafis Google Workspace, drive tersebut tetap tersedia melalui API selama beberapa hari. Selama periode ini, item yang dihapus tidak aktif (berwarna abu-abu) di konsol Cyber Protect dan tidak dicadangkan. Saat item yang dihapus menjadi tidak tersedia melalui API, item tersebut menghilang dari konsol Cyber Protect. Cadangannya (jika ada) dapat ditemukan di **Penyimpanan cadangan** > **Cadangan aplikasi Cloud**.

Membuat proyek Google Cloud pribadi.

Untuk menambahkan organisasi Google Workspace Anda ke layanan Cyber Protection menggunakan proyek Google Cloud pribadi khusus, Anda perlu melakukan hal berikut:

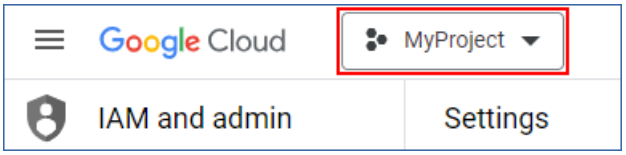
1. Buat proyek Google Cloud baru.
2. Aktifkan API yang diperlukan untuk proyek ini.
3. Konfigurasi kredensial untuk proyek ini.
   a. Konfigurasi layar persetujuan OAuth.
   b. Buat dan konfigurasi akun layanan untuk layanan Cyber Protection.
4. Izinkan akses proyek baru ke akun Google Workspace Anda.

© Acronis International GmbH, 2003-2024

Catatan
Topik ini berisi deskripsi antarmuka pengguna pihak ketiga yang mungkin berubah tanpa pemberitahuan sebelumnya.

Untuk membuat proyek Google Cloud baru

1. Masuk ke Google Cloud Platform (console.cloud.google.com) sebagai Administrator Super.
2. Di konsol Google Cloud Platform, klik pemilih proyek di pojok kiri atas.



3. Pada layar yang terbuka, pilih organisasi, lalu klik **Proyek baru**.

4. Tentukan nama untuk proyek baru Anda.
5. Klik **Buat**.

Hasilnya, proyek Google Cloud baru Anda pun dibuat.

Untuk mengaktifkan API yang diperlukan di proyek ini

1. Di konsol Google Cloud Platform, pilih proyek baru Anda.
2. Dari menu navigasi, pilih **API dan layanan** > **API dan layanan yang diaktifkan**.
3. Nonaktifkan semua API yang aktif secara default di proyek ini, satu demi satu:
   a. Gulir ke bawah halaman **API dan layanan yang diaktifkan**, lalu klik nama API yang diaktifkan.
   Halaman **Detail API/Layanan** dari API yang dipilih akan terbuka.
   b. Klik **Nonaktifkan API**, lalu konfirmasi pilihan Anda dengan mengklik **Nonaktifkan**.
   c. [Jika diminta] Konfirmasikan pilihan Anda dengan mengeklik **Konfirmasi**.
   d. Kembali ke **API dan layanan** > **API dan layanan yang diaktifkan**, dan nonaktifkan API selanjutnya.
4. Dari menu navigasi, pilih **API dan layanan** > **Pustaka**.
5. Di pustaka API, aktifkan API berikut, satu demi satu:
   - Admin SDK API
   - Gmail API
   - Google Calendar API
   - Google Drive API
   - Google People API

© Acronis International GmbH, 2003-2024

Gunakan bilah pencarian untuk menemukan API yang dibutuhkan. Untuk mengaktifkan API, klik namanya, lalu klik **Aktifkan**. Untuk mencari API selanjutnya, kembali ke pustaka API dengan memilih **API dan layanan** > **Pustaka** dari menu navigasi.

Untuk konfigurasi layar persetujuan OAuth

1. Dari menu navigasi di Google Cloud Platform, pilih **API dan layanan** > **layar persetujuan OAuth**.
2. Di jendela yang terbuka, pilih **Internal** untuk tipe pengguna, lalu klik **Buat**.
3. Di bidang **Nama apl**, tentukan nama untuk aplikasi Anda.
4. Di bidang **Email dukungan pengguna**, masukkan email Administrator Super.
5. Di bidang **Informasi kontak developer**, masukkan email Administrator Super.
6. Biarkan bidang lain kosong, lalu klik **Simpan dan lanjut**
7. Di halaman **Cakupan**, klik **Simpan dan lanjut**, tanpa mengubah apa pun.
8. Di halaman **Ringkasan**, pastikan pengaturan Anda, lalu klik **Kembali ke dasbor**.

Untuk membuat dan mengonfigurasi akun layanan untuk layanan Cyber Protection.

1. Dari menu navigasi di Google Cloud Platform, pilih **IAM & Admin** > **Akun layanan**.
2. Klik **Buat akun layanan**.
3. Tentukan nama untuk akun layanan.
4. [Opsional] Tentukan deskripsi untuk akun layanan.
5. Klik **Buat dan lanjutkan**.
6. Jangan mengubah apa pun dalam langkah **Izinkan akses akun layanan ini ke proyek** dan **Izinkan akses pengguna ke akun layanan ini**.
7. Klik **Selesai**.
   Laman **Akun layanan** akan terbuka.
8. Pada halaman **Akun layanan**, pilih akun layanan yang baru, lalu di bawah **Tindakan**, klik **Kelola kunci**.
9. Pada **Kunci**, klik **Tambahkan kunci** > **Buat kunci baru**, lalu pilih tipe kunci **JSON**.
10. Klik **Buat**.
    Hasilnya, file JSON dengan kunci pribadi akun layanan tersebut diunduh secara otomatis ke mesin Anda. Simpan file ini dengan aman karena Anda memerlukannya untuk menambahkan organisasi Google Workspace Anda ke layanan Cyber Protection.

Untuk mengizinkan akses proyek baru ke akun Google Workspace Anda

1. Dari menu navigasi di Google Cloud Platform, pilih **IAM & Admin** > **Akun Layanan**.
2. Dalam daftar, temukan akun layanan yang Anda buat, lalu salin ID klien yang ditampilkan di kolom **ID Klien OAuth 2.0**.
3. Masuk ke konsol Google Admin (admin.google.com) sebagai Administrator Super.

© Acronis International GmbH, 2003-2024

4. Dari menu navigasi, pilih **Keamanan** > **Akses dan kontrol data** > **Kontrol API**.
5. Gulir ke bawah halaman **Kontrol API**, lalu pada **Delegasi seluruh domain**, klik **Kelola delegasi seluruh domain**.
   Halaman **Delegasi seluruh domain** pun terbuka.
6. Pada laman **Delegasi seluruh domain**, klik **Tambahkan baru**.
   Jendela **Tambahkan ID klien baru** akan terbuka.
7. Di bidang **ID Klien**, masukkan ID klien milik akun layanan klien.
8. Di bidang **cakupan OAuth**, salin dan tempel daftar cakupan berikut yang dipisahkan dengan koma:

   ```
   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
   ```

   Cara lainnya, Anda dapat menambahkan satu item per baris ke dalam cakupan:
   - 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. Klik **Izinkan**.

Hasilnya, proyek Google Cloud baru Anda dapat mengakses data di akun Google Workspace Anda. Untuk mencadangkan data, Anda perlu menautkan proyek ini ke layanan Cyber Protection. Untuk informasi lebih lanjut tentang cara melakukan ini, lihat "Untuk menambahkan organisasi Google Workspace menggunakan proyek Google Cloud pribadi khusus" (hlm. 640).

Jika Anda perlu membatalkan akses proyek Google Cloud ke akun Google Workspace, dan juga akses ke layanan Cyber Protection, hapus klien API yang proyek Anda gunakan.

Untuk membatalkan akses ke akun Google Workspace Anda

1. Di konsol Google Admin (admin.google.com), masuk sebagai Administrator Super.
2. Dari menu navigasi, pilih **Keamanan** > **Akses dan kontrol data** > **Kontrol API**.
3. Gulir ke bawah halaman **Kontrol API**, lalu pada **Delegasi seluruh domain**, klik **Kelola delegasi seluruh domain**.
   Halaman **Delegasi seluruh domain** pun terbuka.
4. Di halaman **Delegasi seluruh domain**, pilih klien API yang proyek Anda gunakan, lalu klik **Hapus**.

© Acronis International GmbH, 2003-2024

Hasilnya, proyek Google Cloud dan layanan Cyber Protection Anda tidak akan dapat mengakses akun Google Workspace dan mencadangkan data di situ.

Menemukan sumber daya Google Workspace

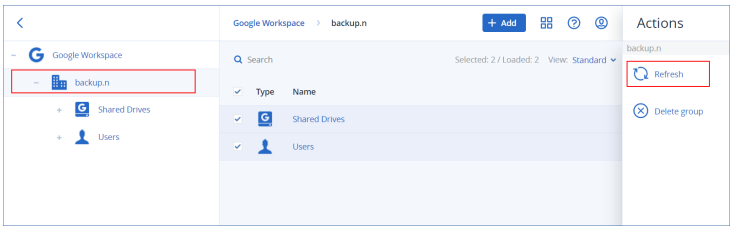
Saat Anda menambahkan organisasi Google Workspace ke layanan Cyber Protection, sumber daya di organisasi ini, seperti kotak surat dan Google Drive, akan disinkronkan ke konsol Cyber Protect. Operasi ini disebut penemuan dan dicatat di **Pemantauan** > **Aktivitas**.

Setelah operasi penemuan selesai, Anda dapat melihat sumber daya organisasi Google Workspace pada tab **Perangkat** > **Google Workspace** di konsol Cyber Protect, dan Anda dapat menerapkan rencana pencadangan di sana.

Operasi penemuan otomatis berjalan sekali sehari untuk menjaga agar daftar sumber daya di konsol Cyber Protect tetap mutakhir. Anda juga dapat menyinkronkan daftar ini sesuai permintaan, dengan menjalankan kembali operasi penemuan secara manual.

Untuk menjalankan kembali operasi penemuan secara manual

1. Di konsol Cyber Protect, buka **Perangkat** > **Google Workspace**.
2. Pilih organisasi Google Workspace Anda, lalu, di panel **Tindakan**, klik **Menyegarkan**.



Catatan
Anda dapat menjalankan operasi penemuan secara manual hingga 10 kali per jam. Ketika jumlah ini tercapai, operasi yang diizinkan diatur ulang menjadi satu kali per jam, dan kemudian setiap jam proses tambahan tersedia, hingga total 10 proses per jam tercapai lagi.

Pengaturan frekuensi pencadangan Google Workspace

Secara default, pencadangan Google Workspace berjalan sekali sehari dan tidak ada opsi penjadwalan tambahan yang tersedia.

Jika paket Cadangan Tingkat Lanjut diaktifkan di penyewa Anda, Anda dapat mengonfigurasi pencadangan yang lebih sering. Anda dapat memilih jumlah cadangan per hari, namun Anda tidak dapat mengonfigurasi waktu mulai pencadangan. Pencadangan dimulai secara otomatis pada interval perkiraan yang bergantung pada beban saat ini dari agen awan, yang melayani banyak pelanggan di pusat data. Ini memastikan pemuatan yang merata di siang hari, dan kualitas layanan yang sama untuk semua pelanggan.

Opsi berikut tersedia.

© Acronis International GmbH, 2003-2024

Opsi penjadwalan	Perkiraan interval antara setiap pencadangan
Sekali sehari	24 jam
Dua kali sehari (default)	12 jam
3 kali sehari	8 jam
6 kali sehari	4 jam

Catatan
Bergantung pada beban pada agen awan dan kemungkinan pelambatan di sisi Google Workspace, pencadangan mungkin akan dimulai lebih lambat dari yang dijadwalkan atau memerlukan waktu lebih lama untuk menyelesaikannya. Jika pencadangan memerlukan waktu lebih lama dari interval rata-rata antara dua pencadangan, pencadangan berikutnya akan dijadwalkan ulang, yang mungkin akan menghasilkan lebih sedikit cadangan per hari daripada yang dipilih. Sebagai contoh, hanya dua cadangan per hari yang mungkin dapat diselesaikan, meskipun Anda memilih enam cadangan per hari.

Melindungi data Gmail

Apa saja item yang dapat dicadangkan?

Anda dapat mencadangkan kotak surat pengguna Gmail. Pencadangan kotak surat juga mencakup data Kalender dan Kontak. Sebagai pilihan, Anda dapat memilih untuk mencadangkan kalender bersama.

Item berikut *dilewati* selama pencadangan:

- Kalender **Ulang Tahun**, **Pengingat**, **Tugas**
- Folder yang dilampirkan ke acara kalender
- Folder **Direktori** dalam Kontak

Item Kalender berikut ini *dilewati,* karena batasan API Kalender Google:

- Slot janji temu
- Ruang konferensi suatu acara
- Pengaturan kalender **Notifikasi acara sepanjang hari**
- Pengaturan kalender **Otomatis menerima undangan** (di kalender untuk kamar atau ruang bersama)

Item Kontak berikut ini *dilewati,* karena batasan API Orang Google:

- Folder **Kontak lain**
- Profil eksternal kontak (**profil Directory**, **profil Google**)
- Bidang kontak **File sebagai**

© Acronis International GmbH, 2003-2024

Apa saja item yang dapat dipulihkan?

Item berikut dapat dipulihkan dari cadangan kotak surat:

- Kotak surat
- Folder email (Menurut terminologi Google, "label". **Label** ditampilkan di perangkat lunak pencadangan sebagai folder, agar sesuai dengan presentasi data lainnya.)
- Pesan email
- Acara kalender
- Kontak

Anda dapat menggunakan Pencarian untuk menemukan item di dalam cadangan.

Ketika memulihkan kotak surat dan item kotak surat, Anda dapat memilih apakah item di lokasi target akan ditimpa atau tidak.

Pembatasan

- Foto kontak tidak dapat dipulihkan
- Item kalender **Tidak di kantor** dipulihkan sebagai acara kalender reguler, karena batasan API Kalender Google

Memilih kotak surat Gmail

Pilih kotak surat seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Untuk memilih kotak surat Gmail

1. Klik **Google Workspace**.
2. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, pilih organisasi yang data penggunanya ingin Anda cadangkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk mencadangkan kotak surat semua pengguna (termasuk kotak surat yang akan dibuat di masa mendatang), perluas simpul **Pengguna**, pilih **Semua pengguna**, lalu klik **Pencadangan Grup**.
   - Untuk mencadangkan pengguna individual atau kotak surat bersama, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih Pengguna yang kotak suratnya ingin Anda cadangkan, lalu klik **Cadangkan**.
4. Pada panel rencana proteksi:
   - Pastikan bahwa item **Gmail** dipilih di **Apa yang akan dicadangkan**.
   - Jika Anda ingin mencadangkan kalender yang dibagi dengan pengguna terpilih, aktifkan switch **Termasuk kalender yang dibagi**.

© Acronis International GmbH, 2003-2024

- Tentukan apakah Anda membutuhkan pencarian teks lengkap melalui pesan email yang dicadangkan. Untuk mengakses opsi ini, klik ikon roda > **Opsi pencadangan** > **Pencarian teks lengkap**.

Memulihkan kotak surat dan item kotak surat

Memulihkan kotak surat

1. Klik **Google Workspace**.
2. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang kotak suratnya ingin Anda pulihkan, lalu klik **Pemulihan**.

   Jika pengguna dihapus, pilih pengguna di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.

   Anda dapat mencari pengguna dan grup berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.

   Catatan
   Untuk melihat hanya titik pemulihan yang berisi kotak surat, pilih **Gmail** di **Filter berdasarkan konten**.
5. Klik **Pulihkan** > **Keseluruhan kotak surat**.
6. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, klik **organisasi Google Workspace** untuk melihat, mengubah, atau menentukan organisasi target.

   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus memilih organisasi target baru dari organisasi terdaftar yang tersedia.
7. Di **Pulihkan ke kotak surat**, lihat, ubah, atau tentukan kotak surat target.

   Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan kotak surat target.

   Anda tidak dapat membuat kotak surat target baru selama pemulihan. Untuk memulihkan kotak surat ke versi yang baru, pertama-tama Anda perlu membuat kotak surat target di organisasi Google Workspace yang diinginkan, lalu izinkan agen awan menyinkronkan perubahan tersebut. Agen awan secara otomatis melakukan sinkronisasi dengan Google Workspace setiap 24 jam. Untuk menyinkronkan perubahan dengan segera, di konsol Cyber Protect, pilih organisasi di halaman **Google Workspace**, lalu klik **Menyegarkan**.
8. Klik **Mulai pemulihan**.
9. Pilih salah satu opsi penimpaan:
   - **Timpa item yang ada**
   - **Jangan timpa item yang ada**
10. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

© Acronis International GmbH, 2003-2024

Memulihkan item kotak surat

1. Klik **Google Workspace**.
2. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna dengan kotak surat yang awalnya berisi item yang ingin Anda pulihkan, lalu klik **Pemulihan**.

   Jika pengguna dihapus, pilih pengguna di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.

   Anda dapat mencari pengguna dan grup berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.

   Catatan
   Untuk melihat hanya titik pemulihan yang berisi kotak surat, pilih **Gmail** di **Filter berdasarkan konten**.

5. Klik **Pulihkan** > **Pesan Email**.
6. Jelajahi folder yang diperlukan. Jika pencadangan tidak dienkripsi, Anda dapat menggunakan pencarian untuk mendapatkan daftar item yang diperlukan.

   Opsi pencarian berikut tersedia. Wildcard tidak didukung.
   - Untuk pesan email: cari berdasarkan subjek, pengirim, penerima, tanggal, nama lampiran, dan isi pesan.

     Saat memilih berdasarkan tanggal, Anda dapat memilih tanggal mulai atau tanggal berakhir (keduanya bersifat inklusif), atau kedua tanggal untuk melakukan pencarian dalam suatu rentang waktu.

     Melakukan pencarian berdasarkan nama yang ditautkan atau dalam konten pesan memberikan hasil hanya jika opsi **Pencarian teks lengkap** diaktifkan selama pencadangan. Anda dapat menentukan bahasa fragmen pesan yang akan dicari sebagai parameter tambahan.
   - Untuk acara: cari berdasarkan judul dan tanggal.
   - Untuk kontak: cari berdasarkan nama, alamat email, dan nomor telepon.
7. Pilih item yang ingin Anda pulihkan. Untuk dapat memilih folder, klik ikon "pulihkan folder":

   Selain itu, Anda dapat melakukan hal-hal berikut:
   - Ketika item dipilih, klik **Tampilkan konten** untuk melihat kontennya, termasuk lampiran. Klik nama file terlampir untuk mengunduhnya.
   - Hanya jika cadangan tidak dienkripsi, gunakan pencarian, dan pilih satu item pada hasil pencarian: klik **Tampilkan versi** untuk memilih versi item yang akan dipulihkan. Anda dapat memilih versi yang dicadangkan, yang lebih baru atau lebih lama dari titik pemulihan yang dipilih.
8. Klik **Pulihkan**.

© Acronis International GmbH, 2003-2024

9. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, klik **organisasi Google Workspace** untuk melihat, mengubah, atau menentukan organisasi target.
   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus memilih organisasi target baru dari organisasi terdaftar yang tersedia.
10. Di **Pulihkan ke kotak surat**, lihat, ubah, atau tentukan kotak surat target.
    Secara default, kotak surat asli dipilih. Jika kotak surat ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan kotak surat target.
11. Di **Jalur**, lihat atau ubah folder target di kotak surat target. Secara default, folder asli dipilih.
12. Klik **Mulai pemulihan**.
13. Pilih salah satu opsi penimpaan:
    - **Timpa item yang ada**
    - **Jangan timpa item yang ada**
14. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Melindungi file Google Drive

Apa saja item yang dapat dicadangkan?

Anda dapat mencadangkan keseluruhan Google Drive, atau file dan folder individual. File dicadangkan bersama dengan izin berbaginya.

Penting
Item berikut ini tidak dicadangkan:

- Folder **Dibagikan dengan saya**
- Folder **Komputer** (dibuat oleh klien Pencadangan dan Sinkronisasi)

Pembatasan

Di luar format file khusus Google, Google Docs, Google Sheets, dan Google Slides didukung penuh untuk cadangan dan pemulihan. Format khusus Google lainnya mungkin tidak sepenuhnya didukung atau mungkin tidak didukung sama sekali – misalnya, file Google Drawings dipulihkan sebagai file `.svg`, file Google Sites dipulihkan sebagai file `.txt`, file Google Jamboard dipulihkan sebagai file `.pdf`, dan file Google My Maps dilewati selama pencadangan.

Catatan
Format file yang bukan khusus Google – misalnya, `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip`, didukung sepenuhnya untuk cadangan dan pemulihan.

Apa saja item yang dapat dipulihkan?

Anda dapat memulihkan keseluruhan Google Drive, atau file atau folder apa pun yang dicadangkan.

© Acronis International GmbH, 2003-2024

Anda dapat memilih untuk memulihkan izin atau membiarkan file menerima turunan izin dari folder tujuan pemulihan file.

Pembatasan

- Komentar di file tidak dipulihkan.
- Berbagi tautan untuk file dan folder tidak dapat dipulihkan.
- **Pengaturan Pengguna** berupa hanya baca untuk file yang dibagi (**Mencegah editor mengubah akses dan menambah orang baru** dan **Menonaktifkan opsi untuk mengunduh, mencetak, dan menyalin bagi pengomentar dan pembaca**) tidak dapat diubah selama pemulihan.
- Kepemilikan folder yang dibagi tidak dapat diganti selama pemulihan jika opsi **Mencegah editor dari mengubah akses dan menambah orang baru** diaktifkan untuk folder ini. Pengaturan ini mencegah Google Drive API membuat izin folder. Kepemilikan file dalam folder dipulihkan dengan benar.

Memilih file Google Drive

Pilih file seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Untuk memilih file Google Drive

1. Klik **Google Workspace**.
2. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, pilih organisasi yang data penggunanya ingin Anda cadangkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk mencadangkan file semua pengguna (termasuk pengguna yang akan dibuat di waktu mendatang), perluas simpul **Pengguna**, pilih **Semua pengguna**, lalu klik **Cadangan grup**.
   - Untuk mencadangkan file pengguna individual, perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang filenya ingin Anda cadangkan, lalu klik **Cadangkan**.
4. Pada panel rencana proteksi:
   - Pastikan bahwa item **Google Drive** dipilih di **Apa yang harus dicadangkan**.
   - Di **Item untuk dicadangkan**, lakukan salah satu hal berikut:
     - Simpan pengaturan default **[Semua]** (semua file).
     - Tentukan file dan folder untuk mencadangkan dengan menambahkan nama atau jalur mereka.

       Anda dapat menggunakan karakter wildcard (*, **, dan ?). Untuk informasi lebih lanjut tentang menentukan jalur dan menggunakan wildcard, lihat "Filter file".
     - Tentukan file dan folder yang akan dicadangkan dengan menjelajahi.

       Tautan **Jelajahi** hanya tersedia saat membuat rencana proteksi untuk pengguna tunggal.
   - [Opsional] Di **Item untuk dicadangkan**, klik **Tampilkan pengecualian** untuk menentukan file dan folder yang akan dilewati selama pencadangan.

© Acronis International GmbH, 2003-2024

Pengecualian file akan mengesampingkan pemilihan file tersebut; yaitu jika Anda menentukan file yang sama di kedua bidang, file ini akan dilewati selama pencadangan.

- Jika Anda ingin mengaktifkan notarisasi semua file yang dipilih untuk pencadangan, aktifkanlah switch **Notarisasi**. Untuk informasi lebih lanjut tentang notarisasi, lihat "Notarisasi".

Memulihkan Google Drive dan file Google Drive

Memulihkan keseluruhan Google Drive

1. Klik **Google Workspace**.
2. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang Google Drive-nya ingin Anda pulihkan, lalu klik **Pemulihan**.

   Jika pengguna dihapus, pilih pengguna di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.

   Anda dapat mencari pengguna berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.

   Catatan
   Untuk melihat hanya titik pemulihan yang berisi file Google Drive, pilih **Google Drive** di **Filter berdasarkan konten**.

5. Klik **Pulihkan** > **Seluruh Drive**.
6. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, klik **organisasi Google Workspace** untuk melihat, mengubah, atau menentukan organisasi target.

   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus memilih organisasi target baru dari organisasi terdaftar yang tersedia.
7. Di bagian **Pulihkan ke drive**, lihat, ubah, atau tentukan pengguna target atau drive Shared target.

   Secara default, pengguna asli dipilih. Jika pengguna ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan pengguna target atau drive Shared target.

   Jika cadangan berisi file yang dibagi, file akan dipulihkan ke folder root pada drive target.
8. Pilih apakah akan memulihkan izin berbagi untuk file.
9. Klik **Mulai pemulihan**.

© Acronis International GmbH, 2003-2024

10. Pilih salah satu opsi penimpaan:

Opsi	Deskripsi
Timpa file yang ada jika lebih lama	Jika ada file dengan nama yang sama di lokasi tujuan, dan lebih lama dari file sumber, file sumber akan disimpan di lokasi tujuan, menggantikan versi yang lebih lama.
Timpa file yang ada	Semua file yang ada di lokasi tujuan akan ditimpa, terlepas dari tanggal terakhir diubah.
Jangan timpa file yang ada	Jika ada file dengan nama yang sama di lokasi tujuan, tidak ada perubahan yang diterapkan padanya, dan file sumber tidak disimpan ke lokasi tujuan.

11. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Memulihkan file Google Drive

1. Klik **Google Workspace**.
2. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **Pengguna**, pilih **Semua pengguna**, pilih pengguna yang file Google Drive-nya ingin Anda pulihkan, lalu klik **Pemulihan**.

   Jika pengguna dihapus, pilih pengguna di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.

   Anda dapat mencari pengguna berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.

   Catatan
   Untuk melihat hanya titik pemulihan yang berisi file Google Drive, pilih **Google Drive** di **Filter berdasarkan konten**.

5. Klik **Pulihkan** > **File/folder**.
6. Jelajahi ke folder yang diperlukan atau gunakan pencarian untuk mendapatkan daftar file dan folder yang diperlukan.
7. Pilih file yang ingin Anda pulihkan.

   Jika cadangan tidak dienkripsi dan Anda memilih satu file, Anda dapat mengklik **Tampilkan versi** untuk memilih versi file yang akan dipulihkan. Anda dapat memilih versi yang dicadangkan, yang lebih baru atau lebih lama dari titik pemulihan yang dipilih.
8. Jika Anda ingin mengunduh suatu file, pilih file tersebut, klik **Unduh**, pilih lokasi untuk menyimpan file, lalu klik **Simpan**. Jika tidak, lewati langkah ini.
9. Klik **Pulihkan**.
10. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, klik **organisasi Google Workspace** untuk melihat, mengubah, atau menentukan organisasi target.

© Acronis International GmbH, 2003-2024

Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus memilih organisasi target baru dari organisasi terdaftar yang tersedia.

11. Di bagian **Pulihkan ke drive**, lihat, ubah, atau tentukan pengguna target atau drive Shared target.

    Secara default, pengguna asli dipilih. Jika pengguna ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan pengguna target atau drive Shared target.
12. Di **Jalur**, lihat atau ubah folder target dalam Google Drive pengguna target atau drive Shared target. Secara default, lokasi asli dipilih.
13. Pilih apakah akan memulihkan izin berbagi untuk file.
14. Klik **Mulai pemulihan**.
15. Pilih salah satu opsi penimpaan file:

Opsi	Deskripsi
Timpa file yang ada jika lebih lama	Jika ada file dengan nama yang sama di lokasi tujuan, dan lebih lama dari file sumber, file sumber akan disimpan di lokasi tujuan, menggantikan versi yang lebih lama.
Timpa file yang ada	Semua file yang ada di lokasi tujuan akan ditimpa, terlepas dari tanggal terakhir diubah.
Jangan timpa file yang ada	Jika ada file dengan nama yang sama di lokasi tujuan, tidak ada perubahan yang diterapkan padanya, dan file sumber tidak disimpan ke lokasi tujuan.

16. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Melindungi file drive Shared

Apa saja item yang dapat dicadangkan?

Anda dapat mencadangkan keseluruhan drive Shared, atau file dan folder individual. File dicadangkan bersama dengan izin berbaginya.

Penting
Folder **Dibagikan dengan saya** tidak dicadangkan.

Pembatasan

- Drive Shared tanpa anggota tidak dapat dicadangkan, karena batasan Google Drive API.
- Di luar format file khusus Google, Google Docs, Google Sheets, dan Google Slides didukung penuh untuk cadangan dan pemulihan. Format khusus Google lainnya mungkin tidak sepenuhnya didukung atau mungkin tidak didukung sama sekali – misalnya, file Google Drawings dipulihkan sebagai file `.svg`, file Google Sites dipulihkan sebagai file `.txt`, file Google Jamboard dipulihkan sebagai file `.pdf`, dan file Google My Maps dilewati selama pencadangan.

© Acronis International GmbH, 2003-2024

Catatan
Format file yang bukan khusus Google – misalnya, `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip`, didukung sepenuhnya untuk cadangan dan pemulihan.

Apa saja item yang dapat dipulihkan?

Anda dapat memulihkan keseluruhan drive Shared, atau file atau folder apa pun yang dicadangkan.

Anda dapat memilih untuk memulihkan izin atau membiarkan file menerima turunan izin dari folder tujuan pemulihan file.

Item berikut ini tidak dipulihkan:

- Izin berbagi untuk file yang dibagi dengan pengguna di luar organisasi tidak akan dipulihkan jika berbagi di luar organisasi dinonaktifkan di drive Shared target.
- Izin berbagi untuk file yang dibagi dengan pengguna yang bukan merupakan anggota drive Shared target tidak akan dipulihkan jika **Berbagi dengan non-anggota** dinonaktifkan di drive Shared target.

Pembatasan

- Komentar di file tidak dipulihkan.
- Berbagi tautan untuk file dan folder tidak dapat dipulihkan.

Memilih file drive Shared

Pilih file seperti yang dijelaskan di bawah ini, lalu tentukan pengaturan lain dari rencana proteksi yang sesuai.

Untuk memilih file drive Shared

1. Klik **Google Workspace**.
2. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, pilih organisasi yang data penggunanya ingin Anda cadangkan. Jika tidak, lewati langkah ini.
3. Lakukan salah satu langkah berikut:
   - Untuk mencadangkan file di semua drive Shared (termasuk drive Shared yang akan dibuat di masa mendatang), perluas simpul **drive Shared**, pilih **Semua drive Shared**, lalu klik **Pencadangan grup**.
   - Untuk mencadangkan file di drive Shared individual, perluas simpul **drive Shared**, pilih **Semua drive Shared**, pilih drive Shared untuk mencadangkan, lalu klik **Pencadangan**.
4. Pada panel rencana proteksi:
   - Di **Item untuk dicadangkan**, lakukan salah satu hal berikut:
     - Simpan pengaturan default **[Semua]** (semua file).
     - Tentukan file dan folder untuk mencadangkan dengan menambahkan nama atau jalur mereka.

© Acronis International GmbH, 2003-2024

Anda dapat menggunakan karakter wildcard (*, **, dan ?). Untuk informasi lebih lanjut tentang menentukan jalur dan menggunakan wildcard, lihat "Filter file".

- Tentukan file dan folder yang akan dicadangkan dengan menjelajahi.

  Tautan **Jelajahi** hanya tersedia saat membuat rencana proteksi untuk drive Shared tunggal.

- [Opsional] Di **Item untuk dicadangkan**, klik **Tampilkan pengecualian** untuk menentukan file dan folder yang akan dilewati selama pencadangan.

  Pengecualian file akan mengesampingkan pemilihan file tersebut; yaitu jika Anda menentukan file yang sama di kedua bidang, file ini akan dilewati selama pencadangan.
- Jika Anda ingin mengaktifkan notarisasi semua file yang dipilih untuk pencadangan, aktifkanlah switch **Notarisasi**. Untuk informasi lebih lanjut tentang notarisasi, lihat "Notarisasi".

Memulihkan drive Shared dan file drive Shared

Memulihkan keseluruhan drive Shared

1. Klik **Google Workspace**.
2. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **drive Shared**, pilih **Semua drive Shared**, pilih drive Shared yang ingin Anda pulihkan, lalu klik **Pemulihan**.

   Jika drive Shared dihapus, pilih drive tersebut di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tampilkan cadangan**.

   Anda dapat mencari drive Shared berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.
5. Klik **Pulihkan** > **Seluruh drive Shared**.
6. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, klik **organisasi Google Workspace** untuk melihat, mengubah, atau menentukan organisasi target.

   Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus memilih organisasi target baru dari organisasi terdaftar yang tersedia.
7. Di bagian **Pulihkan ke drive**, lihat, ubah, atau tentukan drive Shared target atau pengguna target. Jika Anda menentukan seorang pengguna, datanya akan dipulihkan ke Google Drive pengguna ini.

   Secara default, drive Shared asli dipilih. Jika drive Shared ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan drive Shared target atau pengguna target.
8. Pilih apakah akan memulihkan izin berbagi untuk file.
9. Klik **Mulai pemulihan**.

© Acronis International GmbH, 2003-2024

10. Pilih salah satu opsi penimpaan:

Opsi	Deskripsi
Timpa file yang ada jika lebih lama	Jika ada file dengan nama yang sama di lokasi tujuan, dan lebih lama dari file sumber, file sumber akan disimpan di lokasi tujuan, menggantikan versi yang lebih lama.
Timpa file yang ada	Semua file yang ada di lokasi tujuan akan ditimpa, terlepas dari tanggal terakhir diubah.
Jangan timpa file yang ada	Jika ada file dengan nama yang sama di lokasi tujuan, tidak ada perubahan yang diterapkan padanya, dan file sumber tidak disimpan ke lokasi tujuan.

11. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Memulihkan file drive Shared

1. Klik **Google Workspace**.
2. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, pilih organisasi yang data cadangannya ingin Anda pulihkan. Jika tidak, lewati langkah ini.
3. Perluas simpul **drive Shared**, pilih **Semua drive Shared**, pilih drive Shared yang awalnya berisi file yang ingin Anda pulihkan, lalu klik **Pemulihan**.

   Jika drive Shared dihapus, pilih drive tersebut di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tampilkan cadangan**.

   Anda dapat mencari drive Shared berdasarkan nama. Wildcard tidak didukung.
4. Pilih titik pemulihan.
5. Klik **Pulihkan** > **File/folder**.
6. Jelajahi ke folder yang diperlukan atau gunakan pencarian untuk mendapatkan daftar file dan folder yang diperlukan.
7. Pilih file yang ingin Anda pulihkan.

   Jika cadangan tidak dienkripsi dan Anda memilih satu file, Anda dapat mengklik **Tampilkan versi** untuk memilih versi file yang akan dipulihkan. Anda dapat memilih versi yang dicadangkan, yang lebih baru atau lebih lama dari titik pemulihan yang dipilih.
8. Jika Anda ingin mengunduh suatu file, pilih file tersebut, klik **Unduh**, pilih lokasi untuk menyimpan file, lalu klik **Simpan**. Jika tidak, lewati langkah ini.
9. Klik **Pulihkan**.
10. Jika beberapa organisasi Google Workspace ditambahkan ke layanan Cyber Protection, klik **organisasi Google Workspace** untuk melihat, mengubah, atau menentukan organisasi target.

    Secara default, organisasi asli dipilih. Jika organisasi ini tidak lagi terdaftar di layanan Cyber Protection, Anda harus memilih organisasi target baru dari organisasi terdaftar yang tersedia.
11. Di bagian **Pulihkan ke drive**, lihat, ubah, atau tentukan drive Shared target atau pengguna target. Jika Anda menentukan seorang pengguna, datanya akan dipulihkan ke Google Drive pengguna ini.

© Acronis International GmbH, 2003-2024

Secara default, drive Shared asli dipilih. Jika drive Shared ini tidak ada atau organisasi non-asli dipilih, Anda harus menentukan drive Shared target atau pengguna target.

12. Di **Jalur**, lihat atau ubah folder target dalam drive Shared target atau Google Drive pengguna target. Secara default, lokasi asli dipilih.
13. Pilih apakah akan memulihkan izin berbagi untuk file.
14. Klik **Mulai pemulihan**.
15. Pilih salah satu opsi penimpaan file:

Opsi	Deskripsi
Timpa file yang ada jika lebih lama	Jika ada file dengan nama yang sama di lokasi tujuan, dan lebih lama dari file sumber, file sumber akan disimpan di lokasi tujuan, menggantikan versi yang lebih lama.
Timpa file yang ada	Semua file yang ada di lokasi tujuan akan ditimpa, terlepas dari tanggal terakhir diubah.
Jangan timpa file yang ada	Jika ada file dengan nama yang sama di lokasi tujuan, tidak ada perubahan yang diterapkan padanya, dan file sumber tidak disimpan ke lokasi tujuan.

16. Klik **Memproses** untuk mengonfirmasi keputusan Anda.

Notarisasi

Notarisasi memungkinkan Anda untuk membuktikan bahwa file tersebut asli dan tidak berubah sejak dicadangkan. Kami menyarankan Anda untuk mengaktifkan notarisasi ketika mencadangkan file dokumen hukum atau file lain yang membutuhkan keaslian yang terbukti.

Notarisasi tersedia hanya untuk cadangan file Google Drive dan file drive Shared Google Workspace.

Cara menggunakan notarisasi

Untuk mengaktifkan notarisasi semua file yang dipilih untuk pencadangan, aktifkan switch **Notarisasi** saat membuat rencana proteksi.

Saat mengonfigurasi pemulihan, file yang dinotariskan akan ditandai dengan ikon khusus, dan Anda dapat memverifikasi keaslian file.

Cara kerjanya

Selama pencadangan, agen akan menghitung kode hash dari file yang dicadangkan, membangun pohon hash (berdasarkan pada struktur folder), menyimpan pohon di cadangan, lalu mengirimkan root pohon hash ke layanan notaris. Layanan notaris menyimpan root pohon hash dalam database blockchain Ethereum untuk memastikan bahwa nilai ini tidak berubah.

Saat memverifikasi keaslian file, agen akan menghitung hash file, lalu membandingkannya dengan hash yang disimpan di pohon hash dalam cadangan. Jika hash tidak cocok, file tersebut akan dianggap tidak asli. Jika tidak, keaslian file dijamin oleh pohon hash.

© Acronis International GmbH, 2003-2024

Untuk memverifikasi bahwa pohon hash itu sendiri tidak terganggu, agen akan mengirimkan root pohon hash ke layanan notaris. Layanan notaris akan membandingkannya dengan yang disimpan dalam database blockchain. Jika hash cocok, file yang dipilih dijamin asli. Jika tidak, perangkat lunak akan menampilkan pesan bahwa file tersebut tidak asli.

Memverifikasi keaslian file dengan Layanan Notaris

Jika notarisisasi diaktifkan selama pencadangan, Anda dapat memverifikasi keaslian file yang dicadangkan.

Untuk memverifikasi keaslian file

1. Lakukan salah satu langkah berikut:
   - Untuk memastikan keaslian file Google Drive, pilih file seperti dijelaskan dalam langkah 1-7 di bagian "Memulihkan file Google Drive".
   - Untuk memastikan keaslian file drive Shared Google Workspace, pilih file seperti dijelaskan dalam langkah 1-7 di bagian "Memulihkan file drive Shared".
2. Pastikan bahwa file yang dipilih ditandai dengan ikon berikut: . Ini berarti bahwa file tersebut sudah dinotariskan.
3. Lakukan salah satu langkah berikut:
   - Klik **Verifikasi**.
     Perangkat lunak akan memeriksa keaslian file dan menampilkan hasilnya.
   - Klik **Dapatkan sertifikat**.
     Sertifikat yang mengonfirmasi notarisasi file dibuka di jendela browser web. Jendela ini juga berisi instruksi yang memungkinkan Anda memverifikasi keaslian file secara manual.

Pencarian dalam cadangan cloud ke cloud

Ketika memulihkan data, Anda dapat mencari item cadangan tertentu alih-alih menjelajahi arsip cadangan.

Dalam cadangan yang tidak dienkripsi, pencarian selalu bisa dilakukan. Hanya pencarian (berbasis indeks) yang ditingkatkan yang didukung.

Pencarian berbasis indeks lebih cepat dan menyediakan opsi tambahan, seperti menampilkan versi dari item yang dicadangkan, mencari dalam nama lampiran, dan pencarian teks lengkap dalam cadangan Gmail.

Dalam cadangan yang dienkripsi, Anda juga dapat mengaktifkan pencarian (berbasis indeks) yang ditingkatkan. Jika Anda tidak mengaktifkan pencarian yang ditingkatkan, pencarian dasar akan tersedia untuk cadangan kotak surat Microsoft 365. Untuk semua beban kerja lainnya, pencarian tidak akan tersedia.

Tabel di bawah ini merangkum opsi yang tersedia untuk cadangan yang dienkripsi.

© Acronis International GmbH, 2003-2024

Jenis beban kerja	Apa yang dipulihkan	Pencarian yang ditingkatkan dinonaktifkan	Pencarian yang ditingkatkan diaktifkan
Beban kerja Microsoft 365			
Kotak surat	Pesan email	Pencarian dasar (berbasis non-indeks) tersedia	Pencarian yang ditingkatkan (berbasis indeks) tersedia
OneDrive	File/folder	Pencarian tidak tersedia	Pencarian yang ditingkatkan (berbasis indeks) tersedia
Situs SharePoint	File SharePoint	Pencarian tidak tersedia	Pencarian yang ditingkatkan (berbasis indeks) tersedia
Teams	Saluran	Pencarian tidak tersedia	Pencarian yang ditingkatkan (berbasis indeks) tersedia
	Pesan email	Pencarian dasar (berbasis non-indeks) tersedia	Pencarian yang ditingkatkan (berbasis indeks) tersedia
	Situs tim	Pencarian tidak tersedia	Pencarian yang ditingkatkan (berbasis indeks) tersedia
Beban kerja Google Workspace			
Kotak surat	Pesan email	Pencarian tidak tersedia	Pencarian yang ditingkatkan (berbasis indeks) tersedia
Google Drive	File/folder	Pencarian tidak tersedia	Pencarian yang ditingkatkan (berbasis indeks) tersedia
Shared Drive	File/folder	Pencarian tidak tersedia	Pencarian yang ditingkatkan (berbasis indeks) tersedia

Pencarian teks lengkap

Pencarian teks lengkap hanya tersedia untuk cadangan Gmail, dan ini diaktifkan secara default. Dengan itu, Anda dapat mencari di tubuh teks dari email yang dicadangkan. Jika opsi ini dinonaktifkan, Anda hanya dapat mencari berdasarkan subjek, pengirim, penerima, dan tanggal.

Indeks pencarian teks lengkap membutuhkan antara 10 dan 30 persen dari ruang penyimpanan yang diisi oleh cadangan Gmail. Indeks tanpa data pencarian teks lengkap jauh lebih kecil. Untuk menghemat ruang penyimpanan, Anda dapat menonaktifkan pencarian teks lengkap dan membersihkan porsi indeks yang berisi data pencarian teks lengkap.

Indeks pencarian

Indeks pencarian menyediakan kemampuan pencarian yang ditingkatkan dalam arsip cadangan cloud ke cloud.

© Acronis International GmbH, 2003-2024

Arsip secara otomatis diindeks setelah setiap operasi pencadangan. Proses pengindeksan tidak mempengaruhi kinerja pencadangan karena pengindeksan dan pencadangan dilakukan oleh komponen perangkat lunak yang berbeda.

Hasil pencarian bisa ditampilkan setelah operasi pengindeksan selesai, yang mungkin memakan waktu hingga 24 jam. Pengindeksan cadangan pertama, yang penuh, biasanya memakan waktu lebih lama daripada pengindeksan cadangan bertahap selanjutnya.

Semua indeks berisi metadata yang mendukung fungsi pencarian utama, yaitu pencarian berdasarkan subjek, pengirim, penerima, atau tanggal. Indeks untuk cadangan Gmail berisi data tambahan jika pencarian teks lengkap diaktifkan.

Memeriksa ukuran indeks pencarian

Indeks pencarian bertambah besar seiring waktu. Indeks untuk arsip cadangan di mana pencarian teks penuh diaktifkan, mungkin bisa mencapai 30 persen dari ukuran arsip.

Untuk memeriksa ukuran indeks pencarian

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Di tab **Penyimpanan cadangan**, klik **Cadangan aplikasi cloud**.
3. Periksa nilai di kolom **Ukuran Indeks**.

Memperbarui, membangun ulang, atau menghapus indeks

Untuk memecahkan masalah terkait pencarian dalam cadangan cloud ke cloud, Anda dapat memperbarui, membangun ulang, atau menghapus indeks pencarian.

Catatan
Kami merekomendasikan Anda untuk menghubungi tim Dukungan sebelum memperbarui, membangun ulang, atau menghapus indeks.

Cara memperbarui, membangun ulang, atau menghapus indeks

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Di tab **Penyimpanan cadangan**, klik **Cadangan aplikasi cloud**.
   Pilih arsip yang indeksnya ingin Anda perbarui, bangun ulang, atau hapus.
   Ketersediaan tindakan-tindakan ini tergantung pada tingkat dan peran administrator, sebagai berikut:

© Acronis International GmbH, 2003-2024

Level akun	Peran	Dapat memperbarui indeks	Dapat membuat ulang indeks	Dapat menghapus indeks
Mitra penyewa	Administrator perusahaan	+	+	+
	Administrator siber proteksi	+	-	-
	Administrator proteksi	+	-	-
	Administrator hanya baca proteksi	-	-	-
Penyewa pelanggan	Administrator perusahaan	+	-	-
	Administrator proteksi	+	-	-
	Administrator hanya baca proteksi	-	-	-
Unit	Administrator unit	+	-	-
	Administrator proteksi	+	-	-
	Administrator hanya baca proteksi	-	-	-

3. Di panel **Aksi**, pilih tindakan yang ingin Anda lakukan:
   - **Perbarui indeks**—titik pemulihan dalam arsip diperiksa, dan indeks yang hilang ditambahkan.
   - **Membangun ulang indeks**—indeks untuk semua titik pemulihan di arsip dihapus, dan kemudian indeks dibuat lagi.
   - **Hapus indeks**—indeks untuk semua titik pemulihan di arsip dihapus.
4. [Untuk arsip terenkripsi] Tentukan kata sandi enkripsi, lalu klik **OK**.
5. Pilih cakupan dari tindakan, lalu klik **OK**.
   Tergantung pada arsip dan tindakan yang dipilih, satu atau beberapa opsi berikut tersedia:
   - **Metadata saja**
   - **Isi saja**
   - **Pencarian metadata dan isi**

Mengaktifkan pencarian yang ditingkatkan dalam cadangan yang dienkripsi

Saat membuat rencana pencadangan untuk cadangan cloud ke cloud yang dienkripsi, Anda dapat mengaktifkan pencarian (berbasis indeks) yang ditingkatkan.

Jika Anda tidak mengaktifkan pencarian yang ditingkatkan, pencarian dasar akan tersedia untuk cadangan kotak surat Microsoft 365. Untuk semua beban kerja lainnya, pencarian tidak akan

© Acronis International GmbH, 2003-2024

tersedia. Untuk informasi lebih lanjut tentang opsi yang tersedia, lihat "Pencarian dalam cadangan cloud ke cloud" (hlm. 659).

Catatan
Fungsionalitas ini tersedia di pusat data tertentu dan mungkin tidak dapat diakses oleh semua pelanggan.

Untuk mengaktifkan pencarian dalam cadangan yang dienkripsi

1. Saat membuat rencana pencadangan, aktifkan sakelar **Enkripsi**.
2. Masukkan dan konfirmasi kata sandi enkripsi.
3. Pilih kotak centang **Izinkan pencarian ditingkatkan dalam cadangan enkripsi**.
4. Klik **Selesai**.

Catatan
Anda tidak dapat menonaktifkan enkripsi atau mengubah kata sandi enkripsi di lain waktu. Untuk membuat cadangan tanpa enkripsi atau mengubah kata sandi enkripsi, buatlah rencana pencadangan baru.

Mengaktifkan atau menonaktifkan pencarian yang ditingkatkan dalam rencana yang ada

Anda dapat mengedit Rencana cadangan enkripsi yang ada untuk mengaktifkan atau menonaktifkan Pencarian (berbasis indeks) yang ditingkatkan.

Jika Anda tidak mengaktifkan pencarian yang ditingkatkan, pencarian dasar akan tersedia untuk cadangan kotak surat Microsoft 365. Untuk semua beban kerja lainnya, pencarian tidak akan tersedia. Untuk informasi lebih lanjut tentang opsi yang tersedia, lihat "Pencarian dalam cadangan cloud ke cloud" (hlm. 659).

Dalam cadangan yang tidak dienkripsi, pencarian yang ditingkatkan selalu aktif. Opsi ini tidak dapat dinonaktifkan.

Untuk mengaktifkan atau menonaktifkan pencarian yang ditingkatkan dalam cadangan yang dienkripsi

1. Ketika mengedit rencana pencadangan tempat enkripsi diaktifkan, klik ikon roda di pojok kanan atas.
2. Pada tab **Opsi pencarian**, ubah posisi sakelar sesuai kebutuhan.
3. Klik **Selesai**.
4. Klik **Simpan pengaturan**.

© Acronis International GmbH, 2003-2024

Catatan
Jika Anda mengaktifkan kembali pencarian yang ditingkatkan, semua arsip yang dibuat oleh rencana pencadangan ini akan diindeks lagi. Ini adalah operasi yang memakan waktu.

Menonaktifkan pencarian teks lengkap untuk cadangan Gmail

Pencarian teks lengkap hanya tersedia untuk cadangan Gmail, dan ini diaktifkan secara default. Dengan itu, Anda dapat mencari di tubuh teks dari email yang dicadangkan. Jika opsi ini dinonaktifkan, Anda hanya dapat mencari berdasarkan subjek, pengirim, penerima, dan tanggal.

Anda mungkin ingin menonaktifkan pencarian teks lengkap jika Anda perlu menjaga ukuran indeks pencarian tetap minimal.

Untuk menonaktifkan pencarian teks lengkap

1. Ketika membuat atau mengedit rencana pencadangan, klik ikon roda di pojok kanan atas.
2. Pada tab **Pencarian teks lengkap**, nonaktifkan sakelar.
3. Klik **Selesai**.
4. [Ketika membuat rencana] Klik **Terapkan**.
5. [Ketika mengedit rencana] Klik **Simpan pengaturan**.

Catatan
Jika Anda mengaktifkan kembali pencarian teks lengkap, semua arsip yang dibuat oleh rencana pencadangan ini akan diindeks lagi. Ini adalah operasi yang memakan waktu.

Melindungi Database Oracle

Catatan
Fitur ini tersedia dengan paket Cadangan Lanjutan.

Perlindungan Oracle Database dijelaskan dalam dokumen terpisah yang tersedia di https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf

Perlindungan SAP HANA

Catatan
Fitur ini tersedia dengan paket Cadangan Lanjutan.

Perlindungan SAP HANA dijelaskan dalam dokumen terpisah yang tersedia di https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf

© Acronis International GmbH, 2003-2024

Melindungi data MySQL dan MariaDB

Anda dapat melindungi data MySQL atau MariaDB dengan cadangan keberadaan aplikasi. Cadangan keberadaan aplikasi mengumpulkan metadata aplikasi dan memungkinkan pemulihan granular pada level instans, database, atau tabel.

Catatan
Cadangan keberadaan aplikasi data MySQL atau MariaDB tersedia dengan paket Cadangan Lanjutan.

Untuk melindungi mesin fisik atau virtual yang menjalankan instans MySQL atau MariaDB dengan cadangan keberadaan aplikasi, Anda perlu menginstal Agen untuk MySQL/MariaDB pada mesin ini. Agen untuk MySQL/MariaDB dibundel dengan Agen untuk Linux (64-bit) dan karenanya hanya dapat diinstal pada sistem operasi berbasis Linux 64-bit. Lihat "Sistem operasi dan lingkungan yang Didukung" (hlm. 23).

Untuk mengunduh file instalasi Agen untuk Linux (64 bit)

1. Masuk ke konsol Cyber Protect.
2. Klik ikon akun di sudut kanan atas, lalu pilih **Unduhan**.
3. Klik **Agen untuk Linux (64 bit)**.

   File instalasi diunduh ke mesin Anda. Untuk menginstal agen, lanjutkan seperti yang dijelaskan di "Menginstal agen proteksi di Linux" (hlm. 78) atau "Instalasi atau penghapusan tanpa pengawasan di Linux" (hlm. 104). Pastikan bahwa Anda memilih Agen untuk MySQL/MariaDB yang merupakan komponen opsional.

   Untuk memulihkan database dan tabel ke instans langsung, Agen untuk MySQL/MariaDB memerlukan penyimpanan sementara agar dapat beroperasi. Secara default, direktori `/tmp` digunakan. Anda dapat mengubah direktori ini dengan mengatur variabel lingkungan `ACRONIS_MYSQL_RESTORE_DIR`.

Pembatasan

- Klaster MySQL atau MariaDB tidak didukung.
- Instans MySQL atau MariaDB yang berjalan di kontainer Docker tidak didukung.
- Instans MySQL atau MariaDB yang berjalan pada sistem operasi yang menggunakan sistem file BTRFS tidak didukung.
- Database sistem (`sys`, `mysql`, `information-schema`, dan `performance_schema`) dan database yang tidak berisi tabel apa pun tidak dapat dipulihkan ke instans langsung. Namun, database ini dapat dipulihkan sebagai file, saat memulihkan seluruh instans.
- Pemulihan hanya didukung untuk instans target dari versi yang sama dengan instans yang dicadangkan atau yang lebih baru, dengan batasan berikut:

© Acronis International GmbH, 2003-2024

- Pemulihan dari instans MySQL 5.x ke instans MySQL 8.x tidak didukung.
- Pemulihan ke versi MySQL 5.x yang lebih baru (termasuk versi minor) hanya didukung melalui pemulihan seluruh instans sebagai file. Sebelum mencoba pemulihan, lihat panduan peningkatan versi MySQL resmi untuk versi target, misalnya, panduan peningkatan versi MySQL 5.7.

- Pemulihan dari cadangan yang disimpan pada Secure Zone tidak didukung.
- Database dan tabel tidak dapat dipulihkan oleh Agen untuk MySQL/MariaDB yang berjalan pada mesin tempat AppArmor diinstal. Anda masih dapat memulihkan instans sebagai file atau seluruh mesin.
- Pemulihan ke database target yang dikonfigurasi dengan tautan simbolik tidak didukung. Anda dapat memulihkan database yang dicadangkan sebagai database baru dengan mengubah namanya.

Masalah yang diketahui

Jika Anda mengalami masalah saat memulihkan data dari share Samba yang dilindungi kata sandi, keluar dari konsol Cyber Protect, lalu masuk kembali ke sana. Pilih titik pemulihan yang diinginkan, lalu klik **database MySQL/Maria DB**. Jangan mengeklik **Seluruh mesin** atau **File/folder**.

Mengonfigurasi cadangan keberadaan aplikasi

Prasyarat

- Setidaknya satu instans MySQL atau MariaDB harus berjalan pada mesin yang dipilih.
- Pada mesin tempat instans MySQL atau MariaDB berjalan, agen proteksi harus dimulai dari pengguna root.
- Cadangan keberadaan aplikasi tersedia hanya saat **Seluruh mesin** dipilih sebagai sumber cadangan di rencana proteksi.
- Opsi pencadangan **sektor demi sektor** harus dinonaktifkan di rencana proteksi. Jika tidak, maka tidak mungkin memulihkan aplikasi data.

Untuk mengonfigurasi cadangan keberadaan aplikasi

1. Di konsol Cyber Protect, pilih satu atau lebih mesin yang menjalankan instans MySQL atau MariaDB.

   Anda dapat memiliki satu instans atau lebih pada setiap mesin.
2. Buat rencana proteksi dengan mengaktifkan modul cadangan.
3. Dalam **Apa yang akan dicadangkan**, pilih **Seluruh mesin**.
4. Klik **Cadangan aplikasi**, lalu aktifkan tombol di sebelah **MySQL/MariaDB Server**.
5. Pilih cara menentukan instans MySQL atau MariaDB:
   - **Untuk semua beban kerja**

© Acronis International GmbH, 2003-2024

Gunakan opsi ini jika Anda menjalankan instans dengan konfigurasi identik di beberapa server. Parameter koneksi dan kredensial akses yang sama akan digunakan untuk semua instans.

- **Untuk beban kerja tertentu**

  Gunakan opsi ini untuk menentukan parameter koneksi dan kredensial akses untuk setiap instans.

6. Klik **Tambahkan instans** untuk mengonfigurasi parameter dan kredensial akses.
   a. Pilih jenis koneksi, lalu tentukan hal berikut:
      - [Untuk soket TCP] Alamat dan port IP.
      - [Untuk soket Unix] Jalur soket.
   b. Tentukan kredensial akun pengguna yang memiliki hak istimewa berikut untuk instans:
      - `FLUSH_TABLES` atau `RELOAD` untuk semua database dan tabel (`*.*`)
      - `SELECT` untuk `information_schema.tables`
   c. Klik **OK**.
7. Klik **Selesai**.

Memulihkan data dari cadangan keberadaan aplikasi

Dari cadangan keberadaan aplikasi, Anda dapat memulihkan instans, database, dan tabel MySQL atau MariaDB. Anda juga dapat memulihkan seluruh server tempat instans tersebut berjalan atau file dan folder dari server ini.

Tabel di bawah ini merangkum seluruh opsi pemulihan.

Apa yang dipulihkan	Pulihkan sebagai	Pulihkan ke
Server MySQL Server MariaDB	Seluruh mesin	Mesin* tempat Agen untuk Linux diinstal
Server MySQL Server MariaDB	File atau folder	Mesin* tempat Agen untuk Linux diinstal
Instans	File	Mesin* tempat Agen untuk MySQL/MariaDB diinstal
Database	Database yang sama Database baru	Mesin* tempat Agen untuk MySQL/MariaDB diinstal • Contoh orisinal • Instans lainnya • Database asli

© Acronis International GmbH, 2003-2024

Apa yang dipulihkan	Pulihkan sebagai	Pulihkan ke
		• Database baru
Tabel	Tabel yang sama Tabel baru	Mesin* tempat Agen untuk MySQL/MariaDB diinstal • Contoh orisinal • Instans lainnya • Database asli • Tabel asli • Tabel baru

* Mesin virtual dengan agen di dalamnya diperlakukan sebagai mesin fisik dari sudut pandang cadangan.

Memulihkan seluruh server

Untuk mempelajari cara memulihkan seluruh server tempat instans MySQL dan MariaDB berjalan, lihat "Memulihkan mesin" (hlm. 498).

Memulihkan instans

Dari cadangan keberadaan aplikasi, Anda dapat memulihkan instans MySQL atau MariaDB sebagai file.

Untuk memulihkan instans

1. Di konsol Cyber Protect, select the machine that originally contained the data that you want to recover.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Lakukan salah satu langkah berikut:
   - Jika lokasi cadangan adalah penyimpanan awan atau penyimpanan bersama (yang dapat diakses agen lain), klik **Pilih mesin**, pilih mesin online yang memiliki Agen untuk MySQL/MariaDB, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab **Penyimpanan cadangan**.

   Mesin yang dipilih untuk melakukan tindakan-tindakan di atas menjadi mesin target untuk pemulihan.
4. Klik **Pulihkan** > **Database MySQL/MariaDB**.
5. Pilih instans yang ingin Anda pulihkan, lalu klik **Pulihkan sebagai file**.
6. Pada **Jalur**, pilih direktori tempat file akan dipulihkan.
7. Klik **Mulai pemulihan**.

© Acronis International GmbH, 2003-2024

Memulihkan database

Dari cadangan keberadaan aplikasi, Anda dapat memulihkan database ke instans MySQL atau MariaDB langsung.

1. Di konsol Cyber Protect, select the machine that originally contained the data that you want to recover.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.

   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Lakukan salah satu langkah berikut:
   - Jika lokasi cadangan adalah penyimpanan awan atau penyimpanan bersama (yang dapat diakses agen lain), klik **Pilih mesin**, pilih mesin online yang memiliki Agen untuk MySQL/MariaDB, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab **Penyimpanan cadangan**.

   Mesin yang dipilih untuk melakukan tindakan-tindakan di atas menjadi mesin target untuk pemulihan.
4. Klik **Pulihkan** > **Database MySQL/MariaDB**.
5. Klik nama instans yang diinginkan untuk menelusuri database-nya.
6. Pilih satu atau beberapa database yang ingin Anda pulihkan.
7. Klik **Pulihkan**.
8. Klik **Instans MySQL/MariaDB target** untuk menentukan parameter koneksi dan kredensial akses untuk instans target.
   - Verifikasi instans tempat Anda ingin memulihkan data. Secara default, instans asli dipilih.
   - Tentukan kredensial akun pengguna yang dapat mengakses instans target. Akun pengguna ini harus memiliki hak istimewa berikut untuk semua database dan tabel (`*.*`):
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Klik **OK**.
9. Verifikasi database target.

   Secara default, database asli dipilih.

   Untuk memulihkan database sebagai database baru, klik nama database target dan ubah. Tindakan ini hanya tersedia saat Anda memulihkan database tunggal.
10. Pada **Timpa basis data yang ada**, pilih mode penimpaan.

© Acronis International GmbH, 2003-2024

Secara default, penimpaan diaktifkan dan database yang dicadangkan akan menggantikan database target yang memiliki nama yang sama.

Jika penimpaan dinonaktifkan, database yang dicadangkan akan dilewati selama operasi pemulihan dan tidak akan menggantikan database target yang memiliki nama yang sama.

11. Klik **Mulai pemulihan**.

Memulihkan tabel

Dari cadangan keberadaan aplikasi, Anda dapat memulihkan tabel ke instans MySQL atau MariaDB langsung.

1. Di konsol Cyber Protect, select the machine that originally contained the data that you want to recover.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.

   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Lakukan salah satu langkah berikut:

   - Jika lokasi cadangan adalah penyimpanan awan atau penyimpanan bersama (yang dapat diakses agen lain), klik **Pilih mesin**, pilih mesin online yang memiliki Agen untuk MySQL/MariaDB, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab **Penyimpanan cadangan**.

   Mesin yang dipilih untuk melakukan tindakan-tindakan di atas menjadi mesin target untuk pemulihan.
4. Klik **Pulihkan** > **Database MySQL/MariaDB**.
5. Klik nama instans yang diinginkan untuk menelusuri database-nya.
6. Klik nama database yang diinginkan untuk menelusuri tabelnya.
7. Pilih satu atau beberapa tabel yang ingin Anda pulihkan.
8. Klik **Pulihkan**.
9. Klik **Instans MySQL/MariaDB target** untuk menentukan parameter koneksi dan kredensial akses untuk instans target.
   - Verifikasi instans tempat Anda ingin memulihkan data. Secara default, instans asli dipilih.
   - Tentukan kredensial akun pengguna yang dapat mengakses instans target. Akun pengguna ini harus memiliki hak istimewa berikut untuk semua database dan tabel (`*.*`):
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Klik **OK**.

© Acronis International GmbH, 2003-2024

10. Verifikasi tabel target.

    Secara default, tabel asli dipilih.

    Untuk memulihkan tabel sebagai tabel baru, klik nama tabel target dan ubah. Tindakan ini hanya tersedia saat Anda memulihkan tabel tunggal.
11. Pada **Timpa tabel yang ada**, pilih mode penimpaan.

    Secara default, penimpaan diaktifkan dan tabel yang dicadangkan akan menggantikan tabel target yang memiliki nama yang sama.

    Jika penimpaan dinonaktifkan, tabel yang dicadangkan akan dilewati selama operasi pemulihan dan tidak akan menggantikan tabel target yang memiliki nama yang sama.
12. Klik **Mulai pemulihan**.

Memulihkan rutinitas yang disimpan

Saat Anda memulihkan keseluruhan instans MySQL, rutinitas yang disimpan secara otomatis dipulihkan.

Saat Anda memulihkan database satuan ke instans non-orisinal atau memulihkannya sebagai database baru, rutinitas yang disimpan tidak dapat dipulihkan secara otomatis. Anda dapat memulihkannya secara manual, dengan mengekspornya menjadi file SQL, kemudian menambahkannya ke database yang dipulihkan.

Untuk mengekspor rutinitas yang disimpan dan menambahkannya ke database yang dipulihkan

1. Pada mesin dengan instans MySQL orisinal, buka Terminal.
2. Jalankan perintah berikut untuk mengekspor rutinitas yang disimpan.
3. ```
   mysqldump -p [source_database_name] --routines --no-create-info --no-data > [exported_db_routines.sql]
   ```
4. Pada mesin di mana the database dipulihkan, buka klien baris perintah MySQL.
5. Jalankan perintah berikut untuk menambahkan rutinitas ke database yang dipulihkan.

   ```
   mysql>  use [recovered_database_name];
   ```

   ```
   mysql>  source [path_to_exported_db_routines.sql];
   ```

Melindungi situs web dan server hosting

Melindungi situs web

Situs web dapat rusak akibat akses tidak berizin atau serangan malware. Cadangkan situs web Anda jika Anda ingin mudah mengembalikannya ke status yang sehat, jika terjadi kerusakan.

© Acronis International GmbH, 2003-2024
   ```

Apa yang saya perlukan untuk mencadangkan situs web?

Situs web harus dapat diakses melalui protokol SFTP atau SSH. Anda tidak perlu menginstal agen, cukup tambahkan situs web seperti yang akan dijelaskan nanti di bagian ini.

Apa saja item yang dapat dicadangkan?

Anda dapat mencadangkan item berikut:

- **File konten situs web**
  Semua file dapat diakses ke akun yang Anda tetapkan untuk koneksi SFTP atau SSH.
- **Database tertaut (jika ada) yang di-hosting pada server MySQL.**
  Semua database dapat diakses dengan akun MySQL yang Anda tentukan.

Jika situs web Anda menggunakan database, kami sarankan Anda untuk mencadangkan file dan database, agar dapat memulihkannya ke status konsisten.

Pembatasan

- Satu-satunya lokasi pencadangan yang memungkinkan untuk pencadangan situs web adalah penyimpanan awan.
- Penerapan beberapa rencana proteksi pada suatu situs web dapat dilakukan, tapi hanya salah satunya yang dapat berjalan sesuai jadwal. Rencana lain perlu dimulai secara manual.
- Satu-satunya opsi pencadangan yang tersedia adalah "Nama file cadangan".
- Rencana proteksi situs web tidak ditampilkan di tab **Manajemen** > **Rencana proteksi**.

Mencadangkan situs web

Untuk menambahkan situs web

1. Klik **Perangkat** > **Tambah**.
2. Klik **Situs web**.
3. Konfigurasikan pengaturan akses untuk situs web berikut:
   - Pada **Nama situs web**, buat dan ketik nama untuk situs web Anda. Nama ini akan ditampilkan di konsol Cyber Protect.
   - Pada **Host**, tentukan nama host atau alamat IP yang akan digunakan untuk mengakses situs web melalui SFTP atau SSH. Misalnya, `my.server.com` atau `10.250.100.100`.
   - Pada **Port**, tentukan nomor port.
   - Pada **Nama pengguna** dan **Kata sandi**, tentukan kredensial akun yang dapat digunakan untuk mengakses situs web melalui SFTP atau SSH.

     Penting
     File yang akan dicadangkan hanya file yang dapat diakses ke akun yang ditentukan.

© Acronis International GmbH, 2003-2024

Sebagai ganti kata sandi, Anda dapat menentukan kunci SSH privat Anda sendiri. Untuk melakukan hal ini, pilih kotak centang **Gunakan kunci privat SSH, bukan kata sandi**, lalu tentukan kuncinya.

4. Klik **Berikutnya**.
5. Jika situs web Anda menggunakan database MySQL, konfigurasikan pengaturan akses untuk database. Jika tidak, klik **Lewati**.
   a. Pada **Jenis koneksi**, pilih cara mengakses database dari awan:
      - **Melalui SSH dari host**—Database akan diakses melalui host yang ditentukan pada langkah 3.
      - **Koneksi langsung**—Database akan diakses langsung. Pilih pengaturan ini hanya jika database dapat diakses dari internet.

   b. Pada **Host**, tentukan nama atau alamat IP host di mana server MySQL dijalankan.

   c. Pada **Port**, tentukan nomor port untuk koneksi TCP/IP ke server. Nomor port default adalah 3306.

   d. Pada **Nama pengguna** dan **Kata sandi**, tentukan kredensial akun MySQL.

   Penting
   Database yang akan dicadangkan hanya file yang dapat diakses ke akun yang ditentukan.

   e. Klik **Buat**.

   Situs web muncul di konsol Cyber Protect pada **Perangkat** > **Situs web**.

Untuk mengubah pengaturan koneksi

1. Pilih situs web pada **Perangkat** > **Situs web**.
2. Klik **Detail**.
3. Klik ikon pensil di sebelah pengaturan situs web atau koneksi database.
4. Lakukan perubahan yang diperlukan, lalu klik **Simpan**.

Untuk membuat rencana proteksi bagi situs web

1. Pilih situs web atau beberapa situs web pada **Perangkat** > **Situs web**.
2. Klik **Lindungi**.
3. [Opsional] Aktifkan pencadangan basis data.
   Jika beberapa situs web dipilih, pencadangan basis data dinonaktifkan secara default.
4. [Opsional] Ubah aturan retensi.
5. [Opsional] Aktifkan enkripsi pencadangan.
6. [Opsional] Klik ikon roda gigi untuk mengedit opsi **Nama file cadangan**. Hal ini terlihat wajar untuk dua kasus:
   - Jika Anda mencadangkan situs web ini lebih awal dan ingin melanjutkan rangkaian pencadangan yang ada

© Acronis International GmbH, 2003-2024

- Jika Anda ingin melihat nama kustom pada tab **Penyimpanan cadangan**

7. Klik **Terapkan**.

Anda dapat mengedit, mencabut, dan menghapus rencana proteksi untuk situs web dengan cara yang sama seperti untuk mesin. Operasi ini diuraikan dalam "Operasi dengan rencana proteksi".

Memulihkan situs web

Untuk memulihkan situs web

1. Lakukan salah satu langkah berikut:
   - Di **Perangkat** > **Situs Web**, pilih situs web yang ingin Anda pulihkan, lalu klik **Pemulihan**.
     Anda dapat mencari situs web berdasarkan nama. Wildcard tidak didukung.
   - Jika situs web dihapus, pilih situs web di bagian **Cadangan aplikasi awan** pada tab Penyimpanan cadangan, lalu klik **Tunjukkan cadangan**.
     Untuk memulihkan situs web yang dihapus, Anda harus menambahkan situs target sebagai perangkat.
2. Pilih titik pemulihan.
3. Klik **Pulihkan**, lalu pilih apa yang ingin Anda pulihkan: **Seluruh situs web**, **Basis data** (jika ada), atau **File/folder**.
   Untuk memastikan situs web Anda berada dalam kondisi yang konsisten, kami menyarankan Anda memulihkan file dan database, dalam urutan apa pun.
4. Tergantung pilihan Anda, ikuti salah satu prosedur yang dijelaskan di bawah ini.

Untuk memulihkan seluruh situs web

1. Di **Pulihkan ke situs web**, lihat atau ubah situs web target.
   Secara default, situs web asli dipilih. Jika tidak ada, Anda harus memilih situs web target.
2. Pilih apakah akan memulihkan izin berbagi untuk item yang dipulihkan.
3. Klik **Mulai pemulihan**, lalu konfirmasi tindakan.

Untuk memulihkan database

1. Pilih database yang ingin Anda pulihkan.
2. Jika Anda ingin mengunduh basis data sebagai suatu file, klik **Unduh**, pilih lokasi untuk menyimpan file, lalu klik **Simpan**. Jika tidak, lewati langkah ini.
3. Klik **Pulihkan**.
4. Di **Pulihkan ke situs web**, lihat atau ubah situs web target.
   Secara default, situs web asli dipilih. Jika tidak ada, Anda harus memilih situs web target.
5. Klik **Mulai pemulihan**, lalu konfirmasi tindakan.

Untuk memulihkan file/folder situs web

© Acronis International GmbH, 2003-2024

1. Pilih file/folder yang ingin Anda pulihkan.
2. Jika Anda ingin menyimpan file, klik **Unduh**, pilih lokasi untuk menyimpan file, lalu klik **Simpan**. Jika tidak, lewati langkah ini.
3. Klik **Pulihkan**.
4. Di **Pulihkan ke situs web**, lihat atau ubah situs web target.
   Secara default, situs web asli dipilih. Jika tidak ada, Anda harus memilih situs web target.
5. Pilih apakah akan memulihkan izin berbagi untuk item yang dipulihkan.
6. Klik **Mulai pemulihan**, lalu konfirmasi tindakan.

Melindungi server hosting web

Anda dapat melindungi server hosting web berbasis Linux yang menjalankan panel kontrol Plesk, cPanel, DirectAdmin, VirtualMin, atau ISPManager. Server yang menjalankan panel kontrol hosting web dari vendor lain dilindungi sebagai beban kerja reguler.

Kuota

Server yang menjalankan panel kontrol Plesk, cPanel, DirectAdmin, VirtualMin, atau ISPManager dianggap sebagai server hosting web. Setiap server hosting web yang dicadangkan memakai kuota **Server hosting web**. Jika kuota ini dinonaktifkan atau kelebihan untuk kuota ini terlampaui, kuota akan ditetapkan seperti berikut atau pencadangan akan gagal:

- Jika server adalah fisik, kuota **Server** akan digunakan. Jika kuota ini dinonaktifkan atau kelebihan untuk kuota ini terlampaui, pencadangan akan gagal.
- Jika server adalah virtual, kuota **Mesin virtual** akan digunakan. Jika kuota ini dinonaktifkan atau kelebihan untuk kuota ini terlampaui, pencadangan akan gagal.

Integrasi untuk DirectAdmin, cPanel, dan Plesk

Administrator hosting web yang menggunakan DirectAdmin, Plesk, atau cPanel dapat mengintegrasikan panel kontrol ini dengan layanan Cyber Protection untuk mendapatkan beberapa kapabilitas yang andal, yang meliputi:

- Mencadangkan seluruh server hosting web ke penyimpanan awan dengan cadangan tingkat disk
- Memulihkan seluruh server, termasuk semua situs web dan akun
- Melakukan pemulihan granular dan mengunduh akun, situs web, file individu, kotak surat, atau database
- Mengaktifkan reseller dan pelanggan untuk melakukan pemulihan layanan mandiri datanya sendiri

Untuk melakukan integrasi, Anda perlu menggunakan ekstensi layanan Cyber Protection. Untuk informasi lebih lanjut, silakan lihat panduan integrasi yang sesuai:

- Panduan Integrasi DirectAdmin
- Panduan Integrasi WHM dan cPanel

© Acronis International GmbH, 2003-2024

Operasi khusus dengan mesin virtual

Menjalankan mesin virtual dari cadangan (Pemulihan Instan)

Anda dapat menjalankan mesin virtual dari cadangan tingkat disk yang berisi sistem operasi. Operasi ini, juga disebut sebagai pengembalian instan, memungkinkan Anda untuk mempercepat server virtual dalam hitungan detik. Disk virtual diemulasi langsung dari cadangan sehingga tidak memakai ruang di penyimpanan data (penyimpanan). Ruang penyimpanan hanya diperlukan untuk menyimpan perubahan pada disk virtual.

Kami menyarankan Anda membiarkan mesin virtual sementara ini berfungsi hingga tiga hari. Lalu, Anda dapat menghapusnya atau mengonversinya menjadi mesin virtual biasa (menyelesaikan) tanpa waktu henti.

Selagi mesin virtual sementara ada, aturan retensi tidak dapat diterapkan ke cadangan yang sedang digunakan oleh mesin tersebut. Cadangan dari mesin asli dapat terus dijalankan.

Contoh penggunaan

- **Pemulihan bencana**
  Memulihkan salinan mesin online yang gagal secara instan.
- **Menguji cadangan**
  Jalankan mesin dari cadangan dan pastikan OS dan aplikasi tamu berfungsi dengan benar.
- **Mengakses data aplikasi**
  Saat mesin sedang berjalan, gunakan alat manajemen asli dari aplikasi untuk mengakses dan mengekstrak data yang diperlukan.

Prasyarat

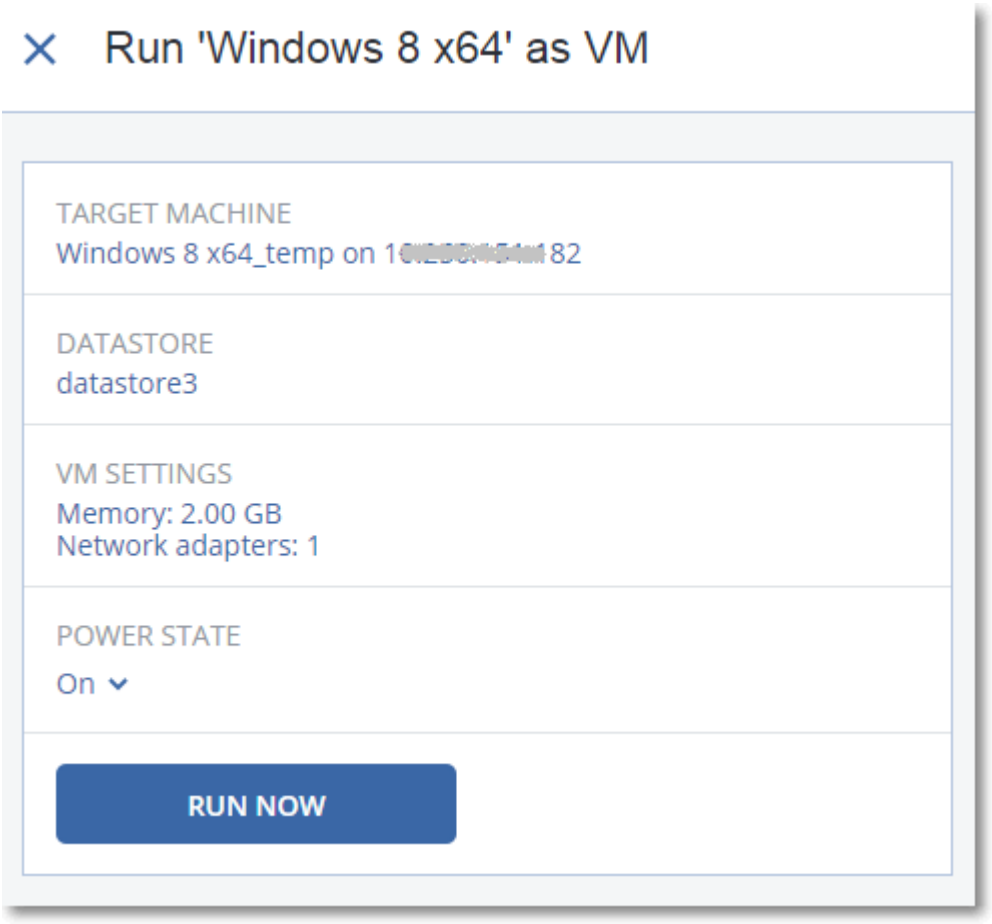
- Setidaknya satu Agen untuk VMware atau Agen untuk Hyper-V harus terdaftar dalam layanan Cyber Protection.
- Cadangan dapat disimpan di folder jaringan atau folder lokal mesin tempat Agen untuk VMware atau Agen untuk Hyper-V diinstal. Jika Anda memilih folder jaringan, folder tersebut harus dapat diakses dari mesin tersebut. Mesin virtual juga dapat dijalankan dari cadangan yang disimpan di penyimpanan awan, tetapi fungsinya akan lebih lambat karena operasi ini memerlukan pembacaan akses acak yang intens dari cadangan.
- Cadangan harus berisi keseluruhan mesin atau semua volume yang diperlukan bagi sistem operasi untuk memulai.
- Cadangan dapat menggunakan mesin fisik dan virtual. Cadangan *kontainer* Virtuozzo tidak dapat digunakan.

© Acronis International GmbH, 2003-2024

- Cadangan yang berisi volume logis Linux (LVM) harus dibuat oleh Agen untuk VMware atau Agen untuk Hyper-V. Mesin virtual harus memiliki jenis yang sama dengan mesin aslinya (ESXi atau Hyper-V).

Menjalankan mesin

1. Lakukan salah satu langkah berikut:
   - Pilih mesin yang dicadangkan, klik **Pemulihan**, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab Penyimpanan cadangan.
2. Klik **Jalankan sebagai VM**.
   Perangkat lunak akan secara otomatis memilih host dan parameter lain yang diperlukan.



3. [Opsional] Klik **Mesin target**, lalu ubah jenis mesin virtual (ESXi atau Hyper-V), host, atau nama mesin virtual.
4. [Opsional] Klik **Penyimpanan data** untuk ESXi atau **Jalur** untuk Hyper-V, lalu pilih penyimpanan data untuk mesin virtual.
   Ubah ke disk virtual yang mengakumulasi sementara mesin sedang berjalan. Pastikan penyimpanan data yang dipilih memiliki cukup ruang bebas. Jika Anda berencana mempertahankan perubahan ini dengan menjadikan mesin virtual permanen, pilih penyimpanan data yang sesuai untuk menjalankan mesin dalam produksi.

© Acronis International GmbH, 2003-2024

5. [Opsional] Klik **Pengaturan VM** untuk mengubah ukuran memori dan koneksi jaringan mesin virtual.
6. [Opsional] Pilih status daya VM (**On**/**Off**).
7. Klik **Jalankan sekarang**.

Hasilnya, mesin akan muncul di antarmuka web dengan salah satu ikon berikut: atau

. Mesin virtual tersebut tidak dapat dipilih untuk pencadangan.

Catatan
Anda dapat melakukan operasi Jalankan sebagai mesin virtual (Pemulihan Instan) dengan cadangan di Microsoft Azure. Namun, operasi ini menghasilkan lalu lintas keluar yang signifikan, yang akan ditambahkan ke tagihan langganan Microsoft Azure Anda. Lalu lintas keluar umum untuk mesin Windows yang dijalankan dari cadangan Microsoft Azure akan berukuran sekitar 5 GB sejak mesin virtual dihidupkan hingga masuk.

Menghapus mesin

Kami menyarankan Anda tidak menghapus mesin virtual sementara secara langsung di vSphere/Hyper-V. Hal ini mungkin menyebabkan artefak di antarmuka web. Selain itu, cadangan yang merupakan sumber dari mesin yang berjalan mungkin tetap terkunci untuk sementara (tidak dapat dihapus karena aturan retensi).

Untuk menghapus mesin virtual yang dijalankan dari cadangan

1. Pada tab **Semua perangkat**, pilih mesin yang berjalan dari cadangan.
2. Klik **Hapus**.

Mesin dihapus dari antarmuka web. Mesin virtual ini juga dihapus dari inventaris dan penyimpanan data vSphere atau Hyper-V (penyimpanan). Semua perubahan yang terjadi pada data ketika mesin sedang berjalan akan hilang.

Finalisasi mesin

Ketika mesin virtual ini berjalan dari cadangan, isi disk virtual akan diambil langsung dari cadangan tersebut. Dengan demikian, mesin tidak akan dapat diakses atau bahkan rusak jika koneksi ke lokasi cadangan atau agen perlindungan hilang.

Anda memiliki opsi untuk menjadikan mesin ini permanen, yaitu memulihkan semua disk virtual, beserta semua perubahan yang terjadi saat mesin sedang berjalan, ke penyimpanan data yang menyimpan perubahan tersebut. Proses ini disebut finalisasi.

Finalisasi dilakukan tanpa waktu henti. Mesin Virtual *tidak* akan dimatikan selama finalisasi.

Lokasi disk virtual akhir ditetapkan dalam parameter operasi **Jalankan sebagai VM** (**Penyimpanan data** untuk ESXi atau **Jalur** untuk Hyper-V). Sebelum memulai finalisasi, pastikan bahwa ruang

© Acronis International GmbH, 2003-2024

kosong, kemampuan berbagi, dan performa penyimpanan data ini sesuai untuk menjalankan mesin dalam produksi.

Catatan
Finalisasi tidak didukung untuk Hyper-V yang berjalan di Windows Server 2008/2008 R2 dan Microsoft Hyper-V Server 2008/2008 R2 karena API yang diperlukan tidak ada dalam versi-versi Hyper-V ini.

Untuk menyelesaikan mesin yang dijalankan dari cadangan

1. Pada tab **Semua perangkat**, pilih mesin yang berjalan dari cadangan.
2. Klik **Menyelesaikan**.
3. [Opsional] Tentukan nama baru untuk mesin.
4. [Opsional] Ubah mode provisi disk. Pengaturan defaultnya adalah **Tipis**.
5. Klik **Menyelesaikan**.

Nama mesin akan langsung berubah. Progres pemulihan akan ditampilkan pada tab **Aktivitas**. Begitu pemulihan selesai, ikon mesin akan berubah ke mesin virtual reguler.

Yang perlu Anda ketahui tentang finalisasi

Finalisasi vs. pemulihan reguler

Proses finalisasi lebih lambat dari pemulihan reguler karena alasan berikut:

- Selama finalisasi, agen akan melakukan akses secara acak ke bagian cadangan yang berbeda-beda. Ketika keseluruhan mesin sedang dipulihkan, agen akan membaca data dari cadangan secara berurutan.
- Jika mesin virtual berjalan selama finalisasi, agen akan membaca data dari cadangan lebih sering, agar kedua proses berjalan secara bersamaan. Selama pemulihan reguler, mesin virtual akan dihentikan.

Finalisasi mesin berjalan dari cadangan awan

Karena akses yang intensif ke data yang dicadangkan, kecepatan finalisasi sangat bergantung pada bandwidth koneksi antara lokasi cadangan dan agennya. Finalisasi akan berjalan lebih lambat untuk cadangan yang berlokasi di awan jika dibandingkan dengan cadangan lokal. Jika koneksi internet sangat lambat atau tidak stabil, finalisasi mesin yang berjalan dari cadangan awan mungkin akan gagal. Kami menyarankan Anda menjalankan mesin virtual dari cadangan lokal jika Anda berencana melakukan finalisasi, dan memiliki pilihan.

© Acronis International GmbH, 2003-2024

Catatan
Kecepatan finalisasi tergantung pada apakah agen terhubung ke host VMware ESXi atau vCenter, seperti yang dijelaskan pada langkah 3 dari "Mengonfigurasi alat virtual" (hlm. 136). Koneksi ke VMware vCenter dapat memperlambat operasi finalisasi karena API VMware tertentu. Untuk mempercepat operasi finalisasi, gunakan Agen untuk VMware yang berbeda untuk melakukan tugas **Jalankan sebagai VM** diikuti dengan finalisasi, tempat Agen ini akan dihubungkan ke host ESXi, alih-alih ke vCenter.

Bekerja di VMware vSphere

Bagian ini menjelaskan operasi yang spesifik untuk lingkungan VMware vSphere.

Replikasi mesin virtual

Replikasi hanya tersedia untuk mesin virtual VMware ESXi.

Replikasi adalah proses pembuatan salinan yang sama (replika) dari sebuah mesin virtual, lalu mempertahankan replika tersebut tetap tersinkron dengan mesin aslinya. Dengan mereplikasi mesin virtual kritis, Anda akan tetap memiliki salinan mesin ini dalam status siap beroperasi.

Replikasi dapat dijalankan secara manual atau dengan jadwal yang Anda tentukan. Replikasi pertama adalah replikasi penuh (menyalin keseluruhan mesin). Semua replikasi berikutnya bersifat inkremental dan dilakukan dengan Pelacakan Perubahan Blok, kecuali jika opsi ini dinonaktifkan.

Replikasi vs. mencadangkan

Tidak seperti pencadangan terjadwal, replika hanya menyimpan status terbaru dari mesin virtual. Replika memakan ruang penyimpanan data, sementara cadangan dapat disimpan pada penyimpanan yang lebih murah.

Namun, menyalakan replika jauh lebih cepat daripada pemulihan dan lebih cepat daripada menjalankan mesin virtual dari cadangan. Ketika dinyalakan, replika bekerja lebih cepat daripada VM yang berjalan dari cadangan, dan tidak perlu memuat Agen untuk VMware.

Contoh penggunaan

- **Replikasi mesin virtual ke lokasi yang jauh.**
  Replikasi memungkinkan Anda untuk mencegah kegagalan sebagian atau keseluruhan sistem, dengan mengkloning mesin virtual dari lokasi utama ke lokasi kedua. Lokasi kedua biasanya terletak di fasilitas jarak jauh yang kemungkinan besar tidak akan terdampak oleh faktor lingkungan, infrastruktur, maupun faktor lainnya yang menyebabkan kegagalan lokasi utama.
- **Replikasi mesin virtual pada lokasi tunggal (dari satu host/penyimpanan data ke host/penyimpanan data lainnya).**
  Replikasi di lokasi dapat digunakan untuk skenario ketersediaan tinggi dan pemulihan bencana.

© Acronis International GmbH, 2003-2024

Yang dapat Anda lakukan dengan sebuah replika

- **Menguji replika**

  Replika akan dinyalakan untuk pengujian. Gunakan vSphere Client atau alat lain untuk memeriksa apakah replika bekerja dengan benar. Replikasi ditangguhkan saat pengujian sedang berlangsung.
- **Failover pada replika**

  Failover adalah transisi beban kerja dari mesin virtual asli ke replikanya. Replikasi ditangguhkan saat failover sedang berlangsung.
- **Mencadangkan replika**

  Cadangan dan replikasi sama-sama membutuhkan akses ke disk virtual, sehingga performa host di mana mesin virtual berjalan juga akan terdampak. Jika Anda menginginkan replika dan cadangan mesin virtual namun tidak ingin menambah beban tambahan pada host produksi, lakukan replikasi mesin ke host yang berbeda, dan siapkan cadangan replika.

Pembatasan

- Jenis mesin virtual berikut tidak dapat direplikasi:
  - Mesin toleransi kegagalan yang berjalan pada ESXi 5.5 ke bawah.
  - Mesin yang berjalan dari cadangan.
  - Replika mesin virtual.
- Beberapa perubahan perangkat keras, seperti menambahkan kartu antarmuka jaringan (NIC) ke host ESXi atau menghapus NIC darinya, mengakibatkan perubahan ID internal dari host. Perubahan ini memengaruhi rencana replikasi VM. Setelah perubahan seperti itu, Anda harus membuat ulang rencana replikasi VM di mana host ESXi dipilih sebagai sumber atau target. Jika tidak, rencana replikasi VM akan gagal.

Membuat rencana replikasi

Rencana replikasi harus dibuat untuk tiap mesin secara individual. Tidak mungkin menerapkan rencana yang ada ke mesin lain.

Untuk membuat rencana replikasi

1. Pilih mesin virtual yang akan direplikasi.
2. Klik **Replikasi**.

   Perangkat lunak akan menampilkan templat rencana replikasi baru.
3. [Opsional] Untuk memodifikasi nama rencana replikasi, klik nama default.
4. Klik **Mesin target**, lalu lakukan langkah berikut:
   a. Pilih apakah akan membuat replika baru atau menggunakan replika mesin asli yang sudah ada.
   b. Pilih host ESXi dan tentukan nama replika yang baru, atau pilih replika yang sudah ada.

© Acronis International GmbH, 2003-2024

Nama default replika yang baru adalah **[Original Machine Name]_replica**.

c. Klik **OK**.

5. [Hanya ketika mereplikasi ke mesin baru] Klik **Penyimpanan Data**, lalu pilih penyimpanan data untuk mesin virtual.
6. [Opsional] Klik **Jadwal** untuk mengubah jadwal replikasi.

   Secara default, replikasi dilakukan setiap hari, Senin hingga Jumat. Anda dapat memilih waktu untuk menjalankan replikasi.

   Jika Anda ingin mengubah frekuensi replikasi, geser slider, lalu tentukan jadwalnya.

   Anda juga dapat melakukan hal berikut:

   - Menetapkan rentang tanggal kapan jadwal akan berlaku efektif. Pilih kotak centang **Jalankan rencana dalam kisaran tanggal**, lalu tentukan rentang tanggal.
   - Nonaktifkan jadwal. Dalam hal ini, replikasi dapat dijalankan secara manual.
7. [Opsional] Klik ikon roda gigi untuk memodifikasi opsi replikasi.
8. Klik **Terapkan**.
9. [Opsional] Untuk menjalankan rencana secara manual, klik **Jalankan sekarang** pada panel rencana.

Setelah rencana replikasi dijalankan, replika mesin virtual akan muncul pada daftar **Semua perangkat** dengan ikon berikut:

Menguji replika

Untuk menyiapkan replika pengujian

1. Pilih replika untuk uji.
2. Klik **Uji replika**.
3. Klik **Mulai tes**.
4. Pilih apakah Anda ingin menghubungkan replika yang menyala ke jaringan. Secara default, replika tidak akan dihubungkan ke jaringan.
5. [Opsional] Jika Anda memilih untuk menghubungkan replika ke jaringan, pilih kotak centang **Hentikan mesin virtual orisinal** untuk menghentikan mesin orisinal sebelum menyalakan replika.
6. Klik **Mulai**.

Untuk menghentikan uji replika

1. Pilih replika untuk pengujian yang sedang berlangsung.
2. Klik **Uji replika**.
3. Klik **Hentikan pengujian**.
4. Konfirmasi keputusan Anda.

© Acronis International GmbH, 2003-2024

Failover pada replika

Untuk melakukan failover mesin pada replika

1. Pilih replika untuk failover.
2. Klik **Tindakan replika**.
3. Klik **Failover**.
4. Pilih apakah Anda ingin menghubungkan replika yang menyala ke jaringan. Secara default, replika akan dihubungkan ke jaringan yang sama dengan mesin aslinya.
5. [Opsional] Jika Anda memilih untuk menghubungkan replika ke jaringan, kosongkan kotak centang **Hentikan mesin virtual orisinal** agar mesin orisinal tetap online.
6. Klik **Mulai**.

Ketika replika dalam status failover, Anda dapat memilih salah satu tindakan berikut:

- **Hentikan failover**

  Hentikan failover jika mesin asli sudah diperbaiki. Replika akan dimatikan. Replikasi akan dilanjutkan.
- **Lakukan failover permanen pada replika**

  Operasi instan ini akan menghapus tanda 'replika' dari mesin virtual, sehingga replikasi terhadapnya tidak mungkin dijalankan lagi. Jika Anda ingin melanjutkan replikasi, edit rencana replikasi untuk memilih mesin ini sebagai sumbernya.
- **Failback**

  Lakukan failback jika Anda melakukan failover ke lokasi yang tidak ditujukan untuk operasi berkelanjutan. Replika akan dipulihkan ke mesin virtual asli atau yang baru. Setelah pemulihan mesin asli selesai, mesin akan dinyalakan dan replikasi dilanjutkan. Jika Anda memilih untuk memulihkan ke mesin baru, edit rencana replikasi untuk memilih mesin ini sebagai sumbernya.

Menghentikan failover

Untuk menghentikan failover

1. Pilih replika yang berada dalam status failover.
2. Klik **Tindakan replika**.
3. Klik **Hentikan Failover**.
4. Konfirmasi keputusan Anda.

Melakukan failover permanen

Untuk melakukan failover permanen

1. Pilih replika yang berada dalam status failover.
2. Klik **Tindakan replika**.
3. Klik **Failover Permanen**.

© Acronis International GmbH, 2003-2024

4. [Opsional] Ubah nama mesin virtual.
5. [Opsional] Pilih kotak centang **Hentikan mesin virtual orisinal**.
6. Klik **Mulai**.

Failback

Untuk melakukan failback dari replika

1. Pilih replika yang berada dalam status failover.
2. Klik **Tindakan replika**.
3. Klik **Failback dari replika**.
   Perangkat lunak akan secara otomatis memilih mesin asli sebagai mesin target.
4. [Opsional] Klik **Mesin target**, lalu lakukan langkah berikut:
   a. Pilih apakah akan Anda ingin melakukan failback ke mesin baru atau mesin yang sudah ada.
   b. Pilih host ESXi dan tentukan nama mesin yang baru, atau pilih mesin yang sudah ada.
   c. Klik **OK**.
5. [Opsional] Ketika melakukan failback ke mesin baru, Anda juga dapat melakukan hal berikut:
   - Klik **Penyimpanan Data** untuk memilih penyimpanan data bagi mesin virtual.
   - Klik **Pengaturan VM** untuk mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual.
6. [Opsional] Klik **Opsi pemulihan** untuk memodifikasi opsi failback.
7. Klik **Mulai pemulihan**.
8. Konfirmasi keputusan Anda.

Opsi replikasi

Untuk memodifikasi opsi replikasi, klik ikon roda gigi di samping nama rencana replikasi, lalu klik **Opsi replikasi**.

Pelacakan Perubahan Blok (CBT)

Opsi ini mirip dengan opsi pencadangan "Pelacakan Perubahan Blok (CBT)".

Provisi disk

Opsi ini menetapkan pengaturan provisi disk untuk replika.

Nilai prasetelnya adalah: **Provisi tipis**.

Nilai berikut tersedia: **Provisi tipis**, **Provisi tebal**, **Simpan pengaturan orisinal**.

Penanganan eror

Opsi ini mirip dengan opsi pencadangan "Penanganan eror".

© Acronis International GmbH, 2003-2024

Perintah pra/pasca

Opsi ini mirip dengan opsi pencadangan "Perintah pra/pasca".

Layanan Menyalin Bayangan Volume VSS untuk mesin virtual

Opsi ini mirip dengan opsi pencadangan "Layanan Menyalin Bayangan Volume VSS untuk mesin virtual".

Opsi failback

Untuk memodifikasi opsi failback, klik **Opsi pemulihan** ketika mengonfigurasi failback.

Penanganan eror

Opsi ini mirip dengan opsi pemulihan "Penanganan eror".

Performa

Opsi ini mirip dengan opsi pemulihan "Performa".

Perintah pra/pasca

Opsi ini mirip dengan opsi pemulihan "Perintah pra/pasca".

Manajemen daya VM

Opsi ini mirip dengan opsi pemulihan "Manajemen daya VM".

Seeding replika awal

Untuk mempercepat replikasi ke lokasi jarak jauh dan menghemat bandwidth jaringan, Anda dapat melakukan seeding replika.

Penting
Untuk melakukan seeding replika, Agen untuk VMware (Alat Virtual) harus berjalan pada ESXi target.

Untuk melakukan seeding replika awal

1. Lakukan salah satu langkah berikut:
   - Jika mesin virtual asli dapat dimatikan, matikan lalu lompat ke langkah 4.
   - Jika mesin virtual asli tidak dapat dimatikan, lanjutkan ke langkah berikutnya.
2. Membuat rencana replikasi.
   Ketika membuat rencana, pada **Mesin target**, pilih **Replika baru** dan ESXi yang menjadi host mesin asli.
3. Jalankan rencana satu kali.
   Replika akan dibuat pada ESXi asli.
4. Ekspor file mesin virtual (atau replikanya) ke hard drive eksternal.

© Acronis International GmbH, 2003-2024

a. Hubungkan hard drive eksternal ke mesin yang menjalankan vSphere Client.
b. Hubungkan vSphere Client ke vCenter/ESXi asli.
c. Pilih replika yang baru dibuat pada inventaris.
d. Klik **File** > **Ekspor** > **Ekspor templat OVF**.
e. Pada **Direktori**, tentukan folder pada hard drive eksternal.
f. Klik **OK**.

5. Transfer hard drive ke lokasi jarak jauh.
6. Impor replika ke ESXi target.
   a. Hubungkan hard drive eksternal ke mesin yang menjalankan vSphere Client.
   b. Hubungkan vSphere Client ke vCenter/ESXi target.
   c. Klik **File** > **Sebarkan templat OVF**.
   d. Pada **Sebarkan dari file atau URL**, tentukan templat yang telah Anda ekspor pada langkah 4.
   e. Selesaikan prosedur impor.
7. Edit rencana replikasi yang Anda buat di langkah 2. Pada **Mesin target**, pilih **Replika yang ada**, lalu pilih replika yang diimpor.

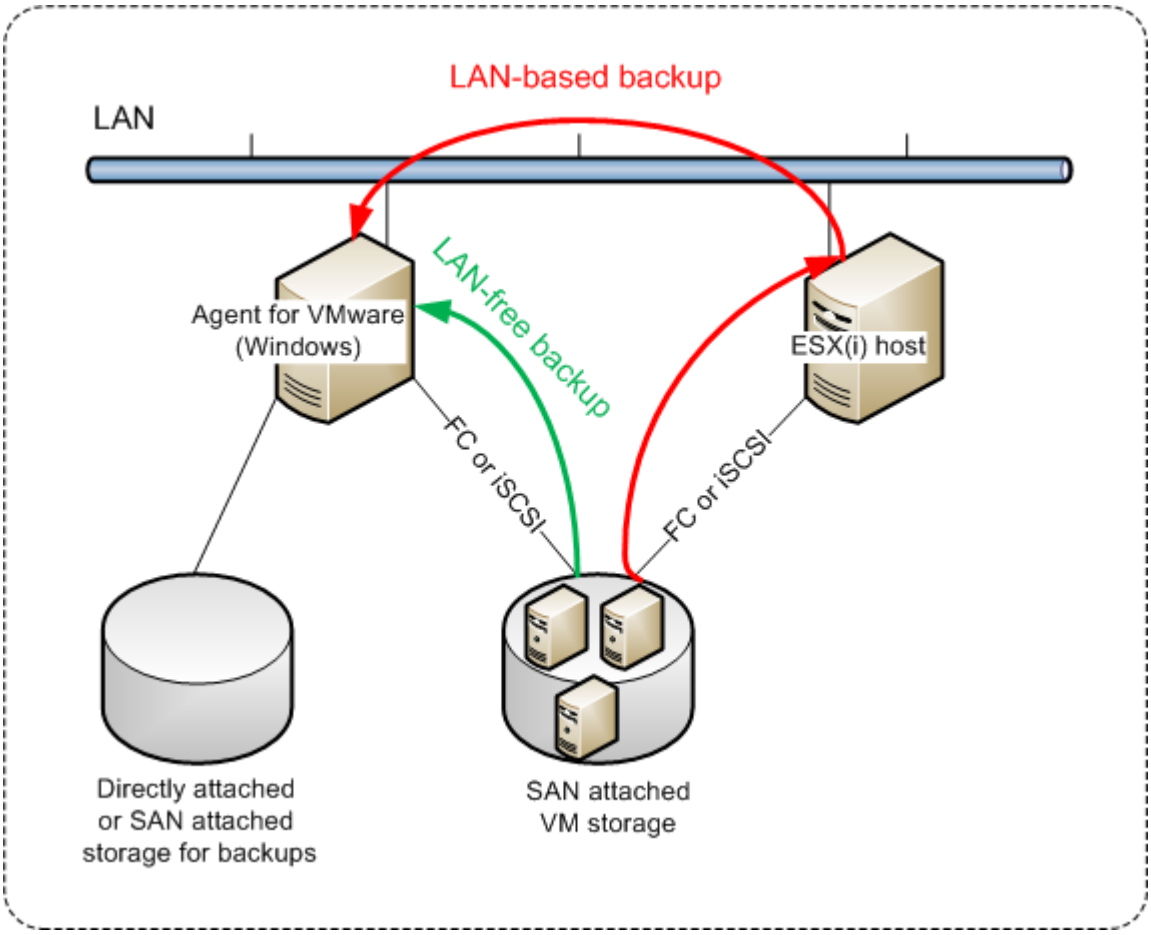
Hasilnya, perangkat lunak akan melanjutkan memperbarui replika. Semua replikasi akan bertambah secara bertahap.

Agen untuk VMware - pencadangan tanpa LAN

Jika ESXi Anda menggunakan penyimpanan yang terpasang SAN, instal agen pada mesin yang terhubung pada SAN yang sama. Agen akan mencadangkan mesin virtual langsung dari penyimpanan, bukan melalui host ESXi dan LAN. Kemampuan ini disebut pencadangan tanpa LAN.

Diagram di bawah ini mengilustrasikan pencadangan dengan berbasis LAN dan tanpa LAN. Akses tanpa LAN ke mesin virtual tersedia jika Anda memiliki saluran fiber (FC) atau iSCSI Storage Area Network. Untuk menghapus sepenuhnya pengiriman data cadangan melalui LAN, simpan cadangan pada disk lokal dari mesin agen atau pada penyimpanan yang terpasang SAN.

© Acronis International GmbH, 2003-2024



Agar agen dapat mengakses penyimpanan data secara langsung

1. Instal Agen untuk VMware pada mesin Windows yang memiliki akses jaringan ke vCenter Server.
2. Hubungkan logical unit number (LUN) yang menjadi host penyimpanan data ke mesin. Pertimbangkan hal berikut:
   - Gunakan protokol yang sama (misalnya iSCSI atau FC) yang digunakan untuk koneksi penyimpanan data ke ESXi.
   - LUN *tidak boleh* diinisialisasi dan harus muncul sebagai disk "offline" pada **Manajemen Disk**. Jika Windows menginisialisasi LUN, maka LUN bisa rusak dan tidak terbaca oleh VMware vSphere.

Akibatnya, agen akan menggunakan mode transpor SAN untuk mengakses disk virtual, misalnya agen akan membaca sektor LUN mentah melalui iSCSI/FC tanpa mengenali sistem file VMFS (yang tidak diketahui oleh Windows).

Pembatasan

- Pada vSphere 6.0 ke atas, agen tidak dapat menggunakan mode transpor SAN jika ada disk VM yang terletak pada Volume Virtual VMware (Vvol) dan ada yang tidak. Pencadangan mesin virtual semacam ini akan gagal.
- Mesin virtual terenkripsi, yang dikenalkan pada VMware vSphere 6.5, akan dicadangkan melalui LAN, meskipun Anda mengonfigurasi mode transpor SAN untuk agen. Agen akan melakukan

© Acronis International GmbH, 2003-2024

fallback pada transpor NBD karena VMware tidak mendukung transpor SAN untuk mencadangkan disk virtual terenkripsi.

Contoh

Jika Anda menggunakan SAN iSCSI, konfigurasikan iSCSI initiator pada mesin yang menjalankan Windows di mana Agen untuk VMware terinstal.

Untuk mengonfigurasi kebijakan SAN

1. Masuk sebagai administrator, buka saran perintah, ketik `diskpart`, lalu tekan **Enter**.
2. Ketik `san`, lalu tekan **Enter**. Pastikan bahwa **Kebijakan SAN: Offline Semua** ditampilkan.
3. Jika nilai lain untuk Kebijakan SAN ditetapkan:
   a. Ketik `san policy=offlineall`.
   b. Tekan **Enter**.
   c. Untuk memeriksa apakah pengaturan telah diterapkan dengan benar, lakukan langkah 2.
   d. Mulai ulang mesin.

Untuk mengonfigurasi iSCSI initiator

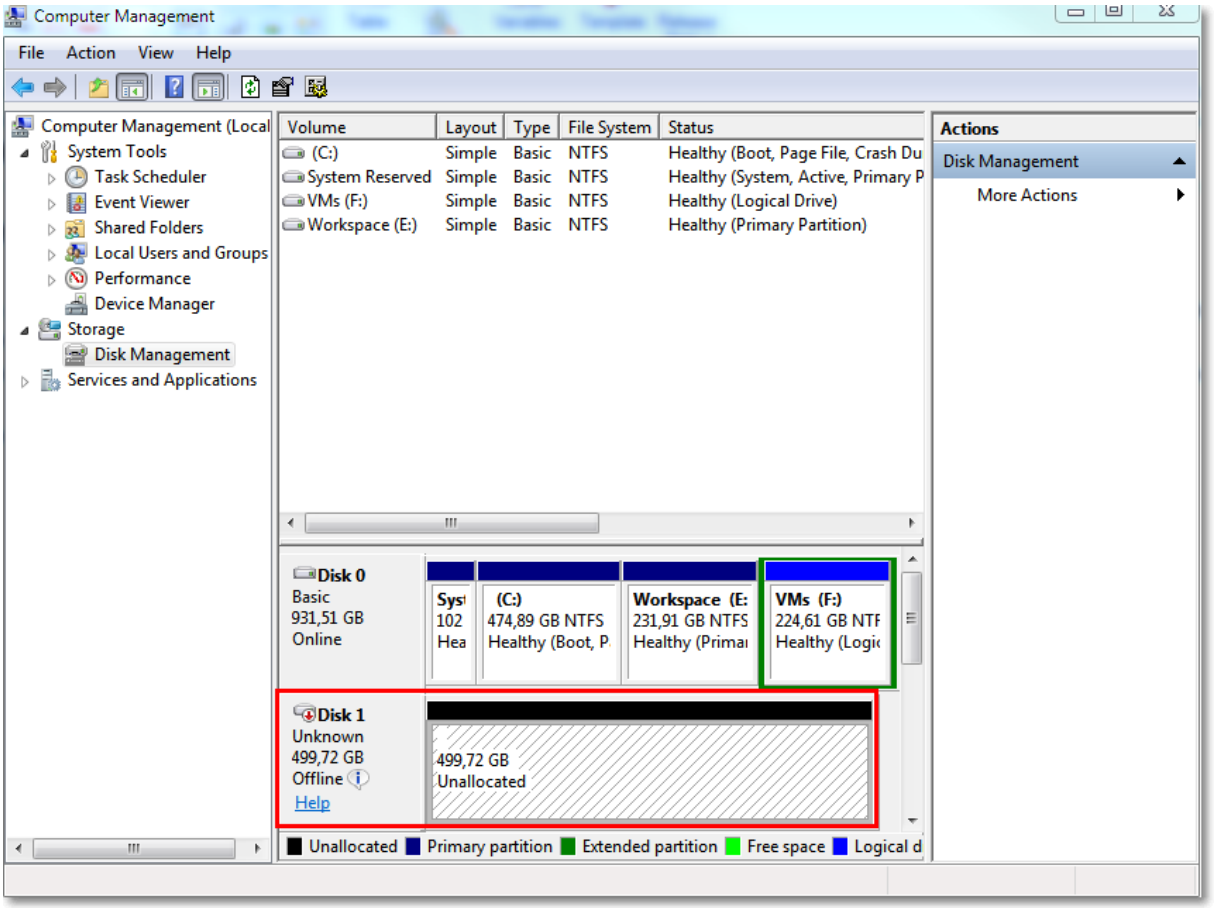
1. Buka **Panel Kontrol** > **Alat Administratif** > **iSCSI Initiator**.

   Catatan
   Untuk menemukan aplet **Alat Administratif**, Anda mungkin perlu mengubah tampilan **Panel Kontrol** ke selain **Beranda** atau **Kategori**, atau gunakan pencarian.

2. Jika ini adalah kali pertama iSCSI Initiator Microsoft diluncurkan, konfirmasikan bahwa Anda ingin memulai layanan iSCSI Initiator Microsoft.
3. Pada tab **Target**, ketik nama domain yang sepenuhnya memenuhi syarat (FQDN) atau alamat IP perangkat SAN target, lalu klik **Hubung Cepat**.
4. Pilih LUN yang menjadi host penyimpanan data, lalu klik **Hubungkan**.
   Jika LUN tidak ditampilkan, pastikan zona target iSCSI mengaktifkan mesin yang menjalankan agen untuk mengakses LUN. Mesin harus ditambahkan ke daftar iSCSI Initiator yang diizinkan pada target ini.
5. Klik **OK**.

SAN LUN yang sudah siap harus muncul pada **Manajemen Disk** seperti yang ditampilkan pada screenshot di bawah ini.

© Acronis International GmbH, 2003-2024



Menggunakan penyimpanan yang terpasang secara lokal

Anda dapat memasang disk tambahan ke Agen untuk VMware (Alat Virtual) sehingga agen dapat mencadangkan ke penyimpanan yang terpasang secara lokal ini. Pendekatan ini akan menghilangkan lalu lintas jaringan antara agen dan lokasi pencadangan.

Alat virtual yang berjalan di host atau klaster yang sama dengan mesin virtual yang dicadangkan memiliki akses langsung ke beberapa penyimpanan data di mana mesin berada. Ini berarti alat dapat memasang disk yang dicadangkan menggunakan transpor HotAdd, sehingga lalu lintas pencadangan akan diarahkan dari satu disk lokal ke disk lainnya. Jika penyimpanan data terhubung sebagai **Disk/LUN** dan bukan **NFS**, pencadangan akan sepenuhnya bebas LAN. Jika dilakukan penyimpanan data NFS, akan ada lalu lintas jaringan antara penyimpanan data dan host.

Dengan menggunakan penyimpanan yang terpasang secara lokal, agen akan dianggap selalu mencadangkan mesin yang sama. Jika banyak agen bekerja di dalam vSphere, dan satu atau beberapa di antaranya akan menggunakan penyimpanan yang terpasang secara lokal, Anda perlu mengikat secara manual setiap agen ke semua mesin yang harus dicadangkan. Jika tidak, jika mesin didistribusikan kembali antara agen oleh server manajemen, pencadangan mesin dapat tersebar ke beberapa penyimpanan.

Anda dapat menambahkan penyimpanan ke agen yang sudah beroperasi atau ketika menyebarkan agen dari templat OVF.

© Acronis International GmbH, 2003-2024

Untuk menyertakan penyimpanan ke agen yang sudah beroperasi

1. Di inventaris VMware vSphere, klik kanan Agen untuk VMware (Alat Virtual).
2. Tambahkan disk dengan mengedit pengaturan mesin virtual. Ukuran disk minimal harus 10 GB.

   Peringatan!
   Berhati-hatilah saat menambahkan disk yang sudah ada. Setelah penyimpanan dibuat, semua data sebelumnya yang ada dalam disk ini akan hilang.

3. Membuka konsol alat virtual. Tautan **Buat penyimpanan** tersedia di bagian bawah layar. Jika tidak ada, klik **Menyegarkan**.
4. Klik tautan **Buat penyimpanan**, pilih disk dan tentukan labelnya. Panjang label dibatasi hingga 16 karakter, karena pembatasan sistem file.

Untuk memilih penyimpanan yang terpasang secara lokal sebagai tujuan pencadangan

- Saat membuat rencana proteksi, di **Tempat menyimpan cadangan**, pilih **Folder lokal**, lalu ketik huruf yang sesuai dengan penyimpanan yang terpasang secara lokal, misalnya, **D:**.

Catatan
Locally Attached Storage (LAS) dirancang untuk lingkungan yang relatif kecil dengan satu agen (Virtual Appliance). Kami telah menguji unit Penyimpanan Terlampir Lokal yang berukuran hingga 5 TB. Anda dapat memasang disk yang lebih besar dengan risiko Anda sendiri, namun konfigurasi seperti itu tidak didukung. Untuk data cadangan berukuran lebih dari 5 TB, kami menyarankan Anda menggunakan jenis penyimpanan lain. Misalnya, Anda dapat membuat dan memasang disk virtual VMware ke mesin virtual acak mana pun dan membuat fitur berbagi jaringan di dalamnya, yang kemudian akan digunakan sebagai tujuan cadangan, alih-alih menggunakan LAS.

Pengikatan mesin virtual

Bagian ini memberi Anda gambaran tentang bagaimana layanan Cyber Protection mengatur operasi beberapa agen dalam VMware vCenter.

Algoritma distribusi di bawah ini berfungsi untuk peralatan dan agen virtual yang diinstal di Windows.

Algoritme distribusi

Mesin virtual didistribusikan secara otomatis antara Agen untuk VMware. Secara rata-rata, artinya setiap agen mengelola jumlah mesin yang sama. Jumlah ruang penyimpanan yang dipakai oleh mesin virtual tidak dihitung.

Namun, ketika memilih agen untuk mesin, perangkat lunak akan mencoba mengoptimalkan performa sistem secara keseluruhan. Secara khusus, perangkat lunak mempertimbangkan agen dan lokasi mesin virtual. Agen yang di-host pada host yang sama akan lebih dipilih. Jika tidak ada agen pada host yang sama, agen dari klaster yang sama akan lebih dipilih.

© Acronis International GmbH, 2003-2024

Setelah mesin virtual ditetapkan ke agen, semua pencadangan mesin ini akan didelegasikan ke agen ini.

Redistribusi

Redistribusi terjadi setiap kali keseimbangan yang ditetapkan rusak, atau, lebih tepatnya, ketika ketidakseimbangan beban di antara agen mencapai 20 persen. Hal ini dapat terjadi ketika terdapat penambahan atau penghapusan mesin atau agen, mesin dimigrasikan ke host atau klaster yang berbeda, atau jika Anda secara manual mengikat mesin ke agen. Jika ini terjadi, layanan Cyber Protection akan meredistribusikan mesin menggunakan algoritme yang sama.

Misalnya, Anda menyadari bahwa Anda membutuhkan lebih banyak agen untuk membantu dengan throughput dan menyebarkan alat virtual tambahan ke klaster. Layanan Cyber Protection akan menetapkan mesin yang paling tepat untuk agen baru. Beban agen lama akan berkurang.

Ketika Anda menghapus agen dari layanan Cyber Protection, mesin yang ditetapkan untuk agen akan diredistribusikan di antara agen yang tersisa. Namun, hal ini tidak akan terjadi jika agen rusak atau dihapus secara manual dari vSphere. Redistribusi hanya akan dimulai setelah Anda menghapus agen tersebut dari antarmuka web.

Melihat riwayat distribusi

Anda dapat melihat hasil dari distribusi otomatis:

- di kolom **Agen** untuk setiap mesin virtual pada bagian **Semua perangkat**
- di bagian **Mesin virtual yang ditetapkan** pada panel **Detail** ketika agen dipilih di bagian **Pengaturan** > **Agen** bagian

Pengikatan manual

Pengikatan Agen untuk VMware memungkinkan Anda mengecualikan mesin virtual dari proses distribusi dengan menentukan agen yang harus selalu mencadangkan mesin ini. Keseimbangan keseluruhan akan dipertahankan, tetapi mesin khusus ini dapat diteruskan ke agen yang lain hanya jika agen asli dihapus.

Untuk mengikat mesin dengan agen

1. Pilih mesin.
2. Klik **Detail**.
   Di bagian **Agen yang ditetapkan**, perangkat lunak akan menunjukkan agen yang saat ini mengelola mesin yang dipilih.
3. Klik **Ubah**.
4. Pilih **Manual**.
5. Pilih agen yang ingin Anda ikatkan dengan mesin.
6. Klik **Simpan**.

Untuk melepaskan ikatan mesin dari agen

© Acronis International GmbH, 2003-2024

1. Pilih mesin.
2. Klik **Detail**.

   Di bagian **Agen yang ditetapkan**, perangkat lunak akan menunjukkan agen yang saat ini mengelola mesin yang dipilih.
3. Klik **Ubah**.
4. Pilih **Otomatis**
5. Klik **Simpan**.

Menonaktifkan penetapan otomatis untuk agen

Anda dapat menonaktifkan penetapan otomatis pada Agen untuk VMware guna mengecualikannya dari proses distribusi dengan menentukan daftar mesin yang harus dicadangkan oleh agen ini. Keseimbangan keseluruhan akan dipertahankan antara agen lain.

Penetapan otomatis tidak dapat dinonaktifkan untuk agen jika tidak ada agen lain yang terdaftar, atau jika penetapan otomatis dinonaktifkan untuk semua agen lainnya.

Untuk menonaktifkan penetapan otomatis untuk agen

1. Klik **Pengaturan** > **Agen-Agen**.
2. Pilih Agen untuk VMware yang ingin Anda nonaktifkan penetapan otomatisnya.
3. Klik **Detail**.
4. Nonaktifkan switch **Penugasan otomatis**.

Contoh penggunaan

- Pengikatan manual sangat berguna jika Anda ingin mesin tertentu (yang sangat besar) akan dicadangkan oleh Agen untuk VMware (Windows) melalui saluran serat sementara mesin lain dicadangkan oleh alat virtual.
- Anda perlu mengikat VM ke agen jika agen memiliki penyimpanan yang terpasang secara lokal.
- Menonaktifkan penetapan otomatis memungkinkan Anda untuk memastikan bahwa mesin tertentu dapat dicadangkan sesuai jadwal yang Anda tentukan. Agen yang hanya mencadangkan satu VM tidak dapat melakukan mencadangkan VM lain ketika waktu yang dijadwalkan tiba.
- Menonaktifkan penetapan otomatis berguna jika Anda memiliki beberapa host ESXi yang terpisah secara geografis. Jika Anda menonaktifkan penetapan otomatis, lalu mengikat VM pada setiap host ke agen yang berjalan di host yang sama, Anda dapat memastikan bahwa agen tidak akan pernah mencadangkan mesin yang berjalan pada host ESXi jarak jauh, sehingga lalu lintas jaringan akan lebih hemat.

Menjalankan skrip pra-beku dan pasca-leleh secara otomatis

Dengan VMware Tool, Anda dapat menjalankan secara otomatis skrip pra-beku dan pasca-leleh di mesin virtual yang Anda cadangkan dalam mode tanpa agen. Maka, contohnya, Anda dapat

© Acronis International GmbH, 2003-2024

menjalankan skrip pendiaman kustom dan membuat cadangan yang konsisten dengan aplikasi untuk mesin virtual yang menjalankan aplikasi yang mengetahui VSS.

Prasyarat

Skrip pra-freeze dan pasca-thaw harus berada di folder tertentu di mesin virtual.

- Untuk mesin virtual Windows, lokasi folder ini bergantung pada versi ESXi host.
  Contohnya, untuk mesin virtual yang berjalan pada host ESXi 6.5, folder ini adalah `C:\Program Files\VMware\VMware Tools\backupScripts.d\`. Anda harus membuat folder `backupScritps.d` secara manual. Jangan simpan tipe file lainnya dalam folder ini karena dapat mengakibatkan VMware Tools tidak stabil.
  Untuk informasi lebih lanjut tentang lokasi skrip pra-freeze dan pasca-thaw untuk versi ESXi lainnya, lihat dokumentasi VMware.
- Untuk mesin virtual Linux, salin skrip Anda masing-masing ke folder `/usr/sbin/pre-freeze-script` dan `/usr/sbin/post-thaw-script`. Skrip dalam `/usr/sbin/pre-freeze-script` dijalankan ketika Anda membuat snapshot dan skrip dalam `/usr/sbin/post-thaw-script` dijalankan ketika snapshot difinalisasi. Skrip harus dapat dieksekusi oleh pengguna VMware Tool.

Untuk menjalankan skrip pra-beku dan pasca-leleh secara otomatis

1. Pastikan bahwa VMware Tools diinstal di mesin virtual tersebut.
2. Pada mesin virtual, masukkan skrip kustom Anda di folder yang diperlukan.
3. Dalam rencana proteksi mesin ini, aktifkan opsi **Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual**.
   Ini membuat snapshot VMware dengan opsi **Sistem file tamu diam** yang diaktifkan, yang kemudian memicu skrip pra-beku dan pasca-leleh di dalam mesin virtual.

Anda tidak perlu menjalankan skrip pendiaman kustom pada mesin virtual yang menjalankan aplikasi yang mengetahui VSS, seperti Microsoft SQL Server atau Microsoft Exchange. Guna membuat cadangan sesuai aplikasi untuk mesin tersebut, aktifkan opsi **Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual** dalam rencana proteksi.

Dukungan untuk migrasi mesin virtual

Bagian ini berisi informasi tentang migrasi mesin virtual dalam lingkungan vSphere, termasuk migrasi antara host ESXi yang merupakan bagian dari klaster vSphere.

vMotion memungkinkan pemindahan status dan konfigurasi mesin virtual ke host lain, selama disk mesin tetap di lokasi yang sama di penyimpanan bersama. Storage vMotion memungkinkan pemindahan disk mesin virtual dari satu penyimpanan data ke yang lainnya.

- Migrasi dengan vMotion, termasuk Storage vMotion, tidak didukung untuk mesin virtual yang menjalankan Agent for VMware (Alat Virtual), dan dinonaktifkan secara otomatis. Mesin virtual ini ditambahkan ke daftar **Pengesampingan VM** dalam konfigurasi klaster vSphere.
- Saat pencadangan mesin virtual dimulai, migrasi dengan vMotion, termasuk Storage vMotion, dinonaktifkan secara otomatis. Mesin virtual ini ditambahkan untuk sementara ke daftar

© Acronis International GmbH, 2003-2024

Pengesampingan VM dalam konfigurasi klaster vSphere. Setelah pencadangan selesai, pengaturan **pengesampingan VM** dikembalikan secara otomatis ke kondisi sebelumnya.

- Pencadangan tidak dapat dimulai untuk mesin virtual jika migrasinya dengan vMotion, termasuk Storage vMotion, sedang berlangsung. Pencadangan untuk mesin ini akan dimulai jika migrasinya selesai.

Mengelola lingkungan virtualisasi

Anda dapat melihat lingkungan vSphere, Hyper-V, dan Virtuozzo dalam presentasi asli mereka. Setelah agen yang sesuai diinstal dan terdaftar, tab **VMware**, **Hyper-V**, atau **Virtuozzo** akan muncul pada **Perangkat**.

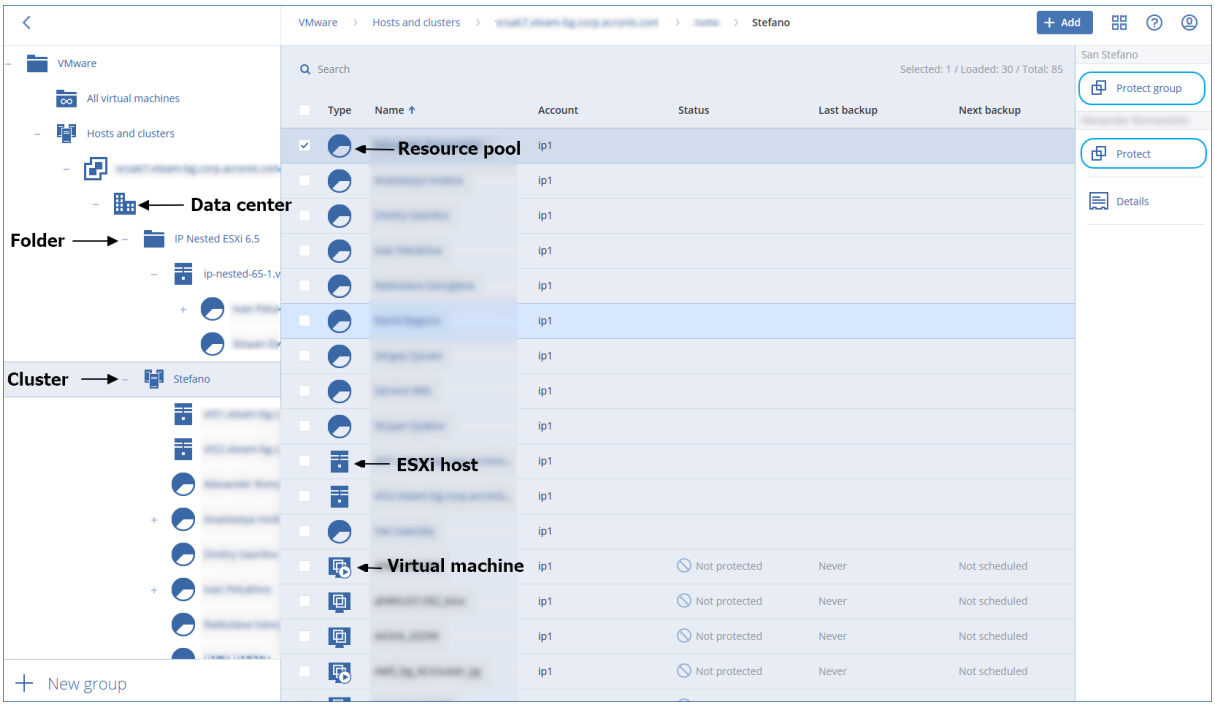
Dalam tab **VMware**, Anda dapat mencadangkan objek infrastruktur vSphere berikut:

- Pusat data
- Folder
- Gugusan
- Host ESXi
- Kolam sumber daya

Setiap objek infrastruktur ini berfungsi sebagai objek grup untuk mesin virtual. Saat Anda menerapkan rencana proteksi ke salah satu objek grup ini, semua mesin virtual yang termasuk di dalamnya, akan dicadangkan. Anda dapat mencadangkan mesin grup yang dipilih dengan mengklik **Lindungi**, atau mesin grup induk di mana grup yang dipilih termasuk dengan mengklik **Lindungi grup**.

Misalnya, Anda telah memilih klaster Stefano, lalu memilih kumpulan sumber daya di dalamnya. Jika Anda mengklik **Lindungi**, semua mesin virtual yang termasuk dalam kumpulan sumber daya yang dipilih akan dicadangkan. Jika Anda mengeklik **Lindungi grup**, semua mesin virtual yang termasuk dalam klaster Stefano akan dicadangkan.

© Acronis International GmbH, 2003-2024



Tab **VMware** memungkinkan Anda mengubah kredensial akses untuk vCenter Server atau host ESXi yang berdiri sendiri tanpa menginstal ulang agen.

Untuk mengubah kredensial akses host vCenter Server atau ESXi

1. Pada **Perangkat**, klik **VMware**.
2. Klik **Host dan Klaster**.
3. Di daftar **Host dan Klaster** (di sebelah kanan pohon **Host dan Klaster**), pilih vCenter Server atau host ESXi yang berdiri sendiri yang ditentukan selama instalasi Agen untuk VMware.
4. Klik **Detail**.
5. Pada **Kredensial**, klik nama pengguna.
6. Tentukan kredensial akses baru, lalu klik **OK**.

Menampilkan status pencadangan di vSphere Client

Anda dapat melihat status pencadangan dan waktu pencadangan mesin virtual di vSphere Client.

Informasi ini muncul dalam ringkasan mesin virtual (**Ringkasan** > **Atribut kustom**/**Anotasi**/**Catatan**, tergantung pada jenis klien dan versi vSphere). Anda juga dapat mengaktifkan kolom **Cadangan terakhir** dan **Status cadangan** di tab **Mesin Virtual** untuk setiap host, pusat data, folder, pool sumber daya, atau seluruh vCenter Server.

Untuk menyediakan atribut ini, Agen untuk VMware harus memiliki privilese berikut ini sebagai tambahan untuk yang dijelaskan dalam "Agen untuk VMware - privilese yang diperlukan":

- **Global** > **Kelola atribut kustom**
- **Global** > **Atur atribut kustom**

© Acronis International GmbH, 2003-2024

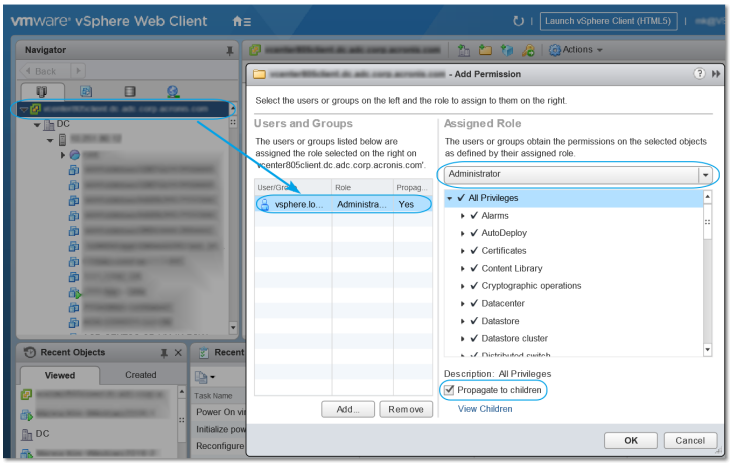
Agen untuk VMware – hak istimewa yang diperlukan

Untuk melakukan pengoperasian apa pun dengan objek vCenter, seperti mesin virtual, host ESXi, klaster, vCenter, dan banyak lagi, Agen untuk VMware mengautentikasi pada host vCenter atau ESXi dengan menggunakan kredensial vSphere yang disediakan oleh pengguna. Akun vSphere yang digunakan untuk koneksi ke vSphere oleh Agen untuk VMware harus memiliki hak istimewa yang diperlukan pada semua tingkat infrastruktur vSphere yang dimulai dari tingkat vCenter.

Tentukan akun vSphere dengan privilese yang diperlukan selama instalasi atau konfigurasi Agen untuk VMware. Jika Anda perlu mengubah akun di lain waktu, lihat bagian "Mengelola lingkungan virtualisasi" (hlm. 694).

Untuk menetapkan izin kepada pengguna vSphere di tingkat vCenter

1. Masuk ke klien web vSphere.
2. Klik kanan pada vCenter dan kemudian klik **Tambah izin**.
3. Pilih atau tambahkan pengguna baru dengan peran yang diperlukan (peran harus mencakup semua izin yang diperlukan dari tabel di bawah).
4. Pilih opsi **Sebarkan ke anak-anak**.



Objek	Privilese	Operasi			
		Cadangkan VM	**Pulihkan ke VM baru**	**Pulihkan ke VM yang sudah ada**	**Jalankan VM dari cadangan**
Operasi kriptografis (mulai dengan vSphere 6.5)	**Tambah disk**	+*			
	Akses Langsung	+*			

© Acronis International GmbH, 2003-2024

Penyimpanan data	**Alokasikan ruang**		+	+	+
	Jelajahi penyimpanan data				+
	Konfigurasikan penyimpanan data	+	+	+	+
	Operasi file tingkat rendah				+
Global	**Lisensi**	+	+	+	+
	Nonaktifkan metode	+	+	+	
	Aktifkan metode	+	+	+	
	Kelola atribut kustom	+	+	+	
	Atur atribut kustom	+	+	+	
Host > **Konfigurasi**	**Konfigurasi partisi penyimpanan**				+
Host > **Operasi lokal**	**Buat VM**				+
	Hapus VM				+
	Konfigurasi ulang VM				+
Jaringan	**Tetapkan jaringan**		+	+	+
Sumber daya	**Tetapkan VM ke pool sumber daya**		+	+	+
Mesin Virtual > **Konfigurasi**	**Tambah disk yang ada**	+	+		+
	Tambah disk baru		+	+	+
	Tambah atau hapus perangkat		+		+
	Tingkat lanjut	+	+	+	
	Ubah jumlah CPU		+		
	Pelacakan perubahan disk	+		+	
	Sewa disk	+		+	

© Acronis International GmbH, 2003-2024

	Memori		+		
	Hapus disk	+	+	+	+
	Ganti nama		+		
	Atur anotasi				+
	Pengaturan		+	+	+
Mesin virtual > **Operasi Tamu**	**Eksekusi Program Operasi Tamu**	+**			
	Kueri Operasi Tamu	+**			
	Modifikasi Operasi Tamu	+**			
Mesin virtual > **Interaksi**	**Dapatkan tiket kontrol tamu** (pada vSphere 4.1. dan 5.0)				+
	Konfigurasikan media CD		+	+	
	Manajemen sistem operasi tamu oleh VIX API (pada vSphere 5.1 ke atas)				+
	Matikan			+	+
	Nyalakan		+	+	+
Mesin virtual > **Inventaris**	**Buat dari yang sudah ada**		+	+	+
	Buat baru		+	+	+
	Daftar				+
	Hapus		+	+	+
	Batalkan pendaftaran				+
Mesin virtual > **Provisi**	**Izinkan akses ke disk**		+	+	+
	Izinkan akses disk hanya-baca	+		+	
	Izinkan unduhan mesin virtual	+	+	+	+

© Acronis International GmbH, 2003-2024

Mesin virtual > **Status** **Mesin virtual** > **Manajemen snapshot** (vSphere 6.5 dan yang lebih baru)	**Buat snapshot**	+		+	+
	Hapus snapshot	+		+	+
vApp	**Tambahkan mesin virtual**				+

* Privilese ini diperlukan hanya untuk mencadangkan mesin terenkripsi.

** Privilese ini diperlukan hanya untuk mencadangkan keberadaan aplikasi.

Mencadangkan mesin Hyper-V klaster

Di klaster Hyper-V, mesin virtual dapat bermigrasi antar simpul klaster. Ikuti rekomendasi ini untuk mengatur pencadangan yang benar dari mesin Hyper-V klaster:

1. Mesin harus tersedia untuk pencadangan, tidak masalah simpul apa yang akan menjadi tujuan migrasi. Untuk memastikan bahwa Agen untuk Hyper-V dapat mengakses mesin di setiap simpul, layanan agen harus dijalankan dalam akun pengguna domain yang memiliki privilese administratif di setiap simpul klaster.
   Kami menyarankan agar Anda menentukan akun untuk layanan agen selama instalasi Agen untuk Hyper-V.
2. Instal Agen untuk Hyper-V pada setiap simpul klaster.
3. Daftarkan semua agen di layanan Cyber Protection.

Ketersediaan Tinggi mesin yang dipulihkan

Saat Anda memulihkan disk pencadangan ke mesin virtual Hyper-V *yang ada*, sifat Ketersediaan Tinggi mesin masih seperti adanya.

Saat Anda memulihkan disk pencadangan ke mesin virtual Hyper-V *yang baru*, mesin yang menghasilkan tidak tersedia. Ini dipertimbangkan sebagai mesin cadangan dan biasanya akan dimatikan. Jika Anda perlu menggunakan mesin di lingkungan produksi, Anda dapat mengonfigurasikannya untuk Ketersediaan Tinggi dari snap-in **Manajemen Klaster Failover**.

Membatasi jumlah total mesin virtual yang dicadangkan secara simultan

Di opsi **Menjadwalkan** pencadangan, Anda dapat membatasi jumlah mesin virtual yang dicadangkan secara terus menerus per rencana proteksi.

© Acronis International GmbH, 2003-2024

Saat agen menjalankan banyak rencana dalam satu waktu, jumlah mesin yang dicadangkan secara terus menerus akan bertambah. Hal ini dapat memengaruhi performa pencadangan dan membebani host serta penyimpanan mesin virtual. Permasalahan tersebut dapat dihindari dengan cara mengonfigurasi batasan pada tingkat agen.

Untuk membatasi jumlah pencadangan yang berjalan secara simultan di tingkat agen

Agen untuk VMware (Windows)

1. Pada mesin dengan agen, buatlah dokumen teks baru, lalu buka menggunakan editor teks.
2. Salin dan tempel baris berikut ke dalam file.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Ganti `00000001` dengan nilai heksadesimal dari batas yang ingin Anda tetapkan.
   Misalnya, `00000001` adalah 1 dan `0000000A` adalah 10.
4. Simpan dokumen sebagai **limit.reg**.
5. Jalankan file sebagai administrator.
6. Konfirmasi bahwa Anda ingin mengedit registri Windows.
7. Mulai ulang agen.
   a. Di menu **Start**, klik **Run**.
   b. Ketikkan **cmd**, lalu klik **OK**.
   c. Pada baris perintah, jalankan perintah berikut:

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

Agen untuk Hyper-V

1. Pada mesin dengan agen, buatlah dokumen teks baru, lalu buka menggunakan editor teks.
2. Salin dan tempel baris berikut ke dalam file.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Ganti `00000001` dengan nilai heksadesimal dari batas yang ingin Anda tetapkan.
   Misalnya, `00000001` adalah 1 dan `0000000A` adalah 10.
4. Simpan dokumen sebagai **limit.reg**.
5. Jalankan file sebagai administrator.

© Acronis International GmbH, 2003-2024

6. Konfirmasi bahwa Anda ingin mengedit registri Windows.
7. Mulai ulang agen.
   a. Di menu **Start**, klik **Run**.
   b. Ketikkan **cmd**, lalu klik **OK**.
   c. Pada baris perintah, jalankan perintah berikut:

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

Alat virtual

Prosedur ini berlaku untuk Agent for VMware (Virtual Appliance), Agent for Scale Computing, Agent for Virtuozzo Hybrid Infrastructure, dan Agent for oVirt.

1. Di konsol alat virtual, tekan CTRL+SHIFT+F2 untuk membuka antarmuka baris perintah.
2. Buka file `/etc/Acronis/MMS.config` di editor teks.
3. Temukan bagian berikut:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Ganti `10` dengan nilai maksimal pencadangan simultan yang ingin Anda tetapkan.
5. Simpan file.
6. Mulai ulang agen dengan menjalankan perintah `reboot`.

Migrasi mesin

Anda dapat melakukan migrasi mesin dengan memulihkan cadangannya ke mesin non-asli.

Tabel berikut meringkas opsi migrasi yang tersedia.

Jenis mesin yang dicadangkan	Tujuan pemulihan yang tersedia							
	Mesin fisik	Mesin virtual ESXi	Mesin virtual Hyper-V	Virtuozzo		Mesin virtual Virtuozzo Hybrid Infrastructure	Mesin virtual Scale Computing HC3	Mesin virtual RHV/oVirt
				Mesin virtual	Kontainer			
Mesin fisik	+	+	+	-	-	+	+*	+
Mesin virtual VMware ESXi	+	+	+	-	-	+	+*	+

© Acronis International GmbH, 2003-2024

Mesin virtual Hyper-V	+	+	+	-	-	+	+*	+
Mesin virtual Virtuozzo	+	+	+	+	-	+	+*	+
Kontainer Virtuozzo	-	-	-	-	+	-	-	-
Mesin virtual Virtuozzo Hybrid Infrastructure	+	+	+	-	-	+	+*	+
Mesin virtual Scale Computing HC3	+	+	+	-	-	+	+	+
Mesin virtual Red Hat Virtualization/oVirt	+	+	+	-	-	+	+*	+

*Jika Boot Aman diaktifkan di mesin sumber, VM yang dipulihkan tidak akan dapat memulai kecuali jika Anda menonaktifkan Boot Aman di konsol VM setelah pemulihan.

Catatan
Anda tidak dapat memulihkan mesin virtual MacOS ke host Hyper-V karena Hyper-V tidak mendukung MacOS. Anda dapat memulihkan mesin virtual MacOS ke host VMware yang diinstal di perangkat keras Mac.

Untuk informasi selengkapnya tentang cara melakukan operasi migrasi, lihat topik berikut:

- Untuk migrasi fisik-ke-virtual (P2V), lihat "Mesin fisik ke virtual" (hlm. 501).
- Untuk migrasi virtual-ke-virtual (V2V), lihat "Memulihkan mesin virtualAnda dapat memulihkan mesin virtual dari cadangannya.Anda tidak dapat memulihkan cadangan di konsol Cyber Protect untuk penyewa dalam mode Kepatuhan. Untuk informasi lebih lanjut tentang cara memulihkan cadangan tersebut, silakan merujuk ke "Memulihkan cadangan untuk penyewa dalam mode Kepatuhan" (hlm. 1).PrasyaratMesin virtual harus dihentikan selama pemulihan ke mesin ini. Secara default, perangkat lunak menghentikan mesin tanpa perintah. Ketika pemulihan selesai, Anda harus memulai mesin secara manual. Anda dapat mengubah perilaku default ini menggunakan opsi pemulihan manajemen daya VM (klik Opsi pemulihan > Manajemen daya VM).ProsedurLakukan salah satu langkah berikut:Pilih mesin yang dicadangkan, klik Pemulihan, lalu pilih titik pemulihan.Pilih titik pemulihan pada tab Penyimpanan cadangan.Klik Pulihkan > Seluruh mesin.Jika Anda ingin memulihkan ke mesin fisik, pilih Mesin fisik di Pulihkan ke. Jika

© Acronis International GmbH, 2003-2024

tidak, lewati langkah ini.Pemulihan ke mesin fisik hanya dimungkinkan jika konfigurasi disk dari mesin target sama persis dengan konfigurasi disk dalam cadangan.Jika hal ini terjadi, lanjutkan ke langkah 4 di "Mesin fisik". Jika tidak, kami sarankan Anda untuk melakukan migrasi V2P menggunakan media yang dapat di-boot.[Opsional] Secara default, perangkat lunak akan otomatis memilih mesin asli sebagai mesin target. Untuk memulihkan ke mesin virtual lain, klik Mesin target, lalu lakukan hal berikut:Pilih hypervisor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3, atau oVirt).Hanya mesin virtual Virtuozzo yang dapat dipulihkan ke Virtuozzo. Untuk informasi lebih lanjut tentang migrasi V2V, lihat "Migrasi mesin".Pilih apakah akan Anda ingin melakukan pemulihan ke mesin baru atau mesin yang sudah ada.Pilih host dan tentukan nama mesin yang baru, atau pilih mesin target yang sudah ada.Klik OK.Siapkan opsi pemulihan tambahan yang Anda perlukan.[Tidak tersedia untuk Virtuozzo Hybrid Infrastructure dan Scale Computing HC3] Untuk memilih penyimpanan data bagi mesin virtual, klik Penyimpanan data untuk ESXi, Jalur untuk Hyper-V dan Virtuozzo, atau Domain penyimpanan untuk Red Hat Virtualization (oVirt), lalu pilih penyimpanan data (penyimpanan) untuk mesin virtual.Untuk melihat mode penyimpanan data (penyimpanan), antarmuka, dan provisi bagi setiap disk virtual, klik Pemetaan disk. Anda dapat mengubah pengaturan ini, kecuali jika Anda memulihkan kontainer Virtuozzo atau mesin virtual Virtuozzo Hybrid Infrastructure.Untuk Virtuozzo Hybrid Infrastructure, Anda hanya dapat memilih kebijakan penyimpanan untuk disk target. Untuk melakukannya, pilih disk target yang diinginkan, lalu pilih Ubah. Di bilah yang terbuka, klik ikon roda gigi, pilih kebijakan penyimpanan, lalu klik Selesai.Bagian pemetaan juga memungkinkan Anda memilih disk individual untuk pemulihan. [Tersedia untuk VMware ESXi, Hyper-V, dan Virtuozzo] Untuk mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual, klik Pengaturan VM.[Untuk Virtuozzo Hybrid Infrastructure] Untuk mengubah ukuran memori dan jumlah prosesor mesin virtual, pilih Cara. [Hanya tersedia untuk mesin Windows tempat agen perlindungan diinstal.] Aktifkan tombol pemulihan Aman untuk memastikan bahwa data yang dipulihkan bebas malware. Untuk informasi lebih lanjut mengenai cara pemulihan aman bekerja, lihat "Pemulihan aman" (hlm. 1).Klik Mulai pemulihan.Ketika memulihkan ke mesin virtual yang ada, konfirmasi bahwa Anda ingin menimpa disk.Progres pemulihan akan ditampilkan pada tab Aktivitas." (hlm. 1).

- Untuk migrasi virtual-ke-fisik (V2P), lihat "Memulihkan mesin virtualAnda dapat memulihkan mesin virtual dari cadangannya.Anda tidak dapat memulihkan cadangan di konsol Cyber Protect untuk penyewa dalam mode Kepatuhan. Untuk informasi lebih lanjut tentang cara memulihkan cadangan tersebut, silakan merujuk ke "Memulihkan cadangan untuk penyewa dalam mode Kepatuhan" (hlm. 1).PrasyaratMesin virtual harus dihentikan selama pemulihan ke mesin ini. Secara default, perangkat lunak menghentikan mesin tanpa perintah. Ketika pemulihan selesai, Anda harus memulai mesin secara manual. Anda dapat mengubah perilaku default ini menggunakan opsi pemulihan manajemen daya VM (klik Opsi pemulihan > Manajemen daya VM).ProsedurLakukan salah satu langkah berikut:Pilih mesin yang dicadangkan, klik Pemulihan, lalu pilih titik pemulihan.Pilih titik pemulihan pada tab Penyimpanan cadangan.Klik Pulihkan > Seluruh mesin.Jika Anda ingin memulihkan ke mesin fisik, pilih Mesin fisik di Pulihkan ke. Jika tidak, lewati langkah ini.Pemulihan ke mesin fisik hanya dimungkinkan jika konfigurasi disk dari mesin target sama persis dengan konfigurasi disk dalam cadangan.Jika hal ini terjadi, lanjutkan ke langkah 4 di "Mesin fisik". Jika tidak, kami sarankan Anda untuk melakukan migrasi V2P

© Acronis International GmbH, 2003-2024

menggunakan media yang dapat di-boot.[Opsional] Secara default, perangkat lunak akan otomatis memilih mesin asli sebagai mesin target. Untuk memulihkan ke mesin virtual lain, klik Mesin target, lalu lakukan hal berikut:Pilih hypervisor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3, atau oVirt).Hanya mesin virtual Virtuozzo yang dapat dipulihkan ke Virtuozzo. Untuk informasi lebih lanjut tentang migrasi V2V, lihat "Migrasi mesin".Pilih apakah akan Anda ingin melakukan pemulihan ke mesin baru atau mesin yang sudah ada.Pilih host dan tentukan nama mesin yang baru, atau pilih mesin target yang sudah ada.Klik OK.Siapkan opsi pemulihan tambahan yang Anda perlukan.[Tidak tersedia untuk Virtuozzo Hybrid Infrastructure dan Scale Computing HC3] Untuk memilih penyimpanan data bagi mesin virtual, klik Penyimpanan data untuk ESXi, Jalur untuk Hyper-V dan Virtuozzo, atau Domain penyimpanan untuk Red Hat Virtualization (oVirt), lalu pilih penyimpanan data (penyimpanan) untuk mesin virtual.Untuk melihat mode penyimpanan data (penyimpanan), antarmuka, dan provisi bagi setiap disk virtual, klik Pemetaan disk. Anda dapat mengubah pengaturan ini, kecuali jika Anda memulihkan kontainer Virtuozzo atau mesin virtual Virtuozzo Hybrid Infrastructure.Untuk Virtuozzo Hybrid Infrastructure, Anda hanya dapat memilih kebijakan penyimpanan untuk disk target. Untuk melakukannya, pilih disk target yang diinginkan, lalu pilih Ubah. Di bilah yang terbuka, klik ikon roda gigi, pilih kebijakan penyimpanan, lalu klik Selesai.Bagian pemetaan juga memungkinkan Anda memilih disk individual untuk pemulihan. [Tersedia untuk VMware ESXi, Hyper-V, dan Virtuozzo] Untuk mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual, klik Pengaturan VM.[Untuk Virtuozzo Hybrid Infrastructure] Untuk mengubah ukuran memori dan jumlah prosesor mesin virtual, pilih Cara. [Hanya tersedia untuk mesin Windows tempat agen perlindungan diinstal.] Aktifkan tombol pemulihan Aman untuk memastikan bahwa data yang dipulihkan bebas malware. Untuk informasi lebih lanjut mengenai cara pemulihan aman bekerja, lihat "Pemulihan aman" (hlm. 1).Klik Mulai pemulihan.Ketika memulihkan ke mesin virtual yang ada, konfirmasi bahwa Anda ingin menimpa disk.Progres pemulihan akan ditampilkan pada tab Aktivitas." (hlm. 1) dan "Memulihkan disk menggunakan media yang dapat di-boot" (hlm. 506).

Migrasi melalui media yang dapat di-boot

Sebagai alternatif dari migrasi mesin yang Anda lakukan di konsol Cyber Protect, Anda dapat memulihkan mesin menggunakan media yang dapat di-boot.

Anda sebaiknya menggunakan media yang dapat di-boot dalam kasus berikut:

- Melakukan migrasi yang tidak didukung secara asli.

  Misalnya, gunakan media yang dapat di-boot untuk memulihkan mesin fisik atau mesin virtual non-Virtuozzo sebagai mesin virtual Virtuozzo pada host Virtuozzo.
- Melakukan migrasi mesin Linux yang berisi volume logis (LVM).

  Gunakan Agen untuk Linux atau media yang dapat di-boot untuk membuat cadangan, lalu gunakan media yang dapat di-boot untuk memulihkan cadangan.
- Menyediakan driver untuk perangkat keras tertentu yang penting untuk bootabilitas pada sistem.

  Bangun media yang dapat di-boot dengan kemampuan menggunakan driver yang diperlukan. Untuk informasi lebih lanjut, lihat "Pembangun Media Yang Dapat Di-Boot" (hlm. 707).

© Acronis International GmbH, 2003-2024

Mesin virtual Microsoft Azure and Amazon EC2

Untuk mencadangkan mesin virtual Microsoft Azure atau Amazon EC2, instal agen perlindungan pada mesin. Operasi pencadangan dan pemulihan sama dengan mesin fisik. Meskipun demikian, mesin ini dihitung sebagai virtual saat Anda mengatur kuota untuk jumlah mesin.

Perbedaan dari mesin fisik adalah bahwa Mesin virtual Microsoft Azure and Amazon EC2 tidak dapat di-booting dari media yang dapat di-booting. Jika Anda perlu memulihkan ke mesin virtual Microsoft Azure atau Amazon EC2 baru, ikuti prosedur di bawah ini.

Catatan
Prosedur pemulihan berikut hanya berlaku untuk cadangan mesin yang berisi semua driver yang diperlukan untuk dijalankan di Microsoft Azure secara native (cadangan dibuat dari Azure VM, mesin Hyper-V lokal, atau mesin sumber Windows Server 2016 dan yang lebih baru). Untuk pemulihan platform, lihat artikel basis pengetahuan ini.

Untuk memulihkan mesin sebagai mesin virtual Microsoft Azure atau Amazon EC2

1. Buat mesin virtual baru dari gambar/templat di Microsoft Azure atau Amazon EC2. Mesin baru harus memiliki konfigurasi disk yang sama dengan mesin yang ingin Anda pulihkan.
2. Instal Agen untuk Windows atau Agen untuk Linux di mesin baru.
3. Pulihkan mesin yang dicadangkan seperti dijelaskan pada "Mesin fisik". Ketika mengonfigurasi pemulihan, pilih mesin baru sebagai mesin target.

Membuat media yang dapat di-boot untuk memulihkan sistem operasi

Media yang dapat di-boot adalah CD, DVD, drive flash USB, atau media yang dapat dilepas lainnya yang memungkinkan Anda untuk menjalankan agen proteksi baik di lingkungan berbasis Linux atau Windows Preinstallation Environment/Windows Recovery Environment (WinPE/WinRE), tanpa bantuan sistem operasi. Tujuan utama media yang dapat di-boot adalah untuk memulihkan sistem operasi yang tidak dapat dimulai.

Catatan
Media yang dapat di-boot tidak mendukung drive hybrid.

Media yang dapat di-boot kustom atau siap pakai?

Menggunakan Pembangun Media Yang Dapat Di-Boot, Anda dapat membuat sendiri media yang dapat di-boot (berbasis Linux atau berbasis WinPE) untuk komputer Windows, Linux, atau macOS. Di kedua media yang dapat di-boot kustom berbasis Linux atau berbasis WinPE/WinRE, Anda dapat mengonfigurasi pengaturan tambahan, seperti pendaftaran otomatis, pengaturan jaringan, atau pengaturan server proxy. Di media yang dapat di-boot kustom berbasis WinPE/WinRE, Anda juga dapat menambahkan driver.

© Acronis International GmbH, 2003-2024

Atau, Anda dapat mengunduh media yang dapat di-boot siap pakai (hanya berbasis Linux). Anda hanya dapat menggunakan media yang dapat di-boot siap pakai untuk operasi pemulihan dan akses ke fitur Universal Restore.

Media yang dapat di-boot berbasis Linux atau WinPE/WinRE?

Berbasis Linux

Media yang dapat di-boot berbasis Linux berisi agen proteksi berbasis kernel Linux. Agen dapat melakukan booting dan menjalankan operasi pada perangkat keras yang kompatibel dengan PC, termasuk logam, dan mesin dengan sistem file yang rusak atau tidak didukung.

Berbasis WinPE/WinRE

Media yang dapat di-boot berbasis WinPE berisi sistem Windows minimal yang disebut Windows Preinstallation Environment (WinPE) dan plugin Cyber Protection untuk WinPE, yaitu modifikasi dari agen proteksi yang dapat dijalankan di lingkungan prapenginstalan. Media yang dapat di-boot berbasis WinRE menggunakan Windows Recovery Environment dan tidak membutuhkan penginstalan atau paket Windows tambahan.

WinPE terbukti menjadi solusi bootable yang paling mudah di lingkungan besar dengan perangkat keras yang beragam.

Kelebihan:

- Menggunakan Cyber Protection di Windows Preinstallation Environment memberikan lebih banyak fungsionalitas daripada menggunakan media yang dapat di-boot berbasis Linux. Setelah mem-boot perangkat keras yang kompatibel dengan PC ke WinPE, Anda tidak hanya dapat menggunakan agen proteksi, tetapi juga perintah dan skrip PE serta plugin lain yang telah ditambahkan ke PE.
- Media yang dapat di-boot berbasis PE membantu mengatasi beberapa masalah media yang dapat di-boot terkait Linux, seperti dukungan untuk pengontrol RAID tertentu atau tingkat susunan RAID tertentu saja. Media berbasis WinPE 2.x dan yang lebih baru memungkinkan pemuatan dinamis driver perangkat yang diperlukan.

Batasan:

- Media yang dapat di-boot berbasis WinPE versi lebih lama dari 4.0 tidak dapat melakukan boot pada mesin yang menggunakan Unified Extensible Firmware Interface (UEFI).

Membuat media fisik yang dapat di-boot

Kami sangat menyarankan Anda untuk membuat dan menguji media yang dapat di-boot segera setelah mulai menggunakan cadangan tingkat disk. Selain itu, Anda disarankan untuk membuat ulang media setelah setiap pembaruan besar pada agen perlindungan.

Anda dapat memulihkan Windows atau Linux menggunakan media yang sama. Untuk memulihkan macOS, buat media terpisah di mesin yang menjalankan macOS.

© Acronis International GmbH, 2003-2024

Untuk membuat media fisik yang dapat di-boot di Windows atau Linux

1. Buat file ISO media yang dapat di-boot kustom atau unduh file ISO siap pakai.

   Untuk membuat file ISO kustom, gunakan "Pembangun Media Yang Dapat Di-Boot" (hlm. 707).

   Untuk mengunduh file ISO yang sudah jadi, di konsol Cyber Protect, pilih mesin, lalu klik **Pilih** > **Lebih banyak cara untuk pulih...** > **Unduh gambar ISO**.
2. [Opsional] Di konsol Cyber Protect, menghasilkan token pendaftaran. Token pendaftaran ditampilkan secara otomatis saat Anda mengunduh file ISO siap pakai.

   Token ini memberikan media yang dapat di-boot akses ke penyimpanan awan, tanpa perlu mengisi kata sandi dan masuk.
3. Buat media fisik yang dapat di-boot dengan cara berikut:
   - Salin file ISO ke CD/DVD.
   - Buat USB flash drive yang dapat di-boot menggunakan file ISO dan salah satu alat gratis yang tersedia secara online.

     Gunakan `ISO ke USB` atau `RUFUS` jika Anda perlu mem-boot mesin UEFI, dan `Win32DiskImager` untuk mesin BIOS. Di Linux, Anda dapat menggunakan utilitas `dd`.

   Untuk mesin virtual, Anda dapat menghubungkan file ISO sebagai drive CD/DVD ke mesin yang ingin Anda pulihkan.

Untuk membuat media fisik yang dapat di-boot di macOS

1. Di mesin yang terinstal Agen untuk Mac, klik **Aplikasi** > **Pembangun Media Penyelamat**.
2. Perangkat lunak ini menampilkan status koneksi media yang dapat dilepas. Pilih salah satu yang ingin Anda jadikan sebagai media yang dapat di-boot.

   Peringatan!
   Semua data di dalam disk akan dihapus.
3. Klik **Buat**.
4. Tunggu saat perangkat lunak membuat media yang dapat di-boot.

Pembangun Media Yang Dapat Di-Boot

Pembangun Media yang Dapat Di-boot adalah alat khusus untuk membuat media yang dapat di-boot. Semua ini diinstal sebagai komponen opsional pada mesin tempat agen proteksi diinstal.

Mengapa menggunakan Pembangun Media yang Dapat Di-Boot?

Media siap pakai yang dapat di-boot yang tersedia untuk diunduh di konsol Cyber Protect didasarkan pada kernel Linux. Tidak seperti Windows PE, media tersebut tidak memungkinkan penyuntikan driver kustom selama proses.

Pembangun Media yang Dapat Di-Boot memungkinkan Anda untuk membuat citra media yang dapat di-boot berbasis Linux dan berbasis WinPE kustom.

© Acronis International GmbH, 2003-2024

32-bit atau 64-bit?

Pembangun Media Yang Dapat Di-Boot membuat media yang dapat di-boot dengan komponen 32-bit dan 64-bit. Dalam sebagian besar kasus, Anda membutuhkan media 64-bit untuk mem-boot mesin yang menggunakan Unified Extensible Firmware Interface (UEFI).

Media yang dapat di-boot berbasis Linux

Untuk membuat media bootable berbasis Linux

1. Mulai **Pembangun Media Yang Dapat Di-Boot**.
2. Di **Tipe media yang dapat di-boot**, pilih **Default (media berbasis Linux)**.
3. Pilih cara volume dan sumber daya jaringan akan direpresentasikan:
   - Media yang dapat di-boot dengan representasi volume serupa Linux akan menampilkan volume sebagai, misalnya, hda1 dan sdb2. Media tersebut mencoba merekonstruksi perangkat MD dan volume logis (LVM) sebelum memulai pemulihan.
   - Media yang dapat di-boot dengan representasi volume, seperti Windows akan menampilkan volume sebagai, misalnya, C: dan D:. Media tersebut memberikan akses ke volume dinamis (LDM).
4. [Opsional] Tentukan parameter dari kernel Linux. Pisahkan beberapa parameter dengan spasi. Misalnya, agar dapat memilih mode tampilan untuk agen yang dapat di-boot, setiap kali media dimulai, ketik: **vga = ask**. Untuk informasi lebih lanjut tentang parameter yang tersedia, lihat "Parameter Kernel:" (hlm. 709).
5. [Opsional] Pilih bahasa untuk media yang dapat di-boot.
6. [Opsional] Pilih mode boot (BIOS atau UEFI) yang akan digunakan Windows setelah pemulihan.
7. Pilih komponen yang akan ditempatkan pada media – agen Cyber Protection yang dapat di-boot.
8. [Opsional] Tentukan interval batas waktu untuk menu boot. Jika pengaturan ini tidak dikonfigurasi, pemuat akan menunggu Anda memilih apakah akan mem-boot sistem operasi (jika ada) atau komponen.
9. [Opsional] Jika Anda ingin mengautomasi operasi agen yang dapat di-boot, pilih kotak centang **Gunakan skrip berikut**. Kemudian, pilih salah satu skrip dan tentukan parameter skrip. Untuk informasi lebih lanjut tentang skrip, lihat "Skrip dalam media yang dapat di-boot" (hlm. 711).
10. [Opsional] Pilih cara pendaftaran media yang dapat di-boot pada layanan Cyber Protection saat booting. Untuk informasi lebih lanjut tentang pengaturan pendaftaran, lihat "Mendaftarkan media yang dapat di-boot" (hlm. 720).
11. Tentukan pengaturan jaringan untuk adaptor jaringan mesin yang dapat dapat di-boot atau biarkan konfigurasi DHCP otomatis.
12. [Opsional] Jika server proksi diaktifkan di jaringan Anda, tentukan nama host/alamat IP dan port-nya.
13. Pilih tipe file hasil pembuatan media yang dapat di-boot:

© Acronis International GmbH, 2003-2024

- Profil ISO
- File ZIP

14. Pilih nama file untuk file media yang dapat di-boot.
15. Periksa pengaturan Anda di layar ringkasan, lalu klik **Lanjutkan**.

Parameter Kernel:

Anda dapat menentukan satu atau lebih parameter kernel Linux yang akan diterapkan secara otomatis ketika media yang dapat di-boot dimulai. Parameter ini biasanya digunakan ketika Anda mendapat masalah saat bekerja dengan media yang dapat di-boot. Biasanya, Anda dapat membiarkan bidang ini kosong.

Anda juga dapat menentukan salah satu dari parameter ini dengan menekan F11 saat berada di menu boot.

Parameter

Saat menentukan beberapa parameter, pisahkan dengan spasi.

- **acpi=off**
  Menonaktifkan Advanced Configuration and Power Interface (ACPI). Anda mungkin perlu menggunakan parameter ini ketika mengalami masalah dengan konfigurasi perangkat keras tertentu.
- **noapic**
  Menonaktifkan Advanced Programmable Interrupt Controller (APIC). Anda mungkin perlu menggunakan parameter ini ketika mengalami masalah dengan konfigurasi perangkat keras tertentu.
- **vga=ask**
  Perintah untuk mode video yang akan digunakan oleh antarmuka pengguna grafis media yang dapat di-boot. Tanpa parameter **vga**, mode video akan terdeteksi secara otomatis.
- **vga=** *mode_number*
  Menentukan mode video yang akan digunakan oleh antarmuka pengguna grafis dari media yang dapat di-boot. Nomor mode diberikan oleh *mode_number* dalam format heksadesimal—misalnya: **vga=0x318**
  Resolusi layar dan jumlah warna yang terkait dengan nomor mode mungkin akan berbeda pada mesin yang berbeda. Kami menyarankan Anda menggunakan parameter **vga=ask** terlebih dahulu untuk memilih nilai *mode_number*.
- **quiet**
  Menonaktifkan tampilan pesan startup saat kernel Linux memuat, dan memulai konsol manajemen setelah kernel dimuat.
  Parameter ini ditentukan tersirat saat membuat media yang dapat di-boot, tetapi Anda dapat menghapus parameter ini saat berada di menu boot.

© Acronis International GmbH, 2003-2024

Tanpa parameter ini, semua pesan pengaktifan akan ditampilkan, diikuti oleh command prompt. Untuk memulai konsol manajemen dari command prompt, jalankan perintah: **/bin/product**

- **nousb**

  Menonaktifkan pemuatan subsistem USB (Universal Serial Bus).
- **nousb2**

  Menonaktifkan dukungan USB 2.0. Perangkat USB 1.1 tetap berfungsi dengan parameter ini. Parameter ini memungkinkan Anda untuk menggunakan beberapa drive USB dalam mode USB 1.1, jika tidak berfungsi dalam mode USB 2.0.
- **nodma**

  Menonaktifkan akses memori langsung (DMA) untuk semua drive hard disk IDE. Mencegah pembekuan kernel pada beberapa perangkat keras.
- **nofw**

  Menonaktifkan dukungan antarmuka FireWire (IEEE1394).
- **nopcmcia**

  Menonaktifkan deteksi perangkat keras PCMCIA.
- **nomouse**

  Menonaktifkan dukungan mouse.
- *module_name* **=off**

  Menonaktifkan modul yang namanya diberikan dengan *module_name*. Misalnya, untuk menonaktifkan penggunaan modul SATA, tentukan: **sata_sis=off**
- **pci=bios**

  Memaksa penggunaan PCI BIOS, bukan mengakses perangkat keras secara langsung. Anda mungkin perlu menggunakan parameter ini jika mesin memiliki jembatan host PCI non-standar.
- **pci=nobios**

  Menonaktifkan penggunaan PCI BIOS; hanya metode akses perangkat keras langsung yang diizinkan. Anda mungkin perlu menggunakan parameter ini ketika media yang dapat di-boot gagal untuk memulai, yang mungkin disebabkan oleh BIOS.
- **pci=biosirq**

  Menggunakan panggilan PCI BIOS untuk mendapatkan tabel perutean interupsi. Anda mungkin perlu menggunakan parameter ini jika kernel tidak dapat mengalokasikan permintaan interupsi (IRQ) atau menemukan bus PCI sekunder pada motherboard.

  Panggilan ini mungkin tidak berfungsi dengan baik pada beberapa mesin. Tapi, ini mungkin adalah satu-satunya cara untuk mendapatkan tabel perutean interupsi.
- **LAYOUTS=en-US, de-DE, fr-FR, ...**

  Menentukan tata letak keyboard yang dapat digunakan dalam antarmuka pengguna grafis media yang dapat di-boot.

  Tanpa parameter ini, hanya dua tata letak yang dapat digunakan: Bahasa Inggris (AS) dan tata letak yang sesuai dengan bahasa yang dipilih dalam menu boot media.

  Anda dapat menentukan tata letak berikut:

  Belgia: **be-BE**

© Acronis International GmbH, 2003-2024

Ceko: **cz-CZ**
Inggris: **en-GB**
Inggris (AS): **en-US**
Prancis: **fr-FR**
Prancis (Swiss): **fr-CH**
Jerman: **de-DE**
Jerman (Swiss): **de-CH**
Italia: **it-IT**
Polandia: **pl-PL**
Portugis: **pt-PT**
Portugis (Brasil): **pt-BR**
Rusia: **ru-RU**
Serbia (Sirilik): **sr-CR**
Serbia (Latin): **sr-LT**
Spanyol: **es-ES**
Saat bekerja dalam media yang dapat di-boot, gunakan CTRL + SHIFT untuk menelusuri tata letak yang tersedia.

Skrip dalam media yang dapat di-boot

Jika Anda ingin media yang dapat di-boot menjalankan serangkaian operasi yang sudah ditentukan, Anda dapat menentukan skrip saat membuat media dengan Pembangun Media Yang Dapat Di-Boot. Maka, setiap kali mesin di-boot dari media, skrip tersebut akan jalan dan antarmuka pengguna tidak akan ditampilkan.

Anda dapat memilih salah satu skrip yang telah ditentukan atau membuat skrip kustom dengan mengikuti konvensi skrip.

Skrip yang sudah ditentukan

Pembangun Media yang Dapat Di-boot menyediakan skrip yang sudah ditentukan sebelumnya:

- Pemulihan dari penyimpanan awan (**entire_pc_cloud**)
- Pemulihan dari berbagi jaringan (**entire_pc_share**)

Skrip berada di folder berikut pada mesin tempat Pembangun Media yang Dapat Di-boot diinstal:

- Di Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Di Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Pemulihan dari penyimpanan awan

Di Pembangun Media yang Dapat Di-boot, tentukan parameter skrip berikut:

© Acronis International GmbH, 2003-2024

1. Nama file cadangan.
2. [Opsional] Kata sandi yang akan digunakan skrip untuk mengakses cadangan yang dienkripsi.

Pemulihan dari berbagi jaringan

Di Pembangun Media yang Dapat Di-boot, tentukan parameter skrip berikut:

- Jalur ke jaringan bersama.
- Nama pengguna dan kata sandi untuk jaringan bersama.
- Nama file cadangan. Untuk mengetahui nama file cadangan:
  a. Di konsol Cyber Protect, buka **Penyimpanan cadangan** > **Lokasi**.
  b. Pilih jaringan bersama (klik **Tambah lokasi** jika jaringan bersama tidak ada dalam daftar).
  c. Pilih cadangan.
  d. Klik **Detail**. Nama file ditampilkan di bawah **Nama file cadangan**.
- [Opsional] Kata sandi yang akan digunakan skrip untuk mengakses cadangan yang dienkripsi.

Skrip kustom

Penting
Pembuatan skrip khusus membutuhkan pengetahuan bahasa perintah Bash dan JavaScript Object Notation (JSON). Jika Anda tidak terbiasa dengan Bash, tempat yang baik untuk mempelajarinya adalah http://www.tldp.org/LDP/abs/html. Spesifikasi JSON tersedia di http://www.json.org.

File skrip

Skrip Anda harus berada di direktori berikut pada mesin tempat Pembangun Media yang Dapat Di-boot diinstal:

- Di Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Di Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Skrip harus terdiri dari setidaknya tiga file:

- **<script_file>.sh** - file dengan skrip Bash Anda. Saat membuat skrip, hanya gunakan set perintah shell terbatas, yang dapat Anda temukan di https://busybox.net/downloads/BusyBox.html. Selain itu, perintah berikut juga dapat digunakan:
  - `acrocmd` - utilitas baris perintah untuk pencadangan dan pemulihan
  - `product` - perintah yang memulai antarmuka pengguna media yang dapat di-boot

  File ini dan file tambahan apa pun yang disertakan skrip (misalnya, dengan menggunakan perintah dot) harus berada di subfolder **bin**. Dalam skrip, tentukan jalur file tambahan sebagai **/ConfigurationFiles/bin/<some_file>**.
- **autostart** - file untuk memulai **<script_file>.sh**. Konten file harus sebagai berikut:

© Acronis International GmbH, 2003-2024

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - file JSON yang berisi hal-hal berikut:
  - Nama dan deskripsi skrip yang akan ditampilkan di Pembangun Media yang Dapat Di-boot.
  - Nama-nama variabel skrip yang akan dikonfigurasi melalui Pembangun Media yang Dapat Di-boot.
  - Parameter kontrol yang akan ditampilkan di Pembangun Media yang Dapat Di-boot untuk setiap variabel.

Struktur autostart.json

Objek level atas

Pasangan		Diperlukan	Deskripsi
Nama	**Jenis nilai**		
`displayName`	string	Iya	Nama skrip yang akan ditampilkan di Pembangun Media yang Dapat Di-boot.
`description`	string	Tidak	Deskripsi skrip yang akan ditampilkan di Pembangun Media yang Dapat Di-boot.
`timeout`	number	Tidak	Batas waktu (dalam detik) untuk menu boot sebelum memulai skrip. Jika pasangan tidak ditentukan, batas waktu akan selama sepuluh detik.
`variables`	objek	Tidak	Setiap variabel untuk **<script_file>.sh** yang ingin Anda konfigurasi melalui Pambangun Media yang Dapat Di-boot. Nilai harus berupa set pasangan berikut: pengidentifikasi string untuk variabel dan objek variabel (lihat tabel di bawah).

Objek variabel

Pasangan		Diperlukan	Deskripsi
Nama	**Jenis nilai**		
`displayName`	string	Iya	Nama variabel yang digunakan dalam **<script_file>.sh**.

© Acronis International GmbH, 2003-2024

`type`	string	Iya	Jenis kontrol yang ditampilkan di Pembangun Media yang Dapat Di-boot. Kontrol ini digunakan untuk mengonfigurasi nilai variabel. Untuk mengetahui semua jenis yang didukung, lihat tabel di bawah ini.
`description`	string	Iya	Label kontrol yang ditampilkan di atas kontrol di Pembuat Media yang Dapat Di-boot.
`default`	string jika `type` adalah `string`, `multiString`, `kata sandi`, atau `enum` number jika `type` adalah `number`, `spinner`, atau `checkbox`	Tidak	Nilai default untuk kontrol. Jika pasangan tidak ditentukan, nilai default akan menjadi string kosong atau nol, berdasarkan pada tipe kontrol. Nilai default untuk kotak centang dapat berupa `0` (status yang dihapus) atau `1` (status yang dipilih).
`order`	number (non-negatif)	Iya	Urutan kontrol di Pembangun Media Yang Dapat Di-Boot Semakin tinggi nilainya, semakin rendah kontrol ditempatkan relatif terhadap kontrol lain yang didefinisikan dalam **autostart.json**. Nilai awal harus `0`.
`min` (khusus untuk `spinner`)	number	Tidak	Nilai minimum kontrol putaran dalam kotak putaran. Jika pasangan tidak ditentukan, nilainya akan `0`.
`maks` (khusus untuk `spinner`)	number	Tidak	Nilai maksimum kontrol putaran dalam kotak putaran. Jika pasangan tidak ditentukan, nilainya akan `100`.
`step` (khusus untuk `spinner`)	number	Tidak	Nilai langkah kontrol putaran dalam kotak putaran. Jika pasangan tidak ditentukan, nilainya akan `1`.
`items` (khusus untuk `enum`)	larik string	Iya	Nilai untuk daftar drop-down.
`required`	number	Tidak	Menentukan apakah nilai kontrol dapat kosong (`0`)

© Acronis International GmbH, 2003-2024

(untuk `string`, `multiString`, `password`, dan `enum`)			atau tidak (`1`). Jika pasangan tidak ditentukan, nilai kontrol dapat kosong.

Jenis kontrol

Nama	Deskripsi
`string`	Kotak teks baris tunggal yang tidak dibatasi digunakan untuk memasukkan atau mengedit string pendek.
`multiString`	Kotak teks multi-baris yang tidak dibatasi digunakan untuk memasukkan atau mengedit string panjang.
`kata sandi`	Kotak teks baris tunggal yang tidak dibatasi digunakan untuk memasukkan kata sandi secara aman.
`number`	Kotak teks baris tunggal dan hanya numerik digunakan untuk memasukkan atau mengedit angka.
`spinner`	Kotak teks baris tunggal dan hanya numerik digunakan untuk memasukkan atau mengedit angka, dengan kontrol putaran. Juga disebut kotak putaran.
`enum`	Daftar drop-down standar, dengan set nilai tetap yang telah ditentukan.
`kotak centang`	Kotak centang dengan dua status - status yang dihapus atau status yang dipilih.

Sampel **autostart.json** di bawah ini berisi semua jenis kontrol yang dapat digunakan untuk mengonfigurasi variabel untuk **<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,
```


© Acronis International GmbH, 2003-2024

```
                "description": "This is a 'multiString' control:",
                "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
        },
        "var_number": {
                "displayName": "VAR_NUMBER",
                "type": "number", "order": 3,
                "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
        }
}
```


© Acronis International GmbH, 2003-2024

}

Media yang dapat di-boot berbasis WinPE dan WinRE

Anda dapat membuat citra WinRE tanpa persiapan tambahan, atau membuat citra WinPE setelah menginstal Windows Automated Installation Kit (AIK) atau Windows Assessment and Deployment Kit (ADK).

Citra WinRE

Pembuatan citra WinRE didukung untuk sistem operasi berikut:

- Windows 7 (64-bit)
- Windows 8 (32-bit dan 64-bit)
- Windows 8.1 (32-bit dan 64-bit)
- Windows 10 (32-bit dan 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)

Citra WinPE

Setelah menginstal Windows Automated Installation Kit (AIK), atau Windows Assessment and Deployment Kit (ADK), Pembangun Media Yang Dapat Di-Boot mendukung distribusi WinPE yang didasarkan pada kernel berikut:

- Windows Vista (PE 2.0)
- Windows Vista SP1 dan Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) dengan atau tanpa suplemen untuk 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)

Pembangun Media yang Dapat Di-boot mendukung distribusi WinPE 32-bit dan 64-bit. Distribusi WinPE 32-bit juga dapat bekerja pada perangkat keras 64-bit. Namun, Anda memerlukan distribusi 64-bit untuk mem-boot mesin yang menggunakan Unified Extensible Firmware Interface (UEFI).

Catatan
Citra PE berbasis WinPE 4 dan yang lebih baru membutuhkan sekitar 1 GB RAM agar dapat bekerja.

© Acronis International GmbH, 2003-2024

Membuat media WinPE atau WinRE yang dapat di-boot

Pembangun Media Yang Dapat Di-Boot menyediakan dua metode untuk mengintegrasikan Cyber Protection dengan WinPE dan WinRE:

- Membuat file ISO dengan plugin Cyber Protection dari nol.
- Menambahkan plugin Cyber Protection ke file WIM untuk tujuan mendatang apa pun (pembuatan ISO manual, menambahkan alat lain ke citra dan lainnya).

Untuk membuat media WinPE atau WinRE yang dapat di-boot

1. Jalankan Pembangun Media yang Dapat Di-Boot pada mesin tempat agen proteksi diinstal.
2. Di **Tipe media yang dapat di-boot**, pilih **Windows PE** atau **Windows PE (64-bit)**. Media 64-bit diperlukan untuk mem-boot mesin yang menggunakan Unified Extensible Firmware Interface (UEFI).
3. Pilih subtipe media yang dapat di-boot: **WinRE** atau **WinPE**.

   Membuat media WinRE yang dapat di-boot tidak memerlukan penginstalan paket tambahan.

   Untuk membuat media WinPE 64-bit, Anda perlu mengunduh Windows Automated Installation Kit (AIK) atau Windows Assessment and Deployment Kit (ADK). Untuk membuat media WinPE 32-bit, selain mengunduh AIK atau ADK, Anda perlu melakukan tindakan berikut ini:

   a. Klik **Unduh Plug-in untuk WinPE (32-bit)**.

   b. Simpan plugin ke **%PROGRAM_FILES%\BackupClient\BootableComponents\WinPE32**.
4. [Opsional] Pilih bahasa untuk media yang dapat di-boot.
5. [Opsional] Pilih mode boot (BIOS atau UEFI) yang akan digunakan Windows setelah pemulihan.
6. Tentukan pengaturan jaringan untuk adaptor jaringan mesin yang dapat di-boot atau biarkan konfigurasi DHCP otomatis.
7. [Opsional] Pilih cara pendaftaran media yang dapat di-boot pada layanan Cyber Protection saat booting. Untuk informasi lebih lanjut tentang pengaturan pendaftaran, lihat "Mendaftarkan media yang dapat di-boot" (hlm. 720).
8. [Opsional] Tentukan driver Windows yang akan ditambahkan ke media yang dapat di-boot.

   Setelah Anda mem-boot mesin ke Windows PE atau Windows RE, driver dapat membantu Anda mengakses perangkat tempat cadangan berada. Tambahkan driver 32-bit jika Anda menggunakan distribusi WinPE atau WinRE 32-bit atau driver 64-bit jika Anda menggunakan distribusi WinPE atau WinRE 64-bit.

   Untuk menambahkan driver:

   - Klik **Tambah** dan tentukan jalur ke file .inf yang diperlukan untuk SCSI, RAID, pengontrol SATA, adaptor jaringan, drive pita, atau perangkat lain yang sesuai.
   - Ulangi prosedur ini untuk setiap driver yang ingin Anda sertakan dalam media WinPE atau WinRE yang dihasilkan.
9. Pilih tipe file hasil pembuatan media yang dapat di-boot:

© Acronis International GmbH, 2003-2024

- Profil ISO
- Image WIM

10. Tentukan jalur penuh ke hasil file profil, termasuk nama file.
11. Periksa pengaturan Anda di layar ringkasan, lalu klik **Lanjutkan**.

Untuk membuat image PE (file ISO) dari file WIM yang dihasilkan

- Ganti file boot.wim default di folder Windows PE Anda dengan file WIM yang baru dibuat. Untuk contoh di atas, ketik:

```
salin c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Gunakan alat **Oscdimg**. Untuk contoh di atas, ketik:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

Peringatan!
Jangan menyalin dan menempelkan contoh ini. Ketik perintah secara manual, jika tidak, operasi akan gagal.

Persiapan: WinPE 2.x dan 3.x

Untuk dapat membuat atau memodifikasi citra PE 2.x atau 3.x, instal Pembuat Media Bootable dan Windows Automated Installation Kit (AIK) pada mesin yang sama.

Untuk mempersiapkan mesin

1. Unduh file profil AIK dari situs web Microsoft, sebagai berikut:
   - Untuk Windows Vista (PE 2.0): https://www.microsoft.com/en-us/download/details.aspx?id=10333
   - Untuk Windows Vista SP1 dan Windows Server 2008 (PE 2.1): https://www.microsoft.com/en-us/download/details.aspx?id=9085
   - Untuk Windows 7 (PE 3.0): https://www.microsoft.com/en-gb/download/details.aspx?id=5753
     Untuk Windows 7 SP1 (PE 3.1), Anda juga memerlukan suplemen AIK yang tersedia di https://www.microsoft.com/en-us/download/details.aspx?id=5188
2. Masukkan file profil ke disk DVD atau drive flash USB.
3. Dari file profil, instal file berikut:
   - Microsoft .NET Framework (NETFXx86 atau NETFXx64, tergantung pada perangkat keras Anda)
   - MSXML (Parser XML Microsoft)
   - Windows AIK
4. Instal Pembangun Media yang Dapat Di-boot di mesin yang sama.

© Acronis International GmbH, 2003-2024

Persiapan: WinPE 4.0 ke atas

Untuk dapat membuat atau memodifikasi citra PE 4 atau yang lebih baru, instal Pembuat Media Bootable dan Windows Assessment and Deployment Kit (ADK) pada mesin yang sama.

Untuk mempersiapkan mesin

1. Unduh program penyiapan ADK dari situs web Microsoft.
   Versi Windows berikut mendapatkan dukungan:
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)
   - Windows 8.1 (PE 5.0)
   - Windows 8 (PE 4.0)
2. Pasang Kit Penilaian dan Penyebaran.
3. Instal Pembuat Media Bootable.

Mendaftarkan media yang dapat di-boot

Mendaftarkan media yang dapat di-boot di layanan Cyber Protection memungkinkan Anda mengakses penyimpanan awan untuk cadangan Anda. Anda dapat melakukan prakonfigurasi pendaftaran sambil membuat media yang dapat di-boot. Jika pendaftaran tidak diprakonfigurasi, Anda dapat mendaftarkan medianya setelah mem-boot mesin dengannya.

Untuk memprakonfigurasi pendaftaran di layanan Cyber Protection

1. Di Pembangun Media Yang Dapat Di-Boot, navigasikan ke **Pendaftaran media yang dapat di-boot**.
2. Di **URL layanan**, tetapkan alamat layanan Cyber Protection.
3. [Opsional] Di **Nama tampilan**, tentukan nama untuk mesin yang di-boot.
4. Untuk mengatur pendaftaran otomatis di layanan Cyber Protection, pilih kotak centang **Daftarkan media yang dapat di-boot secara otomatis**, lalu pilih tingkat pendaftaran otomatis.
   - **Tanyakan token pendaftaran saat booting**
     Token harus diberikan setiap kali mesin di-boot dari media.
   - **Gunakan token berikut**
     Mesin akan didaftarkan secara otomatis setiap kali di-boot dari media.

Untuk mendaftarkan media yang dapat di-boot setelah mem-boot mesin dari sana

1. Boot mesin dari media yang dapat di-boot.
2. Di jendela pengaktifan, klik **Daftarkan media**.
3. Di **Server**, tetapkan alamat layanan Cyber Protection.

© Acronis International GmbH, 2003-2024

4. Di **Token pendaftaran**, masukkan token pendaftaran.
5. Klik **Daftar**.

Pengaturan jaringan

Saat membuat media yang dapat di-boot, Anda dapat melakukan prakonfigurasi koneksi jaringan yang akan digunakan oleh agen yang dapat di-boot. Parameter berikut dapat diprakonfigurasi:

- Alamat IP
- Masker subnet
- Gerbang
- Server DNS
- Server WINS

Setelah agen yang dapat di-boot dimulai pada mesin, konfigurasi akan diterapkan ke kartu antarmuka jaringan (NIC) mesin. Jika pengaturan belum diprakonfigurasi, agen akan menggunakan konfigurasi otomatis DHCP.

Anda juga dapat mengonfigurasi pengaturan jaringan secara manual ketika agen yang dapat di-boot berjalan pada mesin.

Prakonfigurasi beberapa koneksi jaringan

Anda dapat melakukan prakonfigurasi pengaturan TCP/IP hingga sepuluh kartu antarmuka jaringan (NIC). Untuk memastikan bahwa masing-masing NIC akan diberikan pengaturan yang sesuai, buat media di server tempat media disesuaikan. Ketika Anda memilih NIC yang ada di jendela wizard, pengaturannya dipilih dan disimpan di media. Alamat MAC dari setiap NIC yang ada juga disimpan di media.

Anda dapat mengubah pengaturan, kecuali alamat MAC, atau mengonfigurasi pengaturan untuk NIC yang tidak ada.

Setelah agen yang dapat di-boot dimulai pada server, agen akan mengambil daftar NIC yang tersedia. Daftar ini diurutkan berdasarkan slot yang ditempati NIC, paling dekat dengan prosesor berada di atas.

Agen yang dapat di-boot menetapkan pengaturan yang sesuai pada setiap NIC yang dikenal, dan mengidentifikasi NIC menurut alamat MAC miliknya. Setelah NIC dengan alamat MAC yang diketahui dikonfigurasi, pengaturan yang Anda buat untuk NIC yang tidak ada akan ditetapkan ke NIC yang tersisa, dimulai dari NIC yang tidak ditetapkan di bagian atas.

Anda dapat menyesuaikan media yang dapat di-boot untuk mesin apa pun, bukan hanya untuk mesin tempat media tersebut dibuat. Untuk melakukannya, konfigurasikan NIC sesuai dengan urutan slotnya pada mesin tersebut: NIC1 menempati slot paling dekat dengan prosesor, NIC2 berada di slot berikutnya dan seterusnya. Ketika agen yang dapat di-boot dimulai pada mesin tersebut, agen tidak akan menemukan NIC dengan alamat MAC dikenal dan akan mengkonfigurasi NIC dalam urutan yang sama.

© Acronis International GmbH, 2003-2024

Contoh

Agen yang dapat di-boot dapat menggunakan salah satu adaptor jaringan untuk komunikasi dengan konsol manajemen melalui jaringan produksi. Konfigurasi otomatis dapat dilakukan untuk koneksi ini. Data yang cukup besar untuk pemulihan dapat ditransfer melalui NIC kedua, termasuk pada jaringan cadangan khusus melalui pengaturan TCP/IP statis.

Menghubungkan ke mesin yang di-boot dari media yang dapat di-boot

Koneksi lokal

Agar dapat beroperasi langsung pada mesin yang di-boot dari media yang dapat di-boot, klik **Kelola mesin ini secara lokal** di jendela startup.

Setelah mesin di-boot dari media yang dapat di-boot, terminal mesin akan menampilkan jendela pengaktifan dengan alamat IP yang diperoleh dari DHCP atau diatur sesuai dengan nilai prakonfigurasi.

Mengonfigurasi pengaturan jaringan

Untuk mengubah pengaturan jaringan untuk sesi saat ini, klik **Konfigurasi jaringan** di jendela pengaktifan. Jendela **Pengaturan Jaringan** yang muncul akan memungkinkan Anda untuk mengonfigurasi pengaturan jaringan untuk setiap kartu antarmuka jaringan (NIC) mesin.

Perubahan yang dilakukan selama sesi akan hilang setelah mesin reboot.

Menambahkan VLAN

Di jendela **Pengaturan Jaringan**, Anda dapat menambahkan jaringan area lokal virtual (VLAN). Gunakan fungsi ini jika Anda memerlukan akses ke lokasi pencadangan yang termasuk dalam VLAN tertentu.

VLAN utamanya digunakan untuk membagi jaringan area lokal ke dalam beberapa segmen. NIC yang terhubung ke port *akses* switch selalu memiliki akses ke VLAN yang ditentukan dalam konfigurasi port. NIC yang terhubung ke port *trunk* switch dapat mengakses VLAN yang diizinkan dalam konfigurasi port hanya jika Anda menentukan VLAN di pengaturan jaringan.

Untuk mengaktifkan akses ke VLAN melalui port trunk

1. Klik **Tambah VLAN**.
2. Pilih NIC yang menyediakan akses ke jaringan area lokal yang mencakup VLAN yang diperlukan.
3. Tentukan pengidentifikasi VLAN.

Setelah Anda mengklik **OK**, entri baru akan muncul di daftar adaptor jaringan.

Jika Anda perlu menghapus VLAN, klik entri VLAN yang diperlukan, lalu klik **Hapus VLAN**.

© Acronis International GmbH, 2003-2024

Operasi lokal dengan media yang dapat di-boot

Operasi dengan media yang dapat di-boot mirip dengan operasi pemulihan yang dilakukan melalui sistem operasi yang berjalan. Perbedaannya adalah sebagai berikut:

1. Pada media yang dapat di-boot dengan representasi volume serupa Windows, volume memiliki huruf drive yang sama seperti di Windows. Volume yang tidak memiliki huruf drive di Windows (seperti volume Cadangan Sistem) diberi huruf bebas sesuai urutannya pada disk.

   Jika media yang dapat di-boot tidak dapat mendeteksi Windows pada mesin atau mendeteksi lebih dari satu, semua volume, termasuk yang tidak memiliki huruf drive, akan diberi huruf sesuai urutannya pada disk. Oleh karena itu, huruf volume mungkin berbeda dengan yang terlihat di Windows. Misalnya, drive D: di bawah media yang dapat di-boot mungkin sesuai dengan drive E: di Windows.

   Catatan
   Sebaiknya Anda menetapkan nama unik untuk volume.

2. Media yang dapat di-boot dengan representasi volume serupa Linux menunjukkan disk dan volume lokal sebagai tidak terpasang (sda1, sda2...).
3. Tugas tidak dapat dijadwalkan. Jika Anda perlu mengulangi operasi, konfigurasikan dari awal.
4. Masa aktif log terbatas pada sesi saat ini. Anda dapat menyimpan entri seluruh isi log atau log terfilter ke file.

Mengatur mode tampilan

Saat Anda mem-boot mesin melalui media yang dapat di-boot berbasis Linux, mode video tampilan dideteksi secara otomatis berdasarkan konfigurasi perangkat keras (spesifikasi monitor dan kartu grafis). Jika mode video terdeteksi secara tidak tepat, lakukan langkah berikut:

1. Di menu boot, tekan F11.
2. Pada baris perintah, masukkan **vga=ask**, kemudian lanjutkan dengan booting.
3. Dari daftar mode video yang didukung, pilih yang sesuai dengan mengetik nomornya (misalnya, **318**), lalu tekan **Enter**.

Jika tidak ingin mengikuti prosedur ini setiap kali Anda mem-boot konfigurasi perangkat keras tertentu, buat ulang media yang dapat di-boot dengan nomor mode sesuai (dalam contoh di atas, **vga=0x318**) yang ditentukan di bidang **Parameter kernel**.

Pemulihan dengan media yang dapat di-boot secara lokal

1. Boot mesin dari media yang dapat di-boot.
2. Klik **Kelola mesin ini secara lokal**.
3. Klik **Pulihkan**.
4. Di **Apa yang akan dipulihkan**, klik **Pilih data**.

© Acronis International GmbH, 2003-2024

5. Pilih file cadangan yang ingin Anda pulihkan.
6. Di panel kiri bawah, pilih drive/volume atau file/folder yang ingin Anda pulihkan, lalu klik **OK**.
7. Konfigurasi aturan penimpaan.
8. Konfigurasi pengeculian pemulihan.
9. Konfigurasi opsi pemulihan.
10. Pastikan bahwa pengaturan Anda benar, dan kemudian klik **OK**.

Operasi jarak jauh dengan media yang dapat di-boot

Catatan
Fitur ini tersedia dengan paket Cadangan Lanjutan.

Untuk melihat media yang dapat di-boot di konsol Cyber Protect, pertama-tama Anda harus mendaftarkannya seperti yang dijelaskan di "Mendaftarkan media yang dapat di-boot" (hlm. 720).

Setelah Anda mendaftarkan media di konsol Cyber Protect, media akan muncul pada tab **Perangkat** > **Media yang dapat di-boot**. Media yang dapat di-boot menghilang dari tab ini saat telah offline selama lebih dari 30 hari.

Anda dapat mengelola media yang dapat di-boot dari jarak jauh di konsol Cyber Protect. Misalnya, Anda dapat memulihkan data, memulai ulang atau mematikan mesin yang di-boot dengan media, atau melihat informasi, aktivitas, dan peringatan tentang media.

Penting
Anda tidak dapat memperbarui media yang dapat di-boot dari jarak jauh, di tab **Pengaturan** > **Agen** di konsol Cyber Protect.

Untuk memperbarui media yang dapat di-boot, buat yang baru, seperti yang dijelaskan di bagian "Pembangun Media Yang Dapat Di-Boot" (hlm. 707). Atau, unduh media yang sudah jadi, dengan mengklik ikon akun Anda > **Unduhan** > **Media yang dapat di-boot** di konsol Cyber Protect.

Untuk memulihkan file atau folder dengan media yang dapat di-boot dari jarak jauh

1. Di konsol Cyber Protect, buka **Perangkat** > **Media yang dapat di-boot**.
1. Pilih media yang ingin Anda gunakan untuk pemulihan data.
2. Klik **Pemulihan**.
3. Pilih lokasi, lalu pilih cadangan yang Anda perlukan. Perlu dicatat bahwa cadangan difilter berdasarkan lokasi.
4. Pilih titik pemulihan, lalu klik **Pulihkan file/folder**.
5. Jelajahi ke folder yang diperlukan atau gunakan bilah pencarian untuk mendapatkan daftar file dan folder yang diperlukan.

   Pencarian bersifat bebas bahasa.

© Acronis International GmbH, 2003-2024

Anda dapat menggunakan satu atau lebih karakter wildcard (* dan ?). Untuk detail lebih lanjut tentang penggunaan wildcard, lihat "Filter file (Penyertaan/Pengecualian)" (hlm. 460).

6. Klik untuk memilih file yang ingin Anda pulihkan, lalu klik **Pulihkan**.
7. Di **Jalur**, pilih tujuan pemulihan.
8. [Opsional] Untuk konfigurasi pemulihan lanjutan, klik **Opsi pemulihan**. Untuk informasi lebih lanjut, lihat "Opsi pemulihan" (hlm. 518).
9. Klik **Mulai pemulihan**.
10. Pilih salah satu opsi penimpaan file:
    - **Timpa file yang ada**
    - **Timpa file yang ada jika lebih lama**
    - **Jangan timpa file yang ada**

    Pilih apakah Anda ingin mulai kembali mesin secara otomatis.
11. Klik **Lanjutkan** untuk memulai pemulihan. Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

Untuk memulihkan disk, volume, atau seluruh mesin dengan media yang dapat di-boot dari jarak jauh

1. Pada tab **Perangkat**, buka grup **Media yang dapat di-boot**, lalu pilih media yang ingin Anda gunakan untuk pemulihan data.
2. Klik **Pemulihan**.
3. Pilih lokasi, lalu pilih cadangan yang Anda perlukan. Perlu dicatat bahwa cadangan difilter berdasarkan lokasi.
4. Pilih titik pemulihan, lalu klik **Pulihkan** > **Seluruh mesin**.

   Jika perlu, konfigurasikan mesin target dan pemetaan volume seperti yang dijelaskan di "Memulihkan mesin fisikBagian ini menjelaskan pemulihan mesin fisik menggunakan antarmuka web.Gunakan media yang dapat di-boot, bukan antarmuka web jika Anda perlu memulihkan:Mesin yang menjalankan macOSMesin dari penyewa dalam mode KepatuhanSistem operasi apa pun pada bare metal atau mesin offlineStruktur volume logis (volume dibuat oleh Logical Volume Manager di Linux). Media memungkinkan Anda membuat ulang struktur volume logis secara otomatis.Anda tidak dapat memulihkan cadangan tingkat disk dari Mac berbasis Intel ke Mac yang menggunakan prosesor silikon Apple, dan sebaliknya. Anda dapat memulihkan file dan folder.Pemulihan dengan mulai kembaliPemulihan sistem operasi dan pemulihan volume yang terenkripsi dengan BitLocker memerlukan mulai kembali. Anda dapat memilih untuk memulai kembali mesin secara otomatis atau menetapkan status Interaksi diperlukan. Sistem operasi yang dipulihkan kembali online secara otomatis.Volume terenkripsi yang dicadangkan dipulihkan menjadi tidak terenkripsi.Pemulihan volume terenkripsi BitLocker memerlukan adanya volume tidak-terenkripsi di mesin yang sama, dan volume ini memiliki setidaknya ruang bebas sebesar 1 GB. Jika kondisi ini tidak terpenuhi, pemulihan gagal.Memulihkan sistem volume terenkripsi tidak memerlukan tindakan tambahan apa pun. Untuk memulihkan bukan-sistem volume terenkripsi, Anda harus menguncinya terlebih dahulu,

© Acronis International GmbH, 2003-2024

dengan membuka file yang ditempatkan dalam volume ini. Sebaliknya, pemulihan akan terus berlanjut tanpa mulai kembali dan volume yang dipulihkan mungkin tidak dikenali oleh Windows.Jika pemulihan gagal dan mesin Anda dimulai kembali dengan pesan kesalahan Tidak dapat mendapatkan file dari partisi, coba nonaktifkan Boot Aman. Untuk informasi lebih lanjut tentang cara melakukannya, lihat Menonaktifkan Boot Aman di dokumentasi Microsoft.Untuk memulihkan mesin fisikPilih mesin yang dicadangkan.Klik Pemulihan.Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Lakukan yang berikut ini:Jika lokasi cadangan adalah awan atau penyimpanan bersama (yaitu agen lain dapat mengaksesnya), klik Pilih mesin, pilih mesin target yang online, lalu pilih titik pemulihan.Pilih titik pemulihan pada tab Penyimpanan cadangan.Pulihkan mesin seperti yang dijelaskan pada "Memulihkan disk menggunakan media yang dapat di-boot".Klik Pulihkan > Seluruh mesin.Perangkat lunak memetakan secara otomatis disk dari cadangan ke disk mesin target.Untuk memulihkan ke mesin fisik lain, klik Mesin target, lalu pilih mesin target yang sedang online.Jika Anda tidak puas dengan hasil pemetaan atau pemetaan disk tidak berhasil, klik Pemetaan volume untuk memetakan ulang disk secara manual.Bagian pemetaan juga memungkinkan Anda memilih disk atau volume individual untuk pemulihan. Anda dapat beralih antara memulihkan disk dan volume menggunakan tautan Alihkan ke... di sudut kanan atas.[Hanya tersedia untuk mesin Windows tempat agen perlindungan diinstal.] Aktifkan tombol pemulihan Aman untuk memastikan bahwa data yang dipulihkan bebas malware. Untuk informasi lebih lanjut mengenai cara pemulihan aman bekerja, lihat "Pemulihan aman" (hlm. 1).Klik Mulai pemulihan.Konfirmasi bahwa Anda ingin menimpa disk dengan versi yang dicadangkannya. Pilih apakah Anda ingin mulai kembali mesin secara otomatis.Progres pemulihan akan ditampilkan pada tab Aktivitas." (hlm. 1).

5. Untuk konfigurasi pemulihan lanjutan, klik **Opsi pemulihan**. Untuk informasi lebih lanjut, lihat "Opsi pemulihan" (hlm. 518).
6. Klik **Mulai pemulihan**.
7. Konfirmasi bahwa Anda ingin menimpa disk dengan versi yang dicadangkannya. Pilih apakah Anda ingin mulai kembali mesin secara otomatis.
8. Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

Untuk memulai ulang mesin yang di-boot dari jarak jauh

1. Pada tab **Perangkat**, buka grup **Media yang dapat di-boot**, lalu pilih media yang ingin Anda gunakan untuk pemulihan data.
2. Klik **Boot Ulang**.
3. Konfirmasikan bahwa Anda ingin memulai ulang mesin yang di-boot dengan media.

Untuk mematikan mesin yang di-boot dari jarak jauh

1. Pada tab **Perangkat**, buka grup **Media yang dapat di-boot**, lalu pilih media yang ingin Anda gunakan untuk pemulihan data.
2. Klik **Matikan**.
3. Konfirmasikan bahwa Anda ingin mematikan mesin yang di-boot dengan media.

© Acronis International GmbH, 2003-2024

Untuk melihat informasi tentang media yang dapat di-boot

1. Pada tab **Perangkat**, buka grup **Media yang dapat di-boot**, lalu pilih media yang ingin Anda gunakan untuk pemulihan data.
2. Klik **Detail**, **Aktivitas**, atau **Peringatan** untuk melihat informasi terkait.

Untuk menghapus media yang dapat di-boot dari jarak jauh

1. Pada tab **Perangkat**, buka grup **Media yang dapat di-boot**, lalu pilih media yang ingin Anda gunakan untuk pemulihan data.
2. Klik **Hapus** untuk menghapus media yang dapat di-boot dari konsol Cyber Protect.
3. Konfirmasikan bahwa Anda ingin menghapus media yang dapat di-boot.

Startup Recovery Manager

Startup Recovery Manager adalah komponen yang dapat di-boot dan berada di hard drive. Dengan Startup Recovery Manager, Anda dapat memulai utilitas penyelamatan yang dapat di-boot tanpa menggunakan media yang dapat di-boot terpisah.

Jika terjadi kegagalan, restart mesin, tunggu petunjuk **Tekan F11 untuk Acronis Startup Recovery Manager** muncul, lalu tekan F11 atau pilih Startup Recovery Manager dari menu boot (jika Anda menggunakan pemuat boot GRUB). Startup Recovery Manager mulai dan Anda dapat melakukan pemulihan.

Pembatasan

- [Tidak berlaku untuk GRUB yang diinstal ke master boot record] Mengaktifkan Startup Recovery Manager menimpa master boot record (MBR) dengan kode boot-nya sendiri. Akibatnya, Anda mungkin perlu mengaktifkan kembali pemuat boot pihak ketiga setelah aktivasi.
- [GRUB tidak berlaku] Sebelum mengaktifkan Startup Recovery Manager di Linux, kami menyarankan Anda untuk menginstal pemuat boot ke boot record partisi root atau ke boot record partisi /boot alih-alih menginstalnya ke master boot record. Jika tidak, konfigurasi ulang pemuat boot secara manual setelah aktivasi.

Mengaktifkan Startup Recovery Manager

Untuk mengaktifkan prompt waktu booting **Tekan F11 untuk Acronis Startup Recovery Manager** (atau menambahkan item **Startup Recovery Manager** ke menu GRUB), Anda harus mengaktifkan Startup Recovery Manager.

© Acronis International GmbH, 2003-2024

Catatan
Mengaktifkan Startup Recovery Manager pada mesin dengan volume sistem yang tidak dienkripsi memerlukan setidaknya 100 MB ruang bebas tersedia pada mesin ini. Pemulihan dengan restart memerlukan tambahan 100 MB.

Untuk mengaktifkan Startup Recovery Manager pada mesin yang memiliki volume yang dienkripsi BitLocker, mesin ini harus memiliki setidaknya satu volume yang tidak dienkripsi di mana ada setidaknya 500 MB ruang bebas. Pemulihan dengan restart memerlukan tambahan 500 MB ruang bebas.

Operasi pencadangan yang membuat cadangan pemulihan Sekali klik akan gagal jika Startup Recovery Manager tidak diaktifkan.

Untuk mengaktifkan Startup Recovery Manager

Pada mesin Windows atau Linux yang dipasangi agen

1. Di konsol Cyber Protect, pilih mesin yang ingin Anda aktifkan Startup Recovery Manager.
2. Klik **Detail**.
3. Aktifkan switch **Startup Recovery Manager**.

Pada mesin yang tidak dipasangi agen

1. Boot mesin dengan menggunakan media yang dapat di-boot.
2. Di antarmuka grafis media yang dapat di-boot, klik **Alat Bantu** > **Aktifkan Startup Recovery Manager**.
3. Pilih **Aktifkan**.
4. Klik **OK**.
5. Di tab **Detail**, periksa baris **Hasil** untuk memastikan bahwa aktivasi telah berhasil, lalu klik **Tutup**.

Menonaktifkan Startup Recovery Manager

Deaktivasi menonaktifkan prompt waktu booting **Tekan F11 untuk Acronis Startup Recovery Manager** (atau menghapus item **Startup Recovery Manager** dari menu GRUB).

Jika Startup Recovery Manager tidak diaktifkan, Anda masih dapat memulihkan mesin yang gagal booting dengan menggunakan media yang dapat di-boot terpisah.

Catatan
Operasi pencadangan yang membuat cadangan pemulihan Sekali klik akan gagal jika Startup Recovery Manager tidak diaktifkan.

Untuk menonaktifkan Startup Recovery Manager

Pada mesin Windows atau Linux yang dipasangi agen

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, pilih mesin yang ingin Anda nonaktifkan Startup Recovery Manager.
2. Klik **Detail**.
3. Nonaktifkan switch **Startup Recovery Manager**.

Pada mesin yang tidak dipasangi agen

1. Boot mesin dengan menggunakan media yang dapat di-boot.
2. Di antarmuka grafis media yang dapat di-boot, klik **Alat Bantu** > **Nonaktifkan Startup Recovery Manager**.
3. Pilih **Nonaktifkan**.
4. Klik **OK**.
5. Pada tab **Detail**, periksa baris **Hasil** untuk memastikan bahwa penonaktifan berhasil, lalu klik **Tutup**.

© Acronis International GmbH, 2003-2024

Menerapkan pemulihan bencana

Catatan
- Fungsionalitas ini tidak mendukung lokasi cadangan Microsoft Azure.

Tentang Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) – bagian dari Cyber Protection yang menyediakan pemulihan bencana sebagai layanan (DRaaS). Cyber Disaster Recovery Cloud memberi Anda solusi yang cepat dan stabil untuk meluncurkan salinan yang akurat dari mesin Anda di situs awan, lalu mengalihkan beban kerja dari mesin asli yang rusak ke server pemulihan di awan jika terjadi bencana alam atau bencana karena manusia.

Anda dapat mengatur dan mengonfigurasi pemulihan bencana dengan cara berikut:

- Buat rencana proteksi yang disertai modul pemulihan bencana dan terapkan pada perangkat Anda. Ini akan menyiapkan infrastruktur pemulihan bencana default secara otomatis. Lihat Membuat rencana proteksi pemulihan bencana.
- Atur fungsi infrastruktur awan pemulihan bencana secara manual dan kontrol setiap langkah. Lihat "Mengatur server pemulihan" (hlm. 776).

Fungsi utama

Catatan
Beberapa fitur mungkin memerlukan pelisensian tambahan sesuai model pelisensian yang diterapkan.

- Kelola layanan Cyber Disaster Recovery Cloud dari satu konsol
- Perluas hingga 23 jaringan lokal ke awan, dengan menggunakan terowongan VPN yang aman
- Buat koneksi ke situs awan tanpa penyebaran alat VPN[1] apa pun (mode hanya-awan)
- Buat koneksi titik-ke-situs ke situs lokal dan situs awan Anda
- Lindungi mesin Anda menggunakan server pemulihan di awan
- Lindungi aplikasi dan alat menggunakan server utama di awan
- Jalankan operasi pemulihan bencana otomatis untuk cadangan yang dienkripsi
- Lakukan failover uji dalam jaringan yang terisolasi
- Gunakan runbook untuk mempercepat lingkungan produksi di awan

[1] [Pemulihan Bencana] Mesin virtual khusus yang memungkinkan koneksi antara jaringan lokal dan situs awan melalui terowongan VPN yang aman. Alat VPN disebarkan di situs lokal.

© Acronis International GmbH, 2003-2024

Persyaratan perangkat lunak

Sistem Operasi yang Didukung

Perlindungan dengan server pemulihan telah diuji untuk sistem operasi berikut:

- 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 – semua opsi instalasi, kecuali untuk Nano Server
- Windows Server 2019 – semua opsi instalasi, kecuali untuk Nano Server
- Windows Server 2022 – semua opsi instalasi, kecuali untuk Nano Server

Perangkat lunak ini dapat berfungsi dengan sistem operasi Windows dan distribusi Linux lainnya, tetapi ini tidak dijamin.

Catatan
Perlindungan dengan server pemulihan telah diuji untuk Microsoft Azure VM dengan sistem operasi berikut.

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – semua opsi instalasi, kecuali untuk Nano Server
- Windows Server 2019 – semua opsi instalasi, kecuali untuk Nano Server
- Windows Server 2022 – semua opsi instalasi, kecuali untuk Nano Server
- Server Ubuntu 20.04 LTS - Gen2 (Kanonis). Untuk informasi lebih lanjut tentang akses konsol server pemulihan, baca https://kb.acronis.com/content/71616.

Platform virtualisasi yang didukung

Perlindungan mesin virtual dengan server pemulihan telah diuji untuk platform virtualisasi berikut:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 dengan Hyper-V
- Windows Server 2012/2012 R2 dengan Hyper-V

© Acronis International GmbH, 2003-2024

- Windows Server 2016 dengan Hyper-V – semua opsi instalasi, kecuali untuk Nano Server
- Windows Server 2019 dengan Hyper-V – semua opsi instalasi, kecuali untuk Nano Server
- Windows Server 2022 dengan Hyper-V – semua opsi instalasi, kecuali untuk Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Mesin Virtual berbasis Kernel (KVM) — hanya tamu virtual sepenuhnya (HVM). Tamu paravirtual (PV) tidak didukung.
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

Alat VPN telah diuji untuk platform virtualisasi berikut:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 dengan Hyper-V
- Windows Server 2012/2012 R2 dengan Hyper-V
- Windows Server 2016 dengan Hyper-V – semua opsi instalasi, kecuali untuk Nano Server
- Windows Server 2019 dengan Hyper-V – semua opsi instalasi, kecuali untuk Nano Server
- Windows Server 2022 dengan Hyper-V – semua opsi instalasi, kecuali untuk Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Perangkat lunak ini dapat berfungsi dengan platform dan versi virtualisasi lainnya, tetapi ini tidak dijamin.

Pembatasan

Platform dan konfigurasi berikut tidak didukung di Cyber Disaster Recovery Cloud:

1. Platform yang tidak didukung:
   - Agen untuk Virtuozzo
   - macOS
   - Sistem operasi desktop Windows tidak didukung karena persyaratan produk Microsoft.
   - Edisi Azure Windows Server

     Azure Edition adalah versi khusus dari Windows Server yang dibangun khusus untuk dijalankan baik sebagai mesin virtual Azure IaaS (VM) di Azure maupun sebagai VM pada klaster Azure Stack HCI. Berbeda dengan edisi Standard dan Datacenter, Azure Edition tidak memiliki lisensi untuk dijalankan pada perangkat keras bare metal, Hyper-V klien Windows, Hyper-V Server Windows, hypervisor pihak ketiga, atau di cloud pihak ketiga.
2. Konfigurasi yang tidak didukung:

© Acronis International GmbH, 2003-2024

Microsoft Windows

- Disk dinamis tidak didukung
- Sistem operasi desktop Windows tidak didukung (karena persyaratan produk Microsoft)
- Layanan Active Directory dengan replikasi FRS tidak didukung
- Media yang dapat dilepas tanpa format GPT atau MBR (disebut "superfloppy") tidak didukung

Linux

- Sistem file tanpa tabel partisi
- Beban kerja Linux yang dicadangkan dengan agen dari OS tamu dan memiliki volume dengan konfigurasi Manajer Volume Logis (LVM) lanjutan berikut: Volume Striped, volume Mirrored, volume RAID 0, RAID 4, RAID 5, RAID 6, atau RAID 10.

Catatan
Beban kerja yang memiliki beberapa sistem operasi terpasang tidak didukung.

3. Tipe pencadangan yang tidak didukung:
   - Titik pemulihan perlindungan data berkelanjutan (CDP) tidak kompatibel.

     Penting
     Jika Anda membuat server pemulihan dari cadangan yang memiliki titik pemulihan CDP, selama failback atau mencadangkan server pemulihan, Anda akan kehilangan data yang terdapat dalam titik pemulihan CDP.

   - Cadangan forensik tidak dapat digunakan untuk membuat server pemulihan nanti.

Server pemulihan memiliki satu antarmuka jaringan. Jika mesin asli memiliki beberapa antarmuka jaringan, hanya satu yang akan diemulasi.

Server awan tidak dienkripsi.

Versi percobaan Cyber Disaster Recovery Cloud

Anda dapat menggunakan versi percobaan dari Acronis Cyber Disaster Recovery Cloud untuk periode waktu 30 hari. Dalam hal ini, Pemulihan Bencana memiliki batasan berikut bagi penyewa mitra:

- Tidak ada akses ke internet publik untuk pemulihan dan server utama. Anda tidak dapat menetapkan alamat IP publik ke server.
- VPN Multisitus IPsec tidak tersedia.

© Acronis International GmbH, 2003-2024

Keterbatasan saat menggunakan Penyimpanan Cloud Geo-redundan

Penyimpanan Cloud Geo-redundan menyediakan lokasi sekunder untuk data cadangan Anda. Lokasi sekunder berada di wilayah yang secara geografis berbeda dari lokasi penyimpanan utama. Pemisahan wilayah secara geografis memastikan bahwa - jika terjadi bencana yang berdampak pada salah satu wilayah dan membuat data cadangan tidak dapat dipulihkan - wilayah lainnya tidak akan terpengaruh, dan operasi akan terus berlanjut.

Penting
Layanan Pemulihan Bencana tidak didukung jika lokasi penyimpanan cadangan dialihkan dari lokasi utama ke lokasi sekunder geo-redundan.

Kesesuaian Pemulihan Bencana dengan perangkat lunak enkripsi

Pemulihan bencana kompatibel dengan perangkat lunak enkripsi tingkat disk berikut:

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

Catatan
- Untuk beban kerja dengan enkripsi tingkat disk, kami merekomendasikan Anda untuk menginstal agen proteksi di sistem operasi tamu dari beban kerja tersebut, dan melakukan pencadangan berbasis agen.
- Failover dan failback tidak akan didukung untuk pencadangan tanpa agen dari beban kerja yang dienkripsi.

Untuk informasi lebih lanjut tentang kompatibilitas Cyber Protection dengan perangkat lunak enkripsi, lihat "Kompatibilitas dengan perangkat lunak enkripsi" (hlm. 42).

Titik komputasi

Dalam Pemulihan Bencana, titik komputasi digunakan sebagai server utama dan server pemulihan selama uji failover dan produksi failover. Titik komputasi mencerminkan sumber daya komputasi yang digunakan untuk menjalankan server (mesin virtual) di cloud.

Konsumsi titik komputasi selama pemulihan bencana bergantung pada parameter server, dan durasi periode waktu saat server dalam tahap failover. Semakin kuat server dan semakin lama periode waktu, lebih banyak titik komputasi akan dikonsumsi. Dan semakin banyak titik komputasi yang dikonsumsi, semakin besar harga yang akan ditagihkan kepada Anda.

© Acronis International GmbH, 2003-2024

Semua server yang berjalan di Acronis Cloud akan dikenakan biaya untuk titik komputasi, tergantung jenis yang dikonfigurasi dan terlepas dari kondisi mereka (dinyalakan atau dimatikan).

Server pemulihan dalam keadaan Standby tidak menggunakan titik komputasi dan tidak akan dikenakan biaya untuk titik komputasi.

Dalam tabel di bawah ini, Anda dapat melihat contoh untuk delapan server di cloud dengan berbagai jenis, dan titik komputasi yang akan mereka konsumsi per jam. Anda dapat mengubah jenis server di tab **Detail**.

Tipe	CPU	RAM	Titik komputasi
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

Dengan menggunakan informasi di dalam tabel, Anda dapat dengan mudah memperkirakan berapa banyak titik komputasi yang akan dikonsumsi oleh server (mesin virtual).

Misalnya, jika Anda perlu untuk melindungi dengan Pemulihan Bencana salah satu mesin virtual dengan 4 vCPU* dari 16 GB RAM, dan satu mesin virtual dengan 2 vCPU dengan 8 GB RAM, mesin virtual pertama akan mengonsumsi 8 titik komputasi per jam, dan mesin virtual kedua - 4 titik komputasi per jam. Jika kedua mesin virtual berada pada tahap failover, total konsumsi akan menghabiskan 12 titik komputasi per jam, atau 288 titik komputasi selama satu hari penuh (12 titik komputasi X 24 jam = 288 titik komputasi).

* vCPU merujuk pada unit pemrosesan pusat (CPU) fisik yang ditugaskan ke mesin virtual, dan merupakan entitas yang bergantung pada waktu.

Catatan
Jika kelebihan untuk kuota **Titik komputasi** telah tercapai, semua server utama dan pemulihan akan dimatikan. Tidak akan mungkin menggunakan server-server ini hingga awal periode penagihan berikutnya, atau sampai Anda meningkatkan kuota. Periode penagihan default adalah satu bulan kalender penuh.

© Acronis International GmbH, 2003-2024

Mengatur fungsi pemulihan bencana

Catatan
Beberapa fitur mungkin memerlukan pelisensian tambahan sesuai model pelisensian yang diterapkan.

Untuk mengatur fungsi pemulihan bencana

1. Konfigurasi jenis konektivitas ke situs awan:
   - Koneksi titik-ke-situs
   - Koneksi VPN Terbuka Situs-ke-situs
   - Koneksi VPN IPsec Multi-situs
   - Mode hanya-awan
2. Buat rencana proteksi dengan modul pencadangan diaktifkan dan pilih keseluruhan mesin atau sistem plus volume boot untuk pencadangan. Setidaknya diperlukan satu rencana proteksi untuk membuat server pemulihan.
3. Terapkan rencana proteksi pada server lokal untuk dilindungi.
4. Buat server pemulihan untuk setiap server lokal Anda yang ingin Anda lindungi.
5. Jalankan failover uji untuk memeriksa cara kerjanya.
6. [Opsional] Membuat server utama untuk replikasi aplikasi.

Hasilnya, Anda telah mengatur fungsi pemulihan bencana untuk melindungi server lokal Anda dari bencana.

Jika terjadi bencana, Anda dapat menjalankan failover beban kerja ke server pemulihan di awan. Setidaknya satu titik pemulihan harus dibuat sebelum gagal pada server pemulihan. Ketika situs lokal Anda sudah pulih dari bencana, Anda dapat mengalihkan beban kerja kembali ke situs lokal dengan melakukan failback. Untuk informasi lebih lanjut tentang proses failback, lihat "Prasyarat" (hlm. 789) dan "Prasyarat" (hlm. 794).

Membuat rencana proteksi pemulihan bencana

Buat rencana proteksi yang disertai modul Pemulihan Bencana dan terapkan pada perangkat Anda.

Secara default, saat membuat rencana proteksi baru, modul Pemulihan Bencana dinonaktifkan. Setelah mengaktifkan fungsionalitas pemulihan bencana dan menerapkan rencana ke perangkat Anda, infrastruktur jaringan awan dibuat, termasuk *server pemulihan* untuk tiap perangkat yang terlindungi. *Server pemulihan* adalah mesin virtual di awan yang merupakan salinan dari perangkat terpilih. Untuk setiap perangkat terpilih, server pemulihan dengan pengaturan default dibuat dalam keadaan siaga (mesin virtual tidak berjalan). Server pemulihan diukur secara otomatis, bergantung pada CPU dan RAM perangkat yang dilindungi. Infrastruktur jaringan awan default juga dibuat

© Acronis International GmbH, 2003-2024

secara otomatis: Gateway VPN dan jaringan di situs awan, yang terhubung dengan server pemulihan.

Jika Anda membatalkan, menghapus, atau mematikan modul Pemulihan Bencana rencana proteksi, server pemulihan dan jaringan awan tidak akan terhapus secara otomatis. Anda dapat menghapus infrastruktur pemulihan bencana secara manual, jika diperlukan.

Catatan

- Setelah Anda mengonfigurasi pemulihan bencana, Anda dapat melakukan failover uji atau produksi dari salah satu titik pemulihan yang dihasilkan setelah server pemulihan dibuat untuk perangkat. Titik pemulihan yang dibuat sebelum perangkat terlindungi pemulihan bencana (misalnya sebelum server pemulihan dibuat) tidak dapat digunakan untuk failover.
- Rencana proteksi pemulihan bencana tidak dapat diaktifkan jika alamat IP perangkat tidak dapat dideteksi. Misalnya, ketika mesin virtual dicadangkan tanpa agen dan alamat IP tidak ditetapkan.
- Saat Anda menerapkan rencana proteksi, jaringan dan alamat IP yang sama ditetapkan di situs awan. Konektivitas VPN IPsec perlu agar segmen jaringan awan dan situs lokal tidak tumpang tindih. Jika konektivitas VPN IPsec Multi-situs dikonfigurasi, lalu Anda menerapkan rencana proteksi ke satu atau beberapa perangkat, Anda harus memperbarui jaringan awan dan menetapkan ulang alamat IP server awan. Untuk informasi lebih lanjut, lihat "Menetapkan kembali alamat IP" (hlm. 766).

Untuk membuat rencana proteksi pemulihan bencana

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih mesin yang ingin Anda lindungi.
3. Klik **Lindungi**, lalu klik **Buat rencana**.
   Pengaturan default rencana proteksi akan dibuka.
4. Konfigurasikan opsi pencadangan.
   Untuk menggunakan fungsionalitas pemulihan bencana, rencana ini harus mencadangkan seluruh mesin, atau hanya disk-nya, yang diperlukan untuk booting dan menyediakan layanan yang dibutuhkan, ke penyimpanan awan.
5. Aktifkan modul Pemulihan bencana dengan mengklik switch di sebelah nama modul.
6. Klik **Buat**.
   Rencana dibuat dan diterapkan pada mesin yang dipilih.

Selanjutnya

- Anda dapat mengedit konfigurasi default server pemulihan. Untuk informasi lebih lanjut, lihat "Mengatur server pemulihan" (hlm. 776).
- Anda dapat mengedit konfigurasi jaringan default. Untuk informasi lebih lanjut, lihat "Mengatur konektivitas" (hlm. 740).

© Acronis International GmbH, 2003-2024

- Anda dapat melihat informasi lebih lanjut tentang parameter default server pemulihan dan infrastruktur jaringan awan. Untuk informasi lebih lanjut, lihat "Mengedit Parameter default server pemulihan" (hlm. 738) dan "Infrastruktur jaringan awan" (hlm. 739).

Mengedit Parameter default server pemulihan

Saat Anda membuat dan menerapkan rencana proteksi pemulihan bencana, server pemulihan dengan parameter default dibuat. Anda dapat mengedit parameter default ini nanti.

Catatan
Server pemulihan dibuat secara otomatis, jika tidak tersedia. Server pemulihan yang ada tidak diubah atau dibuat ulang.

Untuk mengedit parameter default server pemulihan

1. Buka **Perangkat** > **Seluruh perangkat**.
2. Pilih perangkat, kemudian klik **Pemulihan Bencana**.
3. Edit parameter default server pemulihan.
   Parameter server pemulihan dijelaskan dalam tabel berikut.

Server pemulihan parameter	Default nilai	Deskripsi
CPU dan RAM	otomatis	Jumlah CPU virtual dan ukuran RAM untuk server pemulihan. Pengaturan default akan ditentukan secara otomatis berdasarkan konfigurasi CPU dan RAM perangkat asli.
Jaringan awan	otomatis	Jaringan awan yang akan dihubungkan dengan server. Untuk detail mengenai cara jaringan awan dikonfigurasi, lihat Infrastruktur jaringan awan.
Alamat IP di jaringan produksi	otomatis	Alamat IP yang akan dimiliki server dalam jaringan produksi. Secara default, alamat IP mesin asli telah diatur.
Uji alamat IP	dinonaktifkan	Uji alamat IP memberikan Anda kemampuan menguji failover di jaringan uji yang terisolasi dan terhubung ke server pemulihan melalui RDP atau SSH selama failover uji. Di mode tes failover, gateway VPN akan menggantikan alamat IP uji dengan alamat IP produksi menggunakan protokol NAT. Jika uji alamat IP tidak ditentukan, konsol akan menjadi satu-satunya cara untuk mengakses server selama failover uji.
Akses Internet	diaktifkan	Mengaktifkan server pemulihan untuk mengakses Internet selama failover nyata atau uji. Secara

© Acronis International GmbH, 2003-2024

		default, port TCP 25 ditolak untuk koneksi keluar.
Gunakan Alamat publik	dinonaktifkan	Memiliki alamat IP publik membuat server pemulihan tersedia dari Internet selama failover atau failover uji. Jika Anda tidak menggunakan alamat IP publik, server hanya akan tersedia pada jaringan produksi Anda. Untuk menggunakan alamat IP publik, Anda harus mengaktifkan akses internet. Alamat IP publik akan ditampilkan setelah Anda menyelesaikan konfigurasi. Secara default, port TCP 443 terbuka untuk koneksi masuk.
Tentukan ambang batas RPO	dinonaktifkan	Ambang batas RPO menentukan interval waktu maksimum yang diizinkan antara titik pemulihan dan waktu terkini. Nilai dapat diatur antara 15 – 60 menit, 1 – 24 jam, 1 – 14 hari.

Infrastruktur jaringan awan

Infrastruktur jaringan awan terdiri dari gateway VPN di situs awan dan jaringan awan tempat server pemulihan akan terhubung.

Catatan
Menerapkan rencana proteksi pemulihan bencana membuat infrastruktur jaringan awan pemulihan hanya jika tidak tersedia. Jaringan awan yang ada tidak diubah atau dibuat ulang.

Sistem ini memeriksa alamat IP perangkat dan jika tidak terdapat jaringan awan yang tepat untuk alamat IP tersebut, sistem secara otomatis akan membuat jaringan awan yang sesuai. Jika Anda memiliki jaringan awan yang tepat untuk alamat IP server pemulihan, jaringan awan yang ada tidak akan diubah atau dibuat ulang.

- Jika Anda tidak memiliki jaringan awan yang ada atau Anda mengatur konfigurasi pemulihan bencana untuk pertama kalinya, jaringan awan akan dibuat dengan rentang maksimum yang direkomendasikan oleh IANA untuk penggunaan pribadi (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) berdasarkan rentang alamat IP perangkat Anda. Anda dapat mempersempit jaringan dengan mengedit mask jaringan.
- Jika Anda memiliki perangkat pada beberapa jaringan lokal, jaringan di situs awan dapat menjadi superset jaringan lokal. Anda dapat mengonfigurasi ulang jaringan di bagian **Konektivitas**. Lihat "Mengelola jaringan" (hlm. 760).
- Jika Anda ingin mengatur konektivitas VPN Terbuka Situs-ke-Situs, unduh dan atur perangkat VPN. Lihat "Mengonfigurasi VPN Terbuka Situs-ke-situs" (hlm. 751). Pastikan rentang jaringan awan cocok dengan rentang jaringan lokal Anda yang terhubung ke alat VPN.
- Untuk mengubah konfigurasi jaringan default, klik tautan **Pergi ke konektivitas** pada modul Pemulihan Bencana milik Rencana proteksi atau navigasikan ke **Pemulihan Bencana** > **Konektivitas**.

© Acronis International GmbH, 2003-2024

Mengatur konektivitas

Bagian ini menjelaskan konsep jaringan yang Anda perlukan untuk memahami cara kerja semuanya dalam Cyber Disaster Recovery Cloud. Anda akan mempelajari cara mengonfigurasi berbagai jenis konektivitas ke situs awan, sesuai kebutuhan Anda. Terakhir, Anda akan mempelajari cara mengelola jaringan di awan dan pengaturan alat VPN, dan gateway VPN.

Konsep pengaturan jaringan

Catatan
Beberapa fitur mungkin memerlukan pelisensian tambahan sesuai model pelisensian yang diterapkan.

Dengan Cyber Disaster Recovery Cloud, Anda dapat menentukan jenis konektivitas berikut ke situs awan:

- **Mode hanya-awan**

  Jenis koneksi ini tidak memerlukan penyebaran alat VPN di situs lokal.

  Jaringan lokal dan awan adalah jaringan independen. Jenis koneksi ini menyiratkan bahwa failover pada semua server terlindungi di situs lokal atau failover parsial server independen yang tidak perlu berkomunikasi dengan situs lokal.

  Server awan di situs awan dapat diakses melalui VPN titik-ke-situs VPN, dan alamat IP publik (jika ditetapkan).
- **Koneksi VPN Terbuka Situs-ke-situs**

  Jenis koneksi ini memerlukan penyebaran alat VPN di situs lokal.

  Dengan koneksi VPN Terbuka Situs-ke-situs, Anda dapat memperluas jaringan Anda ke awan dan menyimpan alamat IP.

  Situs lokal Anda terhubung ke situs awan melalui terowongan VPN yang aman. Jenis koneksi ini cocok apabila Anda memiliki beberapa server yang sangat bergantung di situs lokal, seperti server web dan server database. Jika terjadi failover parsial, ketika salah satu server ini dibuat kembali di situs awan sedangkan server lain di situs lokal, kesemuanya akan tetap dapat saling berkomunikasi melalui terowongan VPN.

  Server awan di situs awan dapat diakses melalui jaringan lokal, VPN titik-ke-situs VPN, dan alamat IP publik (jika ditetapkan).
- **Koneksi VPN IPsec Multi-situs**

  Jenis koneksi ini membutuhkan perangkat VPN lokal yang mendukung IPsec IKE v2.

  Saat Anda mulai mengonfigurasi koneksi VPN IPsec Multi-situs, Cyber Disaster Recovery Cloud secara otomatis gateway VPN awan dengan alamat IP publik dibuat.

  Dengan VPN IPsec Multi-situs, situs lokal Anda terhubung ke situs awan melalui terowongan VPN IPsec yang aman.

© Acronis International GmbH, 2003-2024

Jenis koneksi ini sesuai dengan skenario Pemulihan Bencana jika Anda memiliki satu atau beberapa situs lokal yang mengeola beban kerja kritis atau layanan yang sangat bergantung.

Jika terjadi failover sebagian dari salah satu server, server dibuat ulang di situs awan sementara yang lain tetap berada di situs lokal, dan mereka masih dapat saling berkomunikasi melalui terowongan VPN IPsec.

Jika terjadi failover sebagian pada salah satu situs lokal, situs lokal lainnya tetap beroperasi, dan masih dapat saling berkomunikasi melalui terowongan VPN IPsec.

- **Akses VPN jarak jauh titik-ke-situs**

  Akses VPN jarak jauh Titik-ke-situs yang aman ke beban kerja situs awan dan lokal dari luar dengan menggunakan perangkat titik akhir Anda.

  Untuk akses situs lokal, jenis koneksi ini memerlukan penyebaran alat VPN di situs lokal.

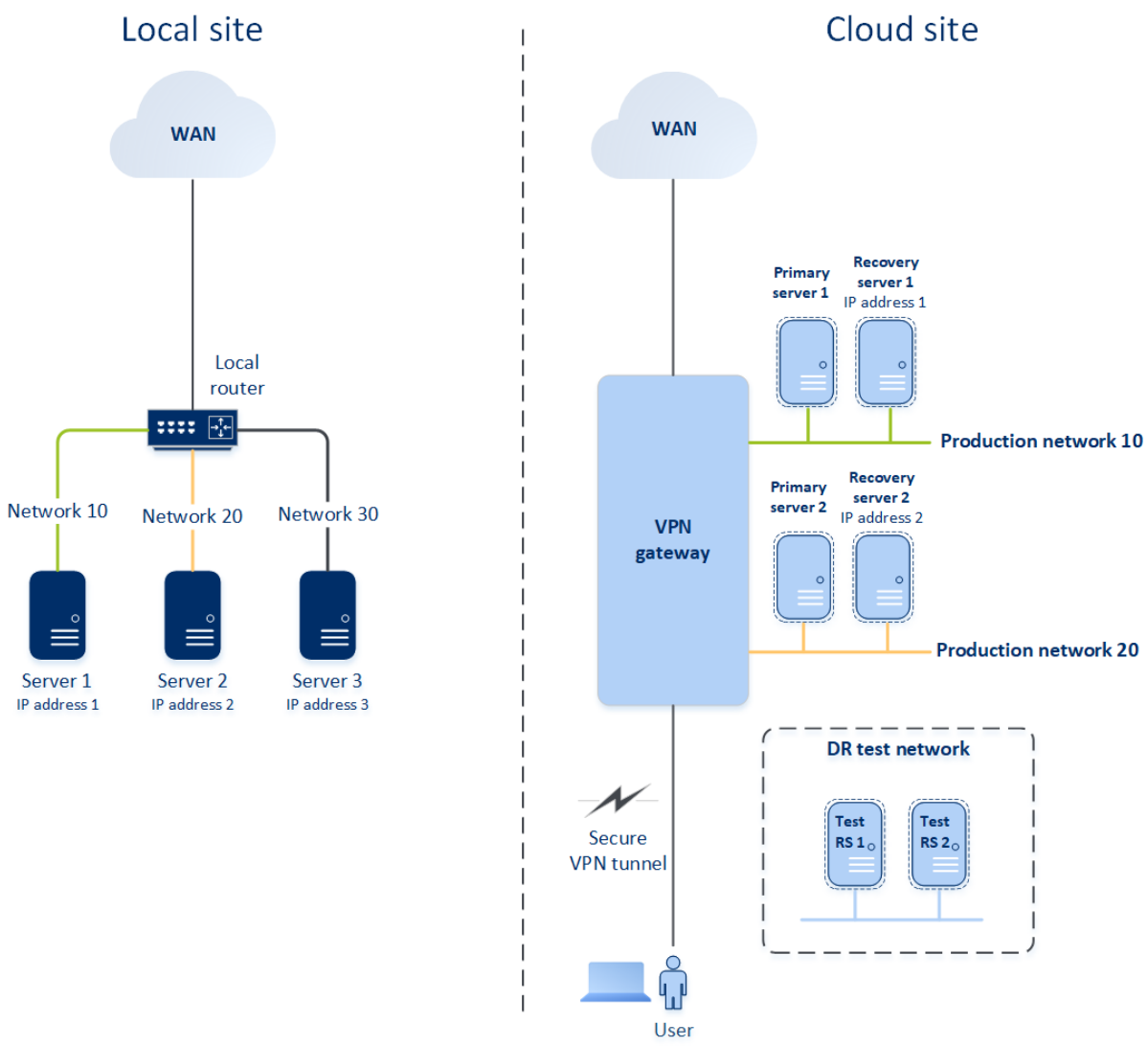
Mode hanya-awan

Mode hanya-awan tidak memerlukan penyebaran alat VPN di situs lokal. Hal ini menyiratkan bahwa Anda memiliki dua jaringan independen: satu di situs lokal, yang lainnya di situs awan. Perutean dijalankan dengan router di situs awan.

Cara kerja perutean

Jika mode hanya-awan dijalankan, perutean dilaksanakan dengan router di situs awan sehingga server dari jaringan awan yang lain dapat berkomunikasi satu sama lain.

© Acronis International GmbH, 2003-2024



Koneksi VPN Terbuka Situs-ke-situs

Catatan

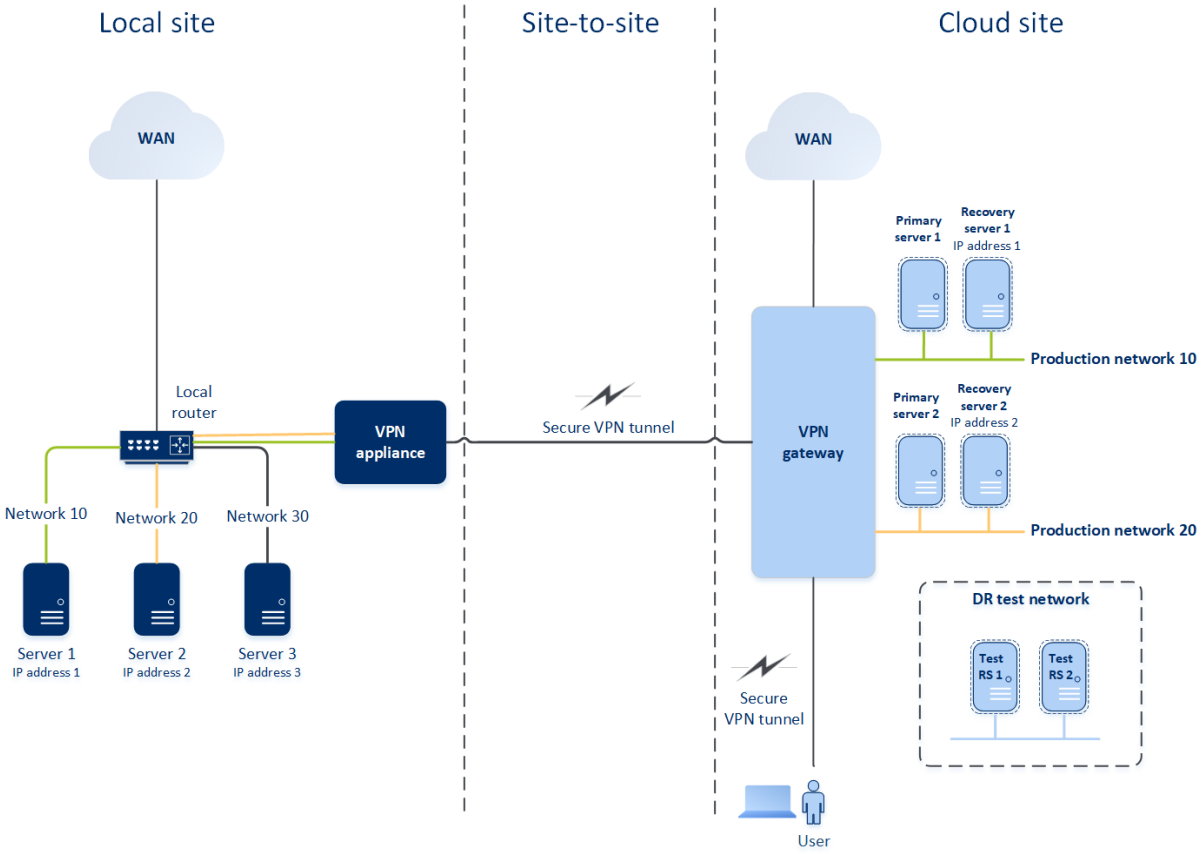
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Untuk memahami cara kerja pengaturan jaringan di Cyber Disaster Recovery Cloud, kami akan membuat contoh kasus di mana Anda memiliki tiga jaringan dengan satu mesin di setiap situs lokal. Anda akan mengonfigurasi perlindungan dari bencana untuk dua jaringan – Jaringan 10 dan Jaringan 20.

Pada diagram di bawah ini, Anda dapat melihat situs lokal tempat mesin Anda dikelola dan situs awan yang meluncurkan server awan jika terjadi bencana.

Dengan solusi Cyber Disaster Recovery Cloud, Anda dapat melakukan failover pada semua beban kerja dari mesin yang rusak di situs lokal ke server awan di awan. Anda dapat melindungi hingga 23 jaringan dengan Cyber Disaster Recovery Cloud.

© Acronis International GmbH, 2003-2024



Untuk membangun komunikasi VPN Terbuka Situs-ke-situs antara situs lokal dan awan, **alat VPN** dan **gateway VPN** digunakan. Saat Anda mulai mengonfigurasi koneksi VPN Terbuka Situs-ke-situs di konsol Cyber Protect, gateway VPN secara otomatis diterapkan di situs awan. Lalu, Anda harus menyebarkan alat VPN di situs lokal Anda, menambahkan jaringan yang akan dilindungi, dan mendaftarkan alat di awan. Cyber Disaster Recovery Cloud membuat replika jaringan lokal Anda di awan. Terowongan VPN yang aman dibuat antara alat VPN dan gateway VPN. Terowongan tersebut memberikan ekstensi ke awan untuk jaringan lokal Anda. Jaringan produksi di awan dihubungkan dengan jaringan lokal Anda. Server lokal dan server awan dapat berkomunikasi melalui terowongan VPN ini seolah-olah keduanya berada di segmen Ethernet yang sama. Perutean dijalankan dengan router lokal Anda.

Untuk setiap mesin sumber yang akan dilindungi, Anda harus membuat server pemulihan di situs awan. Server pemulihan tetap dalam keadaan **Standby** hingga failover terjadi. Jika terjadi bencana dan Anda memulai proses failover (dalam **mode produksi**), server pemulihan yang merepresentasikan salinan sebenarnya dari mesin Anda yang terlindungi akan diluncurkan di awan. Server pemulihan tersebut dapat diberi alamat IP yang sama dengan mesin sumber dan dapat diluncurkan di segmen Ethernet yang sama. Klien Anda dapat terus menggunakan server tanpa menyadari terjadinya perubahan latar belakang.

Anda juga dapat memulai proses failover di **mode uji**. Ini artinya mesin sumber masih berfungsi, dan pada saat bersamaan server pemulihan terkait dengan alamat IP yang sama diluncurkan di awan. Untuk mencegah konflik alamat IP, jaringan virtual khusus dibuat di awan – **jaringan uji**. Jaringan uji diisolasi untuk mencegah duplikasi alamat IP mesin sumber dalam satu segmen

© Acronis International GmbH, 2003-2024

Ethernet. Untuk mengakses server pemulihan dalam mode failover pengujian, saat Anda membuat server pemulihan, Anda harus menetapkan **Alamat IP Uji** ke server tersebut. Ada parameter lain untuk server pemulihan yang dapat ditentukan, yang akan dibahas di bagian terkait di bawah ini.

Cara kerja perutean

Saat koneksi Situs-ke-situs dibuat, perutean antarjaringan awan dilakukan dengan perute lokal Anda. Server VPN tidak melakukan perutean antara server awan yang terletak di jaringan awan yang berbeda. Jika server awan dari satu jaringan ingin berkomunikasi ke server dari jaringan awan lain, lalu lintas ini berjalan melalui terowongan VPN ke router lokal di situs lokal, kemudian router lokal ini merutekannya ke jaringan lain, dan kembali melalui terowongan ke server tujuan di situs awan.

Gateway VPN

Komponen utama yang memungkinkan komunikasi antara situs lokal dan situs awan adalah **gateway VPN**. Ini adalah mesin virtual di awan tempat perangkat lunak khusus diinstal, dan jaringan dikonfigurasi secara khusus. Gateway VPN memiliki fungsi berikut:

- Menghubungkan segmen Ethernet dari jaringan lokal dan jaringan produksi Anda di awan dalam mode L2.
- Memberikan aturan iptable dan ebtable.
- Bekerja sebagai perute dan NAT default untuk mesin di jaringan uji dan produksi.
- Bekerja sebagai server DHCP. Semua mesin dalam jaringan produksi dan uji mendapat konfigurasi jaringan (alamat IP, pengaturan DNS) melalui DHCP. Setiap saat, server awan akan mendapatkan alamat IP yang sama dari server DHCP. Jika Anda perlu mengatur konfigurasi DNS kustom, Anda harus hubungi tim dukungan.
- Bekerja sebagai caching DNS.

Konfigurasi jaringan gateway VPN

Gateway VPN memiliki beberapa antarmuka jaringan:

- Antarmuka eksternal, terhubung ke internet
- Antarmuka produksi, terhubung ke jaringan produksi
- Antarmuka uji, terhubung ke jaringan uji

Selain itu, dua antarmuka virtual ditambahkan untuk koneksi Titik-ke-situs dan Situs-ke-situs.

Ketika gateway VPN disebarkan dan diinisialisasi, beberapa penghubung dibuat – satu untuk antarmuka eksternal, dan satu untuk antarmuka klien dan produksi. Meskipun penghubung klien-produksi dan antarmuka uji menggunakan alamat IP yang sama, gateway VPN dapat merutekan paket dengan tepat menggunakan teknik tertentu.

Alat VPN

Alat VPN adalah mesin virtual di situs lokal dengan Linux yang memiliki instalasi perangkat lunak khusus, dan konfigurasi jaringan khusus. Alat tersebut memungkinkan komunikasi antara situs lokal

© Acronis International GmbH, 2003-2024

dan situs awan.

Server pemulihan

Server pemulihan – replika dari mesin asli berdasarkan cadangan server terlindungi yang disimpan di awan. Server pemulihan digunakan untuk mengalihkan beban kerja dari server asli jika terjadi bencana.

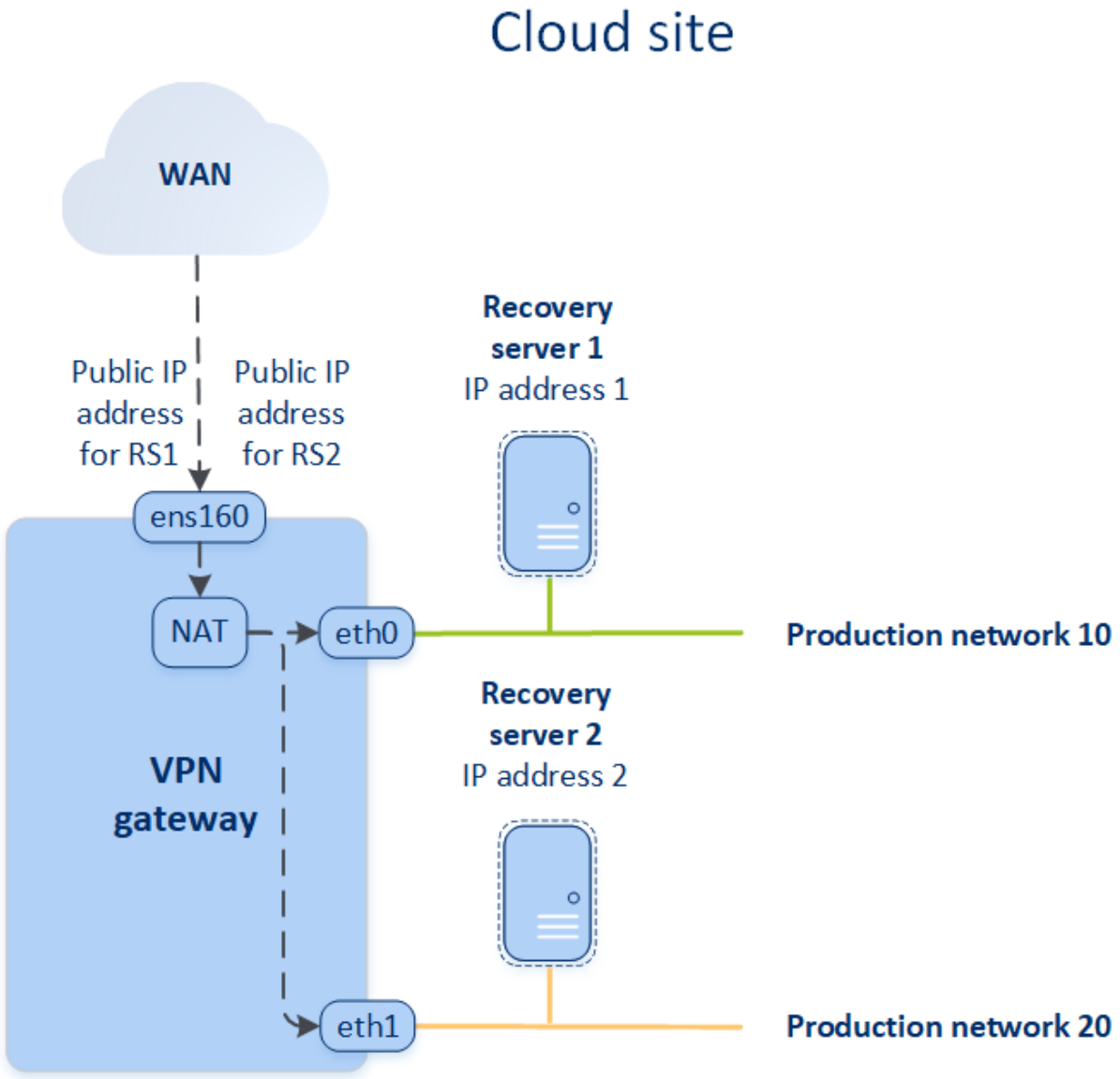
Ketika membuat server pemulihan, Anda harus menentukan parameter jaringan berikut:

- **Jaringan awan** (wajib): jaringan awan yang akan terhubung dengan server pemulihan.
- **Alamat IP di jaringan produksi** (wajib): alamat IP dengan mesin virtual untuk server pemulihan akan diluncurkan. Alamat ini digunakan di jaringan produksi dan uji. Sebelum peluncuran, mesin virtual dikonfigurasi untuk mendapatkan alamat IP melalui DHCP.
- **Alamat IP uji** (opsional): alamat IP untuk mengakses server pemulihan dari jaringan produksi klien selama failover pengujian, untuk mencegah alamat IP produksi diduplikasi di jaringan yang sama. Alamat IP ini berbeda dari alamat IP di jaringan produksi. Server di situs lokal dapat menjangkau server pemulihan selama failover uji melalui alamat IP uji, sedangkan akses pada arah yang berlawanan tidak tersedia. Akses internet dari server pemulihan dalam jaringan uji tersedia jika opsi **akses internet** dipilih selama pembuatan server pemulihan.
- **Alamat IP publik** (opsional): alamat IP untuk mengakses server pemulihan dari Internet. Jika server tidak memiliki alamat IP publik, server hanya dapat dijangkau dari jaringan lokal.
- **Akses internet** (opsional): memungkinkan server pemulihan untuk mengakses internet (pada kasus failover produksi dan uji).

Alamat IP publik dan uji

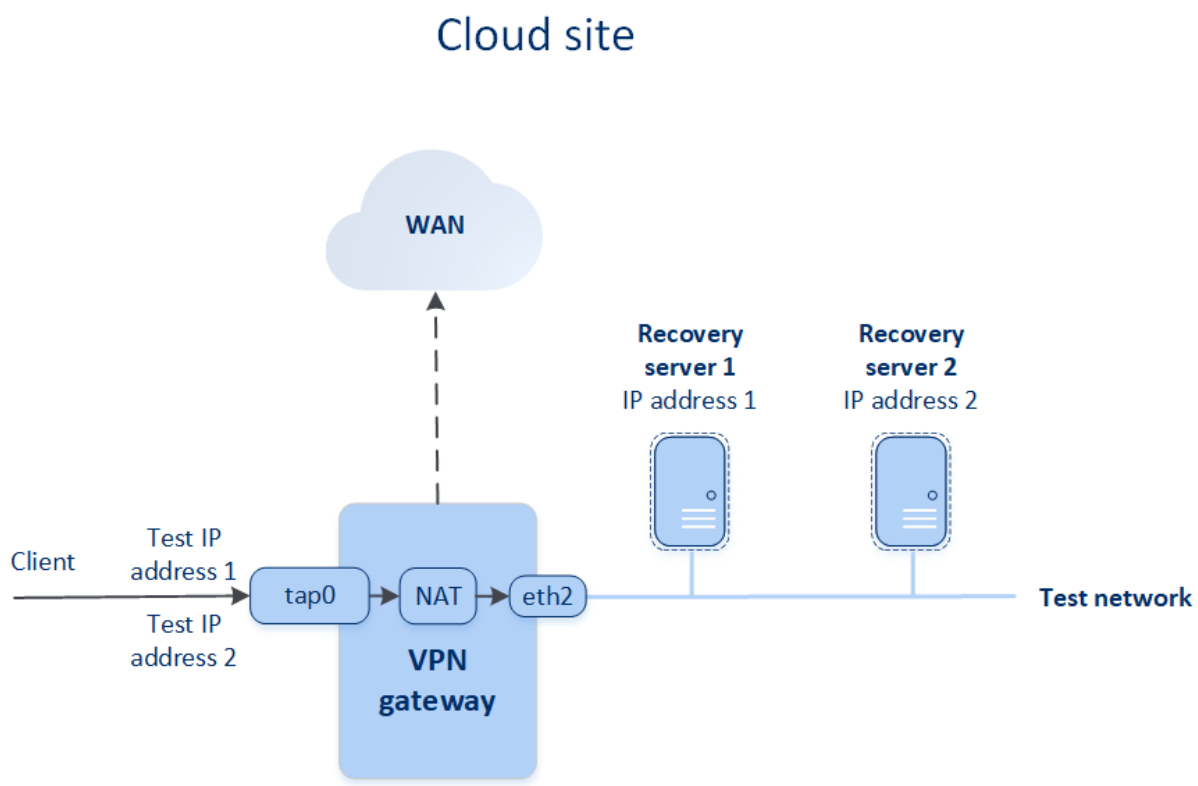
Jika Anda menetapkan alamat IP publik saat membuat server pemulihan, server pemulihan menjadi tersedia dari Internet melalui alamat IP ini. Ketika paket datang dari internet dengan tujuan alamat IP publik, gateway VPN memetakan ulang paket tersebut ke alamat IP produksi terkait menggunakan NAT, lalu mengirimkannya ke server pemulihan yang sesuai.

© Acronis International GmbH, 2003-2024



Jika Anda menetapkan alamat IP uji saat membuat server pemulihan, server pemulihan menjadi tersedia di jaringan uji melalui alamat IP ini. Saat menjalankan failover uji, mesin asli masih berjalan ketika server pemulihan dengan alamat IP yang sama diluncurkan di jaringan uji di awan. Tidak ada konflik alamat IP karena jaringan uji terisolasi. Server pemulihan di jaringan uji dapat dijangkau oleh alamat IP uji mereka, yang dipetakan ulang ke alamat IP produksi melalui NAT.

© Acronis International GmbH, 2003-2024



Untuk informasi lebih lanjut tentang VPN Terbuka Situs-ke-situs, lihat "VPN Terbuka Situs-ke-situs - Informasi tambahan" (hlm. 186).

Server utama

Server utama – mesin virtual yang tidak memiliki mesin yang tertaut di situs lokal jika dibandingkan dengan server pemulihan. Server utama digunakan untuk melindungi aplikasi dengan replikasi, atau menjalankan berbagai layanan tambahan (seperti server web).

Biasanya, server utama digunakan untuk replikasi data real-time di seluruh server yang menjalankan aplikasi penting. Anda mengatur replikasi sendiri menggunakan alat asli aplikasi. Misalnya, replikasi Active Directory atau replikasi SQL dapat dikonfigurasi di antara server lokal dan server utama.

Atau, server utama dapat dimasukkan dalam AlwaysOn Availability Group (AAG) atau Database Availability Group (DAG).

Kedua metode tersebut memerlukan pengetahuan mendalam tentang aplikasi dan hak administrator. Server utama selalu memakai sumber daya komputasi dan ruang pada penyimpanan pemulihan bencana yang cepat. Pemeliharaan diperlukan di pihak Anda: memantau replikasi, menginstal pembaruan perangkat lunak, serta mencadangkan. Keunggulannya adalah RPO dan RTO minimal dengan muatan minimal di lingkungan produksi (dibandingkan dengan mencadangkan seluruh server ke awan).

Server utama selalu diluncurkan hanya di jaringan produksi dan memiliki parameter jaringan berikut:

© Acronis International GmbH, 2003-2024

- **Jaringan awan** (wajib): jaringan awan yang akan terhubung dengan server utama.
- **Alamat IP di jaringan produksi** (wajib): alamat IP yang akan dimiliki server utama dalam jaringan produksi. Secara default, alamat IP gratis pertama dari jaringan produksi Anda telah diatur.
- **Alamat IP publik** (opsional): alamat IP untuk mengakses server utama dari Internet. Jika server tidak memiliki alamat IP publik, server hanya dapat dijangkau dari jaringan lokal, bukan melalui internet.
- **Akses internet** (opsional): memungkinkan server utama untuk mengakses internet.

Koneksi VPN IPsec Multi-situs

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Anda dapat menggunakan konektivitas VPN IPsec Multi-situs untuk terhubung ke situs lokal tunggal, atau beberapa situs lokal ke Cyber Disaster Recovery Cloud melalui koneksi VPN IPsec L3 yang aman.

Jenis konektivitas ini berguna untuk skenario Pemulihan Bencana jika Anda mengalami salah satu kasus penggunaan berikut:

- Anda memiliki satu situs lokal yang mengelola beban kerja kritis.
- Anda memiliki beberapa situs lokal yang mengelola beban kerja kritis, contohnya kantor di lokasi berbeda.
- Anda menggunakan situs perangkat lunak pihak ketiga, atau situs penyedia layanan terkelola dan terhubung dengan keduanya melalui terowongan VPN IPsec.

Untuk membuat komunikasi VPN IPsec Multi-situs antara situs lokal dan situs awan, **gateway VPN** digunakan. Saat Anda mulai mengonfigurasi koneksi Multisitus IPsec VPN di konsol Cyber Protect, gateway VPN secara otomatis diterapkan di situs awan. Anda perlu mengonfigurasi segmen jaringan awan dan memastikan bahwa seluruh segmen tersebut tidak tumpang tindih dengan segmen jaringan lokal. Terowongan VPN yang aman dibuat di antara situs lokal dan situs awan. Server lokal dan server awan dapat berkomunikasi melalui terowongan VPN ini, seolah-olah keduanya berada di segmen Ethernet yang sama.

Untuk setiap mesin sumber yang akan dilindungi, Anda harus membuat server pemulihan di situs awan. Server pemulihan tetap dalam keadaan **Standby** hingga failover terjadi. Jika terjadi bencana dan Anda memulai proses failover (dalam **mode produksi**), server pemulihan yang merepresentasikan salinan sebenarnya dari mesin Anda yang terlindungi akan diluncurkan di awan. Klien Anda dapat terus menggunakan server tanpa menyadari terjadinya perubahan latar belakang.

Anda juga dapat meluncurkan proses failover di **mode uji**. Artinya, mesin sumber masih berfungsi dan pada saat bersamaan server pemulihan terkait diluncurkan di awan pada jaringan virtual khusus yang dibuat di awan – **jaringan uji**. Jaringan uji diisolasi untuk mencegah duplikasi alamat IP di segmen jaringan awan lainnya.

© Acronis International GmbH, 2003-2024

Gateway VPN

Komponen utama yang memfasilitasi komunikasi antara situs lokal dan situs awan adalah **gateway VPN**. Ini adalah mesin virtual di awan yang memiliki perangkat lunak khusus terinstal di sana, dan jaringanya dikonfigurasi secara spesifik. Gateway VPN menyediakan fungsi berikut:

- Menghubungkan segmen Ethernet dari jaringan lokal dan jaringan produksi Anda di awan dalam mode IPsec L3.
- Bekerja sebagai perute dan NAT default untuk mesin di jaringan uji dan produksi.
- Bekerja sebagai server DHCP. Semua mesin dalam jaringan produksi dan uji mendapat konfigurasi jaringan (alamat IP, pengaturan DNS) melalui DHCP. Setiap saat, server awan akan mendapatkan alamat IP yang sama dari server DHCP.
  Jika ingin, Anda dapat menetapkan konfigurasi DNS kustom. Untuk informasi lebih lanjut, lihat "Melakukan konfigurasi pada server DNS kustom" (hlm. 767).
- Bekerja sebagai caching DNS.

Cara kerja perutean

Perutean antarjaringan awan dilaksanakan dengan perute di situs awan sehingga server dari jaringan awan berbeda dapat saling berkomunikasi.

Akses VPN jarak jauh titik-ke-situs

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

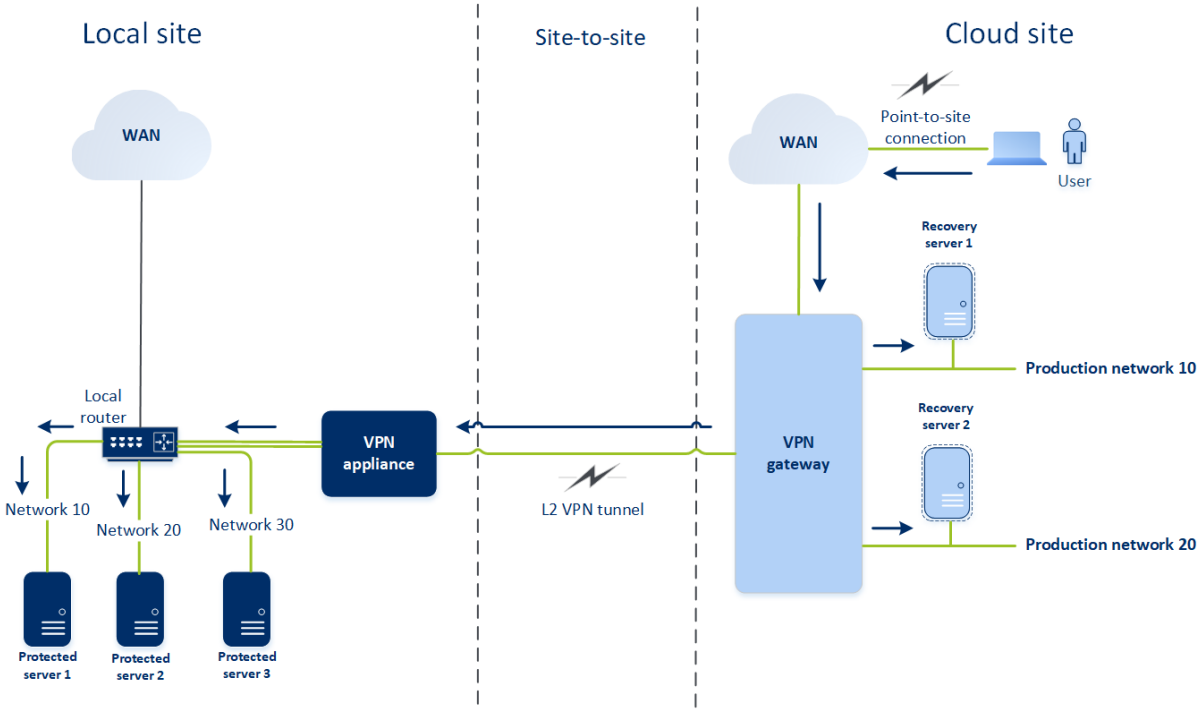
Koneksi Titik-ke-situs adalah koneksi yang aman dari luar menggunakan perangkat titik akhir Anda (seperti komputer atau laptop) ke situs awan dan lokal melalui VPN. Ini tersedia setelah Anda membuat koneksi VPN Terbuka Situs-ke-situs ke situs Cyber Disaster Recovery Cloud. Jenis koneksi ini bermanfaat untuk kasus berikut:

- Di berbagai perusahaan, layanan korporat dan sumber daya web tersedia hanya dari jaringan korporat. Anda dapat menggunakan koneksi Titik-ke-situs agar dapat terhubung dengan aman ke situs lokal.
- Jika terjadi bencana, saat beban kerja dialihkan ke situs awan dan jaringan lokal sedang down, Anda membutuhkan akses ke server awan. Hal ini dapat dilakukan melalui koneksi Titik-ke-situs ke situs awan.

Untuk koneksi Titik-ke-situs ke situs lokal, Anda harus menginstal alat VPN pada situs lokal, mengonfigurasi koneksi Situs-ke-situs, lalu koneksi Titik-ke-situs ke situs lokal. Dengan demikian, karyawan jarak jauh Anda akan memiliki akses ke jaringan perusahaan melalui L2 VPN.

Skema berikut menunjukkan situs lokal, situs awan, dan komunikasi antar-server yang disorot dengan warna hijau. Terowongan L2 VPN menghubungkan situs lokal dan awan Anda. Saat pengguna membuat koneksi Titik-ke-situs, komunikasi ke situs lokal dilakukan melalui situs awan.

© Acronis International GmbH, 2003-2024



Konfigurasi Titik-ke-situs menggunakan sertifikat untuk autentikasi ke klien VPN. Kredensial pengguna tambahan digunakan untuk autentikasi. Perhatikan hal berikut tentang koneksi Titik-ke-situs ke situs lokal:

- Pengguna harus menggunakan kredensial Cyber Protect Cloud untuk autentikasi di klien VPN. Mereka harus memiliki peran pengguna "Administrator Perusahaan" atau "Perlindungan Cyber".
- Jika Anda membuat kembali konfigurasi VPN Terbuka, Anda harus memberikan konfigurasi yang telah diperbarui kepada semua pengguna dengan menggunakan koneksi Titik-ke-situs ke situs awan.

Penghapusan otomatis untuk lingkungan pelanggan yang tidak digunakan di situs awan

Layanan Pemulihan Bencana melacak penggunaan lingkungan pelanggan yang dibuat untuk pemulihan bencana dan secara otomatis menghapusnya jika tidak digunakan.

Kriteria berikut digunakan untuk menentukan aktif atau tidaknya pelanggan sewa:

- Saat ini, terdapat setidaknya satu server awan atau terdapat beberapa server awan dalam tujuh hari terakhir.

  ATAU

- Opsi **akses VPN ke situs lokal** diaktifkan dan terowongan VPN Terbuka Situs-ke-Situs telah disiapkan atau terdapat data yang dilaporkan dari perangkat VPN selama 7 hari terakhir.

Semua penyewa lainnya dianggap sebagai penyewa tidak aktif. Terkait penyewa tersebut, sistem akan menerapkan hal berikut:

© Acronis International GmbH, 2003-2024

- Menghapus gateway VPN dan semua sumber daya awan yang terkait dengan penyewa.
- Membatalkan pendaftaran perangkat VPN.

Penyewa yang tidak aktif akan dikembalikan ke keadaan sebelum konfigurasi konektivitas.

Konfigurasi konektivitas awal

Bagian ini menjelaskan skenario konfigurasi konektivitas.

Melakukan konfigurasi pada mode hanya-Awan

Untuk melakukan konfigurasi pada koneksi dalam mode hanya-awan

1. Di konsol Cyber Protect, buka **Pemulihan Bencana** > **Konektivitas**.
2. Pilih **Hanya-awan** dan klik **Konfigurasi**.
   Hasilnya, gateway VPN dan jaringan awan dengan alamat dan mask yang ditentukan akan diterapkan pada situs awan.

Untuk mempelajari cara mengelola jaringan Anda di awan dan menentukan pengaturan gateway VPN, lihat "Mengelola jaringan awan".

Mengonfigurasi VPN Terbuka Situs-ke-situs

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Persyaratan untuk alat VPN

Persyaratan sistem

- 1 CPU
- RAM 1 GB
- Ruang disk 8 GB

Port

- TCP 443 (outbound) – untuk koneksi VPN
- TCP 80 (outbound) – untuk pembaruan alat otomatis

Pastikan firewall dan komponen lain dari sistem keamanan jaringan Anda memungkinkan koneksi melalui port ini ke alamat IP mana pun.

Mengonfigurasi koneksi VPN Terbuka Situs-ke-situs

Alat VPN memperluas jaringan lokal Anda hingga ke awan melalui terowongan VPN yang aman. Koneksi semacam ini sering disebut sebagai koneksi "Situs-ke-situs" (S2S). Anda dapat mengikuti prosedur di bawah ini atau menonton tutorial video.

© Acronis International GmbH, 2003-2024

Untuk mengonfigurasi koneksi melalui alat VPN

1. Di konsol Cyber Protect, buka **Pemulihan Bencana** > **Konektivitas**.
2. Pilih **Koneksi VPN Terbuka Situs-ke-situs**, kemudian klik **Konfigurasi**.
   Sistem mulai menyebarkan gateway VPN di awan. Ini akan memerlukan beberapa saat. Sementara itu, Anda dapat melanjutkan ke langkah berikutnya.

   Catatan
   Gateway VPN disediakan tanpa tambahan biaya. Server akan dihapus jika fungsi Pemulihan Bencana tidak digunakan, misalnya server utama atau pemulihan tidak ada di awan selama tujuh hari.

3. Pada blok **Alat VPN**, klik **Unduh dan sebarkan**. Unduh alat VPN untuk VMware vSphere atau Microsoft Hyper-V sesuai platform virtualisasi yang Anda gunakan.
4. Sebarkan alat dan hubungkan ke jaringan produksi.
   Pada vSphere, pastikan bahwa **Mode campuran** dan **Pemancaran palsu** diaktifkan dan atur ke **Terima** untuk semua switch virtual yang menghubungkan alat VPN ke jaringan produksi. Untuk mengakses pengaturan ini, dalam vSphere Client, pilih host > **Ringkasan** > **Jaringan**, lalu pilih switch > **Edit pengaturan...** > **Keamanan**.
   Pada Hyper-V, buat mesin virtual **Generasi 1** dengan memori sebesar 1024 MB. Selain itu, kami menyarankan Anda mengaktifkan **Memori Dinamis** pada mesin. Setelah mesin dibuat, buka **Pengaturan** > **Perangkat keras** > **Adaptor Jaringan** > **Fitur Lanjutan** dan pilih kotak centang **Aktifkan spoofing alamat MAC**.
5. Hidupkan alat.
6. Buka konsol alat dan masuk dengan nama pengguna dan kata sandi "admin"/"admin".
7. [Opsional] Ubah kata sandi.
8. [Opsional] Ubah pengaturan jaringan bila perlu. Tentukan antarmuka mana yang akan digunakan sebagai WAN untuk koneksi Internet.
9. Daftarkan peralatan dalam layanan Cyber Protection menggunakan kredensial administrator perusahaan.
   Kredensial ini hanya digunakan sekali untuk memperoleh sertifikasi. URL pusat data telah ditentukan sebelumnya.

   Catatan
   Jika autentikasi dua faktor dikonfigurasi untuk akun Anda, Anda juga akan diminta untuk memasukkan kode TOTP. Jika autentikasi dua faktor diaktifkan namun tidak dikonfigurasikan untuk akun Anda, Anda tidak dapat mendaftarkan alat VPN. Pertama, Anda harus membuka halaman login konsol Cyber Protect dan menyelesaikan konfigurasi autentikasi dua faktor untuk akun Anda. Untuk rincian selengkapnya tentang autentikasi dua faktor, buka Panduan Administrator Portal Manajemen.

Saat konfigurasi selesai, alat akan memiliki status **Online**. Alat terhubung ke gateway VPN dan mulai melaporkan informasi tentang jaringan dari semua antarmuka aktif ke layanan Cyber Disaster

© Acronis International GmbH, 2003-2024

Recovery Cloud. Konsol Cyber Protect menunjukkan antarmuka, berdasarkan informasi dari alat VPN.

Mengonfigurasi VPN IPsec Multi-situs

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Anda dapat mengonfigurasi koneksi VPN IPsec Multi-situs dengan dua cara berikut:

- dari **Pemulihan Bencana** > tab **Konektivitas**.
- dengan menerapkan rencana proteksi pada satu atau beberapa perangkat, lalu secara manual beralih dari koneksi VPN Terbuka Situs-ke-situs yang dibuat secara otomatis ke koneksi VPN IPsec Multi-situs, mengonfigurasi pengaturan VPN IPsec Multi-situs, dan menetapkan ulang alamat IP.

Untuk mengonfigurasi koneksi VPN IPsec Multi-situs dari tab Konektivitas

1. Di konsol Cyber Protect, buka **Pemulihan Bencana** > **Konektivitas**.
2. Di bagian **Koneksi VPN multi-situs**, klik **Konfigurasi**.
   Gateway VPN diterapkan di situs awan.
3. Konfigurasi pengaturan VPN IPsec Multi-situs.

Untuk mengonfigurasi koneksi VPN IPsec Multi-situs dari rencana proteksi

1. Di konsol Cyber Protect, buka **Perangkat**.
2. Terapkan rencana proteksi ke satu atau beberapa perangkat dari daftar.
   Pengaturan server pemulihan dan infrastruktur awan secara otomatis dikonfigurasi untuk konektivitas VPN Terbuka Situs-ke-situs.
3. Buka **Pemulihan Bencana** > **Konektivitas**.
4. Klik **Tampilkan properti**.
5. Klik **Beralih ke VPN IPsec Multi-situs**.
6. Konfigurasi pengaturan VPN IPsec Multi-situs.
7. Tetapkan ulang alamat IP jaringan awan dan server awan.

Mengonfigurasi pengaturan VPN IPsec Multi-situs

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Setelah mengonfigurasi VPN IPsec Multi-situs, Anda harus mengonfigurasi pengaturan situs awan dan situs lokal di tab **Pemulihan Bencana** > **Konektivitas**.

© Acronis International GmbH, 2003-2024

Prasyarat

- Konektivitas VPN IPsec Multi-situs dikonfigurasi. Untuk mengetahui informasi lebih lanjut tentang mengonfigurasi konektivitas VPN IPsec Multi-situs, lihat "Mengonfigurasi VPN IPsec Multi-situs" (hlm. 753).
- Setiap gateway VPN IPsec lokal memiliki alamat IP publik.
- Jaringan awan Anda memiliki alamat IP yang memadai untuk server awan yang berupa salinan mesin terlindungi Anda (di jaringan produksi), dan untuk server pemulihan (dengan satu atau dua alamat IP, tergantung kebutuhan).
- [Jika Anda menggunakan firewall di antara situs lokal dan situs awan] Protokol IP dan port UDP berikut diizinkan di situs lokal: IP Protocol ID 50 (ESP), UDP Port 500 (IKE), dan UDP Port 4500.
- Konfigurasi NAT-T di situs lokal dinonaktifkan.

Untuk mengonfigurasi koneksi VPN IPsec Multi-situs

1. Tambahkan satu atau beberapa jaringan ke situs awan.
   a. Klik **Tambahkan Jaringan**.

   Catatan
   Saat Anda menambahkan jaringan awan, jaringan uji terkait akan ditambahkan secara otomatis dengan alamat dan mask jaringan yang sama agar dapat menjalankan uji failover. Server awan di jaringan uji akan memiliki alamat IP yang sama seperti di jaringan produksi awan. Jika Anda perlu mengakses server awan dari jaringan produksi selama uji failover, tetapkan alamat IP uji kedua untuk server pemulihan pada saat server tersebut dibuat.

   b. Ketik alamat IP jaringan pada kolom **Alamat jaringan**.
   c. Ketik mask jaringan pada kolom **Mask jaringan**.
   d. Klik **Tambah**.
2. Konfigurasikan pengaturan untuk setiap situs lokal yang ingin Anda sambungkan ke situs awan, menurut rekomendasi untuk situs lokal. Untuk informasi lebih lanjut tentang rekomendasi ini, lihat "Rekomendasi umum untuk situs lokal" (hlm. 755).
   a. Klik **Tambahkan Koneksi**.
   b. Masukkan nama untuk gateway VPN lokal.
   c. Masukkan alamat IP publik dari gateway VPN lokal.
   d. [Opsional] Masukkan deskripsi gateway VPN lokal.
   e. Klik **Berikutnya**.
   f. Pada kolom **Kunci yang dibagikan sebelumnya**, ketik kunci yang dibagikan sebelumnya, atau klik **Buat kunci baru yang dibagikan sebelumnya** untuk menggunakan nilai yang dibuat secara otomatis.

© Acronis International GmbH, 2003-2024

Catatan
Anda harus menggunakan kunci yang dibagikan sebelumnya dan sama untuk gateway VPN lokal dan awan.

g. Klik **Pengaturan keamanan IPsec/IKE** untuk mengkonfigurasi pengaturan. Untuk mengetahui informasi lebih lanjut tentang pengaturan yang dapat Anda konfigurasi, lihat "Pengaturan keamanan IPsec/IKE" (hlm. 756).

Catatan
Anda dapat menggunakan pengaturan default, yang diisi secara otomatis, atau menggunakan nilai kustom. Hanya koneksi protokol IKEv2 yang didukung. **Langkah Pengaktifan** default saat membangun VPN adalah **Tambahkan** (gateway VPN lokal Anda memulai koneksi), tetapi Anda dapat mengubahnya menjadi **Mulai** (gateway VPN awan memulai koneksi) atau **Rute** (cocok untuk firewall yang mendukung opsi rute).

h. Konfigurasikan **Kebijakan jaringan**.
Kebijakan jaringan menentukan jaringan yang disambungkan dengan VPN IPsec. Ketik alamat IP dan mask jaringan dengan menggunakan format CIDR. Segmen jaringan lokal dan awan tidak boleh tumpang tindih.

i. Klik **Simpan**.

Rekomendasi umum untuk situs lokal

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Saat Anda mengonfigurasi situs lokal untuk konektivitas VPN IPsec Multi-situs, pertimbangkan rekomendasi berikut:

- Untuk setiap Fase IKE, tetapkan setidaknya salah satu nilai yang dikonfigurasi di situs awan untuk parameter berikut: Algoritme enkripsi, Algoritme hash, dan nomor grup Diffie-Hellman.
- Aktifkan kerahasiaan maju sempurna dengan setidaknya salah satu nilai nomor grup Diffie-Hellman yang dikonfigurasi di situs awan untuk IKE Fase 2.
- Konfigurasi nilai **Selama Masa Aktif** yang sama untuk IKE Fase 1 dan IKE Fase 2 seperti di situs awan.
- Konfigurasi dengan NAT traversal (NAT-T) tidak didukung. Nonaktifkan konfigurasi NAT-T di situs lokal. Jika tidak, maka enkapsulasi UDP tambahan tidak dapat dinegosiasikan.
- Konfigurasi **Tindakan pengaktifan** mendefinisikan sisi mana yang memulai koneksi. Nilai default **Tambahkan** berarti situs lokal memulai koneksi, dan situs awan menunggu inisiasi koneksi. Ubah nilainya ke **Mulai** jika Anda ingin situs awan memulai koneksi, atau ke **Rute** jika Anda ingin kedua sisi mampu memulai koneksi (cocok untuk firewall yang mendukung opsi perutean).

Untuk mengetahui informasi lebih lanjut dan contoh konfigurasi untuk solusi berbeda, lihat:

© Acronis International GmbH, 2003-2024

- Seri artikel berbasis pengetahuan ini
- Contoh video ini

Pengaturan keamanan IPsec/IKE

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Tabel berikut memberikan informasi lebih lanjut tentang parameter keamanan Psec/IKE.

Parameter	Deskripsi
Algoritme enkripsi	Algoritme enkripsi yang akan digunakan untuk memastikan bahwa data tidak dapat dilihat saat transit. Secara default, semua algoritme dipilih. Setidaknya satu dari algoritme yang dipilih harus dikonfigurasi pada perangkat gateway lokal Anda untuk setiap fase IKE.
Algoritme hash	Algoritme hash yang akan digunakan untuk memverifikasi integritas dan keaslian data. Secara default, semua algoritme dipilih. Setidaknya satu dari algoritme yang dipilih harus dikonfigurasi pada perangkat gateway lokal Anda untuk setiap fase IKE.
Nomor grup Diffie-Hellman	Nomor grup Diffie-Hellman menentukan kekuatan kunci yang digunakan dalam proses Internet Key Exchange (IKE). Nomor grup yang lebih tinggi lebih aman tetapi memerlukan waktu tambahan untuk memperhitungkan kode. Secara default, semua grup dipilih. Setidaknya satu dari grup yang dipilih harus dikonfigurasi pada perangkat gateway lokal Anda untuk setiap fase IKE.
Masa aktif (detik)	Nilai masa berlaku menentukan durasi instans koneksi dengan set kunci enkripsi/autentikasi untuk paket pengguna, dari negosiasi yang berhasil hingga kedaluwarsa. Rentang untuk Fase 1: 900-28800 detik dengan default 28800. Rentang untuk Fase 2:900-3600 detik dengan default 3600.

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
	Masa aktif untuk Fase 2 harus kurang dari masa aktif untuk Fase 1. Koneksinya dinegosiasikan ulang melalui saluran penguncian sebelum kedaluwarsa, lihat **Masa margin penguncian ulang**. Jika sisi lokal dan jarak jauh tidak menyetujui masa berlaku tersebut, kekacauan pada koneksi yang digantikan akan terjadi pada sisi dengan masa berlaku lebih lama. Lihat juga **Masa margin penguncian ulang** dan **Fuzz penguncian ulang**.
Masa margin penguncian ulang (detik)	Masa margin sebelum berakhirnya koneksi atau berakhirnya saluran penguncian, ketika sisi lokal dari koneksi VPN mencoba menegosiasikan penggantian. Waktu yang tepat untuk penguncian ulang dipilih secara acak berdasarkan nilai **Fuzz penguncian ulang**. Relevan hanya secara lokal, pihak jarak jauh tidak perlu menyetujuinya. Rentang: 900-3600 detik. Nilai default adalah 3600.
Ukuran jendela pemutaran ulang (paket)	Ukuran jendela pemutaran ulang IPsec untuk koneksi ini. Default -1 menggunakan nilai yang dikonfigurasi dengan charon.replay_window di file strongswan.conf. Nilai lebih besar daripada 32 didukung hanya saat menggunakan backend Netlink. Nilai 0 menonaktifkan proteksi pemutaran ulang IPsec.
Fuzz penguncian ulang (%)	Persentase maksimum untuk peningkatan marginbyte, marginpacket, dan margintime secara acak untuk mengacak interval penguncian ulang (penting untuk host dengan banyak koneksi). Nilai Fuzz penguncian ulang dapat melampaui 100%. Nilai marginTYPE, setelah peningkatan acak, tidak boleh melampaui lifeTYPE, dengan TYPE yang tampil dengan satuan byte, packet, atau time. Nilai 0% menonaktifkan pengacakan. Relevan hanya secara lokal, pihak jarak jauh tidak perlu menyetujuinya.
Batas waktu DPD (detik)	Waktu setelah batas waktu dead peer detection (DPD) terjadi. Anda dapat menetapkan nilai 30 atau

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
	lebih. Nilai default adalah 30.
Tindakan batas waktu dead peer detection (DPD)	Tindakan yang diambil setelah batas waktu dead peer detection (DPD) terjadi. **Mulai ulang** - Memulai ulang sesi saat batas waktu DPD terjadi. **Hapus** - Mengakhiri sesi saat batas waktu DPD terjadi. **Kosong** - Jangan mengambil tindakan saat batas waktu DPD terjadi.
Tindakan pengaktifan	Menentukan sisi mana yang memulai koneksi dan mendirikan terowongan untuk koneksi VPN. **Tambahkan** - gateway VPN lokal Anda memulai koneksi. **Mulai** - gateway VPN awan memulai koneksi. **Rute** - cocok untuk gateway VPN yang mendukung opsi perutean. Terowongan hanya aktif jika ada lalu lintas yang dimulai dari gateway VPN lokal, atau gateway VPN awan.

Rekomendasi untuk ketersediaan Layanan Domain Active Directory

Jika beban kerja terlindungi Anda memerlukan autentikasi di pengontrol domain, Anda sebaiknya memiliki instans Pengontrol Domain Active Directory (AD DC) di situs Pemulihan Bencana.

Pengontrol Domain Active Directory untuk konektivitas VPN L2 Terbuka

Dengan konektivitas VPN L2 Terbuka, alamat IP para beban kerja terlindungi dipertahankan di situs awan selama failover uji atau failover produksi. Maka, AD DC selama failover uji atau failover produksi memiliki alamat IP yang sama dengan situs lokal.

Dengan DNS kustom, Anda dapat menetapkan server DNS kustom pribadi untuk semua server awan. Untuk informasi lebih lanjut, lihat "Melakukan konfigurasi pada server DNS kustom" (hlm. 767).

Pengontrol Domain Active Directory untuk konektivitas VPN L3 IPsec

Dengan konektivitas VPN L3 IPsec, alamat IP para beban kerja yang terlindungi tidak dipertahankan di situs awan. Maka, Anda sebaiknya memiliki instans AD DC khusus tambahan sebagai server utama di situs awan sebelum Anda melakukan failover produksi.

Rekomendasi untuk instans AD DC khusus yang dikonfigurasi sebagai server utama di situs awan adalah sebagai berikut:

© Acronis International GmbH, 2003-2024

- Matikan firewall Windows.
- Gabungkan server utama ke layanan Active Directory.
- Pastikan server utama memiliki akses Internet.
- Tambahkan fitur Active Directory.

Dengan DNS kustom, Anda dapat menetapkan server DNS kustom pribadi untuk semua server awan. Untuk informasi lebih lanjut, lihat "Melakukan konfigurasi pada server DNS kustom" (hlm. 767).

Mengonfigurasi akses VPN jarak jauh Titik-ke-situs

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Jika Anda perlu terhubung ke situs lokal Anda dari jarak jauh, Anda dapat mengkonfigurasi koneksi Titik-ke-situs ke situs lokal. Anda dapat mengikuti prosedur di bawah ini atau menonton tutorial video.

Prasyarat

- Konektivitas VPN Terbuka Situs-ke-situs dikonfigurasi.
- Alat VPN diinstal di situs lokal.

Mengonfigurasi koneksi Titik-ke-situs ke situs lokal

1. Di konsol Cyber Protect, buka **Pemulihan Bencana** > **Konektivitas**.
2. Klik **Tampilkan properti**.
3. Aktifkan opsi **akses VPN ke situs lokal**.
4. Pastikan bahwa pengguna Anda yang perlu membuat koneksi Titik-ke-situs ke situs lokal memiliki:
   - akun pengguna dalam Cyber Protect Cloud. Kredensial ini digunakan untuk autentikasi di klien VPN. Jika tidak, buat akun pengguna di Cyber Protect Cloud.
   - peran pengguna "Administrator Perusahaan" atau "Perlindungan Cyber".
5. Konfigurasi klien OpenVPN:
   a. Unduh versi klien VPN Terbuka 2.4.0 atau lebih baru dari lokasi berikut https://openvpn.net/community-downloads/.
   b. Instal klien OpenVPN di mesin tempat Anda ingin terhubung ke situs lokal.
   c. Klik **Unduh konfigurasi untuk OpenVPN**. File konfigurasi valid untuk pengguna di organisasi Anda dengan peran pengguna "Administrator Perusahaan" atau "Perlindungan Cyber".
   d. Impor konfigurasi unduhan ke OpenVPN.

© Acronis International GmbH, 2003-2024

e. Masuk ke klien VPN Terbuka dengan Cyber Protect Cloud kredensial pengguna Anda (lihat langkah 4 di atas).

f. [Opsional] Jika autentikasi dua faktor diaktifkan untuk organisasi Anda, Anda harus menyediakan kode TOTP yang dihasilkan satu kali.

Penting
Jika Anda telah mengaktifkan autentikasi dua faktor untuk akun Anda, Anda harus meregenerasi file konfigurasi dan memperbaruinya untuk klien OpenVPN yang ada. Pengguna harus masuk lagi ke Cyber Protect Cloud untuk mengatur autentikasi dua faktor untuk akun mereka.

Hasilnya, pengguna Anda akan dapat terhubung ke mesin di situs lokal.

Manajemen jaringan

Bagian ini menjelaskan skenario manajemen layanan.

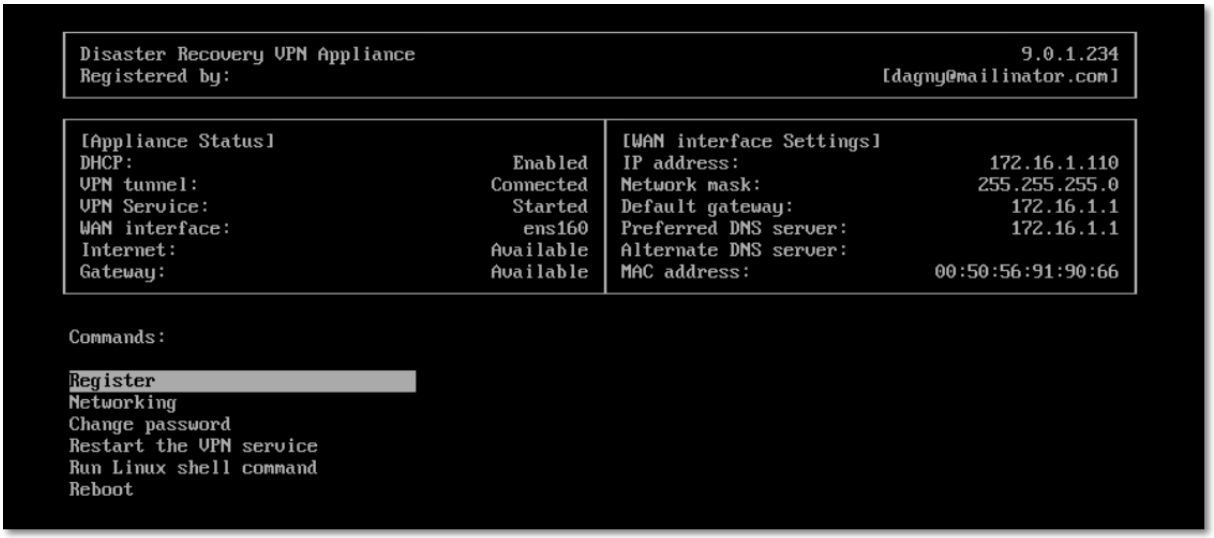
Mengelola jaringan

Catatan
Beberapa fitur mungkin memerlukan pelisensian tambahan sesuai model pelisensian yang diterapkan.

Koneksi VPN Terbuka Situs-ke-situs

Untuk menambahkan jaringan di situs lokal dan memperluasnya ke awan

1. Pada alat VPN, atur antarmuka jaringan baru dengan jaringan lokal yang ingin Anda perluas di awan.
2. Masuk ke konsol alat VPN.
3. Di bagian **Jaringan**, tentukan pengaturan jaringan untuk antarmuka baru.



© Acronis International GmbH, 2003-2024

Alat VPN mulai melaporkan informasi tentang jaringan dari semua antarmuka aktif ke Cyber Disaster Recovery Cloud. Konsol Cyber Protect menunjukkan antarmuka berdasarkan informasi dari alat VPN.

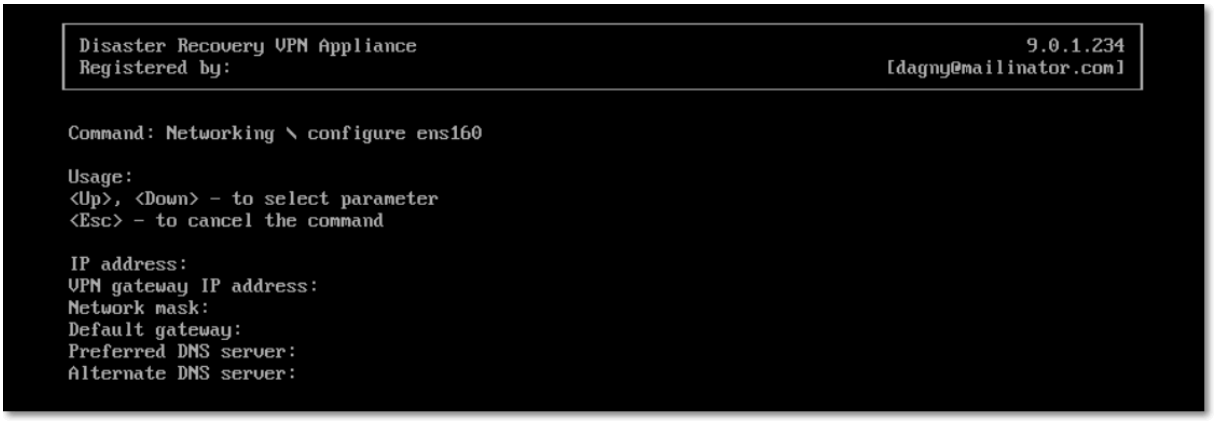
Untuk menghapus jaringan yang diperluas ke awan

1. Masuk ke konsol alat VPN.
2. Di bagian **Jaringan**, pilih antarmuka yang ingin Anda hapus, lalu klik **Hapus pengaturan jaringan**.
3. Konfirmasi operasi.

Hasilnya, perluasan jaringan lokal ke awan melalui terowongan VPN yang aman akan dihentikan. Jaringan ini akan beroperasi sebagai segmen awan yang independen. Jika antarmuka ini digunakan untuk melewati lalu lintas dari (ke) situs awan, semua koneksi jaringan Anda dari (ke) situs awan akan diputus.

Untuk mengubah parameter jaringan

1. Masuk ke konsol alat VPN.
2. Di bagian **Jaringan**, pilih antarmuka yang ingin Anda edit.
3. Klik **Edit pengaturan jaringan**.
4. Pilih salah satu dari dua kemungkinan opsi:
   - Untuk konfigurasi jaringan otomatis melalui DHCP, klik **Gunakan DHCP**. Konfirmasi operasi.
   - Untuk konfigurasi jaringan secara manual, klik **Atur alamat IP statis**. Pengaturan berikut tersedia untuk pengeditan:
     - **Alamat IP**: alamat IP antarmuka di jaringan lokal.
     - **Alamat IP gateway VPN**: alamat IP khusus yang dipertahankan untuk segmen awan jaringan untuk kerja layanan Cyber Disaster Recovery Cloud yang sesuai.
     - **Mask jaringan**: mask jaringan jika jaringan lokal.
     - **Gateway default**: gateway default di situs lokal.
     - **Server DNS disukai**: server DNS sekunder di situs lokal.
     - **Server DNS alternatif**: server DNS sekunder di situs lokal.



© Acronis International GmbH, 2003-2024

- Terapkan perubahan yang diperlukan dan konfirmasi dengan menekan Enter.

Mode hanya-awan

Anda dapat memiliki hingga 23 jaringan di awan.

Untuk menambahkan jaringan awan baru

1. Buka **Pemulihan Bencana** > **Konektivitas**.
2. Di **Situs awan**, klik **Tambahkan jaringan awan**.
3. Tentukan parameter jaringan awan: alamat dan mask jaringan. Ketika sudah siap, klik **Selesai**.

Hasilnya, jaringan awan tambahan dengan alamat dan mask yang ditentukan akan dibuat di situs awan.

Untuk menghapus jaringan awan

Catatan
Anda tidak dapat menghapus jaringan awan jika ada setidaknya satu server awan di dalamnya. Pertama, hapus server awan, lalu hapus jaringan.

1. Buka **Pemulihan Bencana** > **Konektivitas**.
2. Di **Situs awan**, klik alamat jaringan yang ingin Anda hapus.
3. Klik **Hapus** dan konfirmasi operasi.

Mengubah parameter jaringan awan

1. Buka **Pemulihan Bencana** > **Konektivitas**.
2. Di **Situs awan**, klik alamat jaringan yang ingin Anda edit.
3. Klik **Edit.**
4. Tentukan alamat dan mask jaringan, dan klik **Selesai**.

Konfigurasi ulang alamat IP

Untuk performa pemulihan bencana yang tepat, alamat IP yang ditetapkan ke server lokal dan server awan harus sama. Jika terdapat inkonsistensi atau ketidakcocokan alamat IP, Anda akan melihat tanda seru di sebelah jaringan yang terkait dalam **Pemulihan Bencana** > **Konektivitas**.

Tercantum di bawah ini adalah beberapa alasan yang paling lazim atas inkonsistensi alamat IP:

1. Server pemulihan dimigrasikan dari satu jaringan ke jaringan lain atau mask jaringan pada jaringan awan diubah. Hasilnya, server awan memiliki alamat IP dari jaringan yang tidak terhubung dengannya.
2. Jenis konektivitas beralih dari jenis tanpa koneksi Situs-ke-situs menjadi koneksi Situs-ke-situs. Akibatnya, server lokal disiapkan di jaringan yang berbeda dari yang dibuat untuk server pemulihan di situs awan.

© Acronis International GmbH, 2003-2024

3. Jenis konektivitas beralih dari VPN Terbuka Situs-ke-situs menjadi VPN IPsec Multi-situs, atau dari VPN IPsec Multi-situs menjadi VPN Terbuka Situs-ke-situs. Untuk informasi lebih lanjut tentang skenario ini, lihat Beralih koneksi dan Menetapkan ulang alamat IP.
4. Mengedit parameter jaringan berikut pada situs alat VPN:
   - Menambahkan antarmuka via pengaturan jaringan
   - Mengedit mask jaringan secara manual melalui pengaturan antarmuka
   - Mengedit mask jaringan melalui DHCP
   - Mengedit alamat dan mask jaringan secara manual melalui pengaturan antarmuka
   - Mengedit mask dan alamat jaringan melalui DHCP

   Sebagai hasil dari tindakan yang tercantum di atas, jaringan di situs awan dapat mendari subset atau superset dari jaringan lokal, atau antarmuka alat VPN dapat melaporkan pengaturan jaringan yang sama untuk antarmuka yang berbeda.

Untuk menyelesaikan masalah dengan pengaturan jaringan

1. Klik jaringan yang memerlukan konfigurasi ulang alamat IP.
   Anda akan melihat daftar server di jaringan yang dipilih, statusnya, dan alamat IP. Server yang pengaturan jaringannya tidak konsisten dibubuhi tanda seru.
2. Guna mengubah pengaturan jaringan untuk server, klik **Buka server**. Guna mengubah pengaturan jaringan untuk semua server sekaligus, buka **Ubah** dalam blok notifikasi.
3. Ubah alamat IP bila perlu dengan menetapkannya dalam bidang **IP baru** dan **IP uji baru**.
4. Ketika sudah siap, klik **Konfirmasi**.

Pindahkan server ke jaringan yang sesuai

Ketika Anda membuat rencana proteksi pemulihan bencana dan menerapkannya ke perangkat yang dipilih, sistem akan memeriksa alamat IP perangkat dan secara otomatis membuat jaringan awan jika tidak ada jaringan awan yang tepat untuk alamat IP tersebut. Secara default, jaringan awan dikonfigurasi dengan rentang maksimum yang direkomendasikan oleh IANA untuk penggunaan pribadi (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Anda dapat mempersempit jaringan dengan mengedit mask jaringan.

Jika perangkat yang dipilih ada pada beberapa jaringan lokal, jaringan di situs awan dapat menjadi superset jaringan lokal. Dalam hal ini, untuk mengonfigurasi ulang jaringan awan:

1. Klik jaringan awan yang memerlukan konfigurasi ulang ukuran jaringan, lalu klik **Edit**.
2. Konfigurasi ulang ukuran jaringan dengan pengaturan yang benar.
3. Buat jaringan lain yang diperlukan.
4. Klik ikon notifikasi di samping jumlah perangkat yang terhubung ke jaringan.
5. Klik **Pindahkan ke jaringan yang sesuai**.
6. Pilih server yang ingin Anda pindahkan ke jaringan yang sesuai, lalu klik **Pindahkan**.

© Acronis International GmbH, 2003-2024

Mengelola pengaturan alat VPN

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Di konsol Cyber Protect (**Pemulihan Bencana** > **Konektivitas**), Anda dapat:

- Unduh file log.
- Membatalkan pendaftaran alat (jika Anda harus mengatur ulang pengaturan alat VPN atau beralih ke mode hanya-awan).

Untuk mengakses pengaturan ini, klik ikon **i** di blok **alat VPN**.

Dalam konsol alat VPN, Anda dapat:

- Mengubah kata sandi untuk alat ini.
- Melihat/mengubah pengaturan jaringan dan menentukan antarmuka mana yang digunakan sebagai WAN untuk koneksi Internet.
- Mependaftaran/mengubah akun pendaftaran (dengan mengulangi pendaftaran).
- Memulai kembali layanan VPN.
- Mem-boot ulang alat VPN.
- Menjalankan perintah shell Linux (hanya untuk kasus pemecahan masalah tingkat lanjut).

Melakukan instalasi ulang gateway VPN

Jika terdapat masalah dengan gateway VPN yang tidak dapat Anda atasi, Anda mungkin perlu melakukan instalasi ulang gateway VPN. Kemungkinan masalah mencakup berikut ini:

- Gateway VPN dalam status **Kesalahan**.
- Gateway VPN dalam status **Menunggu** untuk jangka waktu yang lama.
- Status gateway VPN belum ditentukan dalam jangka waktu yang lama.

Melakukan instalasi ulang proses gateway VPN meliputi tindakan otomatis berikut: menghapus mesin virtual gateway VPN yang sudah ada secara menyeluruh, menginstal mesin virtual baru dari templat, dan mengaplikasikan pengaturan pada gateway VPN sebelumnya di mesin virtual yang baru.

Prasyarat:

Salah satu jenis konektivitas ke situs awan harus diatur.

Untuk melakukan instalasi ulang gateway VPN

1. Di konsol Cyber Protect, buka **Pemulihan Bencana** > **Konektivitas**.
2. Klik ikon roda gateway VPN, lalu pilih **Instalasi ulang gateway VPN**.

© Acronis International GmbH, 2003-2024

3. Di dialog **Instal ulang gateway VPN**, masukkan log masuk Anda.
4. Klik **Instal ulang**.

Mengaktifkan dan menonaktifkan koneksi Situs-ke-situs

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Anda dapat mengaktifkan koneksi Situs-ke-situs pada kasus berikut:

- Jika Anda ingin server awan di situs awan untuk berkomunikasi dengan server di situs lokal.
- Setelah failover ke awan, infrastruktur lokal pulih, dan Anda ingin fail back server Anda ke situs lokal.

Untuk mengaktifkan koneksi situs-ke-situs

1. Buka **Pemulihan Bencana** > **Konektivitas**.
2. Klik **Tampilkan properti**, lalu aktifkan opsi **Koneksi situs-ke-situs**.

Hasilnya, koneksi VPN situs-ke-situs diaktifkan antara situs lokal dan awan. Layanan Cyber Disaster Recovery Cloud mendapatkan pengaturan jaringan dari alat VPN dan memperluas jaringan lokal ke situs awan.

Jika Anda tidak memerlukan server awan di situs awan untuk berkomunikasi dengan server di situs lokal, Anda dapat menonaktifkan koneksi situs-ke-situs.

Untuk menonaktifkan koneksi situs-ke-situs

1. Buka **Pemulihan Bencana** > **Konektivitas**.
2. Klik **Tampilkan properti**, lalu nonaktifkan opsi **Koneksi situs-ke-situs**.

Hasilnya, situs lokal diputus dari situs awan.

Mengalihkan jenis koneksi Situs-ke-situs

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Anda dapat dengan mudah beralih dari koneksi VPN Terbuka Situs-ke-situs ke koneksi VPN IPsec Multi-situs, dan dari koneksi VPN IPsec Multi-situs ke koneksi VPN Terbuka Situs-ke-situs.

Saat Anda mengganti jenis konektivitas, koneksi VPN aktif akan dihapus, tetapi server awan dan konfigurasi jaringan dipertahankan. Akan tetapi, Anda masih perlu menetapkan ulang alamat IP jaringan dan server awan.

Tabel berikut membandingkan karakteristik dasar koneksi VPN Terbuka Situs-ke-situs dan koneksi VPN IPsec Multi-situs.

© Acronis International GmbH, 2003-2024

	VPN Terbuka situs-ke-situs	VPN IPsec multi-situs
Dukungan situs lokal	Tunggal	Tunggal, Beberapa
Mode Gateway VPN	L2 Open VPN	L3 IPsec VPN
Segmen jaringan	Memperluas jaringan lokal ke jaringan awan	Jaringan lokal dan segmen jaringan awan tidak boleh tumpang tindih
Mendukung akses Titik-ke-situs ke situs lokal	Iya	Tidak
Mendukung akses Titik-ke-situs ke situs awan	Iya	Iya
Membutuhkan item penawaran IP publik	Tidak	Iya

Untuk beralih dari koneksi VPN Terbuka Situs-ke-situs ke koneksi VPN IPsec Multi-situs

1. Di konsol Cyber Protect, buka **Pemulihan Bencana** -> **Konektivitas**.
2. Klik **Tampilkan properti**.
3. Klik **Beralih ke VPN IPsec multi-situs**.
4. Klik **Konfigurasi ulang**.
5. Tetapkan ulang alamat IP jaringan awan dan server awan.
6. Konfigurasi pengaturan koneksi IPsec Multi-situs.

Untuk beralih dari koneksi VPN IPsec Multi-situs ke koneksi VPN Terbuka Situs-ke-situs

1. Di konsol Cyber Protect, buka **Pemulihan Bencana** -> **Konektivitas**.
2. Klik **Tampilkan properti**.
3. Klik **Beralih ke VPN Terbuka Situs-ke-situs**.
4. Klik **Konfigurasi ulang**.
5. Tetapkan ulang alamat IP jaringan awan dan server awan.
6. Konfigurasikan pengaturan koneksi Situs-ke-situs.

Menetapkan kembali alamat IP

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

© Acronis International GmbH, 2003-2024

Anda harus menetapkan ulang alamat IP jaringan awan dan server awan untuk menyelesaikan konfigurasi dalam kasus berikut:

- Setelah Anda beralih dari VPN Terbuka Situs-ke-situs ke VPN IPsec Multi-situs, atau sebaliknya.
- Setelah Anda menerapkan rencana proteksi (jika konektivitas VPN IPsec Multi-situs dikonfigurasi).

Untuk menetapkan kembali alamat IP jaringan awan

1. Dalam tab **Konektivitas** , klik alamat IP dari jaringan awan.
2. Dalam notifikasi pop-up **Jaringan** , klik **Edit**.
3. Ketikkan alamat jaringan dan network mask yang baru.
4. Klik **Selesai**.

Setelah menetapkan ulang alamat IP pada jaringan awan, Anda harus menetapkan ulang server awan milik jaringan awan yang ditetapkan ulang.

Untuk menetapkan kembali alamat IP pada server

1. Dalam tab **Konektivitas** , klik alamat IP pada server dalam jaringan awan.
2. Dalam notifikasi pop-up **Server**, klik **Ubah alamat IP**.
3. Dalam notifikasi pop-up **Ubah alamat IP**, ketik alamat IP baru server, atau gunakan alamat IP yang dibuat secara otomatis yang merupakan bagian dari jaringan awan yang ditetapkan ulang.

   Catatan
   Cyber Disaster Recovery Cloud secara otomatis menetapkan alamat IP dari jaringan awan ke semua server awan yang merupakan bagian dari jaringan awan sebelum penetapan ulang alamat IP jaringan. Anda dapat menggunakan alamat IP yang disarankan untuk menetapkan ulang alamat IP dari semua server awan sekaligus.

4. Klik **Konfirmasi**.

Melakukan konfigurasi pada server DNS kustom

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Saat Anda mengonfigurasi konektivitas, Cyber Disaster Recovery Cloud membuat infrastruktur jaringan awan Anda. Server DHCP awan secara otomatis menetapkan server DNS default ke server pemulihan dan server utama, tetapi Anda dapat mengubah pengaturan default dan mengonfigurasi server DNS kustom. Pengaturan DNS baru akan diterapkan pada saat permintaan berikutnya ke server DHCP.

Prasyarat:

Salah satu jenis konektivitas ke situs awan harus diatur.

Untuk melakukan konfigurasi pada server DNS kustom

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Pemulihan Bencana** > **Konektivitas**.
2. Klik **Tampilkan properti**.
3. Klik **Default (Disediakan oleh Situs Awan)**.
4. Pilih **Server kustom**.
5. Ketik alamat IP server DNS.
6. [Opsional] Jika Anda ingin menambahkan server DNS lain, klik **Tambahkan**, dan ketik alamat IP server DNS.

   Catatan
   Setelah Anda menambahkan server DNS kustom, Anda juga dapat menambahkan server DNS default. Dengan demikian, jika server DNS kustom tidak tersedia, Cyber Disaster Recovery Cloud akan menggunakan server DNS default.

7. Klik **Selesai**.

Menghapus Server DNS kustom

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Anda dapat menghapus Server DNS dari daftar DNS kustom.

Prasyarat:

Server DNS kustom telah dikonfigurasi.

Untuk menghapus Server DNS kustom

1. Di konsol Cyber Protect, buka **Pemulihan Bencana** > **Konektivitas**.
2. Klik **Tampilkan properti**.
3. Klik **Server kustom**.
4. Klik ikon hapus di sebelah Server DNS.

   Catatan
   Operasi penghapusan dinonaktifkan saat hanya ada satu Server DNS kustom yang tersedia. Jika Anda ingin menghapus semua Server DNS kustom, pilih **Default (disediakan oleh Situs Awan)**.

5. Klik **Selesai**.

© Acronis International GmbH, 2003-2024

Mengonfigurasi perutean lokal

Selain jaringan lokal Anda yang diperluas ke awan melalui alat VPN, Anda mungkin memiliki jaringan lokal lain yang tidak terdaftar di alat VPN namun memiliki server yang perlu berkomunikasi dengan server awan. Untuk membuat konektivitas antara server lokal dan server awan tersebut, Anda harus mengonfigurasi pengaturan perutean lokal.

Untuk mengonfigurasi perutean lokal

1. Buka **Pemulihan Bencana**>**Konektivitas**.
2. Klik **Tunjukkan properti**, lalu klik **Perutean lokal**.
3. Tentukan jaringan lokal dalam notasi CIDR.
4. Klik **Simpan**.

Hasilnya, server dari jaringan lokal yang ditentukan akan dapat berkomunikasi dengan server awan.

Mengizinkan lalu lintas DHCP melalui L2 VPN

Jika perangkat di situs lokal Anda mendapatkan alamat IP dari server DHCP, Anda dapat melindungi server DHCP dengan Pemulihan Bencana, mengalihkannya ke awan, dan kemudian mengizinkan lalu lintas DHCP dijalankan melalui L2 VPN. Dengan demikian, server DHCP Anda akan berjalan di awan, tetapi akan terus memberikan alamat IP ke perangkat lokal Anda.

Prasyarat:

Jenis konektivitas L2 VPN Situs-ke-situs ke situs awan harus disetel.

Untuk mengizinkan lalu lintas DHCP melalui koneksi L2 VPN

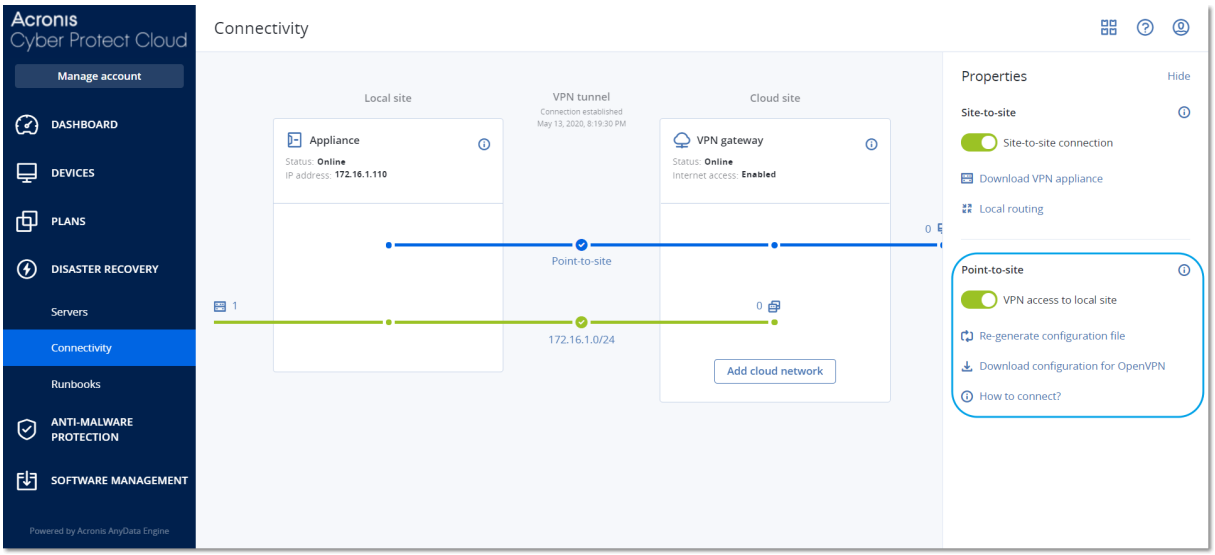
1. Buka tab **Pemulihan Bencana** > **Konektivitas**.
2. Klik **Tampilkan Properti**.
3. Aktifkan tombol **Izinkan lalu lintas DHCP melalui L2 VPN**.

Mengelola pengaturan koneksi titik-ke-situs

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Di konsol Cyber Protect, buka **Pemulihan Bencana** > **Konektivitas** lalu klik **Tampilkan properti** di sudut kanan atas.

© Acronis International GmbH, 2003-2024



Akses VPN ke situs lokal

Opsi ini digunakan untuk mengelola akses VPN ke situs lokal. Opsi ini aktif secara bawaan. Jika dinonaktifkan, akses Titik-ke-situs ke situs lokal tidak akan diizinkan.

Unduh konfigurasi untuk OpenVPN

Item ini akan mengunduh file konfigurasi untuk klien OpenVPN. File tersebut diperlukan untuk membuat koneksi Titik-ke-situs ke situs awan.

Buat kembali konfigurasi

Anda dapat membuat kembali file konfigurasi untuk klien OpenVPN.

Item ini diperlukan dalam kasus berikut:

- Jika Anda menduga bahwa file konfigurasi membahayakan.
- Jika autentikasi dua faktor diaktifkan untuk akun Anda.

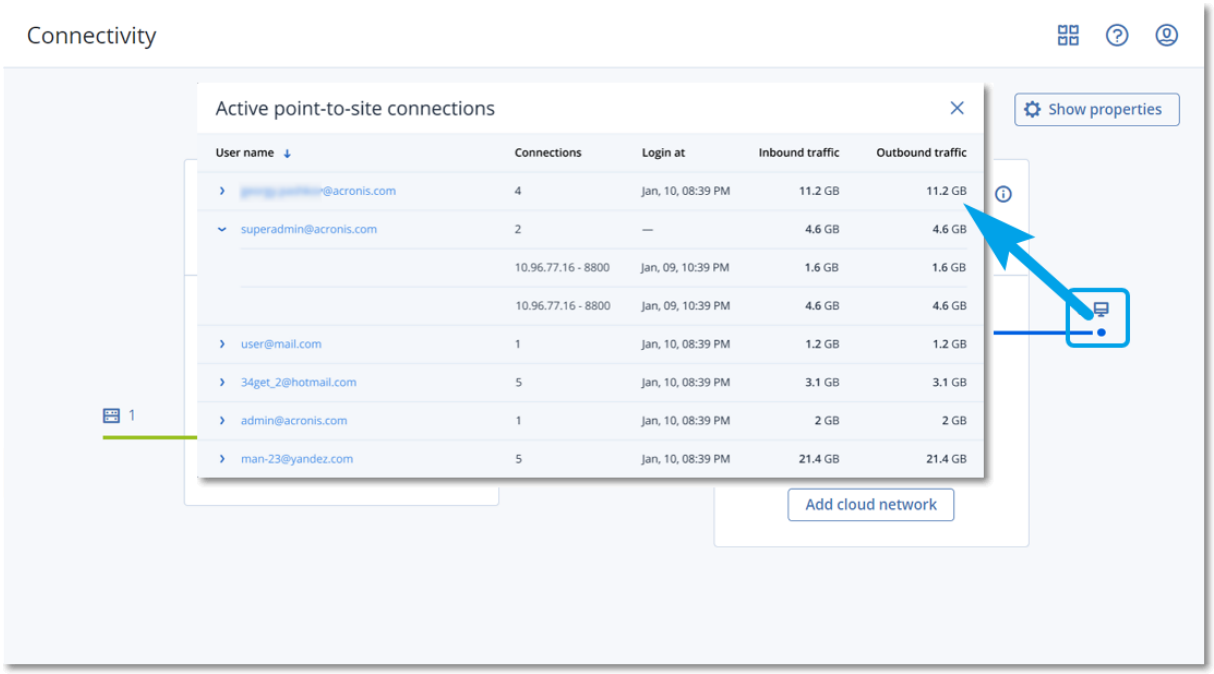
Segera setelah file konfigurasi diperbarui, koneksi dengan file konfigurasi lama tidak lagi dimungkinkan. Pastikan untuk mendistribusikan file baru di antara pengguna yang diizinkan untuk menggunakan koneksi Titik-ke-situs.

Koneksi titik-ke-situs aktif

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Anda dapat melihat semua koneksi titik-ke-situs yang aktif di **Pemulihan bencana** > **Konektivitas**. Klik ikon mesin di garis **Titik-ke-situs** berwarna biru, maka Anda akan melihat informasi mendetail tentang koneksi titik-ke-situs aktif yang dikelompokkan berdasarkan nama pengguna.

© Acronis International GmbH, 2003-2024



Bekerja dengan log

Pemulihan Bencana mengumpulkan log untuk alat VPN dan gateway VPN. Log disimpan sebagai file .txt, yang dikompres dalam arsip .zip. Anda dapat mengunduh dan mengekstrak arsip, dan menggunakan informasi tersebut untuk tujuan pemecahan masalah atau pemantauan.

Daftar berikut ini menjelaskan file log yang merupakan bagian dari arsip .zip, dan informasi di dalamnya.

`dnsmasq.config.txt` - File tersebut berisi informasi tentang konfigurasi layanan yang menyediakan alamat DNS dan DHCP.

`dnsmsq.leases.txt` - File berisi informasi tentang sewa alamat DHCP saat ini.

`dnsmasq_log.txt` - File tersebut berisi log dari layanan dnsmasq.

`ebtables.txt` - File tersebut berisi informasi tentang tabel firewall.

`free.txt` - File berisi informasi tentang memori yang kosong.

`ip.txt` - File berisi log dari konfigurasi antarmuka jaringan, termasuk namanya yang dapat digunakan dalam konfigurasi pengaturan **Mengumpulkan paket jaringan**.

`NetworkManager_log.txt` - File berisi log dari layanan NetworkManager.

`NetworkManager_status.txt` - File berisi informasi tentang status layanan NetworkManager.

`openvpn@p2s_log.txt` - File berisi log dari layanan OpenVPN.

`openvpn@p2s_status.txt` - File berisi informasi tentang status terowongan VPN.

`ps.txt` - File tersebut berisi informasi tentang proses yang sedang berjalan di gateway VPN atau perangkat VPN.

© Acronis International GmbH, 2003-2024

`resolf.conf.txt` - File berisi informasi tentang konfigurasi server DNS.

`routes.txt` - File tersebut berisi informasi tentang rute jaringan.

`uname.txt` - File tersebut berisi informasi tentang versi kernel sistem operasi saat ini.

`uptime.txt` - File tersebut berisi informasi tentang jangka waktu sistem operasi belum dimulai ulang.

`vpnserver_log.txt` - File berisi log dari layanan VPN.

`vpnserver_status.txt` - File berisi informasi tentang status server VPN.

Untuk informasi lebih lanjut tentang file log yang khusus untuk konektivitas VPN IPsec, lihat "File log VPN IPSec Multi-situs" (hlm. 776).

Mengunduh log alat VPN

Anda dapat mengunduh dan mengekstrak arsip yang berisi log alat VPN, dan menggunakan informasi tersebut untuk tujuan pemecahan masalah atau pemantauan.

Untuk mengunduh log alat VPN

1. Di halaman **Konektivitas**, klik ikon roda di sebelah alat VPN.
2. Klik **Unduh log**.
3. [Opsional] Pilih **Kumpulkan paket jaringan**, dan konfigurasikan pengaturan. Untuk informasi lebih lanjut, lihat "Mengumpulkan paket jaringan" (hlm. 772).
4. Klik **Selesai**.
5. Saat arsip .zip siap diunduh, klik **Unduh log**, dan simpan di penyimpanan lokal.

Mengunduh log gateway VPN

Anda dapat mengunduh dan mengekstrak arsip yang berisi log gateway VPN, dan menggunakan informasi tersebut untuk tujuan pemecahan masalah atau pemantauan.

Untuk mengunduh log gateway VPN

1. Di halaman **Konektivitas**, klik ikon roda di sebelah gateway VPN.
2. Klik **Unduh log**.
3. [Opsional] Pilih **Kumpulkan paket jaringan**, lalu konfigurasikan pengaturan. Untuk informasi lebih lanjut, lihat "Mengumpulkan paket jaringan" (hlm. 772).
4. Klik **Selesai**.
5. Saat arsip .zip siap diunduh, klik **Unduh log**, dan simpan di penyimpanan lokal.

Mengumpulkan paket jaringan

Untuk memecahkan masalah dan menganalisis komunikasi antara situs produksi lokal dan server utama atau pemulihan, Anda dapat memilih untuk mengumpulkan paket jaringan di gateway VPN atau alat VPN.

 © Acronis International GmbH, 2003-2024

Setelah mengumpulkan 32000 paket jaringan, atau mencapai batas waktu, pengumpulan paket jaringan berhenti, dan hasilnya dituliskan di file .libpcap yang ditambahkan ke arsip log .zip.

Tabel berikut ini memberikan informasi lebih lanjut tentang pengaturan **Kumpulkan paket jaringan** yang dapat Anda konfigurasikan.

Pengaturan	Deskripsi
Nama antarmuka jaringan	Antarmuka jaringan untuk mengumpulkan paket jaringan. Jika Anda ingin mengumpulkan paket jaringan pada semua antarmuka jaringan, pilih **Semua**.
Batas waktu (detik)	Batas waktu untuk mengumpulkan paket jaringan. Nilai maksimal yang dapat Anda atur adalah 1800.
Pemfilteran	Filter tambahan yang bisa diterapkan pada paket jaringan yang dikumpulkan. Anda dapat memasukkan string berisi protokol, port, arahan, dan kombinasinya, dipisahkan spasi, seperti: "and", "or", "not", " (", ") ", "src", "dst", "net", "host", "port", "ip", "tcp", "udp", "icmp", "arp", "esp". Jika Anda ingin menggunakan tanda kurung, pisahkan dengan spasi. Anda juga dapat memasukkan alamat IP dan alamat jaringan, misalnya: "icmp or arp" dan "port 67 or 68". Untuk informasi lebih lanjut tentang nilai yang dapat Anda masukkan, lihat bantuan tcpdump Linux.

Memecahkan masalah konfigurasi VPN IPsec

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Saat Anda mengkonfigurasi atau menggunakan koneksi VPN IPsec, Anda mungkin mengalami masalah.

Anda dapat mempelajari selengkapnya tentang masalah yang Anda hadapi di file log IPsec, dan memeriksa topik Pemecahan masalah konfigurasi VPN IPsec terkait solusi yang dapat diberikan dari beberapa masalah umum yang mungkin terjadi.

Memecahkan masalah konfigurasi VPN IPsec

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Tabel berikut menjelaskan masalah konfigurasi VPN IPsec yang paling sering terjadi, dan menjelaskan cara memecahkannya.

© Acronis International GmbH, 2003-2024

Masalah	Solusi yang dapat diberikan
Saya melihat pesan kesalahan berikut: **Kesalahan negosiasi IKE fase 1. Periksa pengaturan IKE IPsec pada situs Awan dan Lokal.**	Klik **Coba lagi** dan periksa jika pesan kesalahan yang lebih spesifik muncul. Misalnya, pesan kesalahan yang lebih spesifik mungkin merupakan pesan kesalahan tentang ketidakcocokan algoritme atau kunci yang Dibagikan sebelumnya salah. **Catatan** Untuk alasan keamanan, pembatasan berikut ini berlaku untuk konektivitas VPN IPsec: • IKEv1 dipanggil untuk penghentian di RFC8247 dan tidak didukung karena risiko keamanan. Hanya koneksi protokol IKEv2 yang didukung. • Algoritme Enkripsi berikut tidak dianggap aman dan tidak didukung: DES, dan 3DES. • Algoritme Hash berikut tidak dianggap aman dan tidak didukung: SHA1, dan MD5. • Grup Diffie-Hellman nomor 2 tidak dianggap aman dan tidak didukung.
Koneksi antara situs lokal saya dan situs awan tetap dalam status **Tersambung**.	Periksa: • Jika UDP port 500 terbuka (saat Anda menggunakan firewall). • Konektivitas antara situs lokal dan situs awan. • Jika alamat IP situs lokal sudah benar.
Koneksi antara situs lokal saya dan situs awan tetap dalam status **Menunggu koneksi**.	Anda melihat status ini saat **Langkah pengaktifan** untuk situs awan diatur ke **Tambahkan**, yang berarti bahwa situs awan sedang menunggu situs lokal untuk memulai koneksi. Memulai koneksi dari situs lokal.
Koneksi antara situs lokal saya dan situs awan tetap dalam status **Menunggu lalu lintas**.	Anda melihat status ini ketika **Langkah Pengaktifan** untuk situs awan diatur ke **Rutekan**. Jika Anda mengharapkan koneksi dari situs lokal, lakukan hal berikut: • Dari situs lokal, coba ping mesin virtual di situs awan. Ini adalah perilaku standar yang diperlukan saat membuat terowongan untuk beberapa perangkat, misalnya Cisco ASA. (Mode rute) • Pastikan bahwa situs lokal membuat terowongan dengan mengatur **Langkah Pengaktifan** dari situs lokal ke **Muali**.

© Acronis International GmbH, 2003-2024

Masalah	Solusi yang dapat diberikan
Koneksi antara situs lokal saya dan situs awan telah dibuat, tetapi saya dapat melihat bahwa satu atau beberapa kebijakan jaringan sedang bermasalah.	Masalah ini mungkin disebabkan oleh alasan berikut: • Pemetaan jaringan di situs IPsec awan berbeda dengan pemetaan jaringan di situs lokal. Pastikan bahwa pemetaan jaringan dan urutan kebijakan jaringan di situs lokal dan awan sama persis. • Keadaan ini dibenarkan jika **Langkah pengaktifan** pada situs lokal dan/atau situs awan diatur ke **Rute** (misalnya, pada perangkat Cisco ASA), dan saat ini tidak ada lalu lintas. Anda dapat mencoba melakukan ping untuk memastikan bahwa terowongan telah dibuat. Jika ping tidak berfungsi, periksa pemetaan jaringan di situs lokal dan awan.
Saya ingin memulai ulang koneksi IPsec tertentu.	Untuk memulai ulang koneksi IPsec tertentu: 1. Pada layar **Pemulihan Bencana** > **Konektivitas**, klik koneksi IPsec. 2. Klik **Nonaktifkan koneksi**. 3. Klik kembali koneksi Ipsec. 4. Klik **Aktifkan koneksi**.

Mengunduh file log VPN IPsec

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Anda dapat menemukan informasi tambahan tentang konektivitas IPsec pada file log server VPN. File log tersebut dikompres dalam arsip .zip yang dapat Anda unduh dan ekstrak.

Prasyarat

Konektivitas VPN IPsec Multi-situs dikonfigurasi.

Untuk mengunduh arsip .zip dengan file log

1. Di konsol Cyber Protect, buka **Pemulihan Bencana** > **Konektivitas**.
2. Klik ikon roda di sebelah gateway VPN situs awan.
3. Klik **Unduh log**.
4. Klik **Selesai**.
5. Saat arsip .zip siap diunduh, klik **Unduh log**, dan simpan di penyimpanan lokal.

© Acronis International GmbH, 2003-2024

File log VPN IPSec Multi-situs

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Daftar berikut ini menjelaskan file log VPN IPsec yang merupakan bagian dari arsip zip, dan informasi di dalamnya.

- `ip.txt` - File tersebut berisi log dari konfigurasi antarmuka jaringan. Anda harus melihat dua alamat IP - alamat IP publik dan alamat IP lokal. Jika Anda tidak melihat alamat IP ini di log, berarti ada masalah. Hubungi tim Dukungan.

  Catatan
  Mask untuk alamat IP publik harus 32.

- `swanctl-list-loaded-config.txt` - File tersebut berisi informasi tentang semua situs IPsec. Jika Anda tidak melihat situs di file tersebut, maka konfigurasi IPsec tidak diterapkan. Coba perbarui konfigurasi dan simpan, atau hubungi tim Dukungan.
- `swanctl-list-active-sas.txt` - File tersebut berisi koneksi dan kebijakan yang berstatus aktif atau terhubung.

Mengatur server pemulihan

Bagian ini menjelaskan konsep failover dan failback, pembuatan server pemulihan, dan operasi pemulihan bencana.

Membuat server pemulihan

Untuk membuat server pemulihan yang akan menjadi salinan beban kerja Anda, ikuti prosedur di bawah ini. Anda juga dapat menyaksikan tutorial video yang menunjukkan prosesnya.

Penting
Saat Anda melakukan failover, Anda hanya dapat memilih titik pemulihan yang dibuat setelah pembuatan server pemulihan.

Prasyarat

- Rencana proteksi harus diterapkan pada mesin asli yang ingin Anda lindungi. Rencana ini harus mencadangkan seluruh mesin, atau hanya disk-nya, yang diperlukan untuk boot dan menyediakan layanan yang dibutuhkan, ke penyimpanan awan.
- Salah satu jenis konektivitas ke situs awan harus diatur.

Untuk membuat server pemulihan

© Acronis International GmbH, 2003-2024

1. Pada tab **Semua perangkat**, pilih mesin yang ingin Anda lindungi.
2. Klik **Pemulihan bencana**, lalu klik **Buat server pemulihan**.
3. Pilih jumlah inti virtual dan ukuran RAM.

   Catatan
   Anda dapat melihat titik komputasi untuk setiap opsi. Jumlah titik komputasi menunjukkan biaya pengoperasian server pemulihan per jam. Untuk informasi lebih lanjut, lihat "Titik komputasi" (hlm. 734).

4. Tentukan jaringan awan yang akan dihubungkan dengan server.
5. Pilih opsi **DHCP**.

Opsi DHCP	Deskripsi
Disediakan oleh situs awan	Pengaturan default. Alamat IP server akan diberikan oleh server DHCP yang dikonfigurasi secara otomatis di awan.
Kustom	Alamat IP server akan diberikan oleh server DHCP Anda sendiri di awan.

6. [Opsional] Tentukan **Alamat MAC**.
   Alamat MAC adalah pengidentifikasi unik yang ditetapkan ke adaptor jaringan server. Jika menggunakan DHCP kustom, Anda dapat mengonfigurasinya untuk selalu menetapkan alamat IP tertentu ke alamat MAC tertentu. Dengan cara itu, Anda akan memastikan bahwa server pemulihan selalu mendapatkan alamat IP yang sama. Anda dapat menjalankan aplikasi yang memiliki lisensi yang terdaftar dengan alamat MAC.
7. Tentukan alamat IP yang akan dimiliki server dalam jaringan produksi. Secara default, alamat IP mesin asli telah diatur.

   Catatan
   Jika Anda menggunakan server DHCP, tambahkan alamat IP ini ke daftar pengecualian server untuk menghindari konflik alamat IP.
   Jika menggunakan server DHCP kustom, Anda harus menentukan alamat IP yang sama di **alamat IP di jaringan produksi** seperti yang dikonfigurasi di server DHCP. Jika tidak, uji failover tidak akan berfungsi dengan baik dan server tidak akan dapat dijangkau melalui alamat IP publik.

8. [Opsional] Pilih kotak centang **Uji alamat IP**, lalu tentukan alamat IP.
   Dengan ini, Anda akan dapat menguji failover di jaringan uji yang terisolasi dan terhubung ke server pemulihan melalui RDP atau SSH selama failover uji. Di mode tes failover, gateway VPN akan menggantikan alamat IP uji dengan alamat IP produksi menggunakan protokol NAT.
   Jika Anda membiarkan kotak centang kosong, konsol akan menjadi satu-satunya cara untuk mengakses server selama failover uji.

© Acronis International GmbH, 2003-2024

Catatan
Jika Anda menggunakan server DHCP, tambahkan alamat IP ini ke daftar pengecualian server, untuk menghindari konflik alamat IP.

Anda dapat memilih salah satu alamat IP yang diusulkan atau jenis yang lain.

9. [Opsional] Pilih kotak centang **Akses internet**.
   Hal ini akan mengaktifkan server pemulihan untuk mengakses Internet selama failover nyata atau uji. Secara default, port TCP 25 terbuka untuk koneksi keluar ke alamat IP publik.
10. [Opsional] Atur **Ambang batas RPO**.
    Ambang batas RPO menjelaskan interval waktu maksimum yang diperbolehkan antara titik pemulihan terakhir yang tepat untuk failover dan waktu terkini. Nilai dapat diatur antara 15 – 60 menit, 1 – 24 jam, 1 – 14 hari.
11. [Opsional] Pilih kotak centang **Gunakan alamat IP publik**.
    Memiliki alamat IP publik membuat server pemulihan tersedia dari Internet selama failover atau failover uji. Jika Anda membiarkan kotak centang kosong, server hanya akan tersedia pada jaringan produksi Anda.
    Opsi **Gunakan alamat IP publik** mewajibkan opsi **Akses internet** untuk diaktifkan.
    Alamat IP publik akan ditampilkan setelah Anda menyelesaikan konfigurasi. Secara default, port TCP 443 terbuka untuk koneksi masuk ke alamat IP publik.

    Catatan
    Jika Anda menghapus kotak centang **Gunakan alamat IP publik** atau menghapus server pemulihan, alamat IP publiknya tidak akan terpesan.

12. [Opsional] [Jika cadangan untuk mesin yang terpilih dienkripsi dengan menggunakan enkripsi sebagai properti mesin], tentukan kata sandi yang akan digunakan secara otomatis saat membuat mesin virtual untuk server pemulihan dari cadangan yang dienkripsi.
    a. Klik **Tentukan**, lalu masukkan kata sandi untuk cadangan terenkripsi dan tentukan nama kredensialnya.
       Secera default, Anda akan melihat cadangan terbaru dalam daftar.
    b. [Opsional] Untuk melihat semua cadangan, pilih **Tampilkan semua cadangan**.
    c. Klik **Selesai**.

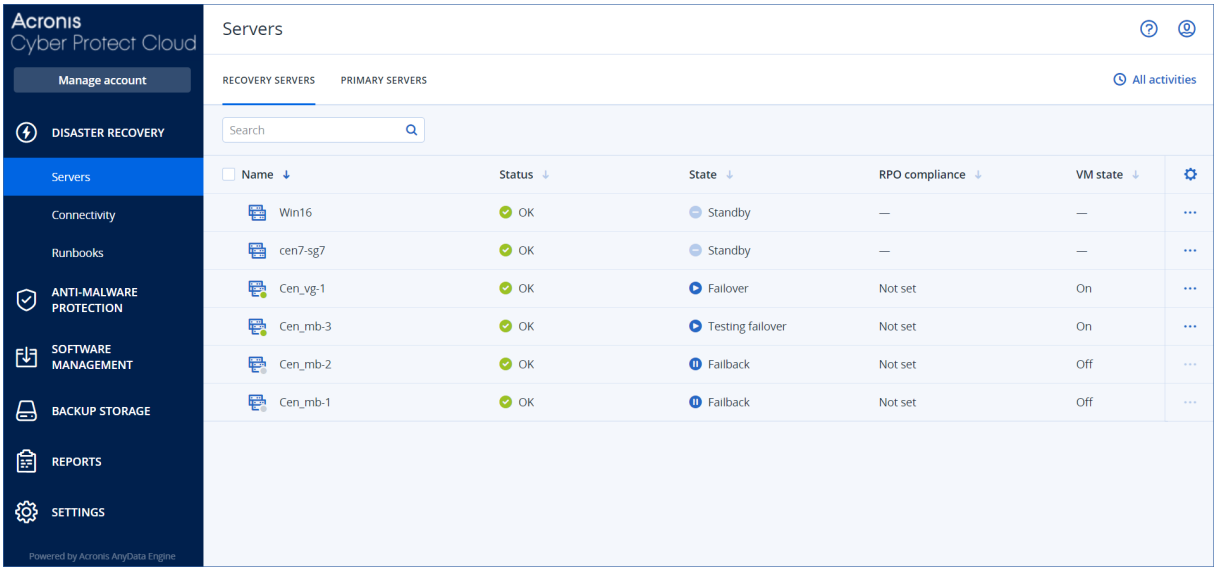
    Catatan
    Meskipun kata sandi yang Anda tentukan akan disimpan di penyimpanan kredensial yang aman, menyimpan kata sandi mungkin bertentangan dengan kewajiban kepatuhan Anda.

13. [Opsional] Ubah nama server pemulihan.
14. [Opsional] Ketik deskripsi untuk server pemulihan.
15. [Opsional] Klik tab **Aturan firewall awan** untuk mengedit aturan firewall default. Untuk informasi lebih lanjut, lihat "Menetapkan aturan firewall untuk server awan" (hlm. 803).

© Acronis International GmbH, 2003-2024

16. Klik **Buat**.

Server pemulihan muncul di tab **Pemulihan Bencana** > **Server** > **Server utama** di konsol Cyber Protect. Anda dapat melihat pengaturannya dengan memilih mesin asli dan mengeklik **Pemulihan bencana**.



Cara kerja failover

Failover produksi

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Ketika server pemulihan dibuat, server tersebut tetap dalam keadaan **Standby** state. Mesin virtual yang sesuai tidak tersedia sampai Anda memulai failover. Sebelum memulai proses failover, Anda harus membuat setidaknya satu cadangan profil disk (dengan volume yang dapat di-boot) dari mesin asli.

Saat memulai proses failover, Anda memilih titik pemulihan (cadangan) mesin asli tempat mesin virtual dengan parameter yang telah ditentukan akan dibuat. Operasi failover menggunakan fungsi "jalankan VM dari cadangan". Server pemulihan mendapatkan **Finalisasi** kondisi transisi. Proses ini berarti mentransfer disk virtual server dari penyimpanan cadangan (penyimpanan 'dingin') ke penyimpanan pemulihan bencana (penyimpanan 'panas').

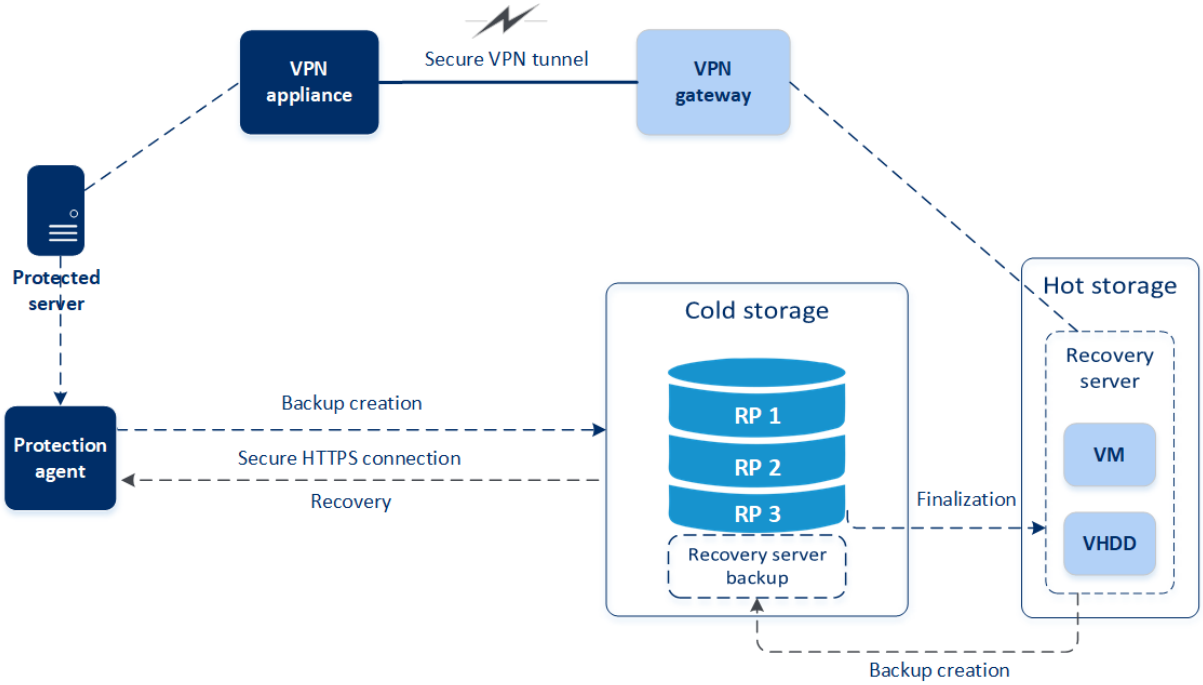
Catatan
Selama **Finalisasi**, server dapat diakses dan dioperasikan meskipun performanya lebih rendah dari saat normal. Anda dapat membuka konsol server dengan mengeklik tautan **Konsol telah siap**. Tautan tersedia di kolom **Status VM** di layar **Pemulihan Bencana** > **Server**, dan di tampilan **Detail** server.

© Acronis International GmbH, 2003-2024

Ketika **Finalisasi** selesai, performa server akan mencapai nilai normal. Status server berubah menjadi **Failover**. Beban kerja sekarang dialihkan dari mesin asli ke server pemulihan di situs awan.

Jika server pemulihan memiliki agen proteksi di dalam, layanan agen akan dihentikan untuk menghindari gangguan (seperti memulai pencadangan atau melaporkan status kedaluwarsa ke komponen cadangan).

Dalam diagram di bawah ini, Anda dapat melihat proses failover dan failback.



Tes failover

Selama **failover uji**, mesin virtual belum menyelesaikannya. Ini berarti agen membaca konten disk virtual langsung dari cadangan, yang mencakup akses acak ke berbagai bagian cadangan, sehingga kinerjanya mungkin lebih lambat dibandingkan kinerja normal. Untuk informasi lebih lanjut tentang proses failover uji, lihat "Menjalankan failover uji" (hlm. 780).

Failover uji otomatis

Ketika dikonfigurasi, failover uji otomatis dilakukan satu kali sebulan tanpa interaksi manual apa pun. Untuk informasi lebih lanjut, lihat "Failover uji otomatis" (hlm. 782) dan "Mengonfigurasi failover uji otomatis" (hlm. 783).

Menjalankan failover uji

Melakukan failover uji berarti memulai server pemulihan dalam menguji VLAN yang diisolasi dari jaringan produksi Anda. Anda dapat menguji beberapa server pemulihan sekaligus dan mengecek interaksinya. Di dalam jaringan uji, server berkomunikasi menggunakan alamat IP produksi mereka, tetapi mereka tidak dapat memulai koneksi TCP atau UDP ke beban kerja di jaringan lokal Anda.

© Acronis International GmbH, 2003-2024

Selama failover uji, mesin virtual (server pemulihan) belum diselesaikan. Agen membaca konten disk virtual langsung dari cadangan dan mengakses berbagai bagian cadangan secara acak. Hal ini mungkin menyebabkan performa server pemulihan dalam status failover uji lebih lambat dari performa normalnya.

Meskipun melakukan failover uji bersifat opsional, kami sarankan Anda agar menjadikannya sebagai proses rutin dengan frekuensi yang Anda anggap memadai dalam aspek biaya dan keamanan. Praktik terbaiknya adalah membuat runbook, yaitu sekumpulan petunjuk yang menjelaskan cara mempercepat lingkungan produksi di awan.

Penting
Anda harus membuat server pemulihan lebih dulu untuk melindungi perangkat dari bencana.

Anda dapat melakukan failover hanya dari titik pemulihan yang dibuat setelah server pemulihan perangkat dibuat.

Setidaknya satu titik pemulihan harus dibuat sebelum gagal pada server pemulihan. Jumlah maksimum titik pemulihan yang didukung adalah 100.

Untuk melakukan failover uji

1. Pilih mesin asli atau pilih server pemulihan yang ingin Anda uji.
2. Klik **Pemulihan Bencana**.
   Deskripsi server pemulihan akan terbuka.
3. Klik **Failover**.
4. Pilih jenis failover **Failover uji**.
5. Pilih titik pemulihan (cadangan), lalu klik **Mulai**.
6. Jika cadangan yang Anda pilih dienkripsi menggunakan enkripsi sebagai properti mesin:
   a. Masukkan kata sandi enkripsi untuk kumpulan cadangan.

      Catatan
      Kata sandi hanya akan disimpan sementara dan hanya akan digunakan untuk operasi failover uji saat ini. Kata sandi secara otomatis dihapus dari penyimpanan kredensial jika failover uji dihentikan, atau setelah failover uji selesai.

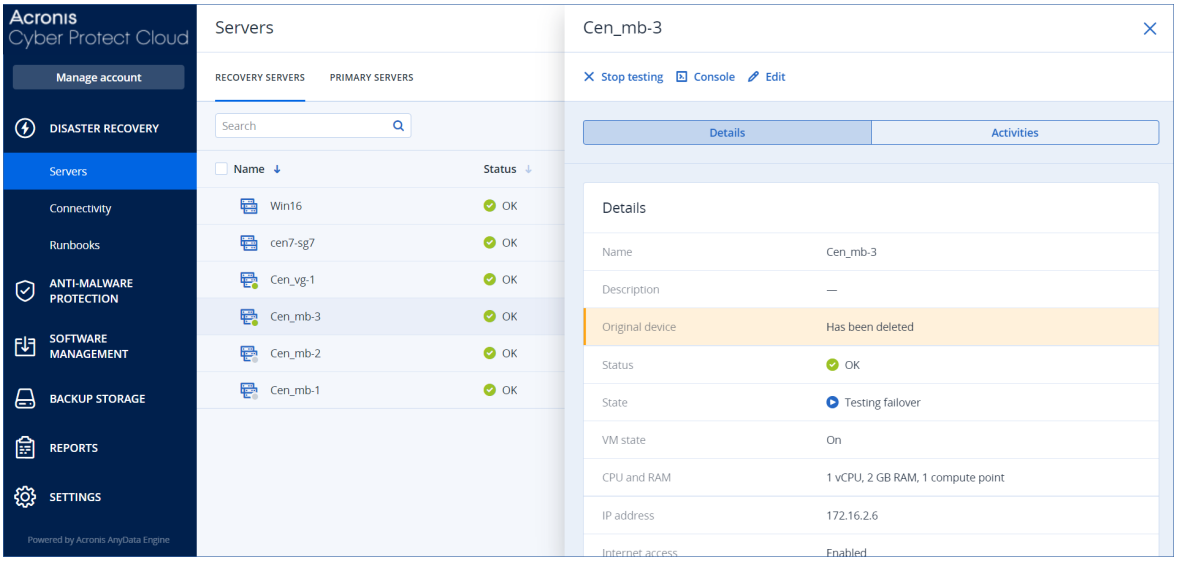
   b. [Opsional] Untuk menyimpan kata sandi kumpulan cadangan dan menggunakannya dalam operasi failover berikutnya, pilih kotak centang **Simpan kata sandi di penyimpanan kredensial aman...** lalu, di bidang **Nama kredensial**, masukkan nama untuk kredensial.

      Penting
      Kata sandi akan disimpan di penyimpanan kredensial aman dan akan diterapkan secara otomatis dalam operasi failover berikutnya. Namun, menyimpan kata sandi mungkin bertentangan dengan kewajiban Anda untuk patuh.

   c. Klik **Selesai**.

© Acronis International GmbH, 2003-2024

Ketika server pemulihan dimulai, statusnya berubah menjadi **Mengetes failover**.



7. Uji server pemulihan menggunakan salah satu metode berikut:
   - Dalam **Pemulihan Bencana** > **Server**, pilih server pemulihan, lalu klik **Konsol**.
   - Hubungkan ke server pemulihan menggunakan RDP atau SSH, dan alamat IP uji yang Anda tentukan ketika membuat server pemulihan. Cobalah koneksi dari dalam dan luar jaringan produksi (seperti yang dijelaskan dalam "Koneksi titik-ke-situs").
   - Jalankan skrip di dalam server pemulihan.

     Skrip dapat memeriksa layar masuk, apakah aplikasi sudah dimulai, koneksi Internet, dan kemampuan mesin lain untuk terhubung ke server pemulihan.
   - Jika server pemulihan memiliki akses ke Internet dan alamat IP publik, Anda mungkin perlu menggunakan TeamViewer.
8. Saat pengujian selesai, klik **Hentikan pengujian**.

   Server pemulihan dihentikan. Semua perubahan yang diterapkan pada server pemulihan selama failover uji tidak dipertahankan.

Catatan
Tindakan **Mulai server** dan **Hentikan server** tidak berlaku untuk operasi failover uji di runbook dan ketika memulai failover uji secara manual. Jika Anda mencoba mengeksekusi tindakan tersebut, kegagalan akan terjadi dengan pesan kesalahan berikut:
Gagal: Tindakan ini tidak berlaku pada keadaan server saat ini.

Failover uji otomatis

Dengan failover uji otomatis, server pemulihan diuji secara otomatis satu kali sebulan tanpa interaksi manual apa pun.

Proses failover uji otomatis terdiri dari bagian berikut:

1. membuat mesin virtual dari titik pemulihan terakhir
2. mengambil tangkapan layar mesin virtual

© Acronis International GmbH, 2003-2024

3. menganalisis apakah sistem operasi mesin virtual berhasil dimulai
4. memberi tahu Anda tentang status failover uji

Catatan
Failover uji otomatis menggunakan titik komputasi.

Anda dapat mengonfigurasi failover uji otomatis di pengaturan server pemulihan. Untuk informasi lebih lanjut, lihat "Mengonfigurasi failover uji otomatis" (hlm. 783).

Perhatikan bahwa, dalam kasus yang sangat jarang terjadi, failover uji otomatis mungkin dilewati dan mungkin tidak dilakukan pada waktu yang dijadwalkan. Hal ini karena failover produksi memiliki prioritas yang lebih tinggi daripada failover uji otomatis, sehingga sumber daya perangkat keras (CPU dan RAM) yang dialokasikan untuk failover uji mungkin dibatasi sementara untuk memastikan ada cukup sumber daya untuk failover produksi bersamaan.

Jika failover uji otomatis dilewati untuk beberapa alasan, peringatan akan muncul.

Catatan
Failover uji otomatis akan gagal jika cadangan dari mesin asli dienkripsi dengan menggunakan enkripsi sebagai properti mesin, dan kata sandi enkripsi tidak ditentukan saat membuat server pemulihan. Untuk informasi lebih lanjut tentang menentukan kata sandi enkripsi, lihat "Membuat server pemulihan" (hlm. 776).

Mengonfigurasi failover uji otomatis

Dengan mengonfigurasi failover uji otomatis, Anda dapat menguji server pemulihan setiap bulan tanpa melakukan tindakan manual apa pun.

Cara mengonfigurasi failover uji otomatis

1. Di konsol, buka **Pemulihan bencana** > **Server** > **Server pemulihan**, lalu pilih server pemulihan.
2. Klik **Edit**.
3. Di bagian **Failover uji otomatis** bagian, pada bidang **Jadwal**, pilih **Bulanan**.
4. [Opsional] Pada **Waktu tunggu tangkapan layar**, ubah nilai default jangka waktu maksimum (dalam menit) bagi sistem untuk mencoba failover uji otomatis.
5. [Opsional] Jika Anda ingin menyimpan nilai **Waktu tunggu tangkapan layar** sebagai default dan mengisinya secara otomatis saat Anda mengaktifkan failover uji otomatis untuk server pemulihan lainnya, pilih **Tetapkan sebagai batas waktu default**.
6. Klik **Simpan**.

Melihat status failover uji otomatis

Anda dapat menampilkan detail failover uji otomatis yang selesai, seperti status, waktu mulai, waktu selesai, durasi, dan tangkapan layar mesin virtual.

Cara melihat status failover uji otomatis server pemulihan

© Acronis International GmbH, 2003-2024

1. Di konsol, buka **Pemulihan bencana** > **Server** > **Server pemulihan**, lalu pilih server pemulihan.
2. Di bagian **Failover uji otomatis**, periksa detail failover uji otomatis terakhir.
3. [Opsional] Klik **Tampilkan tangkapan layar** untuk melihat tangkapan layar mesin virtual.

Menonaktifkan failover uji otomatis

Anda dapat menonaktifkan failover uji otomatis jika ingin menghemat sumber daya atau tidak perlu melakukan failover uji otomatis untuk server pemulihan tertentu.

Cara menonaktifkan failover uji otomatis

1. Di konsol, buka **Pemulihan bencana** > **Server** > **Server pemulihan**, lalu pilih server pemulihan.
2. Klik **Edit**.
3. Di bagian **Failover uji otomatis**, pada bidang **Jadwal**, pilih **Tidak pernah**.
4. Klik **Simpan**.

Melakukan failover

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Failover adalah proses memindahkan beban kerja dari fasilitas Anda ke awan, dan juga status ketika beban kerja tetap di awan.

Saat Anda memulai failover, server pemulihan dimulai di jaringan produksi. Untuk menghindari gangguan dan masalah yang tidak diinginkan, pastikan beban kerja asli tidak online dan tidak dapat diakses melalui VPN.

Untuk menghindari gangguan cadangan terhadap arsip awan yang sama, batalkan rencana proteksi secara manual dari beban kerja yang saat ini berstatus **Failover**. Untuk informasi lebih lanjut tentang mencabut rencana, lihat Mencabut rencana proteksi.

Penting
Anda harus membuat server pemulihan lebih dulu untuk melindungi perangkat dari bencana.

Anda dapat melakukan failover hanya dari titik pemulihan yang dibuat setelah server pemulihan perangkat dibuat.

Setidaknya satu titik pemulihan harus dibuat sebelum gagal pada server pemulihan. Jumlah maksimum titik pemulihan yang didukung adalah 100.

Anda dapat mengikuti instruksi di bawah ini atau menonton tutorial video.

Untuk melakukan failover

© Acronis International GmbH, 2003-2024

1. Pastikan mesin asli tidak tersedia di jaringan.
2. Di konsol Cyber Protect, buka **Pemulihan bencana** > **Server** > **Server pemulihan** lalu pilih server pemulihan.
3. Klik **Failover**.
4. Pilih jenis failover **Failover produksi**.
5. Pilih titik pemulihan (cadangan), lalu klik **Mulai**.
6. [Jika cadangan yang Anda pilih dienkripsi menggunakan enkripsi sebagai properti mesin]
   a. Masukkan kata sandi enkripsi untuk kumpulan cadangan.

      Catatan
      Kata sandi hanya akan disimpan sementara dan hanya akan digunakan untuk operasi failover saat ini. Kata sandi secara otomatis dihapus dari penyimpanan kredensial setelah operasi failover selesai dan server kembali ke status **Siaga**.

   b. [Opsional] Untuk menyimpan kata sandi kumpulan cadangan dan menggunakannya dalam operasi failover berikutnya, pilih kotak centang **Simpan kata sandi di penyimpanan kredensial aman...** lalu, di bidang **Nama kredensial**, masukkan nama untuk kredensial.

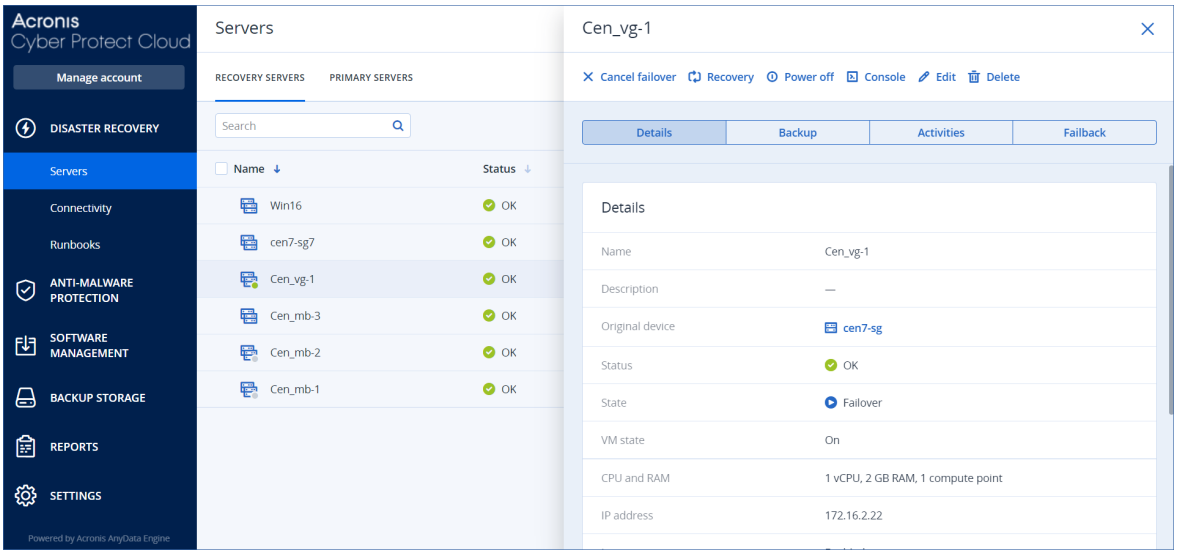
      Penting
      Kata sandi akan disimpan di penyimpanan kredensial aman dan akan diterapkan secara otomatis dalam operasi failover berikutnya. Namun, menyimpan kata sandi mungkin bertentangan dengan kewajiban Anda untuk patuh.

   c. Klik **Selesai**.

   Ketika server pemulihan dimulai, statusnya berubah menjadi **Finalisasi**, dan setelah beberapa saat akan menjadi **Failover.**

Penting
Penting untuk memahami bahwa server tersedia di status **Finalisasi** dan **Failover**. Selama **Finalisasi**, Anda dapat mengakses konsol server dengan mengeklik tautan **Konsol telah siap**. Tautan tersedia di kolom **Status VM** di layar **Pemulihan Bencana** > **Server**, dan di tampilan **Detail** server. Untuk detail, lihat "Cara kerja failover" (hlm. 779).

© Acronis International GmbH, 2003-2024



7. Pastikan server pemulihan dimulai dengan melihat konsolnya. Klik **Pemulihan Bencana** > **Server**, pilih server pemulihan, lalu klik **Konsol**.
8. Pastikan server pemulihan dapat diakses menggunakan alamat IP produksi yang Anda tentukan ketika membuat server pemulihan.

Setelah server pemulihan difinalisasi, rencana proteksi baru akan dibuat dan diterapkan secara otomatis pada server pemulihan. Rencana proteksi ini didasarkan pada rencana proteksi yang digunakan untuk membuat server pemulihan, dengan batasan tertentu. Dalam rencana ini, Anda hanya dapat mengubah jadwal dan aturan retensi. Untuk informasi lebih lanjut, lihat "Mencadangkan server awan".

Jika Anda ingin membatalkan failover, pilih server pemulihan dan klik **Batalkan failover**. Semua perubahan mulai dari momen failover - kecuali cadangan server pemulihan - akan hilang. Server pemulihan akan kembali ke status **Siaga**.

Jika Anda ingin melakukan failback, pilih server pemulihan dan klik **Failback**.

Cara menjalankan failover server menggunakan DNS lokal

Jika Anda menggunakan server DNS pada situs lokal untuk menyelesaikan nama mesin, maka setelah server pemulihan mengalami failover, sesuai dengan mesin yang diandalkan di DNS, akan gagal berkomunikasi karena server DNS yang digunakan di awan berbeda. Secara default, server DNS di situs awan digunakan untuk server awan yang baru dibuat. Jika Anda perlu menerapkan pengaturan DNS khusus, hubungi tim dukungan.

Cara menjalankan failover server DHCP

Infrastruktur lokal Anda mungkin memiliki server DHCP yang terletak di host Windows atau Linux. Jika host tersebut failover ke situs awan, muncul masalah duplikasi server DHCP karena gateway VPN di awan juga menjalankan peran DHCP. Untuk menyelesaikan masalah ini, lakukan salah satu langkah berikut:

© Acronis International GmbH, 2003-2024

- Jika hanya host DHCP yang mengalami failover ke awan, sedangkan server lokal lainnya masih berada di situs lokal, maka Anda harus masuk ke host DHCP di awan dan mematikan server DHCP di sana. Dengan demikian, tidak akan ada konflik dan hanya gateway VPN yang akan bekerja sebagai server DHCP.
- Jika server awan Anda sudah memiliki alamat IP dari host DHCP, Anda harus masuk ke host DHCP di awan dan matikan server DHCP di sana. Anda harus masuk ke server awan dan perbarui sewa DHCP untuk menetapkan alamat IP baru yang dialokasikan dari server DHCP yang benar (di-host di gateway VPN).

Catatan
Instruksi tidak valid jika server DHCP awan Anda dikonfigurasi dengan opsi **DHCP Kustom** dan beberapa server pemulihan atau utama mendapatkan alamat IP dari server DHCP ini.

Cara kerja failback

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Failback adalah proses pemindahan beban kerja dari awan kembali ke mesin fisik atau mesin virtual di situs lokal Anda. Anda dapat melakukan failback di server pemulihan dalam kondisi **Failover**, dan terus menggunakan server di situs lokal Anda.

Anda dapat melakukan failover otomatis ke mesin target virtual atau fisik di situs lokal Anda. Selama failback, Anda dapat mentransfer data cadangan ke situs lokal Anda sementara mesin virtual di cloud terus berjalan. Teknologi ini memungkinkan periode waktu henti yang sangat singkat, yang diperkirakan dan ditampilkan di konsol Cyber Protect. Anda dapat melihatnya dan menggunakan informasi ini untuk merencanakan aktivitas, dan jika perlu, memperingatkan klien tentang periode waktu henti yang akan datang.

Proses failback ke target mesin virtual dan target mesin fisik sedikit berbeda. Untuk informasi lebih lanjut tentang tahapan proses failback, lihat "Failback ke target mesin virtual" (hlm. 788) dan "Failback ke mesin fisik target" (hlm. 792).

Dalam kasus tertentu, ketika Anda tidak dapat menggunakan prosedur failback otomatis, Anda dapat melakukan failback manual. Untuk informasi lebih lanjut, lihat "Kegagalan manual" (hlm. 796).

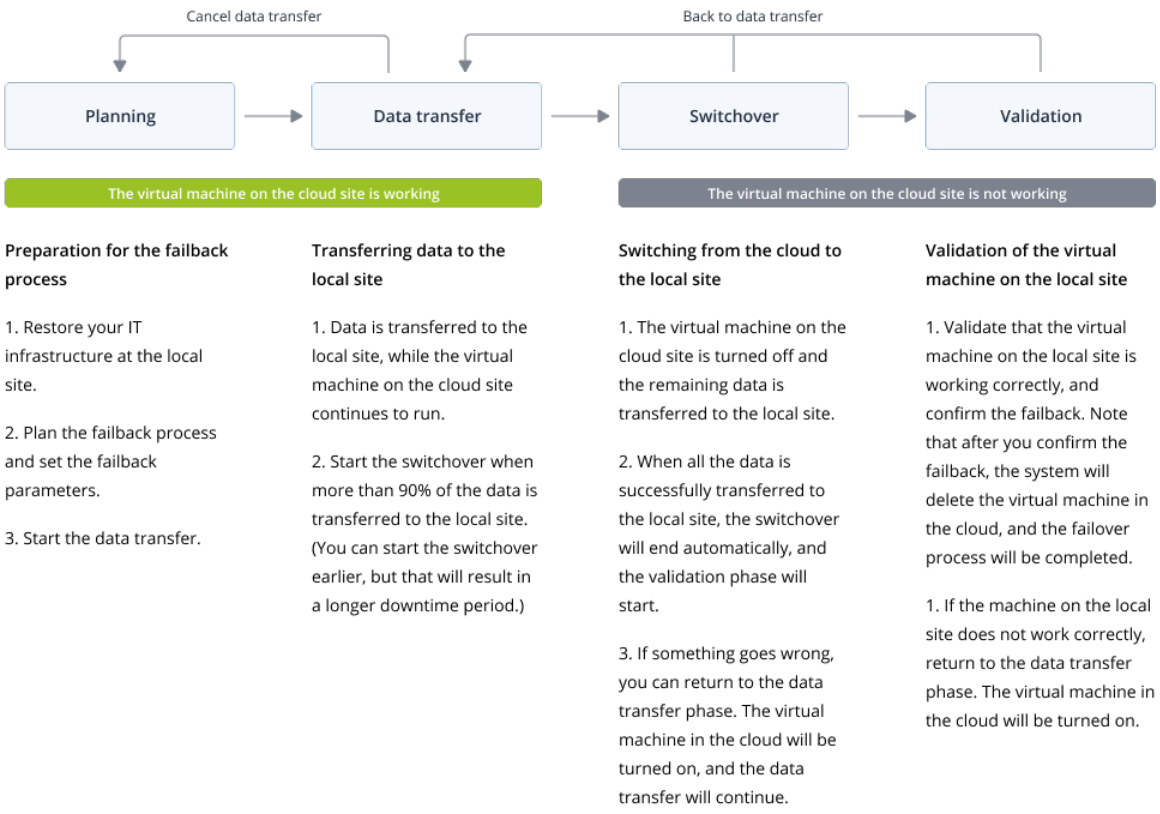
Catatan
Operasi runbook hanya mendukung failback dalam mode manual. Artinya, jika Anda memulai proses failback dengan menjalankan runbook yang menyertakan langkah **Me-restore otomatis server**, prosedurnya akan memerlukan interaksi manual: Anda harus memulihkan mesin secara manual, dan mengonfirmasi atau membatalkan proses failback dari Tab **Pemulihan Bencana** > **Server**.

© Acronis International GmbH, 2003-2024

Failback ke target mesin virtual

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Proses failback ke target mesin virtual terdiri dari empat tahap.



1. **Perencanaan**. Selama fase ini, Anda memulihkan infrastruktur IT di situs lokal Anda (seperti host dan konfigurasi jaringan), mengonfigurasi parameter failback, dan merencanakan kapan memulai transfer data.

   Catatan
   Untuk meminimalkan total waktu proses failback, Anda sebaiknya memulai fase transfer data segera setelah Anda menyiapkan server lokal, lalu melanjutkannya dengan konfigurasi jaringan dan infrastruktur lokal lainnya selama fase transfer data.

2. **Transfer data**. Pada tahap ini, data ditransfer dari situs awan ke situs lokal, sementara mesin virtual di awan terus berjalan. Anda dapat memulai fase berikutnya - peralihan - kapan saja selama fase transfer data, namun Anda harus mempertimbangkan hubungan berikut.
   Makin lama Anda berada pada tahap transfer data,

© Acronis International GmbH, 2003-2024

- semakin lama mesin virtual di cloud terus berjalan.
- semakin banyak data yang akan ditransfer ke situs lokal Anda.
- semakin tinggi biaya yang akan Anda bayarkan (Anda menghabiskan lebih banyak poin komputasi).
- makin singkat periode waktu henti yang akan Anda alami selama tahap peralihan.

Jika Anda ingin meminimalkan waktu henti, mulailah fase peralihan setelah lebih dari 90% data ditransfer ke situs lokal.

Jika tidak ada masalah dengan periode waktu henti yang lebih lama dan tidak ingin menghabiskan lebih banyak poin komputasi untuk menjalankan mesin virtual di awan, Anda dapat memulai tahap peralihan lebih awal.

Jika Anda membatalkan proses failback selama fase transfer data, data yang ditransfer tidak akan dihapus dari situs lokal. Untuk menghindari kemungkinan masalah, hapus data yang ditransfer secara manual sebelum Anda memulai proses failback baru. Proses transfer data berikut akan dimulai dari awal.

3. **Peralihan**. Selama fase ini, mesin virtual di cloud dinonaktifkan, dan data yang tersisa - termasuk penambahan cadangan terakhir - ditransfer ke situs lokal. Jika tidak ada rencana pencadangan yang diterapkan di server pemulihan, pencadangan akan dilakukan secara otomatis selama fase peralihan, yang akan memperlambat proses.

   Anda dapat melihat perkiraan waktu penyelesaian (periode waktu henti) tahap ini di konsol Cyber Protect. Ketika semua data sudah ditransfer ke situs lokal (tidak ada kehilangan data dan mesin virtual di situs lokal adalah salinan persis mesin virtual di awan), fase peralihan selesai. Mesin virtual di situs lokal dipulihkan, dan fase validasi otomatis dimulai.
4. **Validasi**. Selama fase ini, mesin virtual di situs lokal sudah siap dan secara otomatis dimulai. Anda dapat memeriksa apakah mesin virtual bekerja dengan benar, dan:
   - Jika semuanya berfungsi sesuai ekspektasi, konfirmasi failback. Setelah konfirmasi failback, mesin virtual di awan akan dihapus, dan server pemulihan kembali ke kondisi **Siaga**. Tahap ini adalah akhir dari proses failback.
   - Jika terjadi masalah, Anda dapat membatalkan peralihan dan kembali ke tahap transfer data.

Melakukan failback ke mesin virtual

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Anda dapat melakukan failback ke target mesin virtual di situs lokal Anda.

Prasyarat

- Agen yang akan Anda gunakan untuk melakukan failback sedang online dan sedang tidak digunakan untuk operasi failback lainnya.
- Koneksi Internet Anda stabil.
- Setidaknya ada satu cadangan penuh mesin virtual di cloud.

© Acronis International GmbH, 2003-2024

Untuk melakukan failback ke mesin virtual

1. Di konsol Cyber Protect, buka **Pemulihan bencana** > **Server**.
2. Pilih server pemulihan yang ada dalam status **Failover**.
3. Klik tab **Failback**.
4. Di bagian **Parameter failback**, pilih **Mesin virtual** sebagai **Target**, lalu konfigurasi parameter lainnya.

   Perlu diperhatikan bahwa secara default, beberapa **Parameter failback** diisi secara otomatis dengan nilai yang disarankan, tetapi Anda dapat mengubahnya.

   Tabel berikut ini memberikan informasi lebih lanjut tentang **Parameter failback**.

Parameter	Deskripsi
Ukuran cadangan	Jumlah data yang akan ditransfer ke situs lokal Anda selama proses failback. Setelah Anda memulai proses failback ke target mesin virtual, **Ukuran cadangan** akan meningkat selama fase transfer data, karena mesin virtual di awan akan terus berjalan dan menghasilkan data baru. Untuk menghitung estimasi waktu henti selama proses failback ke target mesin virtual, ambil 10% dari nilai **Ukuran cadangan** (sebagaimana saran kami untuk memulai fase peralihan setelah 90% data ditransfer ke situs lokal Anda) dan bagi dengan nilai kecepatan Internet Anda. **Catatan** Nilai kecepatan Internet akan berkurang saat Anda menjalankan beberapa proses failback pada saat yang sama.
Target	Jenis beban kerja di situs lokal Anda yang akan menjadi tujuan Anda memulihkan server awan: **Mesin virtual** atau **Mesin fisik**.
Lokasi mesin target	Lokasi failback: host VMware ESXi atau host Microsoft Hyper-V. Anda dapat memilih dari semua host yang memiliki agen yang terdaftar dengan layanan Perlindungan Cyber.
Agen	Agen yang akan melakukan operasi failback. Anda dapat menggunakan satu agen untuk melakukan satu operasi failback di waktu yang sama. Anda dapat memilih agen yang sedang online dan sedang tidak digunakan untuk proses failback lainnya, memiliki versi yang mendukung fungsionalitas failback, dan memiliki hak untuk mengakses cadangan. Perlu diketahui bahwa Anda dapat menginstal beberapa agen pada host VMware ESXi, dan memulai proses failback yang terpisah menggunakan setiap agen. Proses failback ini dapat dilakukan secara bersamaan.
Pengaturan mesin target	Pengaturan mesin virtual: • **Prosesor virtual**. Pilih jumlah prosesor virtual.

© Acronis International GmbH, 2003-2024

Parameter	Deskripsi
	• **Memori**. Pilih berapa banyak memori yang akan dimiliki mesin virtual. • **Unit**. Pilih unit untuk memori. • [Opsional] **Adaptor jaringan**. Untuk menambahkan adaptor jaringan, klik **Tambah**, lalu pilih jaringan di kolom **Jaringan**. Jika Anda sudah siap dengan perubahan tersebut, klik **Selesai**.
Jalur	(Untuk host Microsoft Hyper-V) Folder di host tempat mesin Anda akan disimpan. Pastikan ada cukup ruang memori yang kosong pada host untuk mesin tersebut.
Penyimpanan data	(Untuk host VMware ESXi) Penyimpanan data di host tempat mesin Anda akan disimpan. Pastikan ada cukup ruang memori yang kosong pada host untuk mesin tersebut.
Mode provisi	Metode alokasi disk virtual. Untuk host Microsoft Hyper-V: • **Bertambah secara dinamis** (nilai default). • **Ukuran tetap**. Untuk host Microsoft Hyper-V: • **Tipis** (nilai default). • **Tebal**.
Nama mesin target	Nama mesin target. Secara default, nama mesin target sama dengan nama server pemulihan. Nama mesin target harus unik pada **Lokasi mesin target** yang dipilih.

5. Klik **Mulai transfer data**, lalu di jendela konfirmasi, klik **Mulai**.

Catatan
Jika tidak ada cadangan dari mesin virtual di cloud, sistem akan melakukan pencadangan secara otomatis sebelum fase transfer data.

Tahap **Transfer data** dimulai. Konsol menampilkan informasi berikut:

Bidang	Deskripsi
Progres	Parameter ini menunjukkan berapa banyak data yang telah ditransfer ke situs lokal, dan jumlah total data yang harus ditransfer. Jumlah total data mencakup data dari cadangan terakhir sebelum fase transfer data dimulai dan cadangan dari data yang baru dibuat (peningkatan cadangan), karena mesin virtual terus berjalan selama fase transfer data. Oleh karena itu, kedua nilai parameter **Progres** meningkat seiring waktu.

© Acronis International GmbH, 2003-2024

Bidang	Deskripsi
Estimasi waktu henti	Parameter ini menunjukkan berapa lama mesin virtual di cloud tidak akan tersedia jika Anda memulai fase peralihan sekarang. Nilai dihitung berdasarkan nilai parameter **Progres**, dan menurun seiring waktu.

6. Klik **Peralihan** lalu, di jendela konfirmasi, klik **Peralihan** lagi.

   Tahap peralihan dimulai. Konsol menampilkan informasi berikut:

Bidang	Deskripsi
Progres	Parameter ini menunjukkan kemajuan pemulihan mesin di situs lokal.
Perkiraan waktu penyelesaian	Parameter ini menunjukkan perkiraan waktu kapan fase peralihan akan selesai dan Anda akan dapat menghidupkan mesin di situs lokal.

Catatan
Jika tidak ada rencana pencadangan yang diterapkan pada mesin virtual di awan, pencadangan akan dilakukan secara otomatis pada fase peralihan, yang akan memperpanjang waktu henti.

7. Setelah fase **Switchover** selesai dan mesin virtual di situs lokal Anda dimulai secara otomatis, lakukan validasi bahwa sistem berfungsi sesuai yang diharapkan.
8. Klik **Konfirmasi failback**, lalu di jendela konfirmasi, klik **Konfirmasi** untuk menyelesaikan proses.

   Mesin virtual di awan dihapus, dan server pemulihan kembali ke kondisi **Siaga**.

Catatan
Menerapkan rencana proteksi di server yang dipulihkan bukan bagian dari proses failback. Setelah proses failback selesai, terapkan rencana proteksi pada server yang dipulihkan untuk memastikan bahwa ia dilindungi kembali. Anda dapat menerapkan rencana proteksi yang sama dengan yang diterapkan pada server asli, atau rencana proteksi baru yang telah mengaktifkan modul **Pemulihan Bencana**.

Failback ke mesin fisik target

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Proses failback otomatis ke mesin fisik target terdiri dari fase berikut:

1. **Perencanaan**. Selama fase ini, Anda memulihkan infrastruktur IT di situs lokal Anda (seperti host dan konfigurasi jaringan), mengonfigurasi parameter failback, dan merencanakan kapan memulai transfer data.
2. **Transfer data**. Pada tahap ini, data ditransfer dari situs awan ke situs lokal, sementara mesin virtual di awan terus berjalan. Anda dapat memulai fase berikutnya - peralihan - kapan saja

© Acronis International GmbH, 2003-2024

selama fase transfer data, namun Anda harus mempertimbangkan hubungan berikut.

Makin lama Anda berada pada tahap transfer data,

- semakin lama mesin virtual di cloud terus berjalan.
- semakin banyak data yang akan ditransfer ke situs lokal Anda.
- semakin tinggi biaya yang akan Anda bayarkan (Anda menghabiskan lebih banyak poin komputasi).
- makin singkat periode waktu henti yang akan Anda alami selama tahap peralihan.

Jika Anda ingin meminimalkan waktu henti, mulailah fase peralihan setelah lebih dari 90% data ditransfer ke situs lokal.

Jika tidak ada masalah dengan periode waktu henti yang lebih lama dan tidak ingin menghabiskan lebih banyak poin komputasi untuk menjalankan mesin virtual di awan, Anda dapat memulai tahap peralihan lebih awal.

Catatan

Proses transfer datanya menggunakan teknologi flashback. Teknologi ini membandingkan data yang tersedia di mesin target dengan data mesin virtual di cloud. Jika sebagian sudah tersedia di mesin target, maka data tidak akan ditransfer lagi. Teknologi ini membuat fase transfer data menjadi lebih cepat.

Karena alasan ini, kami menyarankan Anda memulihkan server ke mesin asli di situs lokal Anda.

3. **Peralihan**. Selama fase ini, mesin virtual di cloud dinonaktifkan, dan data yang tersisa - termasuk penambahan cadangan terakhir - ditransfer ke situs lokal. Jika tidak ada rencana pencadangan yang diterapkan di server pemulihan, pencadangan akan dilakukan secara otomatis selama fase peralihan, yang akan memperlambat proses.
4. **Validasi**. Selama fase ini, mesin fisik di situs lokal sudah siap, dan Anda dapat melakukan boot ulang menggunakan media yang dapat di-boot berbasis Linux. Anda dapat memverifikasi apakah mesin virtual berfungsi dengan benar, dan:
   - Jika semuanya berfungsi sesuai ekspektasi, konfirmasi failback. Setelah konfirmasi failback, mesin virtual di awan akan dihapus, dan server pemulihan kembali ke kondisi **Siaga**. Tahap ini adalah akhir dari proses failback.
   - Jika terjadi masalah, Anda dapat membatalkan failover dan kembali ke fase perencanaan.

Catatan

Setelah melakukan boot ulang pada media yang dapat di-boot, Anda tidak akan dapat menggunakannya lagi. Jika selama fase validasi Anda menemukan masalah, Anda harus mendaftarkan media yang dapat di-boot yang baru, serta memulai kembali proses failback.

Akan tetapi, seiring dengan digunakannya teknologi flashback, data yang sudah ada di situs lokal tidak akan ditransfer lagi dan proses failback akan jauh lebih cepat.

© Acronis International GmbH, 2003-2024

Melakukan failback ke mesin fisik

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Anda dapat melakukan failback otomatis ke mesin fisik target di situs lokal Anda.

Catatan
Proses transfer datanya menggunakan teknologi flashback. Teknologi ini membandingkan data yang tersedia di mesin target dengan data mesin virtual di cloud. Jika sebagian sudah tersedia di mesin target, maka data tidak akan ditransfer lagi. Teknologi ini membuat fase transfer data menjadi lebih cepat.

Karena alasan ini, kami menyarankan Anda memulihkan server ke mesin asli di situs lokal Anda.

Prasyarat

- Agen yang akan Anda gunakan untuk melakukan failback sedang online dan sedang tidak digunakan untuk operasi failback lainnya.
- Koneksi Internet Anda stabil.
- Tersedia media yang dapat di-boot dan terdaftar. Untuk informasi lebih lanjut, lihat "Membuat media yang dapat di-boot untuk memulihkan sistem operasi" di Cyber Protection Panduan Pengguna.
- Mesin fisik target adalah mesin asli di situs lokal Anda, atau memiliki firmware yang sama dengan mesin asli.
- Setidaknya ada satu cadangan penuh mesin virtual di cloud.

Untuk melakukan failback ke mesin fisik

1. Di konsol Cyber Protect, buka **Pemulihan bencana** > **Server**.
2. Pilih server pemulihan yang ada dalam status **Failover**.
3. Klik tab **Failback**.
4. Di bidang **Target**, pilih **Mesin fisik**.
5. Dalam bidang **Target media yang dapat di-boot**, klik **Tentukan**, pilih media yang dapat di-boot, lalu klik **Selesai**.

   Catatan
   Anda sebaiknya menggunakan media yang dapat di-boot dan sudah jadi karena sudah dikonfigurasi. Untuk informasi lebih lanjut, lihat "Membuat media yang dapat di-boot untuk memulihkan sistem operasi" di Cyber Protection Panduan Pengguna.

6. [Opsional] Untuk mengubah pemetaan disk default, pada bidang **Pemetaan disk**, klik **Tentukan**, petakan disk cadangan ke disk mesin target, lalu klik **Selesai**.

© Acronis International GmbH, 2003-2024

7. Klik **Mulai transfer data** lalu, di jendela konfirmasi, klik **Mulai**.

   Catatan
   Jika tidak ada cadangan dari mesin virtual di cloud, sistem akan melakukan pencadangan secara otomatis sebelum fase transfer data.

   Fase transfer data dimulai. Konsol menampilkan informasi berikut:

Bidang	Deskripsi
Progres	Parameter ini menunjukkan berapa banyak data yang telah ditransfer ke situs lokal, dan jumlah total data yang harus ditransfer. Jumlah total data mencakup data dari cadangan terakhir sebelum fase transfer data dimulai dan cadangan dari data yang baru dibuat (peningkatan cadangan), karena mesin virtual terus berjalan selama fase transfer data. Oleh karena itu, nilai **Progres** meningkat seiring waktu. Karena sistem menggunakan teknologi flashback selama transfer data dan tidak mentransfer data yang sudah tersedia di mesin target, kemajuannya mungkin lebih cepat daripada yang dihitung pada awal oleh konsol.
Estimasi waktu henti	Parameter ini menunjukkan berapa lama mesin virtual di cloud tidak akan tersedia jika Anda memulai fase peralihan sekarang. Nilai dihitung berdasarkan nilai parameter **Progres**, dan menurun seiring waktu. Karena sistem menggunakan teknologi flashback selama transfer data dan tidak mentransfer data yang sudah tersedia di mesin target, waktu henti mungkin jauh lebih singkat daripada nilai yang awalnya ditampilkan di konsol.

8. Klik **Peralihan** lalu, di jendela konfirmasi, klik **Peralihan** lagi.
   Tahap peralihan dimulai. Konsol menampilkan informasi berikut:

Bidang	Deskripsi
Progres	Parameter ini menunjukkan kemajuan pemulihan mesin di situs lokal.
Perkiraan waktu penyelesaian	Parameter ini menunjukkan perkiraan waktu kapan fase peralihan akan selesai dan Anda akan dapat menghidupkan mesin di situs lokal.

   Catatan
   Jika tidak ada rencana pencadangan yang diterapkan pada mesin virtual di awan, pencadangan akan dilakukan secara otomatis pada fase peralihan, yang akan memperpanjang waktu henti.

9. Setelah fase **Peralihan** selesai, boot ulang media yang dapat di-boot, lalu verifikasi bahwa mesin fisik di situs lokal Anda berfungsi seperti yang diharapkan.
   Untuk informasi lebih lanjut, lihat "Memulihkan disk menggunakan media yang dapat di-boot" di Cyber Protection Panduan Pengguna.
10. Klik **Konfirmasi failback** lalu, di jendela konfirmasi, klik **Konfirmasi** untuk menyelesaikan prosesnya.

© Acronis International GmbH, 2003-2024

Mesin virtual di awan dihapus, dan server pemulihan kembali ke kondisi **Siaga**.

Catatan
Menerapkan rencana proteksi di server yang dipulihkan bukan bagian dari proses failback. Setelah proses failback selesai, terapkan rencana proteksi pada server yang dipulihkan untuk memastikan bahwa ia dilindungi kembali. Anda dapat menerapkan rencana proteksi yang sama dengan yang diterapkan pada server asli, atau rencana proteksi baru yang telah mengaktifkan modul **Pemulihan Bencana**.

Kegagalan manual

Catatan
Anda sebaiknya menggunakan proses failback dalam mode manual hanya jika Anda disarankan melakukannya oleh tim Dukungan.

Anda juga dapat memulai proses failback dalam mode manual. Dalam hal ini, transfer data dari cadangan di cloud ke situs lokal tidak akan dilakukan secara otomatis. Hal ini harus dilakukan secara manual setelah mesin virtual di cloud dimatikan. Hal ini membuat proses failback dalam mode manual jauh lebih lambat, dan periode waktu henti akan lebih lama.

Proses failback dalam mode manual terdiri dari fase berikut:

1. **Perencanaan**. Selama fase ini, Anda memulihkan infrastruktur IT di situs lokal Anda (seperti host dan konfigurasi jaringan), mengonfigurasi parameter failback, dan merencanakan kapan memulai transfer data.
2. **Peralihan**. Selama fase ini, mesin virtual di cloud dinonaktifkan, dan data yang baru dibuat dicadangkan. Jika tidak ada rencana pencadangan yang diterapkan di server pemulihan, pencadangan akan dilakukan secara otomatis selama fase peralihan, yang akan memperlambat proses. Saat pencadangan selesai, Anda memulihkan mesin ke situs lokal secara manual. Anda dapat memulihkan disk menggunakan media yang dapat di-boot, atau memulihkan seluruh mesin dari penyimpanan cadangan awan.
3. **Validasi**. Selama fase ini, Anda memverifikasi bahwa mesin fisik atau virtual di situs lokal berfungsi dengan benar, dan mengonfirmasi failback. Setelah konfirmasi, mesin virtual di situs awan akan dihapus dan server pemulihan kembali ke kondisi **Siaga**.

Melakukan failback manual

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Anda dapat melakukan failback manual ke mesin fisik atau virtual target di situs lokal Anda.

Untuk melakukan failback manual

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Pemulihan bencana** > **Server**.
2. Pilih server pemulihan yang ada dalam status **Failover**.
3. Klik tab **Failback**.
4. Di bidang **Target**, pilih **Mesin fisik**.
5. Klik ikon roda gigi, lalu aktifkan tombol alih **Gunakan mode manual**.
6. [Opsional] Hitung estimasi waktu henti selama proses failback dengan membagi nilai **ukuran Cadangan** dengan nilai kecepatan Internet Anda.

   Catatan
   Nilai kecepatan Internet akan berkurang saat Anda menjalankan beberapa proses failback pada saat yang sama.

7. Klik **Peralihan**, lalu di jendela konfirmasi, klik **Peralihan** lagi.
   Mesin virtual di situs awan akan dinonaktifkan.

   Catatan
   Jika tidak ada rencana pencadangan yang diterapkan pada mesin virtual di awan, pencadangan akan dilakukan secara otomatis pada fase peralihan, yang akan memperpanjang waktu henti.

8. Pulihkan server dari cadangan cloud ke mesin fisik atau virtual di situs lokal Anda. Untuk informasi lebih lanjut, lihat "Memulihkan mesin" di Cyber Protection Panduan Pengguna.
9. Pastikan pemulihan sudah selesai dan mesin yang dipulihkan berfungsi dengan baik, lalu klik **Mesin dipulihkan**.
10. Jika semuanya sudah berfungsi seperti yang diharapkan, klik **Konfirmasi failback**, lalu di jendela konfirmasi, klik **Konfirmasi** lagi.
    Server pemulihan dan titik pemulihan akan siap untuk failover berikutnya. Untuk membuat titik pemulihan baru, terapkan rencana proteksi pada server lokal.

    Catatan
    Menerapkan rencana proteksi di server yang dipulihkan bukan bagian dari proses failback. Setelah proses failback selesai, terapkan rencana proteksi pada server yang dipulihkan untuk memastikan bahwa ia dilindungi kembali. Anda dapat menerapkan rencana proteksi yang sama dengan yang diterapkan pada server asli, atau rencana proteksi baru yang telah mengaktifkan modul **Pemulihan Bencana**.

Bekerja dengan cadangan yang dienkripsi

Anda dapat membuat server pemulihan dari cadangan yang dienkripsi. Guna memudahkan Anda, Anda dapat mengatur aplikasi kata sandi otomatis untuk cadangan yang dienkripsi selama failover pada server pemulihan.

Saat membuat server pemulihan, Anda dapat menentukan kata sandi yang akan digunakan untuk operasi pemulihan bencana otomatis. Kata sandi tersebut akan disimpan di penyimpanan

© Acronis International GmbH, 2003-2024

Kredensial, penyimpanan yang aman untuk kredensial yang dapat ditemukan di bagian **Pengaturan** > **Kredensial**.

Satu kredensial dapat ditautkan ke beberapa cadangan.

Untuk mengelola kata sandi yang disimpan di Penyimpanan kredensial

1. Buka **Pengaturan** > **Kredensial**.
2. Untuk mengelola kredensial tertentu, klik ikon di kolom terakhir. Anda dapat melihat item-item yang ditautkan dengan kredensial ini.
   - Untuk membatalkan tautan cadangan dari kredensial yang dipilih, klik ikon kotak sampah di dekat cadangan. Hasilnya, Anda harus membuat kata sandi secara manual selama failover ke server pemulihan.
   - Untuk mengedit kredensial, klik **Edit**, lalu tentukan nama atau kata sandi.
   - Untuk menghapus kredensial, klik **Hapus**. Perhatikan bahwa Anda harus membuat kata sandi secara manual selama failover ke server pemulihan.

Operasi dengan mesin virtual Microsoft Azure

Catatan
Beberapa fitur mungkin memerlukan pelisensian tambahan sesuai model pelisensian yang diterapkan.

Anda dapat melakukan failover mesin virtual Microsoft Azure ke Acronis Cyber Protect Awan. Untuk informasi lebih lanjut, lihat "Melakukan failover" (hlm. 784).

Setelah itu, Anda dapat melakukan fallback dari Acronis Cyber Protect Awan kembali ke mesin virtual Azure. Proses failbacknya sama dengan proses failback ke mesin fisik. Untuk informasi lebih lanjut, lihat "Prasyarat" (hlm. 794).

Catatan
Untuk mendaftarkan mesin virtual Azure baru untuk fallback, Anda dapat menggunakan ekstensi VM Cadangan Acronis yang tersedia di Azure.

Anda dapat mengonfigurasikan konektivitas VPN IPsec Multisitus antara Acronis Cyber Protect Awan dan gateway VPN Azure. Untuk informasi lebih lanjut, lihat "Mengonfigurasi VPN IPsec Multi-situs" (hlm. 753).

Mengatur server utama

Bagian ini menjelaskan cara membuat dan mengelola server utama Anda.

© Acronis International GmbH, 2003-2024

Membuat server utama

Prasyarat

- Salah satu jenis konektivitas ke situs awan harus diatur.

Untuk membuat server utama

1. Buka tab **Pemulihan Bencana** > **Server** > **Server utama**.
2. Klik **Buat**.
3. Pilih templat untuk mesin virtual yang baru.
4. Pilih jenis konfigurasi (jumlah inti virtual dan ukuran RAM). Tabel berikut menampilkan jumlah total maksimum ruang disk (GB) untuk setiap jenis.

Tipe	vCPU	RAM (GB)	Jumlah total maksimum ruang disk (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

Catatan
Anda dapat melihat titik komputasi untuk setiap opsi. Jumlah titik komputasi menunjukkan biaya pengoperasian server utama per jam. Untuk informasi lebih lanjut, lihat "Titik komputasi" (hlm. 734).

5. [Opsional] Ganti ukuran disk virtual. Jika Anda membutuhkan lebih dari satu hard disk, klik **Tambah disk**, lalu tentukan ukuran disk yang baru. Saat ini, Anda dapat menambahkan tidak lebih dari 10 disk untuk server utama.
6. Tentukan jaringan awan yang padanya server utama akan dimasukkan.
7. Pilih opsi **DHCP**.

Opsi DHCP	Deskripsi
Disediakan oleh situs awan	Pengaturan default. Alamat IP server akan diberikan oleh server DHCP yang dikonfigurasi secara otomatis di awan.

© Acronis International GmbH, 2003-2024

Opsi DHCP	Deskripsi
Kustom	Alamat IP server akan diberikan oleh server DHCP Anda sendiri di awan.

8. [Opsional] Tentukan **Alamat MAC**.

   Alamat MAC adalah pengidentifikasi unik yang ditetapkan ke adaptor jaringan server. Jika menggunakan DHCP kustom, Anda dapat mengonfigurasinya untuk selalu menetapkan alamat IP tertentu ke alamat MAC tertentu. Tindakan ini memastikan bahwa server utama selalu mendapatkan alamat IP yang sama. Anda dapat menjalankan aplikasi yang memiliki lisensi yang terdaftar dengan alamat MAC.
9. Tentukan alamat IP yang akan dimiliki server dalam jaringan produksi. Secara default, alamat IP gratis pertama dari jaringan produksi Anda telah diatur.

   Catatan

   Jika Anda menggunakan server DHCP, tambahkan alamat IP ini ke daftar pengecualian server untuk menghindari konflik alamat IP.

   Jika menggunakan server DHCP kustom, Anda harus menentukan alamat IP yang sama di **alamat IP di jaringan produksi** seperti yang dikonfigurasi di server DHCP. Jika tidak, uji failover tidak akan berfungsi dengan baik dan server tidak akan dapat dijangkau melalui alamat IP publik.
10. [Opsional] Pilih kotak centang **Akses internet**.

    Pilihan ini akan mengaktifkan server utama untuk mengakses internet. Secara default, port TCP 25 terbuka untuk koneksi keluar ke alamat IP publik.
11. [Opsional] Pilih kotak centang **Gunakan alamat IP publik**.

    Memiliki alamat IP publik membuat server utama tersedia dari internet. Jika Anda membiarkan kotak centang kosong, server hanya akan tersedia pada jaringan produksi Anda.

    Alamat IP publik akan ditampilkan setelah Anda menyelesaikan konfigurasi. Secara default, port TCP 443 terbuka untuk koneksi masuk ke alamat IP publik.

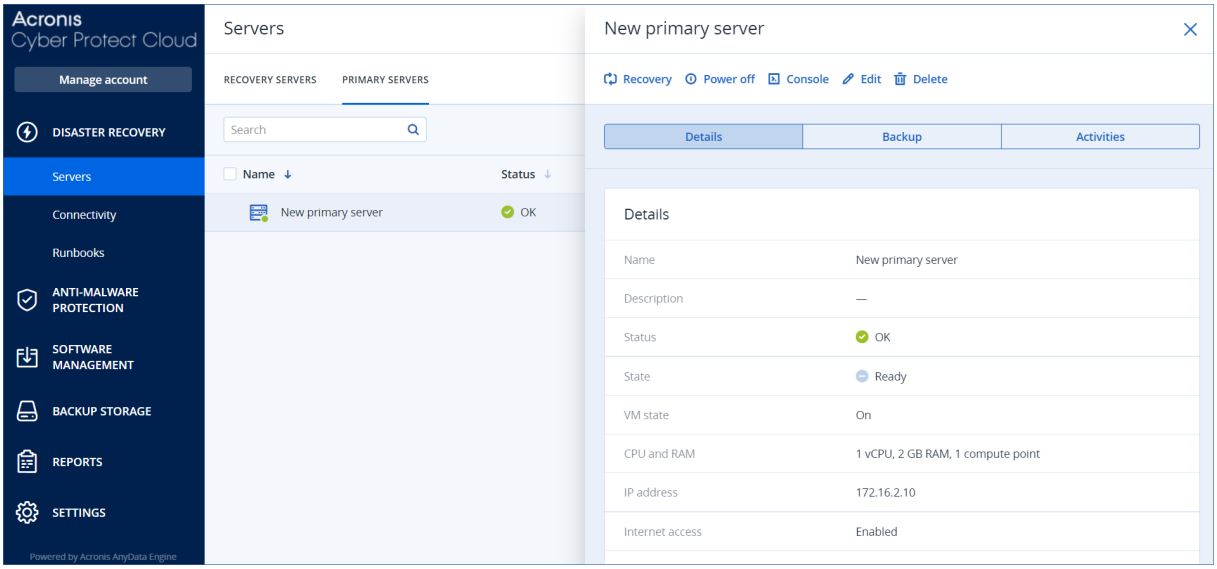
    Catatan

    Jika Anda menghapus kotak centang **Gunakan alamat IP publik** atau menghapus server pemulihan, alamat IP publiknya tidak akan terpesan.
12. [Opsional] Pilih **Tentukan ambang batas RPO**.

    Ambang batas RPO menentukan interval waktu maksimum yang diizinkan antara titik pemulihan dan waktu terkini. Nilai dapat diatur antara 15 – 60 menit, 1 – 24 jam, 1 – 14 hari.
13. Tentukan nama server utama.
14. [Opsional] Tentukan deskripsi untuk server utama.
15. [Opsional] Klik tab **Aturan firewall awan** untuk mengedit aturan firewall default. Untuk informasi lebih lanjut, lihat "Menetapkan aturan firewall untuk server awan" (hlm. 803).
16. Klik **Buat**.

© Acronis International GmbH, 2003-2024

Server utama kini tersedia di jaringan produksi. Anda dapat mengelola server menggunakan konsol, RDP, SSH, atau TeamViewer.



Operasi dengan server utama

Server utama muncul di tab **Pemulihan Bencana** > **Server** > **Server utama** di konsol Cyber Protect.

Untuk memulai atau menghentikan server, klik **Nyalakan** atau **Matikan** di panel server utama.

Untuk mengedit pengaturan server utama, hentikan server, lalu klik **Edit**.

Untuk menerapkan rencana proteksi pada server utama, pilih rencana tersebut dan pada tab **Rencana** klik **Buat**. Anda akan melihat rencana proteksi yang telah ditentukan sebelumnya di mana Anda hanya dapat mengubah jadwal dan aturan retensi. Untuk informasi lebih lanjut, lihat "Mencadangkan server awan".

Mengelola server awan

Untuk mengelola server awan, buka **Pemulihan Bencana** > **Server**. Terdapat dua tab di sana: **Server pemulihan** dan **Server utama**. Untuk menunjukkan semua kolom opsional dalam tabel, klik ikon roda gigi.

Anda dapat menemukan informasi berikut tentang setiap server awan dengan memilihnya.

Nama kolom	Deskripsi
Nama	Nama server awan yang Anda tentukan
Status	Status yang menunjukkan masalah paling parah pada server awan (berdasarkan peringatan aktif)
Keadaan	Kondisi server awan

© Acronis International GmbH, 2003-2024

Status VM	Kondisi kekuatan mesin virtual berkaitan dengan server awan
Lokasi aktif	Lokasi di mana server awan di-host. Misalnya, **Awan**.
Ambang batas RPO	Interval waktu maksimum yang diperbolehkan antara titik pemulihan terakhir yang tepat untuk failover dan waktu terkini. Nilai dapat diatur antara 15-60 menit, 1-24 jam, 1-14 hari.
Kepatuhan RPO	Kepatuhan RPO adalah rasio antara RPO aktual dan ambang batas RPO. Kepatuhan RPO ditampilkan jika ambang batas RPO ditentukan. Kepatuhan RPO dihitung dengan cara berikut: **Kepatuhan RPO = RPO Aktual / Ambang batas RPO** di mana **RPO aktual = waktu terkini – waktu titik pemulihan terakhir** **Status kepatuhan RPO** Bergantung pada nilai rasio antara RPO aktual dan ambang batas RPO, status berikut ini digunakan: • **Patuh**. Kepatuhan RPO < 1x. Server memenuhi ambang batas RPO. • **Melebihi**. Kepatuhan RPO <= 2x. Server melanggar ambang batas. • **Sangat melebihi**. Kepatuhan RPO <= 4x. Server melanggar ambang batas RPO lebih dari 2x. • **Jauh melebihi**. Kepatuhan RPO > 4x. Server melanggar ambang batas RPO lebih dari 4x. • **Menunda (tidak ada cadangan)**. Server dilindungi dengan rencana proteksi namun pencadangan sedang dilakukan dan belum selesai.
RPO aktual	Waktu yang berlalu sejak pembuatan titik pemulihan terakhir
Titik pemulihan terakhir	Tanggal dan waktu saat titik pemulihan terakhir dibuat

Aturan firewall untuk server awan

Anda dapat mengonfigurasi aturan firewall untuk mengontrol lalu lintas masuk dan keluar dari server utama dan pemulihan di situs awan Anda.

Anda dapat mengonfigurasi aturan masuk setelah menyediakan alamat IP publik untuk server awan. Secara default, port TCP 443 diizinkan, dan semua koneksi masuk lainnya ditolak. Anda dapat mengubah aturan firewall default, dan menambah atau menghapus pengecualian Masuk. Jika IP publik tidak disediakan, Anda hanya dapat melihat aturan masuk, tetapi tidak dapat mengonfigurasinya.

Anda dapat mengonfigurasi aturan keluar setelah saat menyediakan akses Internet untuk server awan. Secara default, port TCP 25 ditolak, dan semua koneksi keluar lainnya diizinkan. Anda dapat

© Acronis International GmbH, 2003-2024

mengubah aturan firewall default, dan menambah atau menghapus pengecualian keluar. Jika akses Internet tidak tersedia, Anda hanya dapat melihat aturan keluar, tetapi tidak dapat mengonfigurasinya.

Catatan
Untuk alasan keamanan, ada aturan firewall yang telah ditentukan sebelumnya yang tidak dapat Anda ubah.

Untuk koneksi masuk dan keluar:

- Ping izinkan: Permintaan ICMP echo (tipe 8, kode 0) dan balasan ICMP echo (tipe 0, kode 0)
- Permit ICMP perlu di-frag (tipe 3, kode 4)
- Permit TTL terlampaui (tipe 11, kode 0)

Hanya untuk koneksi masuk:

- Bagian yang tidak dapat dikonfigurasi: Tolak semua

Hanya untuk koneksi keluar:

- Bagian yang tidak dapat dikonfigurasi: Tolak semua

Menetapkan aturan firewall untuk server awan

Anda dapat mengedit aturan firewall default untuk server utama dan pemulihan di awan.

Untuk mengedit aturan firewall server di situs awan Anda

1. Di konsol Cyber Protect, buka **Pemulihan bencana** > **Server**.
2. Jika Anda ingin mengedit aturan firewall dari server pemulihan, klik tab **Server pemulihan**. Atau, jika Anda ingin mengedit aturan firewall dari server utama, klik tab **Server utama**.
3. Klik server, lalu klik **Edit**.
4. Klik tab **Aturan firewall awan**.
5. Jika Anda ingin mengubah tindakan default untuk koneksi masuk:

© Acronis International GmbH, 2003-2024

a. Di kolom drop-down **Masuk**, pilih tindakan default.

Tindakan	Deskripsi
Tolak semua	Menolak lalu lintas masuk apa pun. Anda dapat menambahkan pengecualian dan mengizinkan lalu lintas dari alamat IP, protokol, dan port tertentu.
Izinkan semua	Mengizinkan semua lalu lintas TCP dan UDP masuk. Anda dapat menambahkan pengecualian dan menolak lalu lintas dari alamat IP, protokol, dan port tertentu.

Catatan
Mengubah tindakan default membuat tidak valid dan menghapus konfigurasi aturan masuk yang sudah ada.

b. [Opsional] Jika Anda ingin menyimpan pengecualian yang ada, di jendela konfirmasi, pilih **Simpan pengecualian terisi**.

c. Klik **Konfirmasi**.

6. Jika Anda ingin menambahkan pengecualian:

a. Klik **Tambahkan pengecualian**.

b. Tentukan parameter firewall.

Parameter firewall	Deskripsi
Protokol	Pilih protokol untuk koneksi. Opsi berikut didukung: • **TCP** • **UDP** • **TCP+UDP**
Port server	Pilih port tempat aturan akan diterapkan. Anda dapat menentukan hal berikut: • nomor port spesifik (misalnya, `2298`) • rentang nomor port (misalnya, `6000-6700`) • nomor port apa pun. Gunakan `*` jika Anda ingin aturan berlaku untuk nomor port apa pun.
Alamat IP klien	Pilih alamat IP tempat aturan akan diterapkan. Anda dapat menentukan hal berikut: • alamat IP spesifik (misalnya `192.168.0.0`) • rentang alamat IP menggunakan notasi CIDR (misalnya, `192.168.0.0/24`) • alamat IP apa pun. Gunakan `*` jika Anda ingin aturan berlaku untuk alamat IP apa pun.

© Acronis International GmbH, 2003-2024

7. Jika Anda ingin menghapus pengecualian masuk yang ada, klik ikon tempat sampah di sebelahnya.
8. Jika Anda ingin mengubah tindakan default untuk koneksi keluar:
   a. Di kolom drop-down **Keluar**, pilih tindakan default.

Tindakan	Deskripsi
Tolak semua	Menolak lalu lintas keluar apa pun. Anda dapat menambahkan pengecualian dan mengizinkan lalu lintas ke alamat IP, protokol, dan port tertentu.
Izinkan semua	Mengizinkan semua lalu lintas keluar. Anda dapat menambahkan pengecualian dan menolak lalu lintas dari alamat IP, protokol, dan port tertentu.

Catatan
Mengubah tindakan default membuat tidak valid dan menghapus konfigurasi aturan keluar yang sudah ada.

   b. [Opsional] Jika Anda ingin menyimpan pengecualian yang ada, di jendela konfirmasi, pilih **Simpan pengecualian terisi**.
   c. Klik **Konfirmasi**.
9. Jika Anda ingin menambahkan pengecualian:
   a. Klik **Tambahkan pengecualian**.
   b. Tentukan parameter firewall.

Parameter firewall	Deskripsi
Protokol	Pilih protokol untuk koneksi. Opsi berikut didukung: • **TCP** • **UDP** • **TCP+UDP**
Port server	Pilih port tempat aturan akan diterapkan. Anda dapat menentukan hal berikut: • nomor port spesifik (misalnya, `2298`) • rentang nomor port (misalnya, `6000-6700`) • nomor port apa pun. Gunakan `*` jika Anda ingin aturan berlaku untuk nomor port apa pun.
Alamat IP klien	Pilih alamat IP tempat aturan akan diterapkan. Anda dapat menentukan hal berikut: • alamat IP spesifik (misalnya `192.168.0.0`) • rentang alamat IP menggunakan notasi CIDR (misalnya, `192.168.0.0/24`)

© Acronis International GmbH, 2003-2024

Parameter firewall	Deskripsi
	• alamat IP apa pun. Gunakan * jika Anda ingin aturan berlaku untuk alamat IP apa pun.

10. Jika Anda ingin menghapus pengecualian keluar yang ada, klik ikon tempat sampah di sebelahnya.
11. Klik **Simpan**.

Memeriksa aktivitas firewall awan

Setelah pembaruan konfigurasi aturan firewall server cloud, log aktivitas pembaruan tersedia di konsol Cyber Protect. Anda dapat melihat log dan memeriksa informasi berikut:

- nama pengguna dari pengguna yang memperbarui konfigurasi
- tanggal dan waktu pembaruan
- pengaturan firewall untuk koneksi masuk dan keluar
- tindakan default untuk koneksi masuk dan keluar
- protokol, port, dan alamat IP pengecualian untuk koneksi masuk dan keluar

Untuk melihat detail tentang perubahan konfigurasi aturan firewall awan

1. Di konsol Cyber Protect, klik **Pemantauan** > **Aktivitas**.
2. Klik aktivitas yang sesuai, dan klik **Semua Properti**.
   Deskripsi aktivitasnya adalah **Memperbarui konfigurasi server awan**.
3. Di kolom **konteks**, periksa informasi yang Anda minati.

Mencadangkan server awan

Server utama dan pemulihan dicadangkan tanpa agen pada situs awan. Cadangan ini memiliki batasan berikut.

- Satu-satunya lokasi pencadangan yang memungkinkan adalah penyimpanan awan. Server utama dicadangkan ke penyimpanan **Cadangan server utama**.

  Catatan
  Lokasi pencadangan Microsoft Azure tidak didukung.

- Rencana pencadangan tidak dapat diterapkan ke banyak server. Tiap server harus memiliki rencana pencadangannya sendiri, meskipun semua rencana pencadangan memiliki pengaturan yang sama.

© Acronis International GmbH, 2003-2024

- Hanya satu rencana pencadangan yang dapat diterapkan pada satu server.
- Pencadangan keberadaan aplikasi tidak didukung.
- Enkripsi tidak tersedia.
- Opsi cadangan tidak tersedia.

Ketika Anda menghapus server utama, cadangannya juga akan dihapus.

Server pemulihan hanya dicadangkan pada status failover. Pencadangannya melanjutkan rangkaian pencadangan server aslinya. Ketika failback dilakukan, server asli dapat melanjutkan rangkaian pencadangan ini. Jadi, cadangan server pemulihan hanya dapat dihapus secara manual atau sebagai akibat penerapan aturan retensi. Ketika server pemulihan dihapus, cadangannya akan selalu disimpan.

Catatan
Rencana pencadangan untuk server awan dilakukan berdasarkan waktu UTC.

Orkestrasi (runbook)

Catatan
Beberapa fitur mungkin memerlukan pelisensian tambahan sesuai model pelisensian yang diterapkan.

Runbook adalah serangkaian instruksi yang menjelaskan cara menjalankan lingkungan produksi di cloud. Anda dapat membuat runbook di konsol Cyber Protect. Untuk mengakses layar **Runbook**, pilih **Pemulihan bencana** > **Runbook**.

Mengapa menggunakan runbook?

Dengan runbook, Anda dapat:

- Mengotomasi failover dari satu atau beberapa server
- Memeriksa hasil failover secara otomatis dengan melakukan ping alamat IP server dan memeriksa koneksi ke port yang Anda tentukan
- Mengatur urutan operasi untuk server yang menjalankan aplikasi terdistribusi
- Menyertakan operasi manual dalam alur kerja
- Memverifikasi integritas solusi pemulihan bencana Anda, dengan menjalankan runbook dalam mode uji.

Membuat runbook

Runbook terdiri dari beberapa langkah yang dijalankan secara berurutan. Satu langkah terdiri dari beberapa tindakan yang dimulai secara bersamaan.

Anda dapat mengikuti instruksi di bawah ini atau menonton tutorial video.

© Acronis International GmbH, 2003-2024

Untuk membuat runbook

1. Di konsol Cyber Protection, buka **Pemulihan bencana** > **Runbook**.
2. Klik **Buat runbook**.
3. Klik **Tambah langkah**.
4. Klik **Tambah tindakan**, dan kemudian pilih aksi yang ingin Anda tambahkan ke langkah tersebut.

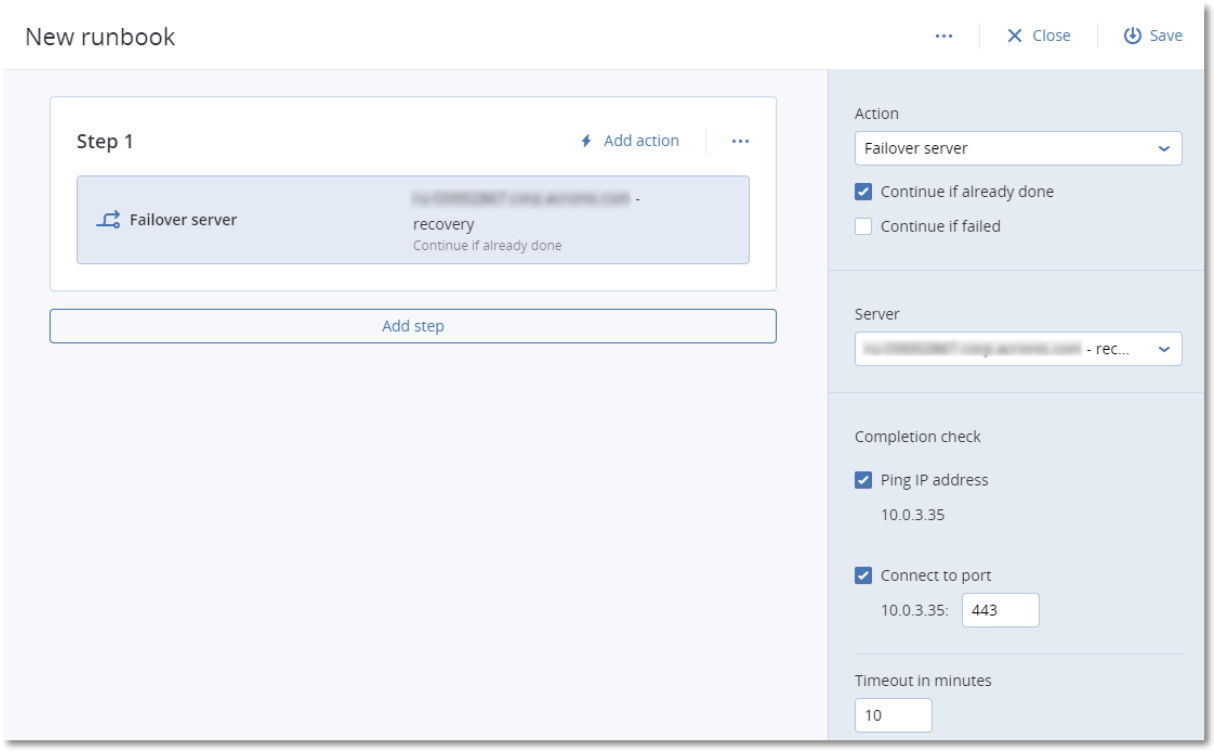
Tindakan	Deskripsi
Failover server	Melakukan failover dari server cloud. Untuk menetapkan tindakan ini, Anda harus memilih server cloud dan mengonfigurasi parameter runbook yang tersedia untuk tindakan ini. Untuk informasi lebih lanjut tentang parameter ini, lihat "Parameter runbook" (hlm. 810). **Catatan** Jika cadangan server yang Anda pilih dienkripsi dengan menggunakan enkripsi sebagai properti mesin, tindakan **Failover server** akan dijeda dan akan otomatis berubah menjadi **Interaksi diperlukan**. Untuk melanjutkan eksekusi runbook, Anda harus memberikan kata sandi untuk cadangan yang dienkripsi.
Failback server	Melakukan failback dari server cloud. Untuk menetapkan tindakan ini, Anda harus memilih server cloud dan mengonfigurasi parameter runbook yang tersedia untuk tindakan ini. Untuk informasi lebih lanjut tentang pengaturan ini, lihat "Parameter runbook" (hlm. 810). **Catatan** Operasi runbook hanya mendukung failback dalam mode manual. Artinya, jika Anda memulai proses failback dengan menjalankan runbook yang menyertakan langkah **Failback server**, prosedurnya akan memerlukan interaksi manual: Anda harus memulihkan mesin secara manual, dan mengonfirmasi atau membatalkan proses failback dari Tab **Pemulihan Bencana** > **Server**.
Hidupkan server	Menghidupkan server cloud. Untuk menetapkan tindakan ini, Anda harus memilih server cloud dan mengonfigurasi parameter runbook yang tersedia untuk tindakan ini. Untuk informasi lebih lanjut tentang pengaturan ini, lihat "Parameter runbook" (hlm. 810). **Catatan** Tindakan **Hidupkan server** tidak berlaku untuk operasi failover uji dalam runbook. Jika Anda mencoba menjalankannya, tindakan tersebut akan gagal dengan pesan kesalahan berikut: Gagal: Tindakan ini tidak berlaku untuk keadaan server saat ini.
Hentikan server	Menghentikan server cloud. Untuk menetapkan tindakan ini, Anda harus memilih server cloud dan mengonfigurasi parameter runbook yang tersedia untuk tindakan ini. Untuk informasi lebih lanjut tentang pengaturan ini, lihat "Parameter runbook" (hlm. 810).

© Acronis International GmbH, 2003-2024

Tindakan	Deskripsi
	Catatan Tindakan **Hentikan server** tidak berlaku untuk operasi failover uji dalam runbook. Jika Anda mencoba menjalankan tindakan seperti itu, itu akan gagal dengan pesan kesalahan berikut: Gagal: Tindakan ini tidak berlaku untuk keadaan server saat ini.
Operasi manual	Operasi manual memerlukan interaksi dari pengguna. Untuk menetapkan tindakan ini, Anda harus memasukkan deskripsi. Ketika urutan runbook mencapai operasi manual, runbook akan dijeda dan tidak akan melanjutkan sampai pengguna melakukan operasi manual yang diperlukan, seperti mengklik tombol konfirmasi.
Jalankan runbook	Menjalankan runbook lain. Untuk menetapkan tindakan ini, Anda harus memilih sebuah runbook. Runbook hanya dapat mencakup satu eksekusi runbook yang diberikan. Misalnya, jika Anda menambahkan tindakan "execute Runbook A", Anda dapat menambahkan tindakan "execute Runbook B", namun tidak dapat menambahkan tindakan "execute Runbook A" lainnya.

5. Tetapkan parameter runbook untuk tindakan tersebut. Untuk informasi lebih lanjut tentang parameter ini, lihat "Parameter runbook" (hlm. 810).
6. [Opsional] Untuk menambahkan deskripsi langkah:
   a. Klik ikon elipsis, lalu klik **Deskripsi**.
   b. Masukkan deskripsi dari langkah tersebut.
   c. Klik **Selesai**.
7. Ulangi langkah 3-6 sampai Anda membuat urutan langkah dan tindakan yang diinginkan.
8. [Opsional] Untuk mengubah nama default dari runbook:
   a. Klik ikon elipsis.
   b. Masukkan nama runbook.
   c. Masukkan deskripsi runbook.
   d. Klik **Selesai**.
9. Klik **Simpan**.
10. Klik **Tutup**.

© Acronis International GmbH, 2003-2024



Parameter runbook

Parameter runbook adalah pengaturan spesifik yang harus dikonfigurasi untuk menetapkan tindakan runbook. Ada dua kategori parameter runbook, yaitu parameter tindakan dan parameter pemeriksaan penyelesaian.

Parameter tindakan menetapkan perilaku runbook tergantung pada keadaan awal tindakan atau hasilnya.

Parameter pemeriksaan penyelesaian memastikan bahwa server tersedia dan menyediakan layanan yang diperlukan. Jika pemeriksaan penyelesaian gagal, tindakan tersebut dianggap gagal.

Tabel berikut menjelaskan parameter runbook yang dapat dikonfigurasi untuk setiap tindakan.

Parameter Runbook	Kategori	Tersedia untuk tindakan	Deskripsi
Lanjutkan jika sudah pernah dilakukan	Parameter tindakan	• **Failover server** • **Hidupkan server** • **Hentikan server** • **Failback server**	Parameter ini menetapkan perilaku runbook ketika tindakan yang diperlukan sudah dilakukan (misalnya, failover sudah dilakukan atau server sudah berjalan). Ketika diaktifkan, runbook mengeluarkan peringatan dan melanjutkan. Ketika dinonaktifkan, tindakan gagal, dan kemudian runbook juga gagal. Secara default, parameter ini diaktifkan.

© Acronis International GmbH, 2003-2024

Parameter Runbook	Kategori	Tersedia untuk tindakan	Deskripsi
Lanjutkan jika gagal	Parameter tindakan	• **Failover server** • **Hidupkan server** • **Hentikan server** • **Failback server**	Parameter ini menetapkan perilaku runbook ketika tindakan yang diperlukan gagal. Ketika diaktifkan, runbook mengeluarkan peringatan dan melanjutkan. Ketika dinonaktifkan, tindakan gagal, dan kemudian runbook juga gagal. Secara default, parameter ini dinonaktifkan.
Ping alamat IP	Cek penyelesaian	• **Hidupkan server**	Perangkat lunak akan melakukan ping alamat IP produksi dari server awan hingga server menjawab atau waktu tunggu habis, mana pun yang terlebih dahulu tercapai.
Koneksikan ke port (443 secara default)	Cek penyelesaian	• **Failover server** • **Hidupkan server**	Perangkat lunak akan berusaha menghubungkan ke server awan menggunakan alamat IP produksinya dan port yang Anda tentukan, hingga server ditetapkan atau waktu tunggu habis, mana pun yang terlebih dahulu tercapai. Dengan cara ini, Anda dapat memeriksa apakah aplikasi yang digunakan pada port yang ditentukan berjalan.
Timeout dalam menit	Cek penyelesaian	• **Failover server** • **Hidupkan server**	Waktu tunggu default adalah 10 menit.

Operasi dengan runbook

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Untuk mengakses daftar operasi, arahkan kursor ke runbook dan klik ikon elipsis. Ketika runbook tidak berjalan, operasi berikut akan tersedia:

- **Eksekusi**
- **Sunting**
- **Klona**
- **Hapus**

© Acronis International GmbH, 2003-2024

Mengeksekusi runbook

Setiap kali Anda mengklik **Eksekusi**, peringatan untuk meminta parameter eksekusi akan muncul. Parameter ini berlaku untuk semua operasi failover dan failback yang dimasukkan dalam runbook. Runbook yang ditentukan dalam operasi **Eksekusi runbook** mewarisi parameter ini dari runbook utama.

- **Mode failover dan failback**

  Pilih apakah Anda ingin menjalankan failover uji (secara default) atau failover nyata (produksi). Mode failback akan sesuai dengan mode failover yang dipilih.
- **Titik pemulihan failover**

  Pilih titik pemulihan terbaru (secara default) atau pilih titik waktu di masa lalu. Jika nanti diperlukan eksekusi, titik pemulihan terdekat sebelum tanggal dan waktu yang ditentukan akan dipilih untuk setiap server.

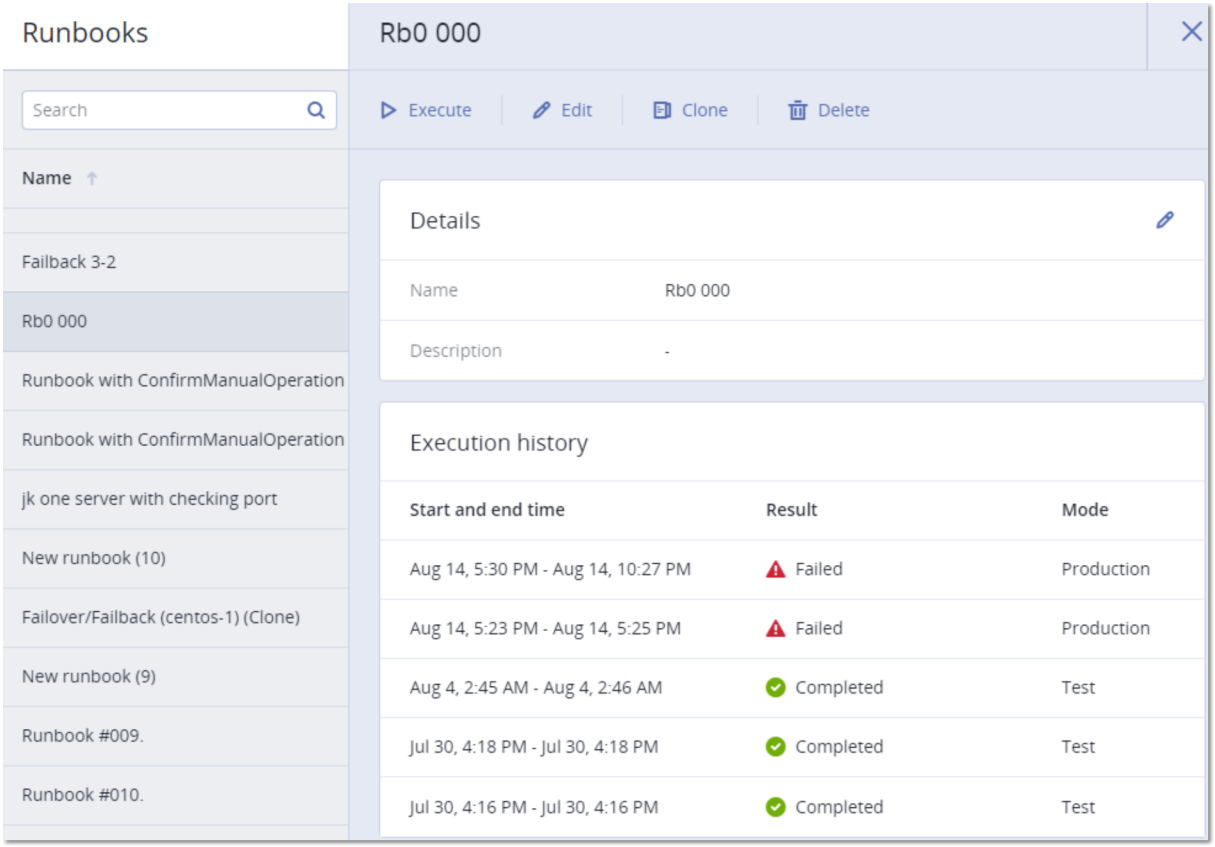
Menghentikan eksekusi runbook

Selama eksekusi runbook, Anda dapat memilih **Setop** dalam daftar operasi. Perangkat lunak akan menyelesaikan semua tindakan yang sudah dimulai kecuali yang memerlukan interaksi pengguna.

Melihat riwayat eksekusi

Ketika Anda memilih runbook pada tab **Runbook**, perangkat lunak akan menampilkan detail runbook dan riwayat eksekusi. Klik baris yang sesuai dengan eksekusi spesifik untuk melihat log eksekusi.

© Acronis International GmbH, 2003-2024



© Acronis International GmbH, 2003-2024

Mengonfigurasi proteksi antivirus dan antimalware Anda

Catatan
Pada mesin Windows, fitur Proteksi Antimalware memerlukan instalasi Agen untuk Proteksi Antimalware, dan fitur penyaringan URL memerlukan instalasi Agen untuk penyaringan URL. Agen-agen ini diinstal secara otomatis untuk beban kerja yang dilindungi jika modul **Antivirus & Proteksi Antimalware** dan/atau **Penyaringan URL** diaktifkan dalam rencana proteksi mereka.

Perlindungan antimalware dalam Cyber Protection memberi Anda manfaat berikut:

- Perlindungan puncak pada semua tahap: proaktif, aktif, dan reaktif.
- Empat teknologi antimalware dalam sistem untuk memberikan perlindungan multilapisan terbaik di kelasnya.
- Manajemen Microsoft Security Essentials dan Microsoft Defender Antivirus.

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Penting
File uji EICAR terdeteksi hanya jika opsi **Antimalware Tingkat Lanjut** diaktifkan dalam rencana proteksi. Namun, tidak terdeteksinya file EICAR tidak memengaruhi kemampuan antimalware Cyber Protection.

Platform yang didukung

Active protection, fitur antivirus dan antimalware didukung pada platform berikut.

Sistem operasi	Versi/Distribusi
Windows	Windows 7 Service Pack 1 dan versi setelahnya Windows Server 2008 R2 Paket Layanan 1 dan yang lebih baru **Catatan** Untuk Windows 7, Anda harus menginstal pemutakhiran berikut dari Microsoft sebelum menginstal agen perlindungan. • Windows 7 Extended Security Updates (ESU) • KB4474419 • KB4490628 Untuk informasi lebih lanjut mengenai pembaruan yang diperlukan, lihat artikel basis pengetahuan ini.
Linux	Red Hat Linux 7.x, 8.x, 9.x

© Acronis International GmbH, 2003-2024

Sistem operasi	Versi/Distribusi
	CloudLinux 6.10, 7.x, 8.x CentOS 6.5 dan versi 6.x yang lebih baru, 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 dan versi yang lebih baru

Fitur yang didukung per platform

Catatan
Perlindungan antimalware untuk Linux dan macOS tersedia dengan paket Advanced Antimalware.

Set fitur	Windows	Linux	macOS
Perlindungan Antivirus and Antimalware			
Fungsionalitas Active Protection yang terintegrasi penuh	Iya	Tidak	Tidak
Proteksi antimalware waktu nyata	Iya	Ya, dengan paket Advanced Antimalware	Ya, dengan paket Advanced Antimalware
Perlindungan antimalware waktu nyata tingkat lanjut dengan deteksi berbasis tanda tangan lokal	Iya	Iya	Iya
Analisis statik untuk file portable yang dapat dieksekusi	Iya	Tidak	Iya*
Pemindaian antimalware sesuai permintaan	Iya	Iya**	Iya
Perlindungan folder jaringan	Iya	Iya	Tidak
Perlindungan sisi server	Iya	Tidak	Tidak
Pindai file arsip	Iya	Tidak	Iya
Pindai drive yang dapat dilepas	Iya	Tidak	Iya
Pindai file baru dan yang diubah saja	Iya	Tidak	Iya

© Acronis International GmbH, 2003-2024

Set fitur	Windows	Linux	macOS
Perlindungan Antivirus and Antimalware			
Pengecualian file/folder	Iya	Iya	Iya***
Pengecualian proses	Iya	Tidak	Iya
Mesin analisis perilaku	Iya	Tidak	Iya
Pencegahan eksploit	Iya	Tidak	Tidak
Karantina	Iya	Iya	Iya
Pembersihan otomatis karantina	Iya	Iya	Iya
Pemfilteran URL (http/https)	Iya	Tidak	Tidak
Daftar putih seluruh perusahaan	Iya	Tidak	Iya
Manajemen firewall****	Iya	Tidak	Tidak
Manajemen Microsoft Defender Antivirus*****	Iya	Tidak	Tidak
Manajemen Microsoft Security Essentials	Iya	Tidak	Tidak
Mendaftarkan dan mengelola perlindungan Antivirus dan Antimalware melalui Windows Security Center	Iya	Tidak	Tidak
Untuk informasi selengkapnya tentang sistem operasi yang didukung dan versinya, lihat "Platform yang didukung" (hlm. 814).			

* Analisis statis untuk file portabel yang dapat dieksekusi hanya didukung untuk pemindaian terjadwal pada macOS.

** Persyaratan mulai tidak didukung untuk pemindaian sesuai permintaan di Linux.

*** Pengecualian file/folder hanya didukung jika Anda menentukan file dan folder yang tidak akan dipindai oleh perlindungan waktu nyata atau pemindaian terjadwal pada macOS.

**** Manajemen firewall didukung di Windows 8 dan yang lebih baru. Windows Server tidak didukung.

***** Manajemen Microsoft Defender Antivirus didukung di Windows 8.1 dan yang lebih baru.

Set fitur	Windows	Linux	macOS
Active Protection			
Deteksi injeksi proses	Iya	Tidak	Tidak

© Acronis International GmbH, 2003-2024

Set fitur	Windows	Linux	macOS
Active Protection			
Pemulihan otomatis file yang terpengaruh dari cache lokal	Iya	Iya	Iya
Pertahanan diri untuk file cadangan Acronis	Iya	Tidak	Tidak
Pertahanan diri untuk perangkat lunak Acronis	Iya	Tidak	Iya (Hanya Active Protection dan komponen antimalware)
Manajemen proses tepercaya/terblokir	Iya	Tidak	Iya
Pengecualian proses/folder	Iya	Iya	Iya
Deteksi ransomware berdasarkan perilaku proses (berbasis AI)	Iya	Iya	Iya
Deteksi proses cryptomining berdasarkan perilaku proses	Iya	Tidak	Tidak
Proteksi drive eksternal (HDD, flash drive, kartu SD)	Iya	Tidak	Iya
Perlindungan folder jaringan	Iya	Iya	Iya
Perlindungan sisi server	Iya	Tidak	Tidak
Perlindungan untuk Zoom, Cisco Webex, Citrix Workspace, dan Microsoft Teams	Iya	Tidak	Tidak
Untuk informasi selengkapnya tentang sistem operasi yang didukung dan versinya, lihat "Platform yang didukung" (hlm. 814).			

Perlindungan antivirus and antimalware

Catatan
Beberapa fitur mungkin memerlukan pelisensian tambahan sesuai model pelisensian yang diterapkan.

Modul **Antivirus & Antimalware** melindungi mesin Windows, Linux, dan macOS Anda dari semua ancaman malware terbaru. Lihat daftar lengkap tentang fitur antimalware yang didukung di "Platform yang didukung" (hlm. 814).

Perlindungan Antivirus & Antimalware didukung dan terdaftar di Windows Security Center.

© Acronis International GmbH, 2003-2024

Fitur antimalware

- Deteksi malware dalam file pada mode proteksi waktu nyata dan sesuai permintaan
- Deteksi perilaku berbahaya ketika proses (untuk Windows)
- Memblokir akses ke URL berbahaya (untuk Windows)
- Menempatkan file berbahaya ke karantina
- Menambahkan aplikasi korporat tepercaya ke daftar izin

Jenis pemindaian

Anda dapat mengonfigurasi perlindungan antivirus dan antimalware agar selalu berjalan di latar belakang atau sesuai permintaan.

Perlindungan waktu nyata

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Perlindungan waktu nyata memeriksa semua file yang sedang dijalankan atau dibuka pada mesin untuk mencegah ancaman malware.

Untuk mencegah kemungkinan masalah kompatibilitas dan performa, perlindungan waktu nyata tidak dapat bekerja secara paralel dengan solusi antivirus lain yang juga menggunakan fitur perlindungan waktu nyata. Status solusi antivirus lainnya yang diinstal ditetapkan melalui Pusat Keamanan Windows. Jika mesin Windows sudah dilindungi dengan solusi antivirus lain, perlindungan waktu nyata dinonaktifkan secara otomatis.

Untuk mengaktifkan perlindungan waktu nyata, nonaktifkan atau hapus instalasi solusi antivirus lainnya. Perlindungan waktu nyata dapat otomatis menggantikan perlindungan waktu nyata Microsoft Defender.

Catatan
Di mesin yang menjalankan sistem operasi Windows Server, Microsoft Defender tidak akan dinonaktifkan secara otomatis saat perlindungan waktu nyata diaktifkan. Administrator harus menonaktifkan Microsoft Defender secara manual untuk menghindari kemungkinan masalah kompatibilitas.

Anda dapat memilih salah satu dari mode pemindaian berikut:

- Deteksi **smart on-access** artinya program antimalware berfungsi di latar belakang, dan secara aktif serta berkelanjutan memindai sistem mesin Anda dari virus dan ancaman berbahaya lainnya sepanjang waktu sistem Anda menyala. Malware akan terdeteksi saat sebuah file dieksekusi dan selama berbagai operasi dengan file tersebut seperti membukanya untuk membaca atau mengedit.

© Acronis International GmbH, 2003-2024

- Deteksi **Sedang dieksekusi** berarti hanya file yang dapat dieksekusi yang akan dipindai pada saat mereka berjalan untuk memastikan file tersebut bersih dan tidak akan menyebabkan kerusakan apa pun pada mesin atau data Anda. Menyalin file yang terinfeksi akan tetap tidak terdeteksi.

Pemindaian terjadwal

Pemindaian antimalware dilakukan sesuai jadwal.

Anda dapat memilih salah satu dari mode pemindaian berikut.

- **Pemindaian cepat**—Hanya memeriksa file sistem beban kerja.
- **Pemindaian penuh**—Memeriksa semua file di beban kerja Anda.
- **Pemindaian kustom**—Memeriksa file/folder yang ditambahkan oleh administrator ke rencana Proteksi.

Setelah pemindaian antimalware selesai, Anda dapat melihat detail tentang beban kerja yang terpengaruh oleh ancaman di widget **Pemantauan** > **Ikhtisar** > Baru saja terpengaruh.

Pengaturan perlindungan Antivirus dan antimalware

Bagian ini menjelaskan fitur yang dapat Anda konfigurasikan di modul **Perlindungan Antivirus & Antimalware** dalam paket perlindungan. Untuk mempelajari cara membuat rencana perlindungan, lihat "Membuat rencana proteksi" (hlm. 214).

Fitur berikut dapat dikonfigurasi dalam modul proteksi Antivirus & Antimalware untuk rencana proteksi:

- "Active Protection" (hlm. 820)
- "Antimalware Tingkat Lanjut" (hlm. 820)
- "Perlindungan folder jaringan" (hlm. 821)
- "Perlindungan sisi server" (hlm. 821)
- "Perlindungan diri" (hlm. 822)
- "Deteksi proses cryptomining" (hlm. 823)
- "Karantina" (hlm. 824)
- "Mesin perilaku" (hlm. 824)
- "Pencegahan eksploit" (hlm. 825)
- "Perlindungan waktu nyata" (hlm. 827)
- "Jadwalkan pemindaian" (hlm. 828)
- "Pengecualian proteksi" (hlm. 831)

© Acronis International GmbH, 2003-2024

Catatan
Tidak semua sistem operasi mendukung fitur Proteksi Antivirus & Antimalware. Untuk informasi lebih lanjut tentang sistem operasi dan fitur yang didukung, lihat "Platform yang didukung" (hlm. 814). Beberapa fitur memerlukan lisensi tertentu untuk tersedia dalam rencana proteksi Anda.

Active Protection

Active Protection melindungi sistem Anda dari perangkat lunak berbahaya bernama ransomware yang mengenkripsi file dan meminta tebusan untuk kode enkripsi.

Pengaturan default: **Diaktifkan**.

Catatan
Agen perlindungan harus dipasang pada mesin yang dilindungi. Untuk informasi selengkapnya tentang sistem operasi dan fitur yang didukung, lihat "Platform yang didukung" (hlm. 814).

Untuk mengonfigurasi Active Protection

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Active Protection**.
3. Di bagian **Tindakan saat deteksi**, pilih salah satu opsi yang tersedia:

   Pengaturan default: **Kembalikan menggunakan cache**

   - **Hanya notifikasi**—Perangkat lunak mengeluarkan peringatan tentang proses yang dicurigai sebagai aktivitas ransomware.
   - **Hentikan proses**—Perangkat lunak mengeluarkan peringatan dan menghentikan proses yang dicurigai sebagai aktivitas ransomware.
   - **Kembalikan menggunakan cache**—Perangkat lunak mengeluarkan peringatan, menghentikan proses, dan mengembalikan perubahan file dengan menggunakan cache layanan.
4. Klik **Selesai** untuk menerapkan opsi yang dipilih pada rencana proteksi Anda.

Antimalware Tingkat Lanjut

Mesin ini menggunakan database ciri khas virus yang disempurnakan untuk meningkatkan efisiensi deteksi antimalware baik dalam pemindaian cepat maupun pemindaian lengkap.

Penting
Fitur ini hanya tersedia jika Anda mengaktifkan paket proteksi Keamanan Tingkat Lanjut. Untuk informasi selengkapnya, lihat https://www.acronis.com/en-us/products/cloud/cyber-protect/security/

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

© Acronis International GmbH, 2003-2024

Untuk mengonfigurasi Antimalware Tingkat Lanjut

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Di bagian **Antimalware Tingkat Lanjut**, gunakan tombol alih untuk mengaktifkan mesin berbasis ciri khas lokal.

Catatan
Perlindungan Antivirus dan Antimalware untuk macOS dan Linux juga memerlukan mesin berbasis tanda tangan lokal. Untuk Windows, perlindungan Antivirus dan Antimalware tersedia dengan atau tanpa mesin ini.

Perlindungan folder jaringan

Fitur **Proteksi folder jaringan** menentukan apakah proteksi Antivirus & Antimalware melindungi folder jaringan yang dipetakan sebagai drive lokal. Perlindungan berlaku untuk folder yang dibagikan melalui protokol SMB atau NFS.

Untuk mengkonfigurasi proteksi folder Jaringan

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Proteksi folder jaringan**.
3. Tambahkan file tempat Anda ingin membuat cadangan folder jaringan:
   - Misalnya, Jika beban kerja Anda adalah Windows, di bidang **Windows**, masukkan jalur file Windows tempat Anda ingin mencadangkan folder jaringan. Nilai defaultnya: C:\ProgramData\Acronis\File Jaringan yang Dipulihkan.
   - Misalnya, Jika beban kerja Anda adalah macOS, di bidang **macOS**, masukkan jalur untuk file macOS tempat Anda ingin mencadangkan folder jaringan. Nilai default: /Perpustakaan/Dukungan Aplikasi/Acronis/File Jaringan yang Dipulihkan/.

   Catatan
   Masukkan jalur folder lokal. Folder jaringan, termasuk folder pada drive yang dipetakan, tidak didukung sebagai tujuan cadangan untuk folder jaringan.
4. Klik **Selesai** untuk menerapkan opsi yang dipilih pada rencana proteksi Anda.

Perlindungan sisi server

Fitur ini menentukan apakah Active protection mampu mengamankan folder jaringan yang Anda bagikan dari koneksi masuk eksternal dari server lain di jaringan yang berpotensi menimbulkan ancaman.

Pengaturan default: **Nonaktif**.

Catatan
Perlindungan sisi server tidak didukung untuk Linux.

© Acronis International GmbH, 2003-2024

Untuk mengatur koneksi tepercaya

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Proteksi sisi server**.
3. Gunakan tombol **Proteksi sisi server** untuk mengaktifkannya.
4. Pilih tab **Tepercaya**.
5. Di bidang **Koneksi tepercaya**, klik **Tambahkan** guna menentukan koneksi yang diizinkan untuk mengubah data.
6. Di bidang **Nama Komputer/Akun**, ketikkan nama komputer dan akun mesin tempat agen proteksi diinstal. Contohnya, `MyComputer\TestUser`.
7. Di bidang **Nama host**, ketikkan nama host mesin yang diizinkan untuk terhubung ke mesin menggunakan agen proteksi.
8. Klik tanda centang di sebelah kanan untuk menyimpan definisi koneksi.
9. Klik **Selesai**.

Untuk mengatur koneksi yang diblokir

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Proteksi sisi server**.
3. Gunakan tombol **Proteksi sisi server** untuk mengaktifkannya.
4. Pilih tab **Diblokir**.
5. Di bidang **Koneksi yang diblokir**, klik **Tambahkan** untuk menentukan koneksi yang tidak diperbolehkan untuk mengubah data.
6. Di bidang **Nama Komputer/Akun**, ketikkan nama komputer dan akun mesin tempat agen proteksi diinstal. Contohnya, `MyComputer\TestUser`.
7. Di bidang **Nama host**, ketikkan nama host mesin yang diizinkan untuk terhubung ke mesin menggunakan agen proteksi.
8. Pilih kotak centang di sebelah kanan untuk menyimpan definisi koneksi.
9. Klik **Selesai**.

Perlindungan diri

Proteksi diri mencegah perubahan tidak sah pada proses perangkat lunak itu sendiri, catatan registri, file yang dapat dijalankan dan konfigurasi, serta cadangan yang terletak di folder lokal Anda.

Administrator dapat mengaktifkan **Perlindungan diri**, tanpa mengaktifkan **Active Protection**.

Pengaturan default: **Aktif**.

Catatan
Swaproteksi tidak didukung untuk Linux.

© Acronis International GmbH, 2003-2024

Untuk mengaktifkan Proteksi diri

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Perlindungan diri**.
3. Gunakan tombol alih **Perlindungan diri** untuk mengaktifkannya.

Untuk mengaktifkan Proteksi kata sandi

1. Setelah fitur **Perlindungan diri** diaktifkan, Anda dapat mengaktifkan fitur **Proteksi kata sandi** dengan menggunakan tombol pengalih.
2. Klik **Buat kata sandi baru** untuk membuat kata sandi guna mengubah atau menghapus agen lokal.
3. Klik **Salin**, lalu tempelkan di tempat yang aman karena ini akan diminta ketika Anda ingin mengubah daftar komponen di lokasi terkait.

   Penting
   Kata sandi tidak akan tersedia setelah Anda menutup jendela. Agar kata sandi ini diterapkan ke perangkat, pengaturan rencana proteksi harus disimpan.

4. Klik **Tutup**.

Proteksi kata sandi mencegah pengguna atau perangkat lunak yang tidak sah menghapus instalasi Agen untuk Windows atau memodifikasi komponennya. Tindakan ini hanya dimungkinkan dengan kata sandi yang dapat diberikan oleh administrator.

Kata sandi tidak pernah diperlukan untuk tindakan berikut:

- Memperbarui instalasi dengan menjalankan program penyiapan setempat
- Memperbarui instalasi dengan menggunakan konsol Cyber Protect
- Memperbaiki instalasi

Pengaturan default: **Dinonaktifkan**

Untuk informasi lebih lanjut tentang cara mengaktifkan **Proteksi kata sandi**, lihat Mencegah penghapusan instalasi atau modifikasi agen yang tidak sah.

Deteksi proses cryptomining

Malware Cryptomining menurunkan kinerja aplikasi yang berguna, meningkatkan tagihan listrik, dan dapat menyebabkan gangguan sistem dan bahkan kerusakan perangkat keras akibat penyalahgunaan. Fitur **Deteksi proses cryptomining** melindungi perangkat Anda dari malware cryptomining untuk mencegah penggunaan sumber daya komputer tanpa izin.

Administrator dapat mengaktifkan **Deteksi proses cryptomining**, tanpa mengaktifkan **Active Protection**. Pengaturan default: **Diaktifkan**.

© Acronis International GmbH, 2003-2024

Catatan
Deteksi proses cryptomining tidak didukung untuk Linux.

Untuk mengkonfigurasi perlindungan folder jaringan

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Deteksi proses cryptomining**.
3. Gunakan tombol **Deteksi proses cryptomining** untuk mengaktifkan atau menonaktifkan fitur ini.
4. Pilih apa yang harus dilakukan dengan proses yang diduga merupakan aktivitas cryptomining:

   Pengaturan default: **Hentikan proses**

   - **Hanya notifikasi**—Perangkat lunak mengeluarkan peringatan.
   - **Hentikan proses** — Perangkat lunak mengeluarkan peringatan dan menghentikan proses.
5. Klik **Selesai** untuk menerapkan opsi yang dipilih pada rencana proteksi Anda.

Karantina

Karantina adalah folder yang digunakan untuk mengisolasi file yang mencurigakan (mungkin terinfeksi) atau berpotensi berbahaya.

Untuk mengonfigurasi Karantina

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Karantina**.
3. Di bidang **Hapus file yang dikarantina setelah**, Anda dapat menentukan jangka waktu dalam satuan hari sebelum file yang dikarantina dihapus nantinya.

   Pengaturan default: **30 hari**
4. Klik **Selesai**.

Untuk informasi lebih lanjut tentang fitur ini, lihat Karantina.

Mesin perilaku

Fitur **Mesin perilaku** melindungi sistem dari malware dengan menggunakan heuristik perilaku untuk mengidentifikasi proses berbahaya.

Pengaturan default: **Diaktifkan**.

Catatan
Mesin perilaku tidak didukung untuk Linux.

Untuk mengkonfigurasi proteksi folder Jaringan

© Acronis International GmbH, 2003-2024

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Mesin perilaku**.
3. Gunakan tombol alih **Mesin perilaku** untuk mengaktifkan atau menonaktifkan fitur ini.
4. Di bagian **Tindakan saat deteksi** pilih tindakan yang akan dilakukan perangkat lunak ketika aktivitas malware terdeteksi:
   Pengaturan default: **Karantina**
   - **Hanya notifikasi**—Perangkat lunak mengeluarkan peringatan tentang proses yang dicurigai sebagai aktivitas malware.
   - **Hentikan proses**—Perangkat lunak mengeluarkan peringatan dan menghentikan proses yang dicurigai sebagai aktivitas malware.
   - **Karantina**—Perangkat lunak mengeluarkan peringatan, menghentikan proses, dan memindahkan file yang dapat dieksekusi ke folder karantina.
5. Klik **Selesai** untuk menerapkan opsi yang dipilih pada rencana proteksi Anda.

Pencegahan eksploit

Penting
Fitur ini hanya tersedia jika Anda mengaktifkan paket proteksi Keamanan Tingkat Lanjut. Untuk informasi selengkapnya, lihat https://www.acronis.com/en-us/products/cloud/cyber-protect/security/

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Pencegahan eksploitasi mendeteksi dan mencegah proses yang terinfeksi menyebar dan mengeksploitasi kerentanan perangkat lunak pada sistem. Ketika eksploit terdeteksi, perangkat lunak dapat mengeluarkan peringatan dan menghentikan proses yang terduga melakukan aktivitas eksploit.

Pencegahan eksploit hanya tersedia dengan agen versi 12.5.23130 (21.08, dirilis pada Agustus 2020) atau yang lebih baru.

Pengaturan default: **Diaktifkan** untuk rencana proteksi yang baru saja dibuat, dan **Dinonaktifkan** untuk rencana proteksi yang sudah ada, yang dibuat dengan versi agen sebelumnya.

Catatan
Pencegahan eksploit tidak didukung untuk Linux.

Anda dapat memilih tindakan yang harus dilakukan program ketika eksploit terdeteksi, dan metode pencegahan eksploit yang diterapkan olehnya.

Untuk mengonfigurasi pencegahan Eksploitasi

© Acronis International GmbH, 2003-2024

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Pencegahan eksploit**.
3. Di bagian **Tindakan saat deteksi**, pilih salah satu opsi yang tersedia:

   Pengaturan default: **Hentikan proses**

   - **Hanya beri tahu**

     Perangkat lunak akan mengeluarkan peringatan tentang proses yang diduga merupakan aktivitas eksploitasi.
   - **Hentikan proses**

     Perangkat lunak akan mengeluarkan peringatan dan menghentikan proses yang dicurigai melakukan aktivitas eksploitasi.
4. Di bagian **Teknik pencegahan eksploitasi yang diaktifkan**, pilih dari opsi yang tersedia yang ingin Anda terapkan:

   Pengaturan default: **Semua metode diaktifkan**

   - **Perlindungan memori**

     Mendeteksi dan mencegah modifikasi mencurigakan pada hak eksekusi di halaman memori. Proses berbahaya menerapkan modifikasi tersebut pada properti halaman, untuk mengaktifkan eksekusi kode shell dari area memori yang tidak dapat dieksekusi seperti stack dan heap.
   - **Perlindungan return-oriented programming (ROP)**

     Mendeteksi dan mencegah upaya penggunaan teknik eksploitasi ROP.
   - **Perlindungan eskalasi hak istimewa**

     Mendeteksi dan mencegah upaya peningkatan hak istimewa yang dibuat oleh kode atau aplikasi yang tidak sah. Eskalasi hak istimewa digunakan oleh kode berbahaya untuk mendapatkan akses penuh dari mesin yang diserang, lalu melakukan tugas penting dan sensitif. Kode yang tidak sah tidak diizinkan untuk mengakses sumber daya sistem kritis atau memodifikasi pengaturan sistem.
   - **Perlindungan injeksi kode**

     Mendeteksi dan mencegah injeksi kode berbahaya ke proses jarak jauh. Injeksi kode digunakan untuk menyembunyikan tujuan aplikasi yang berbahaya di belakang proses yang bersih atau ramah, untuk menghindari deteksi oleh produk antimalware.
5. Klik **Selesai** untuk menerapkan opsi yang dipilih pada rencana proteksi Anda.

Catatan
Proses yang tercantum sebagai proses tepercaya di daftar Pengecualian tidak akan dipindai dari adanya eksploit.

Memungkinkan proses untuk memodifikasi cadangan

Pengaturan **Izinkan proses tertentu untuk memodifikasi cadangan** hanya tersedia saat **Perlindungan diri** diaktifkan.

Opsi ini berlaku untuk file yang memiliki ekstensi .tibx, .tib, .tia, dan yang berada di folder lokal.

© Acronis International GmbH, 2003-2024

Pengaturan ini memungkinkan Anda untuk menentukan proses yang diizinkan untuk memodifikasi file cadangan, meskipun file ini dilindungi oleh perlindungan diri. Opsi ini berguna, misalnya, jika Anda menghapus file cadangan atau memindahkannya ke lokasi lain menggunakan skrip.

Jika pengaturan ini dinonaktifkan, file cadangan hanya dapat dimodifikasi melalui proses yang ditandatangani oleh vendor perangkat lunak pencadangan. Hal ini memungkinkan perangkat lunak untuk menerapkan aturan retensi dan menghapus cadangan saat pengguna meminta ini dari antarmuka web. Proses lain, baik itu mencurigakan atau tidak, tidak dapat memodifikasi cadangan.

Jika pengaturan ini diaktifkan, Anda dapat mengizinkan proses lain untuk memodifikasi cadangan. Tentukan jalur lengkap ke proses yang dapat dieksekusi, dimulai dengan huruf drive.

Pengaturan default: **Dinonaktifkan**.

Perlindungan waktu nyata

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Perlindungan waktu nyata terus-menerus memeriksa sistem komputer Anda dari virus dan ancaman berbahaya lainnya selama komputer dinyalakan kecuali jika dijeda oleh pengguna komputer.

Pengaturan default: **Diaktifkan**.

Penting
Fitur ini hanya tersedia jika Anda mengaktifkan paket proteksi Keamanan Tingkat Lanjut. Untuk informasi selengkapnya, lihat https://www.acronis.com/en-us/products/cloud/cyber-protect/security/

Untuk mengonfigurasi proteksi waktu nyata

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Perlindungan waktu nyata**.
3. Pada daftar drop=down **Tindakan saat deteksi**, pilih salah satu opsi yang tersedia:

   Pengaturan default: **Karantina**

   - **Hanya beri tahu**

     Perangkat lunak mengeluarkan peringatan tentang proses yang dicurigai sebagai aktivitas ransomware.

   - **Blokir dan beri tahu**

     Perangkat lunak memblokir proses tersebut dan mengeluarkan peringatan tentang proses yang dicurigai sebagai aktivitas malware.

   - **Karantina**

© Acronis International GmbH, 2003-2024

4. Perangkat lunak mengeluarkan peringatan, menghentikan proses, dan memindahkan file yang dapat dieksekusi ke folder karantina.
5. Di bagian **Mode pemindaian**, pilih tindakan yang akan dilakukan perangkat lunak ketika virus atau ancaman berbahaya lainnya terdeteksi:

   Pengaturan default: **Smart on-access**

   - **Smart on-access**—Memantau semua aktivitas sistem dan secara otomatis memindai file ketika diakses untuk membaca atau menulis, atau setiap kali program diluncurkan.
   - **Sedang dieksekusi**—Secara otomatis hanya memindai file yang dapat dijalankan saat diluncurkan untuk memastikan file tersebut bersih dan tidak akan menyebabkan kerusakan apa pun pada komputer atau data Anda.
6. Klik **Selesai**.

Jadwalkan pemindaian

Pemindaian on-demand memeriksa sistem komputer Anda dari virus sesuai dengan jadwal yang ditentukan. Pemindaian penuh memeriksa semua file pada perangkat Anda, sementara pemindaian cepat hanya memeriksa file sistem perangkat.

Untuk mengkonfigurasi Jadwalkan pemindaian

Pengaturan default:

- **Pemindaian kustom** dinonaktifkan.
- Pemindaian **Cepat** dan **Penuh** dijadwalkan.

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Jadwalkan pemindaian**.
3. Gunakan tombol alih untuk mengaktifkan jenis pemindaian yang ingin Anda terapkan pada mesin Anda.

Jenis pemindaian yang tersedia:

- **Lengkap** — membutuhkan waktu lebih lama untuk selesai dibandingkan dengan pemindaian cepat karena setiap file akan diperiksa.
- **Cepat** — hanya memindai area umum tempat malware biasanya berada di mesin.
- **Kustom** — Memeriksa file/folder yang dipilih oleh administrator rencana Perlindungan.

Catatan
Anda dapat menjadwalkan ketiga pemindaian - **Cepat**, **Lengkap**, dan **Kustom** - dalam satu rencana proteksi.

Untuk mengonfigurasi pemindaian khusus

- Gunakan **Tombol alih pemindaian khusus** untuk mengaktifkan atau menonaktifkan jenis pemindaian ini.

© Acronis International GmbH, 2003-2024

- Pada daftar drop-down **Tindakan saat deteksi**, pilih salah satu opsi yang tersedia:

Pengaturan default: **Karantina**

Karantina

Perangkat lunak ini mengeluarkan peringatan dan memindahkan file yang dapat dieksekusi ke folder karantina.

Hanya beri tahu

Perangkat lunak mengeluarkan peringatan tentang proses yang dicurigai sebagai malware.

Bidang	Deskripsi
Jadwalkan operasi tugas menggunakan peristiwa berikut	Pengaturan ini menentukan kapan tugas akan dijalankan. Nilai berikut tersedia: • **Jadwalkan berdasarkan waktu** – Ini adalah pengaturan default. Tugas akan berjalan sesuai waktu yang ditentukan. • **Saat pengguna masuk ke sistem** – Secara default, akses masuk (login) pengguna mana pun akan memicu tugas. Anda dapat mengubah pengaturan ini agar hanya akun pengguna tertentu yang dapat memicu tugas. • **Saat pengguna keluar dari sistem** – Secara default, akses keluar (logoff) pengguna mana pun akan memicu tugas. Anda dapat mengubah pengaturan ini agar hanya akun pengguna tertentu yang dapat memicu tugas. **Catatan** Tugas tidak akan berjalan saat sistem dimatikan. Mematikan dan keluar adalah peristiwa berbeda di konfigurasi penjadwalan. • **Pada startup sistem** – Tugas akan berjalan saat sistem operasi dimulai. • **Pada shutdown sistem** – Tugas akan berjalan saat sistem operasi dimatikan.
Jenis jadwal	Bidang ini muncul jika di **Jadwalkan operasi tugas menggunakan peristiwa berikut** Anda telah memilih **Jadwalkan berdasarkan waktu**. Nilai berikut tersedia: • **Bulanan** – Pilih bulan dan minggu atau hari dalam sebulan saat tugas akan berjalan. • **Harian** – Ini adalah pengaturan default. Pilih hari dalam seminggu saat tugas akan dijalankan. • **Per jam** – Pilih hari dalam pekan, jumlah pengulangan, dan interval waktu tugas akan berjalan.
Mulai pada	Bidang ini muncul jika di **Jadwalkan operasi tugas menggunakan**

© Acronis International GmbH, 2003-2024

Bidang	Deskripsi
	peristiwa berikut Anda telah memilih **Jadwalkan berdasarkan waktu** Pilih waktu yang tepat kapan tugas akan dijalankan.
Jalankan dalam rentang tanggal	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Jadwalkan berdasarkan waktu**. Atur periode waktu ketika jadwal yang sudah dikonfigurasi akan berlaku.
Tentukan akun pengguna yang akses masuknya ke sistem operasi akan memulai tugas	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Saat pengguna masuk ke sistem**. Nilai berikut tersedia: • **Semua pengguna** - Gunakan opsi ini jika Anda ingin akses masuk pengguna mana pun memicu tugas. • **Pengguna berikut** - Gunakan opsi ini jika Anda hanya ingin akses masuk akun pengguna tertentu yang memicu tugas.
Tentukan akun pengguna yang logout-nya dari sistem operasi akan memulai tugas	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Saat pengguna keluar dari sistem**. Nilai berikut tersedia: • **Pengguna mana pun** - Gunakan opsi ini jika Anda ingin logout pengguna mana pun memicu tugas. • **Pengguna berikut** - Gunakan opsi ini jika Anda hanya ingin logout akun pengguna tertentu yang memicu tugas.
Persyaratan untuk memulai	Mendefinisikan semua kondisi yang harus dipenuhi secara bersamaan agar tugas dapat dijalankan. Kondisi awal untuk pemindaian antimalware serupa dengan kondisi awal untuk **Modul cadangan** yang dijelaskan dalam "Persyaratan untuk memulai". Anda dapat menetapkan persyaratan awal tambahan berikut: • **Distribusikan waktu mulai tugas dalam rentang waktu** – Opsi ini memungkinkan Anda menentukan jangka waktu tugas untuk menghindari kemacetan jaringan. Anda dapat menentukan penundaan dalam jam atau menit. Misalnya, jika waktu mulai default adalah pukul 10.00 dan penundaannya adalah 60 menit, tugas akan dimulai antara pukul 10.00 sampai 11.00. • **Jika mesin dimatikan, jalankan tugas yang tertinggal pada saat mesin dinyalakan** • **Cegah mode tidur atau hibernasi selama menjalankan tugas** – Opsi ini hanya berlaku untuk mesin yang menjalankan Windows. • **Jika persyaratan awal tidak terpenuhi, tetap jalankan tugas**

© Acronis International GmbH, 2003-2024

Bidang	Deskripsi
	setelahnya – Tentukan periode waktu dalam jam saat tugas akan dijalankan setelahnya, terlepas dari kondisi awal lainnya. **Catatan** Persyaratan awal tidak didukung untuk Linux.

- Pilih kotak centang **Pindai hanya file baru dan yang diubah** jika Anda ingin memindai hanya file yang baru dibuat dan diubah.

Pengaturan default: **Diaktifkan**

- Dua opsi tambahan ditampilkan untuk **Pemindaian khusus** hanya untuk **Pemindaian lengkap**:

1. **Pindai file arsip**

   Pengaturan default: **Diaktifkan**.

   Maks kedalaman rekursi

   Pengaturan default: **16**

   Berapa banyak tingkat arsip tersemat yang dapat dipindai. Misalnya, dokumen MIME > arsip ZIP > arsip Office > isi dokumen.

   Ukuran maks

   Pengaturan default: **100**

   Ukuran maksimum file arsip yang akan dipindai.

2. **Pindai drive yang dapat dilepas**

Pengaturan default: **Dinonaktifkan**

- **Drive jaringan yang dipetakan (jarak jauh)**
- **Perangkat penyimpanan USB** (seperti pena dan hard drive eksternal)
- **CD/DVD**

Catatan
Pindai drive yang dapat dilepas tidak didukung untuk Linux.

Pengecualian proteksi

Pengecualian proteksi memungkinkan Anda menghilangkan kesalahan positif palsu ketika program tepercaya dianggap sebagai ransomware atau malware. Anda dapat menentukan item tepercaya dan diblokir dengan menambahkannya ke daftar pengecualian proteksi.

Dalam daftar item tepercaya, Anda dapat menambahkan file, proses, dan folder agar dianggap aman di sistem, dan untuk mencegah deteksi di masa mendatang.

© Acronis International GmbH, 2003-2024

Dalam daftar item yang diblokir, Anda dapat menambahkan proses dan hash. Opsi ini menjamin bahwa proses tersebut akan diblokir, dan beban kerja Anda akan aman.

Item pengecualian proteksi	Diblokir	Tepercaya
Hash	Ketika hash ditambahkan ke daftar yang diblokir, sistem akan menghentikan proses, berdasarkan hash yang disediakan. Misalnya, ketika Anda menambahkan hash MD5 ini, 938c2cc0dcc05f2b68c4287040cfcf71, proses yang terkait dengan hash ini akan diblokir.	Ketika hash ditambahkan ke daftar tepercaya, sistem akan mengetahui proses apa yang harus diabaikan dengan pemantauan, berdasarkan hash yang disediakan. Misalnya, saat Anda menambahkan hash MD5 ini, 938c2cc0dcc05f2b68c4287040cfcf71, proses yang terkait dengan hash ini akan dipercaya dan dikecualikan dari pemantauan.
Proses	Ketika suatu proses ditambahkan ke daftar yang diblokir, sistem akan mengetahui bahwa proses tersebut harus dipantau, dan proses tersebut akan selalu diblokir. Misalnya, jika Anda menambahkan path ini C:\Users\user1\application\nppInstaller.exe ke daftar yang diblokir, proses khusus ini akan diblokir, dan ketika Anda mencoba membukanya, proses tersebut tidak akan diizinkan untuk dimulai.	Ketika suatu proses ditambahkan ke daftar tepercaya, sistem akan mengetahui bahwa proses tersebut harus dikeluarkan dari pemantauan. **Catatan** Proses yang ditandai oleh Microsoft adalah selalu tepercaya. Misalnya, jika Anda menambahkan path ini C:\Users\user1\application\nppInstaller.exe, proses khusus ini akan dikecualikan dari pemantauan, dan antivirus tidak akan mengganggu proses ini.
File/folder		Ketika file atau folder ditambahkan ke daftar tepercaya, sistem akan mengetahui bahwa file atau folder tersebut harus selalu dianggap aman, dan file atau folder tersebut tidak perlu dipindai/dipantau.

Untuk menentukan item yang akan selalu dipercaya

1. Buka rencana proteksi.
2. Perluas modul **Proteksi Antivirus and Antimalware**.

© Acronis International GmbH, 2003-2024

3. Pilih opsi **Pengecualian**.
   Jendela **Pengecualian proteksi** terbuka.
4. Di bagian **Item tepercaya**, klik **Tambah** untuk memilih dari opsi yang tersedia:
   - Untuk memercayai file, folder, atau proses, pilih opsi **File/folder/proses**. Jendela **Tambahkan file/folder/proses** terbuka.
     - Di bidang **File/proses/folder**, masukkan jalur untuk setiap proses, folder, atau file pada baris baru. Di bagian **Deskripsi**, masukkan deskripsi singkat sehingga Anda dapat mengenali perubahan Anda dalam daftar item tepercaya.
     - Pilih kotak centang **Tambahkan sebagai file/folder** untuk memercayai file/folder. Contoh deskripsi folder: D:\folder\, /home/Folder/folder2, F:\
     - Pilih kotak centang **Tambahkan sebagai proses** untuk memercayai suatu proses. Proses yang dipilih akan dikecualikan dari pemantauan.

       Catatan
       Tentukan jalur lengkap ke proses yang dapat dieksekusi, dimulai dengan huruf drive. Misalnya, `C:\Windows\Temp\er76s7sdkh.exe`.

       Catatan
       Jalur jaringan lokal didukung. mis: \\localhost\folderpath\file.exe

   - Pilih opsi **Hash** untuk menambahkan hash MD5 ke daftar item tepercaya. Jendela **Tambahkan hash** terbuka.
     - Di sini Anda dapat menyisipkan hash MD5 pada baris yang berbeda untuk disertakan sebagai hash tepercaya dalam daftar pengecualian Proteksi. Berdasarkan hash ini, Cyber Protection akan mengecualikan proses yang dijelaskan oleh hash MD5 agar tidak dipantau.

Pengaturan default: Tidak ada pengecualian yang ditentukan secara default.

Untuk menentukan item yang akan selalu diblokir

1. Buka rencana proteksi.
2. Perluas modul **Proteksi Antivirus and Antimalware**.
3. Pilih opsi **Pengecualian proteksi**. Jendela **Pengecualian proteksi** terbuka.

   Di bagian **Item yang diblokir**, klik **Tambah** untuk memilih dari opsi yang tersedia:
   - Untuk memblokir proses, pilih opsi **Proses**. Jendela **Tambahkan proses** terbuka.
     - Di bidang **Proses**, masukkan jalur untuk setiap proses pada baris baru. Di bidang **Deskripsi**, masukkan deskripsi singkat sehingga Anda dapat mengenali perubahan Anda dalam daftar item yang diblokir.

       Catatan
       Proses ini tidak akan bisa dimulai selama Active Protection diaktifkan pada mesin.

   - Untuk memblokir hash, pilih opsi **Hash**. Jendela **Tambahkan hash** ditampilkan.
     - Di bidang **Hash**, masukkan hash untuk setiap proses pada baris baru. Di bidang **Deskripsi**, masukkan deskripsi singkat sehingga Anda dapat mengenali perubahan Anda dalam daftar

© Acronis International GmbH, 2003-2024

item yang diblokir.

Pengaturan default: Tidak ada pengecualian yang ditentukan secara default.

Wildcard

Untuk menentukan folder, Anda dapat menggunakan karakter * dan ?. Tanda bintang (*) menggantikan nol atau lebih banyak karakter. Tanda tanya (?) menggantikan satu karakter. Variabel lingkungan, seperti `%AppData%`, tidak dapat digunakan.

Anda dapat menggunakan wildcard (*) untuk menambahkan item ke daftar pengecualian.

- Wildcard dapat digunakan di tengah atau akhir deskripsi.

Contoh wildcard yang dapat diterima dalam deskripsi:

C:*.pdf

D:\folders\file.*

C:\Users*\AppData\Roaming

- Wildcard tidak dapat digunakan di awal deskripsi.

Contoh wildcard yang tidak dapat diterima dalam deskripsi:

*.docx

*:\folder\

Variabel

Anda juga dapat menggunakan variabel untuk menambahkan item ke daftar Pengecualian proteksi, dengan batasan berikut:

- Untuk Windows, hanya variabel SISTEM yang didukung. Variabel spesifik pengguna, misalnya, %USERNAME%, %APPDATA% tidak didukung. Variabel dengan {username} tidak didukung. Untuk informasi lebih lanjut, lihat https://ss64.com/nt/syntax-variables.html.
- Untuk macOS, variabel lingkungan tidak didukung.
- Untuk Linux, variabel lingkungan tidak didukung.

Contoh format yang didukung:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Deskripsi

Anda dapat menggunakan bidang **Deskripsi** untuk membuat catatan mengenai pengecualian yang ditambahkan ke daftar pengecualian proteksi. Beberapa saran mengenai catatan yang dapat Anda

© Acronis International GmbH, 2003-2024

buat:

- Alasan dan tujuan pengecualian.
- Nama file pengecualian hash yang sebenarnya.
- Tanda waktu.

Jika ada beberapa item yang ditambahkan dalam satu entri, hanya ada 1 komentar yang dapat ditangkap untuk beberapa item.

Active Protection di Cyber Backup edisi Standard

Dalam edisi Cyber Backup Standard, Active Protection adalah modul terpisah dalam rencana proteksi. Sehingga, Active Protection dapat dikonfigurasi secara terpisah dan diterapkan pada perangkat atau sekelompok perangkat yang berbeda-beda.

Di semua edisi lain dari layanan Perlindungan Cyber, Active Protection adalah bagian dari modul **Antivirus & Antimalware** dari rencana perlindungan.

Pengaturan default: **Diaktifkan**.

Catatan
Agen perlindungan harus dipasang pada mesin yang dilindungi. Untuk informasi selengkapnya tentang sistem operasi dan fitur yang didukung, lihat "Platform yang didukung" (hlm. 814).

Cara kerjanya

Active Protection memantau proses yang berjalan pada mesin yang terlindungi. Ketika proses pihak ketiga mencoba mengenkripsi file atau menambang cryptocurrency, Active Protection akan menghasilkan peringatan dan melakukan tindakan tambahan, sebagaimana ditentukan dalam rencana proteksi.

Selain itu, Active Protection juga mencegah perubahan yang tidak sah pada proses perangkat lunak pencadangan itu sendiri, catatan registri, file dan konfigurasi yang dapat dieksekusi, serta cadangan yang berada di folder lokal.

Untuk mengidentifikasi proses berbahaya, Active Protection menggunakan heuristik perilaku. Active Protection membandingkan rangkaian tindakan yang dilakukan oleh proses dengan rangkaian event yang terekam pada database pola perilaku berbahaya. Pendekatan ini memungkinkan Active Protection untuk mendeteksi malware baru berdasarkan perilaku tipikalnya.

Pengaturan Active Protection di Cyber Backup Standard

Pada Cyber Backup edisi Standard, Anda dapat mengonfigurasi fitur Active Protection berikut:

- Tindakan saat deteksi
- Perlindungan diri
- Perlindungan folder jaringan

© Acronis International GmbH, 2003-2024

- Perlindungan sisi server
- Deteksi proses cryptomining
- Pengecualian

Catatan
Active Protection untuk Linux mendukung pengaturan berikut: Tindakan saat deteksi, perlindungan folder Jaringan, dan Pengecualian. Perlindungan folder jaringan selalu aktif dan tidak dapat dikonfigurasi.

Tindakan saat deteksi

Di bagian **Tindakan saat deteksi**, pilih salah satu opsi yang tersedia:

- **Hanya beri tahu**
  Perangkat lunak ini akan mengeluarkan peringatan tentang proses yang dicurigai sebagai aktivitas ransomware.
- **Hentikan proses**
  Perangkat lunak ini akan mengeluarkan peringatan dan menghentikan proses yang dicurigai sebagai aktivitas ransomware.
- **Kembalikan menggunakan cache**
  Perangkat lunak akan mengeluarkan peringatan, menghentikan proses, dan mengembalikan perubahan file menggunakan cache layanan.

Pengaturan default: **Kembalikan menggunakan cache**.

Proteksi diri mencegah perubahan tidak sah pada proses perangkat lunak itu sendiri, catatan registri, file yang dapat dijalankan dan konfigurasi, serta cadangan yang terletak di folder lokal Anda.

Administrator dapat mengaktifkan **Perlindungan diri**, tanpa mengaktifkan **Active Protection**.

Pengaturan default: **Aktif**.

Catatan
Swaproteksi tidak didukung untuk Linux.

Untuk mengaktifkan Proteksi diri

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Perlindungan diri**.
3. Gunakan tombol alih **Perlindungan diri** untuk mengaktifkannya.

Untuk mengaktifkan Proteksi kata sandi

1. Setelah fitur **Perlindungan diri** diaktifkan, Anda dapat mengaktifkan fitur **Proteksi kata sandi** dengan menggunakan tombol pengalih.

© Acronis International GmbH, 2003-2024

2. Klik **Buat kata sandi baru** untuk membuat kata sandi guna mengubah atau menghapus agen lokal.
3. Klik **Salin**, lalu tempelkan di tempat yang aman karena ini akan diminta ketika Anda ingin mengubah daftar komponen di lokasi terkait.

   Penting
   Kata sandi tidak akan tersedia setelah Anda menutup jendela. Agar kata sandi ini diterapkan ke perangkat, pengaturan rencana proteksi harus disimpan.

4. Klik **Tutup**.

Proteksi kata sandi mencegah pengguna atau perangkat lunak yang tidak sah menghapus instalasi Agen untuk Windows atau memodifikasi komponennya. Tindakan ini hanya dimungkinkan dengan kata sandi yang dapat diberikan oleh administrator.

Kata sandi tidak pernah diperlukan untuk tindakan berikut:

- Memperbarui instalasi dengan menjalankan program penyiapan setempat
- Memperbarui instalasi dengan menggunakan konsol Cyber Protect
- Memperbaiki instalasi

Pengaturan default: **Dinonaktifkan**

Untuk informasi lebih lanjut tentang cara mengaktifkan **Proteksi kata sandi**, lihat Mencegah penghapusan instalasi atau modifikasi agen yang tidak sah.

Perlindungan folder jaringan

Pengaturan **Lindungi folder jaringan yang dipetakan sebagai drive lokal** menentukan apakah Active protection melindungi dari proses berbahaya folder jaringan lokal yang dipetakan sebagai drive lokal.

Pengaturan ini berlaku untuk folder yang dibagikan melalui protokol SMB atau NFS.

Jika file awalnya berada di drive yang dipetakan, file tidak dapat disimpan ke lokasi asli ketika diekstraksi dari cache melalui tindakan **Kembalikan menggunakan cache**. Sebaliknya, file akan disimpan ke folder yang ditentukan dalam pengaturan ini. Folder default adalah `C:\ProgramData\Acronis\Restored Network Files` untuk Windows, dan `Library/Application Support/Acronis/Restored Network Files/` untuk macOS. Jika tidak ada, folder akan dibuat. Jika ingin mengubah jalur ini, tentukan folder lokal. Folder jaringan, termasuk folder pada drive yang dipetakan, tidak didukung.

Pengaturan default: **Aktif**.

Fitur ini menentukan apakah Active protection mampu mengamankan folder jaringan yang Anda bagikan dari koneksi masuk eksternal dari server lain di jaringan yang berpotensi menimbulkan

© Acronis International GmbH, 2003-2024

ancaman.

Pengaturan default: **Nonaktif**.

Catatan
Perlindungan sisi server tidak didukung untuk Linux.

Untuk mengatur koneksi tepercaya

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Proteksi sisi server**.
3. Gunakan tombol **Proteksi sisi server** untuk mengaktifkannya.
4. Pilih tab **Tepercaya**.
5. Di bidang **Koneksi tepercaya**, klik **Tambahkan** guna menentukan koneksi yang diizinkan untuk mengubah data.
6. Di bidang **Nama Komputer/Akun**, ketikkan nama komputer dan akun mesin tempat agen proteksi diinstal. Contohnya, `MyComputer\TestUser`.
7. Di bidang **Nama host**, ketikkan nama host mesin yang diizinkan untuk terhubung ke mesin menggunakan agen proteksi.
8. Klik tanda centang di sebelah kanan untuk menyimpan definisi koneksi.
9. Klik **Selesai**.

Untuk mengatur koneksi yang diblokir

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Proteksi sisi server**.
3. Gunakan tombol **Proteksi sisi server** untuk mengaktifkannya.
4. Pilih tab **Diblokir**.
5. Di bidang **Koneksi yang diblokir**, klik **Tambahkan** untuk menentukan koneksi yang tidak diperbolehkan untuk mengubah data.
6. Di bidang **Nama Komputer/Akun**, ketikkan nama komputer dan akun mesin tempat agen proteksi diinstal. Contohnya, `MyComputer\TestUser`.
7. Di bidang **Nama host**, ketikkan nama host mesin yang diizinkan untuk terhubung ke mesin menggunakan agen proteksi.
8. Pilih kotak centang di sebelah kanan untuk menyimpan definisi koneksi.
9. Klik **Selesai**.

Malware Cryptomining menurunkan kinerja aplikasi yang berguna, meningkatkan tagihan listrik, dan dapat menyebabkan gangguan sistem dan bahkan kerusakan perangkat keras akibat

© Acronis International GmbH, 2003-2024

penyalahgunaan. Fitur **Deteksi proses cryptomining** melindungi perangkat Anda dari malware cryptomining untuk mencegah penggunaan sumber daya komputer tanpa izin.

Administrator dapat mengaktifkan **Deteksi proses cryptomining**, tanpa mengaktifkan **Active Protection**. Pengaturan default: **Diaktifkan**.

Catatan
Deteksi proses cryptomining tidak didukung untuk Linux.

Untuk mengkonfigurasi perlindungan folder jaringan

1. Di jendela **Buat rencana proteksi**, perluas modul **Proteksi Antivirus & Antimalware**.
2. Klik **Deteksi proses cryptomining**.
3. Gunakan tombol **Deteksi proses cryptomining** untuk mengaktifkan atau menonaktifkan fitur ini.
4. Pilih apa yang harus dilakukan dengan proses yang diduga merupakan aktivitas cryptomining:

   Pengaturan default: **Hentikan proses**

   - **Hanya notifikasi**—Perangkat lunak mengeluarkan peringatan.
   - **Hentikan proses** — Perangkat lunak mengeluarkan peringatan dan menghentikan proses.
5. Klik **Selesai** untuk menerapkan opsi yang dipilih pada rencana proteksi Anda.

Pengecualian proteksi memungkinkan Anda menghilangkan kesalahan positif palsu ketika program tepercaya dianggap sebagai ransomware atau malware. Anda dapat menentukan item tepercaya dan diblokir dengan menambahkannya ke daftar pengecualian proteksi.

Dalam daftar item tepercaya, Anda dapat menambahkan file, proses, dan folder agar dianggap aman di sistem, dan untuk mencegah deteksi di masa mendatang.

Dalam daftar item yang diblokir, Anda dapat menambahkan proses dan hash. Opsi ini menjamin bahwa proses tersebut akan diblokir, dan beban kerja Anda akan aman.

Item pengecualian proteksi	Diblokir	Tepercaya
Hash	Ketika hash ditambahkan ke daftar yang diblokir, sistem akan menghentikan proses, berdasarkan hash yang disediakan. Misalnya, ketika Anda menambahkan hash MD5 ini, 938c2cc0dcc05f2b68c4287040cfcf71, proses yang terkait dengan hash ini akan diblokir.	Ketika hash ditambahkan ke daftar tepercaya, sistem akan mengetahui proses apa yang harus diabaikan dengan pemantauan, berdasarkan hash yang disediakan. Misalnya, saat Anda menambahkan hash MD5 ini, 938c2cc0dcc05f2b68c4287040cfcf71, proses yang terkait dengan hash ini akan dipercaya dan dikecualikan dari

© Acronis International GmbH, 2003-2024

Item pengecualian proteksi	Diblokir	Tepercaya
		pemantauan.
Proses	Ketika suatu proses ditambahkan ke daftar yang diblokir, sistem akan mengetahui bahwa proses tersebut harus dipantau, dan proses tersebut akan selalu diblokir. Misalnya, jika Anda menambahkan path ini C:\Users\user1\application\nppInstaller.exe ke daftar yang diblokir, proses khusus ini akan diblokir, dan ketika Anda mencoba membukanya, proses tersebut tidak akan diizinkan untuk dimulai.	Ketika suatu proses ditambahkan ke daftar tepercaya, sistem akan mengetahui bahwa proses tersebut harus dikeluarkan dari pemantauan. **Catatan** Proses yang ditandai oleh Microsoft adalah selalu tepercaya. Misalnya, jika Anda menambahkan path ini C:\Users\user1\application\nppInstaller.exe, proses khusus ini akan dikecualikan dari pemantauan, dan antivirus tidak akan mengganggu proses ini.
File/folder		Ketika file atau folder ditambahkan ke daftar tepercaya, sistem akan mengetahui bahwa file atau folder tersebut harus selalu dianggap aman, dan file atau folder tersebut tidak perlu dipindai/dipantau.

Untuk menentukan item yang akan selalu dipercaya

1. Buka rencana proteksi.
2. Perluas modul **Proteksi Antivirus and Antimalware**.
3. Pilih opsi **Pengecualian**.
   Jendela **Pengecualian proteksi** terbuka.
4. Di bagian **Item tepercaya**, klik **Tambah** untuk memilih dari opsi yang tersedia:
   - Untuk memercayai file, folder, atau proses, pilih opsi **File/folder/proses**. Jendela **Tambahkan file/folder/proses** terbuka.
     - Di bidang **File/proses/folder**, masukkan jalur untuk setiap proses, folder, atau file pada baris baru. Di bagian **Deskripsi**, masukkan deskripsi singkat sehingga Anda dapat mengenali perubahan Anda dalam daftar item tepercaya.
     - Pilih kotak centang **Tambahkan sebagai file/folder** untuk memercayai file/folder. Contoh deskripsi folder: D:\folder\, /home/Folder/folder2, F:\
     - Pilih kotak centang **Tambahkan sebagai proses** untuk memercayai suatu proses. Proses yang dipilih akan dikecualikan dari pemantauan.

© Acronis International GmbH, 2003-2024

Catatan
Tentukan jalur lengkap ke proses yang dapat dieksekusi, dimulai dengan huruf drive. Misalnya, `C:\Windows\Temp\er76s7sdkh.exe`.

Catatan
Jalur jaringan lokal didukung. mis: \\localhost\folderpath\file.exe

- Pilih opsi **Hash** untuk menambahkan hash MD5 ke daftar item tepercaya. Jendela **Tambahkan hash** terbuka.
  - Di sini Anda dapat menyisipkan hash MD5 pada baris yang berbeda untuk disertakan sebagai hash tepercaya dalam daftar pengecualian Proteksi. Berdasarkan hash ini, Cyber Protection akan mengecualikan proses yang dijelaskan oleh hash MD5 agar tidak dipantau.

Pengaturan default: Tidak ada pengecualian yang ditentukan secara default.

Untuk menentukan item yang akan selalu diblokir

1. Buka rencana proteksi.
2. Perluas modul **Proteksi Antivirus and Antimalware**.
3. Pilih opsi **Pengecualian proteksi**. Jendela **Pengecualian proteksi** terbuka.

   Di bagian **Item yang diblokir**, klik **Tambah** untuk memilih dari opsi yang tersedia:
- Untuk memblokir proses, pilih opsi **Proses**. Jendela **Tambahkan proses** terbuka.
  - Di bidang **Proses**, masukkan jalur untuk setiap proses pada baris baru. Di bidang **Deskripsi**, masukkan deskripsi singkat sehingga Anda dapat mengenali perubahan Anda dalam daftar item yang diblokir.

Catatan
Proses ini tidak akan bisa dimulai selama Active Protection diaktifkan pada mesin.

- Untuk memblokir hash, pilih opsi **Hash**. Jendela **Tambahkan hash** ditampilkan.
  - Di bidang **Hash**, masukkan hash untuk setiap proses pada baris baru. Di bidang **Deskripsi**, masukkan deskripsi singkat sehingga Anda dapat mengenali perubahan Anda dalam daftar item yang diblokir.

Pengaturan default: Tidak ada pengecualian yang ditentukan secara default.

Wildcard

Untuk menentukan folder, Anda dapat menggunakan karakter * dan ?. Tanda bintang (*) menggantikan nol atau lebih banyak karakter. Tanda tanya (?) menggantikan satu karakter. Variabel lingkungan, seperti `%AppData%`, tidak dapat digunakan.

Anda dapat menggunakan wildcard (*) untuk menambahkan item ke daftar pengecualian.

- Wildcard dapat digunakan di tengah atau akhir deskripsi.

Contoh wildcard yang dapat diterima dalam deskripsi:

© Acronis International GmbH, 2003-2024

C:*.pdf

D:\folders\file.*

C:\Users*\AppData\Roaming

- Wildcard tidak dapat digunakan di awal deskripsi.

Contoh wildcard yang tidak dapat diterima dalam deskripsi:

*.docx

*:\folder\

Variabel

Anda juga dapat menggunakan variabel untuk menambahkan item ke daftar Pengecualian proteksi, dengan batasan berikut:

- Untuk Windows, hanya variabel SISTEM yang didukung. Variabel spesifik pengguna, misalnya, %USERNAME%, %APPDATA% tidak didukung. Variabel dengan {username} tidak didukung. Untuk informasi lebih lanjut, lihat https://ss64.com/nt/syntax-variables.html.
- Untuk macOS, variabel lingkungan tidak didukung.
- Untuk Linux, variabel lingkungan tidak didukung.

Contoh format yang didukung:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Deskripsi

Anda dapat menggunakan bidang **Deskripsi** untuk membuat catatan mengenai pengecualian yang ditambahkan ke daftar pengecualian proteksi. Beberapa saran mengenai catatan yang dapat Anda buat:

- Alasan dan tujuan pengecualian.
- Nama file pengecualian hash yang sebenarnya.
- Tanda waktu.

Jika ada beberapa item yang ditambahkan dalam satu entri, hanya ada 1 komentar yang dapat ditangkap untuk beberapa item.

Pemfilteran URL

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

© Acronis International GmbH, 2003-2024

Malware sering didistribusikan oleh situs yang berbahaya atau terinfeksi dan menggunakan apa yang disebut dengan metode infeksi akibat Pengunduhan drive-by.

Fungsi pemfilteran URL memungkinkan Anda untuk melindungi mesin dari ancaman seperti malware dan phishing dari internet. Anda dapat melindungi organisasi Anda dengan memblokir akses pengguna ke situs web yang mungkin memiliki konten berbahaya.

Pemfilteran URL juga memungkinkan Anda untuk mengendalikan penggunaan web guna mematuhi peraturan eksternal dan kebijakan perusahaan internal. Anda dapat mengonfigurasi akses ke situs web bergantung pada kategori yang terkait dengannya. Pemfilteran URL saat ini mendukung 44 kategori situs web dan memungkinkan untuk mengelola akses ke situs-situs web tersebut.

Saat ini, koneksi HTTP/HTTPS di mesin Windows akan diperiksa oleh agen perlindungan.

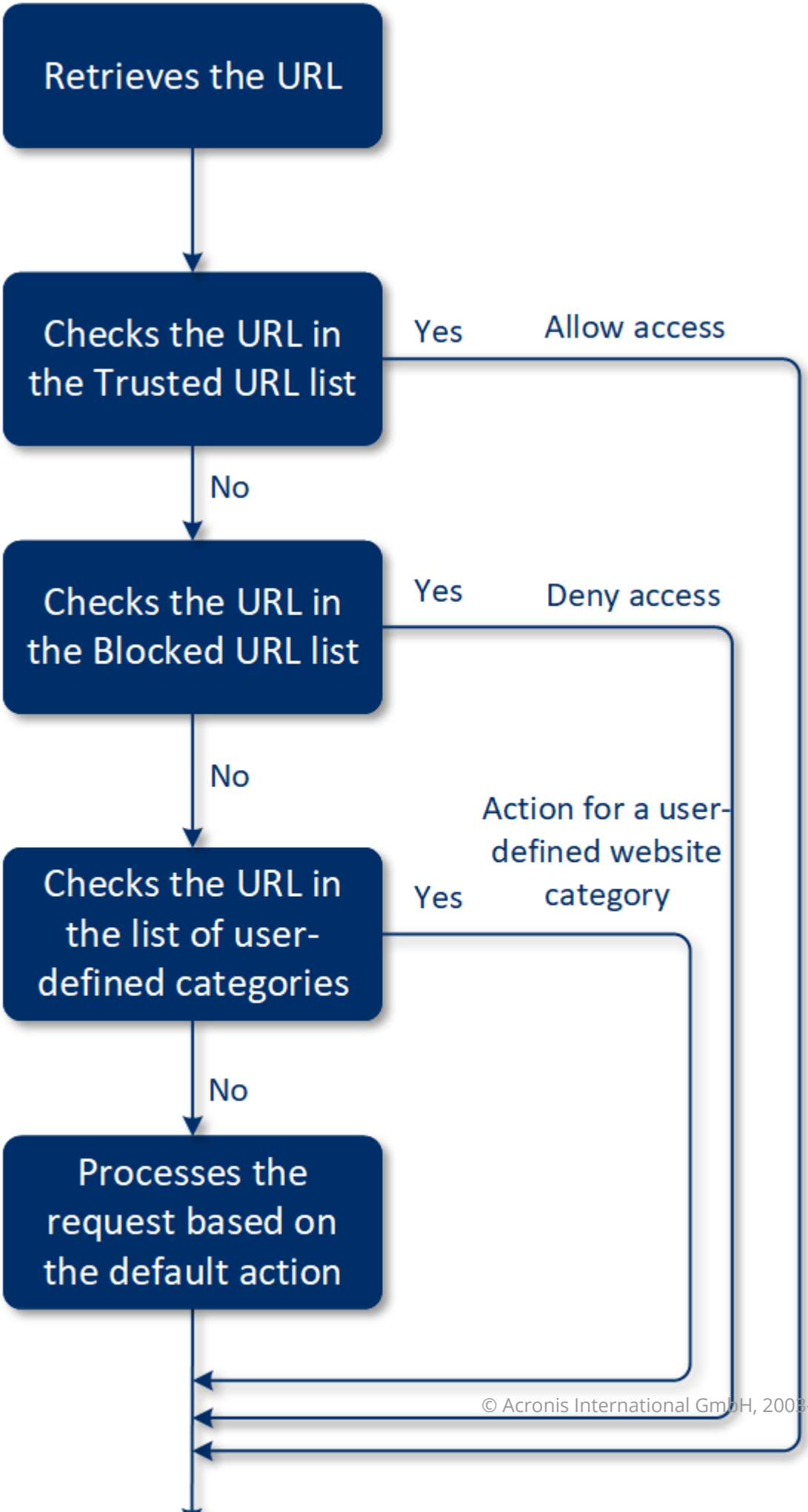
Fitur pemfilteran URL memerlukan koneksi internet agar dapat berfungsi.

Catatan
Untuk mencegah kemungkinan masalah kompatibilitas dengan agen proteksi versi 15.0.26692 (rilis C21.03 HF1) dan versi yang lebih lama, fungsi pemfilteran URL akan secara otomatis dinonaktifkan jika solusi antivirus lain terdeteksi, atau jika layanan Windows Security Center tidak ada di sistem. Di agen proteksi selanjutnya, masalah kompatibilitas diselesaikan sehingga pemfilteran URL selalu diaktifkan sesuai dengan kebijakan.

Cara kerjanya

Pengguna memasukkan tautan URL ke browser. Interceptor mendapatkan tautan dan mengirimnya ke agen perlindungan. Agen mendapatkan URL, menganalisisnya, lalu memeriksa putusannya. Interceptor mengarahkan pengguna ke halaman dengan pesan tindakan yang tersedia untuk melanjutkan secara manual ke halaman yang diminta.

© Acronis International GmbH, 2003-2024



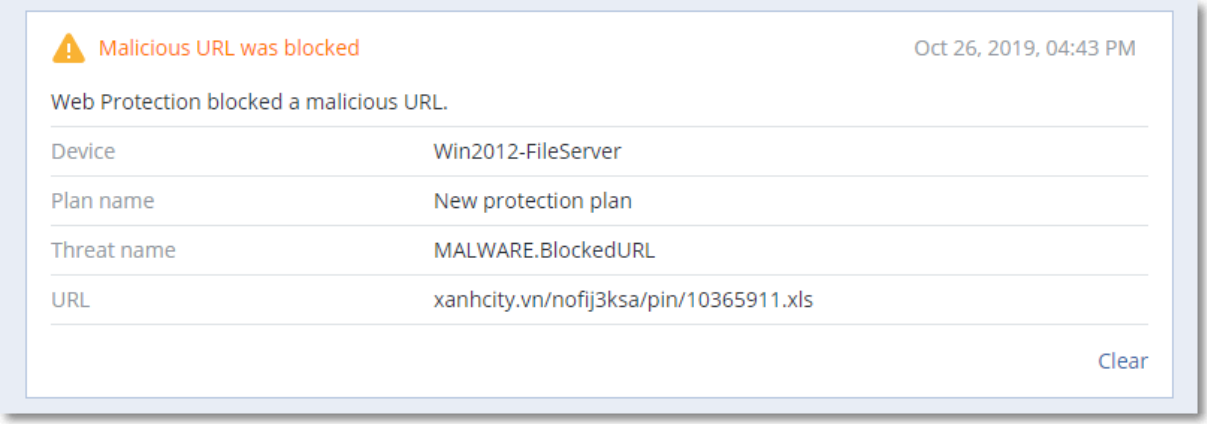
© Acronis International GmbH, 2003-2024

Alur kerja konfigurasi pemfilteran URL

Umumnya, konfigurasi pemfilteran URL terdiri dari langkah-langkah berikut:

1. Anda membuat rencana proteksi dengan modul **pemfilteran URL** yang diaktifkan.
2. Menentukan pengaturan pemfilteran URL (lihat di bawah).
3. Tetapkan rencana proteksi pada mesin.

Untuk memeriksa URL mana yang telah diblokir, buka **Pemantauan**> **Peringatan**.



Pengaturan pemfilteran URL

Pengaturan berikut dapat ditetapkan untuk modul pemfilteran URL.

Akses situs web berbahaya

Tentukan tindakan apa yang akan dilakukan saat pengguna membuka situs web yang berbahaya:

- **Hanya notifikasi**—Perangkat lunak mengeluarkan peringatan tentang proses yang dicurigai sebagai aktivitas ransomware.
- **Blok** —memblokir akses ke situs web berbahaya. Seorang pengguna tidak akan dapat mengakses situs web dan peringatan akan menyala.
- **Selalu tanya pengguna**—tanyakan apakah pengguna ingin melanjutkan ke situs web atau kembali.

Kategori yang akan difilter

Ada 44 kategori situs web yang dapat Anda konfigurasi aksesnya:

- **Izinkan** – mengizinkan akses ke situs web terkait dengan kategori yang dipilih.
- **Tolak** – menolak akses ke situs web terkait dengan kategori yang dipilih.

Secara default, semua kategori diizinkan.

© Acronis International GmbH, 2003-2024

Tampilkan semua pemberitahuan untuk URL yang diblokir berdasarkan kategori – jika diaktifkan, Anda akan mendapat semua pemberitahuan yang ditampilkan di baki untuk URL yang diblokir berdasarkan kategori. Jika situs web memiliki beberapa subdomain, sistem juga membuat pemberitahuan untuk subdomain tersebut, maka jumlah pemberitahuan akan besar.

Di tabel di bawah ini, Anda dapat menemukan deskripsi kategori:

	Kategori situs web	Deskripsi
1	**Periklanan**	Kategori ini mencakup domain yang tujuan utamanya adalah untuk menyajikan iklan.
2	**Papan pesan**	Kategori ini mencakup forum, papan diskusi, dan situs web jenis pertanyaan-jawaban. Tidak termasuk dalam kategori ini adalah bagian khusus dalam situs web perusahaan tempat pelanggan mengajukan pertanyaan.
3	**Situs web pribadi**	Kategori ini mencakup situs web pribadi, serta semua jenis blog: individual, grup, dan bahkan blog perusahaan. Blog adalah jurnal yang diterbitkan di World Wide Web. Blog terdiri dari entri (“postingan”), yang biasanya ditampilkan dalam urutan kronologis terbalik, sehingga postingan terbaru muncul terlebih dahulu.
4	**Situs web perusahaan/bisnis**	Ini adalah kategori luas yang mencakup situs web perusahaan yang biasanya tidak termasuk dalam kategori lainnya.
5	**Perangkat lunak komputer**	Kategori ini mencakup situs web yang menawarkan perangkat lunak komputer, khususnya yang merupakan sumber-terbuka, freeware, atau shareware. Dapat tercakup di dalamnya adalah beberapa toko perangkat lunak online.
6	**Obat-obatan medis**	Kategori ini mencakup situs web yang terkait dengan obat-obatan/alkohol/cerutu yang mendiskusikan penggunaan atau penjualan obat-obatan atau peralatan medis, alkohol, atau produk tembakau (sah). Perhatikan bahwa obat-obatan terlarang termasuk dalam kategori Narkotika.
7	**Pendidikan**	Kategori ini mencakup situs web yang dimiliki lembaga pendidikan resmi, termasuk yang berada di luar domain .edu. Termasuk juga di dalamnya adalah situs web pendidikan, seperti ensiklopedia.
8	**Hiburan**	Kategori ini mencakup situs web yang menyediakan informasi tentang kegiatan dan museum artistik, serta situs web yang meninjau atau menilai konten seperti film, musik, atau kesenian.
9	**Berbagi file**	Kategori ini mencakup situs web berbagi file tempat pengguna dapat mengunggah file dan membaginya dengan orang lain. Termasuk juga di dalamnya adalah situs web untuk berbagi torrent dan pelacak torrent.
10	**Keuangan**	Kategori ini mencakup situs web yang dimiliki semua bank di seluruh

© Acronis International GmbH, 2003-2024

		dunia yang menyediakan akses online. Beberapa koperasi simpan pinjam dan lembaga keuangan lainnya juga termasuk di kategori ini. Namun, beberapa bank lokal mungkin tidak termasuk.
11	**Perjudian**	Kategori ini mencakup situs web perjudian. Ini adalah situs web tipe “casino online” atau “lotre online”, yang biasanya mewajibkan pembayaran sebelum pengguna bisa berjudi memperebutkan uang di roulette, poker, blackjack online, atau game serupa. Beberapa di antaranya sah, yang artinya ada kesempatan untuk menang; dan beberapa lainnya mengandung penipuan, yang artinya tidak ada kesempatan untuk menang. Kategori ini juga mendeteksi situs web “tips dan tipuan bertaruh” yang menjelaskan cara menghasilkan uang di situs web judi dan lotre online.
12	**Game**	Kategori ini mencakup situs web yang menyediakan game online, biasanya berdasarkan applet Adobe Flash atau JAVA. Game yang gratis atau yang memerlukan langganan tidak berpengaruh pada deteksi, namun situs web bergaya kasino terdeteksi dalam kategori Perjudian. Kategori ini tidak mencakup: • Situs web resmi perusahaan yang mengembangkan game video (kecuali jika perusahaan tersebut membuat game online) • Situs web diskusi di mana game dibahas • Situs web di mana game offline dapat diunduh (beberapa di antaranya termasuk dalam Kategori ilegal) • Game yang mewajibkan pengguna untuk mengunduh dan menjalankan file yang dapat dieksekusi, seperti World of Warcraft; itu dapat dicegah dengan cara yang berbeda seperti firewall
13	**Pemerintah**	Kategori ini mencakup situs web pemerintah, termasuk lembaga pemerintah, kedutaan, dan situs web kantor.
14	**Peretasan**	Kategori ini mencakup situs web yang menyediakan alat, artikel, dan platform diskusi tentang peretasan untuk para hacker (peretas). Tercakup juga di dalamnya adalah situs web yang menawarkan eksploit untuk platform umum yang memfasilitasi peretasan akun Facebook atau Gmail.
15	**Aktivitas ilegal**	Kategori ini mencakup situs web yang terkait dengan kebencian, kekerasan, dan rasisme, dan ditujukan untuk memblokir situs web dalam kategori berikut: • Situs web milik organisasi teroris • Situs web dengan konten rasis atau xenofobia • Situs web yang membahas olahraga agresif dan/atau mempromosikan kekerasan
16	**Kesehatan dan kebugaran**	Kategori ini mencakup situs web yang berhubungan dengan lembaga kesehatan, situs web yang terkait dengan pencegahan dan pengobatan

© Acronis International GmbH, 2003-2024

		penyakit, situs web yang menawarkan informasi atau produk tentang penurunan berat badan, diet, steroid, anabolik, atau produk HGH, serta situs web yang menyediakan informasi tentang operasi plastik.
17	**Hobi**	Kategori ini mencakup situs web yang menampilkan sumber daya terkait dengan aktivitas yang biasanya dilakukaan dalam waktu luang seseorang, seperti mengoleksi sesuatu, kesenian dan kerajian, serta bersepeda.
18	**Hosting web**	Kategori ini mencakup layanan hosting situs web gratis dan komersial yang memungkinkan pengguna pribadi dan organisasi untuk membuat dan meluncurkan situs web.
19	**Unduhan ilegal**	Kategori ini mencakup situs web terkait dengan pembajakan perangkat lunak, termasuk: • Situs web pelacak rekan-ke-rekan (BitTorrent, emule, DC++) yang dikenal membantu mendistribusikan konten berhak cipta tanpa persetujuan pemilik hak cipta • Situs web dan papan diskusi Warez (perangkat lunak komersial yang dibajak) • Situs web yang menyediakan crack, pembuat kode, dan nomor seri bagi penggunanya untuk memfasilitasi penggunaan perangkat lunak secara ilegal Beberapa situs web ini juga dapat terdeteksi sebagai pornografi atau alkohol/rokok, karena sering menggunakan iklan porno atau alkohol untuk mendapatkan uang.
20	**Layanan pesan instan**	Kategori ini mencakup situs web layanan pesan instan dan obrolan yang memungkinkan pengguna untuk mengobrol secara waktu-nyata. Selain itu, kategori ini akan mendeteksi yahoo.com dan gmail.com karena keduanya berisi layanan pesan instan yang tersemat.
21	**Pekerjaan/lapangan kerja**	Kategori ini mencakup situs web yang menampilkan papan lowongan kerja, iklan khusus terkait pekerjaan, dan kesempatan berkarir, serta agregator layanan tersebut. Tidak termasuk dalam kategori ini adalah agensi perekrutan atau halaman “pekerjaan” di situs web perusahaan reguler.
22	**Konten dewasa**	Kategori ini mencakup konten yang dilabeli oleh pembuat situs web sebagai yang memerlukan audiens dewasa. Termasuk dalam kategori ini adalah berbagai situs web mulai dari situs web tentang buku Kama Sutra dan pendidikan seks, hingga pornografi ekstrem.
23	**Narkotika**	Kategori ini mencakup situs web yang membagi informasi tentang obat-obatan candu dan ilegal. Tercakup juga dalam kategori ini adalah situs web yang membahas obat-obatan untuk perkembangan atau pertumbuhan.

© Acronis International GmbH, 2003-2024

24	**Berita**	Kategori ini mencakup situs web berita yang menyediakan berita teks dan video. Kategori ini berupaya untuk mencakup situs web berita global dan lokal; namun, beberapa situs web kecil tentang berita mungkin tidak tercakup.
25	**Kencan online**	Kategori ini mencakup situs web kencan online – berbayar dan gratis – di sini pengguna dapat mencari orang lain menggunakan sejumlah kriteria. Mereka juga dapat memposting profil agar orang lain dapat mencari mereka. Kategori ini mencakup situs web kencan online berbayar dan gratis. Oleh karena sebagian besar jejaring sosial populer dapat digunakan sebagai situs web kencan online, beberapa situs web populer seperti Facebook juga terdeteksi dalam kategori ini. Kami menyarankan Anda menggunakan kategori ini dengan kategori Jejaring sosial.
26	**Pembayaran online**	Kategori ini mencakup situs web yang menawarkan pembayaran atau transfer uang secara online. Kategori ini mendeteksi situs web pembayaran populer seperti PayPal atau Moneybookers. Selain itu, kategori ini secara heuristik mendeteksi halaman web di situs web reguler yang meminta informasi kartu kredit, memungkinkan deteksi toko online yang tersembunyi, tidak dikenal, atau ilegal.
27	**Berbagi foto**	Kategori ini mencakup situs web berbagi foto yang tujuan utamaya adalah memungkinkan pengguna untuk mengunggah dan berbagi foto.
28	**Toko online**	Kategori ini mencakup toko online ternama. Situs web dianggap sebagai toko online jika menjual barang atau jasa secara online.
29	**Pornografi**	Kategori ini mencakup situs web yang berisi konten erotis dan pornografi. Termasuk di dalamnya adalah situs web berbayar dan gratis. Kategori ini mencakup situs web yang menyediakan gambar, cerita, dan video, serta akan mendeteksi konten pornografi pada situs web berkonten campuran.
30	**Portal**	Kategori ini mencakup situs web yang mengumpulkan informasi dari berbagai sumber dan beragam domain, dan yang biasanya menawarkan fitur seperti mesin pencarian, email, berita, dan berita hiburan.
31	**Radio**	Kategori ini mencakup situs web yang menawarkan layanan streaming musik di internet, dari stasiun radio online hingga situs web yang menyediakan konten audio sesuai permintaan (gratis atau berbayar).
32	**Agama**	Kategori ini mencakup situs web yang mempromosikan agama atau sekte. Termasuk juga di dalamnya adalah forum diskusi terkait dengan satu atau beberapa agama.
33	**Mesin pencarian**	Kategori ini mencakup situs web mesin pencarian, seperti Google, Yahoo, dan Bing.
34	**Jejaring sosial**	Kategori ini mencakup situs web jejaring sosial. Tercakup dalam kategori

© Acronis International GmbH, 2003-2024

		ini adalah MySpace.com, Facebook.com, Bebo.com, dll. Namun, jejaring sosial khusus, seperti YouTube.com, akan dicantumkan dalam kategori Video/Foto.
35	**Olahraga**	Kategori ini mencakup situs web yang menawarkan informasi, berita, dan panduan olahraga.
36	**Bunuh diri**	Kategori ini mencakup situs web yang mempromosikan, menawarkan, atau mendukung bunuh diri. Tidak termasuk di dalamnya adalah klinik pencegahan bunuh diri.
37	**Tabloid**	Kategori ini didesain terutama untuk pornografi lunak dan situs web gosip selebriti. Banyak situs web berita bergaya tabloid mungkin memiliki subkategori yang tercantum di sini. Deteksi untuk kategori ini juga berdasarkan heuristik.
38	**Membuang waktu**	Kategori ini mencakup situs web di mana seseorang cenderung menghabiskan banyak waktu. Dapat termasuk dalam kategori ini adalah situs web dari kategori lain seperti jejaring sosial atau hiburan.
39	**Berwisata**	Kategori ini mencakup situs web yang menampilkan tawaran dan peralatan berwisata, serta tinjauan dan peringkat tujuan wisata.
40	**Video**	Kategori ini mencakup situs web yang meng-host beragam video atau foto, baik yang diunggah oleh pengguna atau disediakan oleh berbagai penyedia konten. Termasuk di dalamnya adalah situs web seperti YouTube, Metacafe, Google Video, dan situs web foto seperti Picasa atau Flickr. Kategori ini juga mendeteksi video yang tersemat di situs web atau blog lainnya.
41	**Kartun penuh kekerasan**	Kategori ini mencakup situs web yang membahas, membagi, dan menawarkan kartun atau manga yang brutal dan tidak layak bagi anak-anak karena kekerasan, bahasa yang tidak pantas, atau konten seksual. Tidak tercakup dalam kategori ini adalah situs web yang menawarkan kartun mainstream seperti “Tom and Jerry”.
42	**Senjata**	Kategori ini mencakup situs web yang menawarkan senjata untuk dijual atau ditukarkan, dibuat, atau digunakan. Tercakup juga di dalamnya adalah sumber daya perburuan serta penggunaan senapan udara dan BB, serta senjata jarak dekat.
43	**Email**	Kategori ini mencakup situs web yang menyediakan fungsi email seperti aplikasi web.
44	**Proxy web**	Kategori ini mencakup situs web yang menyediakan layanan proxy web. Ini adalah situs web bertipe “browser di dalam browser” saat pengguna membuka suatu halaman web, memasukkan URL yang diminta menjadi suatu formulir, dan mengeklik “Kirim”. Situs proxy web mengunduh halaman yang sebenarnya dan menampilkannya di dalam browser pengguna.

© Acronis International GmbH, 2003-2024

		Berikut adalah alasan terdeteksinya tipe ini (dan mungkin perlu diblokir): • Untuk penelusuran anonim. Karena permintaan ke server web tujuan diajukan dari server web proxy, hanya alamat IP-nya yang terlihat dan jika administrator server melacak pengguna, jejaknya akan berakhir di proxy web – yang akan atau tidak akan menyimpan log yang diperlukan untuk menemukan pengguna asli. • Untuk spoofing lokasi. Alamat IP pengguna sering digunakan untuk melakukan profiling layanan berdasarkan lokasi sumber (beberapa situs web pemerintah nasional hanya dapat tersedia dari alamat IP lokal), dan menggunakan layanan tersebut dapat membantu pengguna untuk melakukan spoof lokasi mereka sesungguhnya. • Untuk mengakses konten terlarang. Jika filter URL sederhana digunakan, filter tersebut hanya melihat URL proxy web dan bukan server sebenarnya yang dikunjungi pengguna. • Untuk menghindari pemantauan perusahaan. Suatu kebijakan bisnis dapat mewajibkan pemantauan penggunaan Internet karyawan. Dengan mengakses semuanya melalui proxy web, pengguna dapat menghindari pemantauan sehingga tidak akan memberikan informasi yang benar. Karena SDK menganalisis halaman HTML (jika diberikan), dan bukan hanya URL, untuk beberapa kategori, SDK masih akan tetap dapat mendeteksi konten. Namun, alasan lainnya tidak dapat dihindari hanya dengan menggunakan SDK.

Pengecualian URL

URL yang dianggap aman dapat ditambahkan ke daftar domain tepercaya. URL yang merepresentasikan ancaman dapat ditambahkan ke daftar domain yang diblokir.

Untuk menentukan URL yang akan selalu dipercaya atau diblokir

1. Di modul pemfilteran URL rencana proteksi, klik **pengecualian URL**.
   Jendela **pengecualian URL** terbuka.
   Opsi berikut ditampilkan:

Item tepercaya—Klik **Tambah** untuk memilih dari opsi yang tersedia:

- **Domain**—Jika Anda memilih opsi ini, jendela **Tambahkan domain** terbuka.
  - Di bidang **Domain**, masukkan setiap domain pada baris baru. Di bidang **Deskripsi**, masukkan deskripsi singkat sehingga Anda dapat mengenali perubahan Anda dalam daftar item yang dipercaya.
- **Proses**—Jika Anda memilih opsi ini, jendela **Tambah proses** ditampilkan.
  - Di bidang **Proses**, masukkan jalur untuk setiap proses pada baris baru. Di bagian **Deskripsi**, masukkan deskripsi singkat sehingga Anda dapat mengenali perubahan Anda dalam daftar item yang dipercaya.

Item yang diblokir—Klik **Tambah**. Jendela **Tambah domain** ditampilkan.

© Acronis International GmbH, 2003-2024

Di bidang **Domain**, masukkan setiap domain pada baris baru. Di bidang **Deskripsi**, masukkan deskripsi singkat sehingga Anda dapat mengenali perubahan Anda dalam daftar item yang diblokir.

Catatan
Jalur jaringan lokal didukung. Misalnya, \\localhost\folderpath\file.exe.

Deskripsi

Anda dapat menggunakan bidang **Deskripsi** untuk membuat catatan tentang pengecualian yang Anda tambahkan di daftar pengecualian URL. Beberapa saran mengenai catatan yang mungkin Anda buat:

- Alasan dan tujuan pengecualian.
- Tanda waktu.

Jika ada beberapa item yang ditambahkan dalam satu entri, hanya ada 1 komentar yang dapat ditangkap untuk beberapa item.

Microsoft Defender Antivirus dan Microsoft Security Essentials

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Microsoft Defender Antivirus

Microsoft Defender Antivirus adalah komponen antimalware bawaan Microsoft Windows yang disertakan mulai dari Windows 8.

Modul Microsoft Defender Antivirus (WDA) memungkinkan Anda mengonfigurasi kebijakan keamanan Microsoft Defender Antivirus dan melacak statusnya melalui konsol Cyber Protect.

Modul ini berlaku untuk beban kerja dengan Microsoft Defender Antivirus yang telah diinstal.

Microsoft Security Essentials

Microsoft Security Essentials adalah komponen antimalware bawaan dari Microsoft Windows yang diberikan Windows sebelum versi 8.

Modul Microsoft Security Essentials memungkinkan Anda mengonfigurasi kebijakan keamanan Microsoft Security Essentials dan melacak statusnya melalui konsol Cyber Protect.

Modul ini berlaku untuk beban kerja dengan Microsoft Security Essentials yang telah diinstal.

Pengaturan untuk Microsoft Security Essentials serupa dengan pengaturan untuk Microsoft Defender Antivirus, tetapi Anda tidak dapat mengonfigurasi perlindungan waktu nyata, dan tidak dapat menentukan pengecualian melalui konsol Cyber Protect.

© Acronis International GmbH, 2003-2024

Jadwalkan pemindaian

Tetapkan jadwal untuk pemindaian terjadwal.

Mode pemindaian:

- **Penuh** – pemeriksaan menyeluruh semua file dan folder selain item yang dipindai dalam pemindaian cepat. Mode ini memerlukan lebih banyak sumber daya mesin untuk dieksekusi dibandingkan dengan pemindaian cepat.
- **Cepat** – pemeriksaan cepat proses dan folder dalam memori di mana malware biasanya ditemukan. Mode ini memerlukan sumber daya mesin yang lebih sedikit untuk dieksekusi.

Tentukan waktu dan hari dalam seminggu untuk melakukan pemindaian.

Pemindaian cepat harian – tentukan waktu untuk pemindaian cepat harian.

Anda dapat mengatur opsi-opsi berikut sesuai kebutuhan Anda:

Mulai pemindaian terjadwal saat mesin aktif tetapi tidak digunakan

Periksa definisi spyware dan virus terbaru sebelum menjalankan pemindaian terjadwal

Batasi penggunaan CPU selama pemindaian hingga

Untuk detail lebih lanjut tentang pengaturan Microsoft Defender Antivirus, lihat https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings

Tindakan default

Tentukan tindakan default yang akan dilakukan untuk ancaman yang terdeteksi dengan berbagai tingkat keparahan:

- **Bersihkan** – membersihkan malware yang terdeteksi di beban kerja.
- **Karantina** – masukkan malware yang terdeteksi ke folder karantina tapi tidak menghapusnya.
- **Hapus** – menghapus malware yang terdeteksi dari beban kerja.
- **Izinkan** – jangan hapus atau karantina malware yang terdeteksi.
- **Ditentukan pengguna** – pengguna akan diminta untuk menentukan tindakan yang akan dilakukan terhadap malware yang terdeteksi.
- **Tidak ada tindakan** – tidak ada tindakan yang akan dilakukan.
- **Blokir** – memblokir malware yang terdeteksi.

Untuk detail lebih lanjut tentang pengaturan tindakan default bagi Microsoft Defender Antivirus, lihat https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings

© Acronis International GmbH, 2003-2024

Perlindungan waktu nyata

Aktifkan **Perlindungan waktu nyata** untuk mendeteksi dan menghentikan malware menginstal atau berjalan pada beban kerja.

Pindai semua unduhan – jika dipilih, pemindaian dilakukan untuk semua file dan lampiran yang diunduh.

Aktifkan pemantauan perilaku – jika dipilih, pemantauan perilaku akan diaktifkan.

Pindai file jaringan – jika dipilih, file jaringan akan dipindai.

Izinkan pemindaian penuh pada drive jaringan yang dipetakan – jika dipilih, drive jaringan yang dipetakan akan dipindai secara menyeluruh.

Izinkan pemindaian email – jika diaktifkan, mesin akan memisahkan file kotak surat dan surat, berdasarkan format khususnya, untuk menganalisis bodi dan lampiran surat.

Untuk detail lebih lanjut tentang pengaturan perlindungan waktu-nyata bagi Microsoft Defender Antivirus, lihat https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings

Tingkat lanjut

Tentukan pengaturan pemindaian lanjutan:

- **Pindai file arsip** – menyertakan file yang diarsipkan seperti file .zip atau .rar dalam pemindaian.
- **Pindai drive yang dapat dilepas** – Pindai drive yang dapat dilepas selama pemindaian penuh.
- **Buat titik pengembalian sistem** – pada beberapa kasus, file atau entri registri yang penting dapat dihapus sebagai "positif palsu", lalu Anda dapat memulihkan dari titik pengembalian.
- **Hapus file yang dikarantina setelah** – tentukan jangka waktu yang setelahnya file yang dikarantina akan dihapus.
- **Kirim sampel file secara otomatis jika analisis lebih lanjut diperlukan:**
  - **Selalu minta** – Anda akan dimintai konfirmasi sebelum pengiriman file.
  - **Kirim sampel aman secara otomatis** – sebagian besar sampel akan dikirim secara otomatis kecuali file yang mungkin berisi informasi pribadi. File tersebut akan memerlukan konfirmasi tambahan.
  - **Kirim semua sampel secara otomatis** – semua sampel akan dikirim secara otomatis.
- **Nonaktifkan GUI Windows Defender Antivirus** – jika dipilih, antarmuka pengguna WDA tidak akan tersedia untuk pengguna. Anda dapat mengelola kebijakan WDA melalui konsol Cyber Protect.
- **MAPS (Layanan Active Protection Microsoft)** – komunitas online yang membantu Anda memilih cara merespons potensi ancaman.
  - **Saya tidak ingin bergabung dengan MAPS** – tidak ada informasi yang akan dikirim ke Microsoft tentang perangkat lunak yang terdeteksi.

© Acronis International GmbH, 2003-2024

- **Keanggotaan dasar** – informasi dasar akan dikirim ke Microsoft tentang perangkat lunak yang terdeteksi.
- **Keanggotaan lanjutan** – informasi terperinci akan dikirim ke Microsoft tentang perangkat lunak yang terdeteksi.

Untuk informasi lebih lanjut, lihat https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/

Untuk detail lebih lanjut tentang pengaturan lanjutan bagi Microsoft Defender Antivirus, lihat https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings

Pengecualian

Anda dapat menentukan file dan folder berikut untuk dikecualikan dari pemindaian:

- **Proses** – file apa pun yang dibaca atau ditulis oleh proses akan dikecualikan dari pemindaian. Anda harus menentukan jalur lengkap menuju file yang dapat dieksekusi dalam proses.
- **File dan folder** – file dan folder yang ditentukan tidak akan disertakan dalam pemindaian. Anda harus menentukan jalur lengkap menuju folder atau file, atau menentukan ekstensi file.

Untuk detail lebih lanjut tentang pengaturan pengecualian bagi Microsoft Defender Antivirus, lihat https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings

Manajemen firewall

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Manajemen firewall memungkinkan Anda mengonfigurasi pengaturan firewall dengan mudah pada beban kerja yang dilindungi.

Fungsionalitas di Cyber Protect ini diberikan melalui komponen Microsoft Defender Firewall bawaan Microsoft Windows. Microsoft Defender Firewall memblokir lalu lintas jaringan yang tidak sah yang mengalir masuk atau keluar dari beban kerja.

Manajemen firewall berlaku untuk beban kerja tempat Microsoft Defender Firewall diinstal.

Sistem operasi Windows yang didukung

Sistem operasi Windows berikut didukung untuk manajemen firewall:

Windows

- Windows 8
- Windows 8.1

© Acronis International GmbH, 2003-2024

- Windows 10
- Windows 11

Windows Server tidak didukung.

Mengaktifkan dan menonaktifkan manajemen firewall

Anda dapat mengaktifkan manajemen firewall saat membuat rencana proteksi. Anda dapat mengubah rencana proteksi yang ada untuk mengaktifkan atau menonaktifkan manajemen firewall.

Untuk mengaktifkan atau menonaktifkan manajemen firewall

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Lakukan salah satu langkah berikut untuk membuka panel rencana proteksi:
   - Jika Anda ingin membuat rencana proteksi baru, pilih mesin untuk melindungi, klik **Lindungi**, lalu klik **Buat rencana**.
   - Jika Anda ingin mengubah rencana proteksi yang ada, pilih mesin terlindungi, klik **Lindungi**, klik elipsis (...) di sebelah nama rencana proteksi, lalu klik **Edit**.
3. Di panel rencana proteksi, navigasikan ke area **Manajemen firewall**, lalu klik untuk mengaktifkan atau menonaktifkan **Manajemen firewall**.
4. Lakukan salah satu langkah berikut untuk menerapkan perubahan Anda:
   - Jika membuat rencana proteksi, klik **Buat**.
   - Jika mengedit rencana proteksi, klik **Simpan**.

Status Microsoft Defender Firewall di area **Manajemen firewall** panel rencana proteksi ditampilkan sebagai **Aktif** atau **Nonaktif**, bergantung pada apakah Anda mengaktifkan atau menonaktifkan manajemen firewall.

Anda juga dapat mengakses panel rencana proteksi dari Tab manajemen. Namun, belum tentu tersedia di semua edisi layanan Cyber Protection.

Karantina

Karantina adalah folder terisolasi khusus di hard disk mesin untuk menyimpan file mencurigakan yang terdeteksi oleh perlindungan Antivirus dan Antimalware guna mencegah penyebaran ancaman lebih lanjut.

Karantina memungkinkan Anda untuk meninjau file yang mencurigakan dan berpotensi berbahaya dari semua mesin dan menentukan apakah akan menghapus atau memulihkan file tersebut. File yang dikarantina akan dihapus secara otomatis jika mesin dihapus dari sistem.

Bagaimana file masuk ke folder karantina?

1. Anda mengonfigurasi rencana proteksi dan menetapkan tindakan default untuk file yang terinfeksi – untuk ditempatkan di Karantina.

© Acronis International GmbH, 2003-2024

2. Selama pemindaian terjadwal atau sesuai permintaan, sistem mendeteksi file berbahaya lalu menempatkan file tersebut di folder yang aman - Karantina.
3. Sistem memperbarui daftar karantina pada mesin.
4. File secara otomatis dibersihkan dari folder karantina setelah jangka waktu yang ditentukan di pengaturan **Hapus file yang dikarantina setelah** dalam rencana proteksi.

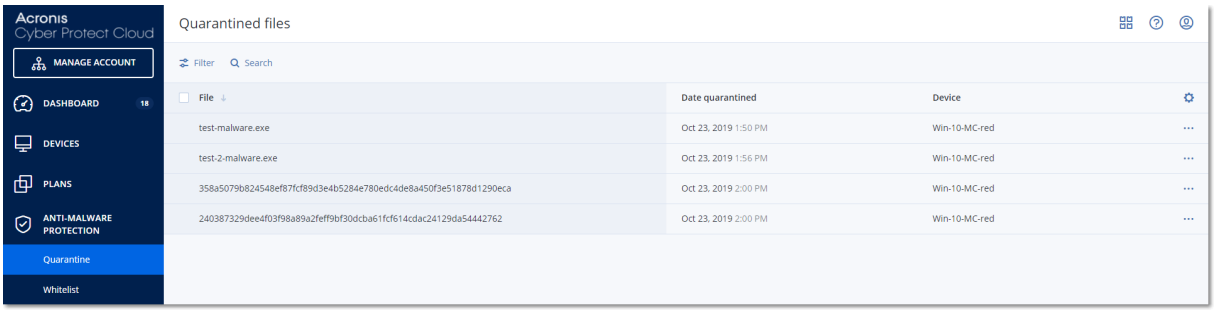
Mengelola file yang dikarantina

Untuk mengelola file yang dikarantina, buka **perlindungan Antimalware** > **Karantina**. Anda akan melihat daftar file yang dikarantina dari semua mesin.

Nama	Deskripsi
File	Nama file.
Tanggal dikarantina	Tanggal dan waktu saat file ditempatkan di Karantina.
Perangkat	Perangkat di mana file yang terinfeksi ditemukan.
Nama ancaman	Nama ancaman.
Rencana proteksi	Rencana proteksi yang mendasari ditempatkannya file mencurigakan di Karantina.

Anda memiliki dua kemungkinan tindakan dengan file yang dikarantina:

- **Hapus** – menghapus secara permanen file yang dikarantina dari semua mesin. Anda dapat hapus semua file dengan file hash yang sama. Anda dapat memulihkan semua file dengan file hash yang sama. Kelompokkan file berdasarkan hash, pilih file yang diperlukan, lalu hapus.
- **Pulihkan** – pulihkan file yang dikarantina ke lokasi asli tanpa ada modifikasi. Jika saat ini ada file dengan nama yang sama di lokasi asli, maka file tersebut akan ditimpa dengan file yang dipulihkan. Perhatikan bahwa file yang dipulihkan akan ditambahkan ke daftar izin dan dilewati selama pemindaian antimalware lebih lanjut.



Lokasi karantina di mesin

Lokasi default file yang dikarantina adalah:

© Acronis International GmbH, 2003-2024

- Untuk mesin Windows: `%programdata%\Acronis\NGMP\quarantine`
- Untuk mesin Mac: `/Library/Application Support/Acronis/NGMP/quarantine`
- Untuk mesin Linux: `/var/lib/Acronis/NGMP/quarantine`

Penyimpanan karantina ada dalam proteksi pertahanan diri penyedia layanan.

Folder kustom layanan mandiri sesuai permintaan

Anda dapat memilih folder kustom pada beban kerja dan memindainya secara langsung dari menu konteks.

Untuk mengakses Pemindaian dengan opsi Cyber Protect di menu konteks

Untuk beban kerja dengan Antivirus dan Antimalware yang diaktifkan dalam rencana proteksi, klik kanan file/folder yang ingin Anda pindai.

Catatan
Opsi ini tersedia hanya bagi administrator beban kerja.

Daftar putih perusahaan

Solusi antivirus dapat mengidentifikasi aplikasi khusus perusahaan yang sah sebagai mencurigakan. Untuk mencegah deteksi positif palsu, aplikasi yang terpercaya ditambahkan secara manual ke daftar putih, yang memakan waktu.

Catatan
Daftar putih perusahaan tidak memengaruhi pemindaian antimalware pada pencadangan.

Cyber Protection dapat mengotomatiskan proses ini: cadangan dipindai oleh modul perlindungan Antivirus dan Antimalware dan data yang dipindai dianalisis sehingga aplikasi semacam itu dipindahkan ke daftar putih, dan deteksi positif palsu dicegah. Selain itu, daftar putih seluruh perusahaan meningkatkan kinerja pemindaian lebih lanjut.

Daftar putih dibuat untuk setiap pelanggan dan hanya berdasarkan pada data pelanggan ini.

Daftar putih dapat diaktifkan dan dinonaktifkan. Saat dinonaktifkan, file yang ditambahkan padanya akan disembunyikan untuk sementara.

Catatan
Hanya akun dengan peran administrator (misalnya administrator Cyber Protection; administrator perusahaan; administrator mitra yang bertindak mewakili administrator perusahaan; administrator unit) dapat mengonfigurasi dan mengelola daftar putih. Fungsi ini tidak tersedia untuk akun administrator hanya baca atau akun pengguna.

© Acronis International GmbH, 2003-2024

Penambahan otomatis ke daftar putih

1. Jalankan pemindaian awan dari cadangan pada setidaknya dua mesin. Anda dapat melakukannya menggunakan rencana pemindaian cadangan.
2. Dalam pengaturan daftar putih, aktifkan sakelar **Pembuatan otomatis daftar putih**.

Penambahan manual ke daftar putih

Bahkan saat switch **Pembuatan otomatis daftar putih** dinonaktifkan, Anda dapat menambahkan file ke daftar putih secara manual.

1. Di konsol Cyber Protect, buka **perlindungan Antimalware** > **Daftar Putih**.
2. Klik **Tambah file**.
3. Tentukan jalur ke file, dan klik **Tambahkan**.

Menambahkan file yang dikarantina ke daftar putih

Anda dapat menambahkan file yang dikarantina ke daftar putih.

1. Di konsol Cyber Protect, buka **perlindungan Antimalware** > **Karantina**.
2. Pilih file yang dikarantina, dan klik **Tambahkan ke daftar putih**.

Pengaturan daftar putih

Saat Anda mengaktifkan switch **Pembuatan otomatis daftar putih**, Anda harus menentukan salah satu tingkat proteksi heuristik berikut:

- **Rendah**
  Aplikasi perusahaan hanya akan ditambahkan ke daftar putih setelah sejumlah waktu dan pemeriksaan. Aplikasi tersebut lebih tepercaya. Akan tetapi, pendekatan ini meningkatkan kemungkinan deteksi positif palsu. Kriteria untuk mempertimbangkan suatu file sebagai bersih dan tepercaya adalah tinggi.
- **Default**
  Aplikasi perusahaan akan ditambahkan ke daftar putih sesuai tingkat proteksi yang disarankan, untuk mengurangi kemungkinan deteksi positif palsu. Kriteria untuk mempertimbangkan suatu file sebagai bersih dan tepercaya adalah sedang.
- **Tinggi**
  Aplikasi perusahaan akan lebih cepat ditambahkan ke daftar putih untuk mengurangi kemungkinan deteksi positif palsu. Akan tetapi, hal ini tidak menjamin bahwa perangkat lunak bersih, dan kemungkinan nanti dapat dikenali sebagai mencurigakan atau malware. Kriteria untuk mempertimbangkan suatu file sebagai bersih dan tepercaya adalah rendah.

© Acronis International GmbH, 2003-2024

Melihat detail tentang item dalam daftar putih

Anda dapat mengelik suatu item dalam daftar putih untuk melihat lebih banyak informasi tentangnya dan menganalisisnya online.

Jika tidak yakin tentang item yang Anda tambahkan, Anda dapat memeriksanya dalam penganalisis VirtusTotal. Saat Anda mengeklik **Periksa VirusTotal**, situs menganalisis file dan URL yang mencurigakan untuk mendeteksi tipe malware menggunakan hash file dari item yang Anda tambahkan. Anda dapat melihat hash tersebut di string **Hash file (MD5)**.

Nilai **Mesin** merepresentasikan jumlah mesin tempat ditemukannya has tersebut selama pemindaian cadangan. Nilai ini dipopulasikan hanya jika item muncul dari Pemindaian cadangan atau Karantina. Bidang ini tetap kosong jika file telah ditambahkan secara manual ke daftar putih.

Pemindaian antimalware pada cadangan

Dengan pemindaian antimalware pada cadangan, Anda dapat mencegah pemulihan file yang terinfeksi dengan memeriksa apakah cadangan Anda bebas dari malware. Pemindaian antimalware dilakukan oleh agen awan yang berada di Cyber Protection pusat data dan tidak ada sumber daya komputasi lokal yang digunakan.

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

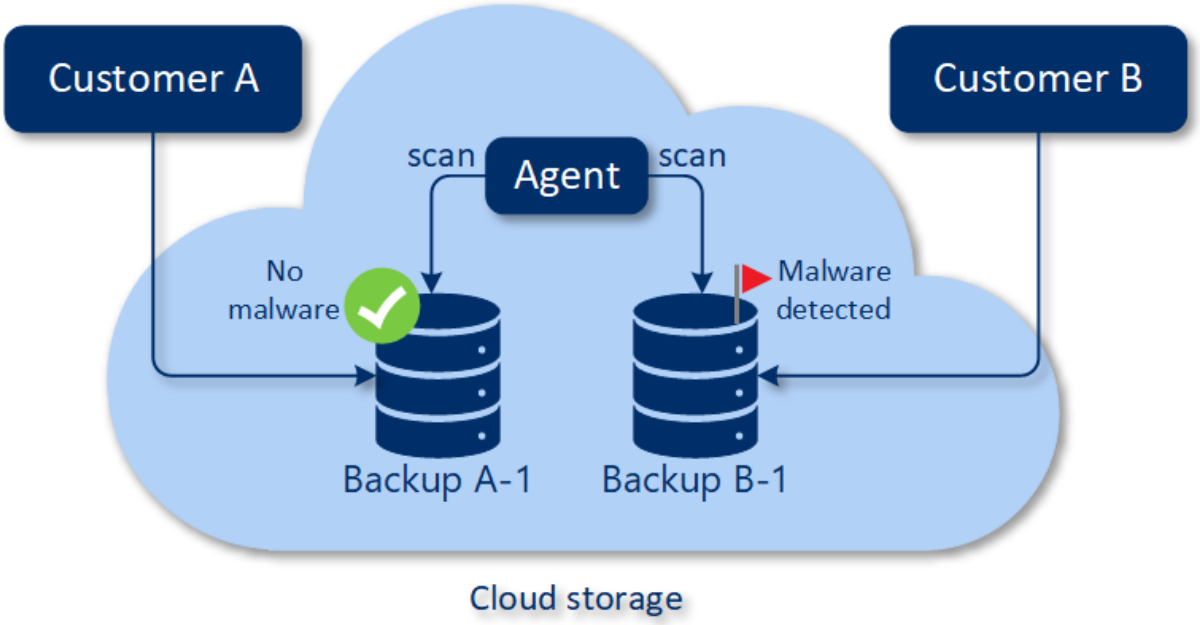
Untuk melakukan pemindaian antimalware, Anda perlu mengonfigurasi rencana pemindaian cadangan. Untuk informasi lebih lanjut tentang cara melakukan ini, lihat "Rencana pemindaian cadangan" (hlm. 196).

Setiap rencana pemindaian cadangan membuat tugas pemindaian untuk agen awan dan menambahkan tugas ini ke antrean, yaitu satu per pusat data. Tugas pemindaian diproses sesuai urutannya dalam antrean. Selain itu, waktu pemindaian tergantung pada ukuran cadangan. Itulah mengapa ada penundaan antara membuat rencana pemindaian cadangan dan menyelesaikan pemindaian.

Cadangan yang Anda pilih untuk pemindaian dapat berada dalam salah satu status berikut:

- Belum dipindai
- Tidak ada malware
- Malware terdeteksi

© Acronis International GmbH, 2003-2024



Anda dapat memeriksa hasil pemindaian cadangan di widget **Detail pemindaian cadangan (ancaman)**. Anda dapat menemukannya di konsol Cyber Protect, pada tab **Pemantauan** > tab **Ikhtisar**.

Pembatasan

- Pemindaian antimalware didukung untuk **Keseluruhan mesin** atau cadangan **Disk/volume** dari beban kerja berikut ini:
  - Mesin Windows tempat agen perlindungan diinstal.
  - Mesin virtual Windows yang dicadangkan pada tingkat hypervisor (pencadangan tanpa agen) oleh Agen untuk Hyper-V dan Agen untuk VMware (Windows).

  Pemindaian antimalware tidak didukung untuk pencadangan yang dibuat oleh perangkat virtual, seperti Agen untuk VMware (Alat virtual), Agen untuk Virtuozzo, Agen untuk Scale Computing HC3.
- Hanya volume dengan sistem file NTFS, dan partisi GPT atau MBR yang akan dipindai.
- Hanya penyimpanan awan default yang didukung sebagai lokasi cadangan. Penyimpanan lokal dan penyimpanan awan milik mitra tidak didukung.
- Ketika Anda memilih cadangan untuk dipindai, Anda dapat memilih set cadangan yang termasuk cadangan Perlindungan data berkelanjutan (CDP). Namun. hanya cadangan non-CDP dalam set cadangan ini yang akan dipindai. Untuk informasi lebih lanjut tentang cadangan CDP, lihat "Perlindungan data berkelanjutan (CDP)" (hlm. 408).
- Ketika Anda melakukan pemulihan aman dari seluruh mesin, Anda dapat memilih set cadangan yang termasuk cadangan CDP. Namun, operasi pemulihan ini tidak akan menggunakan data dalam cadangan CDP. Untuk memulihkan data CDP, jalankan operasi pemulihan **File/folder** tambahan.

© Acronis International GmbH, 2003-2024

Bekerja dengan fitur proteksi Tingkat Lanjut

Secara default, Cyber Protect menyertakan fitur yang mencakup sebagian besar ancaman keamanan cyber. Anda dapat menggunakan fitur ini tanpa biaya tambahan. Selain itu, Anda dapat mengaktifkan fitur tingkat lanjut untuk meningkatkan perlindungan beban kerja Anda.

- Jika fitur Proteksi lanjutan tersedia untuk Anda gunakan, fitur tersebut akan muncul dalam rencana proteksi yang ditandai dengan ikon Fitur lanjutan .
- Jika fitur Perlindungan Lanjutan tidak tersedia untuk Anda, hubungi administrator Anda untuk mengaktifkan paket Perlindungan Lanjutan yang diperlukan.
- Jika administrator mengizinkan Anda membeli paket keamanan tambahan, Anda dapat memilih untuk mengaktifkan fitur Lanjutan. Sebuah pesan akan mengarahkan Anda ke layar yang memberi tahu Anda bahwa tagihan tambahan diberlakukan.

Catatan
Jika setidaknya satu fitur diaktifkan, Anda harus membeli paket Proteksi lanjutan yang sesuai.

Catatan
Jika semua fitur Lanjutan dinonaktifkan pada paket proteksi Anda, rencana proteksi Lanjutan yang sesuai akan dinonaktifkan.

Paket perlindungan tingkat lanjut	Fitur proteksi lanjutan
Cadangan Tingkat Lanjut	Melindungi beban kerja Anda secara terus-menerus dan memastikan agar perubahan pada pekerjaan Anda di menit-menit terakhir sekalipun tidak akan hilang. Fitur-fiturnya meliputi: • Pemulihan sekali klik • Perlindungan data berkelanjutan • Dukungan pencadangan untuk klaster Microsoft SQL Server dan klaster Microsoft Exchange – Always On Availability Groups (AAG) dan Database Availability Groups (DAG) • Dukungan pencadangan untuk MariaDB, MySQL, Oracle DB, dan SAP HANA • Peta perlindungan data dan pelaporan kepatuhan • Pemrosesan data off-host • Frekuensi pencadangan untuk beban kerja Microsoft 365 dan Google Workspace • Operasi jarak jauh dengan media yang dapat di-boot • Pencadangan langsung ke penyimpanan cloud publik Microsoft Azure
Keamanan Tingkat Lanjut + EDR	Melindungi beban kerja Anda secara terus-menerus dari semua ancaman malware. Fitur-fiturnya meliputi: • Mengelola insiden di halaman Insiden terpusat • Visualisasikan cakupan dan dampak insiden

© Acronis International GmbH, 2003-2024

	• Rekomendasi dan langkah remediasi • Periksa serangan yang diungkapkan secara publik pada beban kerja Anda menggunakan umpan Ancaman • Simpan peristiwa keamanan selama 180 hari • Perlindungan antivirus dan antimalware dengan deteksi berbasis tanda tangan lokal (dengan perlindungan waktu nyata) • Pencegahan eksploit • Pemfilteran URL • Manajemen firewall titik akhir • Cadangan forensik, cadangan pemindaian untuk malware, pemulihan aman, daftar izin perusahaan • Rencana proteksi cerdas (integrasi dengan peringatan CPOC) • Pemindaian cadangan terpusat untuk malware • Penghapusan jarak jauh • Microsoft Defender Antivirus • Microsoft Security Essentials
Manajemen Tingkat Lanjut	Memungkinkan Anda untuk memasang patch pada kerentanan di beban kerja yang dilindungi. Fitur-fitur meliputi: • Manajemen patch • Kesehatan disk • Inventaris perangkat lunak • Pemasangan patch fail-safe • Pembuatan Skrip Cyber • Bantuan jarak jauh • Transfer dan berbagi file • Memilih sesi untuk dihubungkan • Mengamati beban kerja dalam beberapa tampilan • Mode koneksi: kontrol, hanya lihat, dan tutup • Koneksi melalui aplikasi Bantuan Cepat • Berbagai protokol koneksi jarak jauh: NEAR dan Berbagi Layar Apple • Sesi perekaman untuk koneksi NEAR • Transmisi tangkapan layar • Laporan riwayat sesi • 24 monitor • Pemantauan berbasis ambang batas • Pemantauan berbasis anomali
Advanced Data Loss Prevention	Mencegah kebocoran informasi sensitif dari beban kerja yang dilindungi. Fitur-fiturnya meliputi: • Pencegahan sadar-konten kehilangan data dari beban kerja melalui perangkat periferal dan komunikasi jaringan • Deteksi otomatis bawaan untuk informasi pengenal pribadi (PII), informasi

© Acronis International GmbH, 2003-2024

	kesehatan yang dilindungi (PHI), dan data Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), serta dokumen dalam kategori “Ditandai sebagai Informasi Rahasia” • Pembuatan kebijakan pencegahan kehilangan data otomatis dengan bantuan pengguna akhir opsional • Penegakan pencegahan kehilangan data adaptif dengan penyesuaian kebijakan berbasis pembelajaran otomatis • Logging audit terpusat berbasis awan, peringatan, dan pemberitahuan pengguna akhir

Advanced Data Loss Prevention

Modul Advanced Data Loss Prevention menganalisa konten dan konteks dari transfer data dalam beban kerja terlindungi dan mencegah kebocoran data sensitif melalui perangkat periferal atau transfer jaringan di dalam dan di luar jaringan perusahaan berdasarkan kebijakan alur data.

Fitur Advanced Data Loss Prevention dapat disertakan di dalam rencana proteksi mana pun untuk penyewa pelanggan jika paket layanan Proteksi dan Advanced Data Loss Prevention diaktifkan untuk pelanggan ini.

Sebelum Anda mulai menggunakan modul Advanced Data Loss Prevention, pastikan Anda telah membaca dan memahami konsep dasar dan logika dari manajemen Advanced DLP yang dijelaskan di Panduan fundamental.

Anda juga mungkin perlu meninjau dokumen Spesifikasi Teknis.

Membuat kebijakan alur data dan aturan kebijakan

Prinsip utama dari pencegahan kehilangan data menuntut agar pengguna sistem IT perusahaan harus diizinkan untuk menangani data sensitif hanya sejauh yang diperlukan untuk melakukan tugas pekerjaan mereka. Transfer data sensitif lain mana pun- yang tidak relevan dengan proses bisnis - harus diblokir. Oleh karena itu, penting untuk membedakan antara transfer data yang terkait dengan bisnis dan rogue, atau alur.

Kebijakan alur data berisi aturan yang menentukan alur data mana yang dizinkan dan yang dilarang, sehingga mencegah terjadinya transfer informasi sensitif tidak sah saat modul Pencegahan Kehilangan Data diaktifkan dalam rencana proteksi dan berjalan dalam mode Penerapan.

Setiap kategori sensitivitas dalam kebijakan berisi satu aturan default, ditandai dengan tanda bintang (*) dan satu atau lebih aturan eksplisit (non-default) yang menentukan alur data untuk pengguna atau grup tertentu. Baca lebih lanjut tentang jenis aturan kebijakan di Panduan fundamental.

Kebijakan alur data biasanya dibuat secara otomatis ketika Advanced Data Loss Prevention sedang berjalan dalam mode observasi. Waktu yang diperlukan untuk membangun kebijakan alur data representatif sekitar satu bulan, tapi mungkin dapat berbeda tergantung pada proses bisnis dalam

© Acronis International GmbH, 2003-2024

organisasi Anda. Kebijakan alur data juga dapat dibuat, dikonfigurasi, atau diedit secara manual oleh perusahaan atau administrator unit.

Untuk memulai pembuatan kebijakan alur data otomatis

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Navigasi ke **Manajemen** > **Rencana proteksi**.
3. Klik **Buat rencana**.
4. Perluas bagian **Pencegahan Kehilangan Data** lalu klik baris **Mode**.
5. Dalam dialog Mode, pilih **Mode Observasi**, lalu pilih cara memproses transfer data:

Opsi	Deskripsi
Izinkan semua	Seluruh transfer data sensitif dari beban kerja pengguna diperlakukan sebagaimana mestinya untuk proses dan keamanan bisnis. Aturan baru dibuat untuk setiap alur data terdeteksi yang tidak cocok dengan aturan yang telah ditentukan dalam kebijakan.
Benarkan semua	Seluruh transfer data sensitif dari beban kerja pengguna diperlakukan sebagaimana mestinya untuk proses bisnis, namun berisiko. Oleh karena itu, untuk setiap transfer data sensitif yang dicegat ke penerima atau tujuan mana pun baik yang di dalam dan luar organisasi yang tidak cocok dengan aturan alur data yang dibuat sebelumnya, pengguna harus memasukkan pembenaran bisnis satu-waktu. Saat pembenaran dikirimkan, aturan alur data baru dibuat dalam kebijakan alur data.
Gabungan	Logika Izinkan semua diterapkan untuk seluruh alur data sensitif internal, dan logika Benarkan semua diterapkan untuk seluruh alur data sensitif eksternal. **Catatan** Untuk informasi lebih lanjut tentang data internal dan eksternal, lihat Deteksi tujuan mandiri

6. Simpan rencana proteksi dan terapkan ke beban kerja dari yang Anda ingin kumpulkan datanya untuk membangun kebijakan.

Catatan
Kebocoran data tidak dicegah selama mode observasi.

Untuk mengonfigurasikan Kebijakan alur data secara manual

1. Di konsol Cyber Protect, arahkan ke **Perlindungan** > **Kebijakan aliran data**.
2. Klik **Aturan alur data baru**.
   Panel aturan data baru diperluas di sebelah kanan.
3. Pilih kategori sensitivitas, tambah pengirim dan penerima, lalu tentukan izin transfer data untuk kategori terpilih, pengirim, dan penerima.

© Acronis International GmbH, 2003-2024

Opsi	Deskripsi
Izinkan	Izinkan pengirim ini untuk melakukan transfer data kategori sensitivitas ini kepada penerima ini.
Pengecualian	Jangan izinkan pengirim ini untuk melakukan transfer data kategori sensitivitas ini kepada penerima ini, tapi izinkan pengirim tersebut untuk mengirimkan pengecualian ke aturan untuk transfer tertentu. Saat pengirim ini mencoba untuk melakukan transfer data kategori sensitivitas ini kepada penerima ini, blokir transfernya dan minta pengirim untuk mengirimkan pengecualian agar mengizinkan transfer ini. Saat pengecualian dikirimkan, transfer data diizinkan untuk diproses. **Penting** Semua transfer data setelahnya antara pengirim ini dan penerima untuk kategori sensitivitas ini akan diizinkan selama lima menit setelah pengecualian dikirimkan.
Tolak	Jangan izinkan pengirim ini untuk melakukan transfer data kategori sensitivitas ini kepada penerima ini, dan jangan izinkan pengirim tersebut untuk meminta pengecualian kepada aturan.

4. (Opsional) Pilih tindakan yang harus dieksekusi saat aturan dipicu.

Tindakan	Deskripsi
Tulis dalam log	Simpan rekaman peristiwa dalam log audit saat aturan dipicu. Kami menyarankan untuk memilih tindakan ini untuk aturan dengan izin **Pengecualian**.
Buat peringatan	Buat peringatan di tab **Peringatan** Cyber Protect saat aturan dipicu. Jika pemberitahuan diaktifkan untuk administrator, surel pemberitahuan juga akan dikirimkan.
Beri tahukan pengguna akhir jika transfer data ditolak	Beri tahukan pengguna secara waktu nyata dengan peringatan di layar saat mereka memicu aturan.

5. Klik **Simpan**.
6. Ulangi langkah 2 hingga 5 untuk membuat beberapa kategori dan opsi aturan sensitivitas yang berbeda, dan pastikan bahwa aturan yang dihasilkan sesuai dengan opsi yang Anda pilih.

Struktur kebijakan alur data

Di tampilan **Kebijakan alur data**, aturan kebijakan dikelompokkan berdasarkan kategori data sensitif yang dikontrol berbagai aturan tersebut. Pengidentifikasi kategori sensitivitas ditampilkan tepat di atas kelompok aturan kebijakan.

© Acronis International GmbH, 2003-2024

- Sensitif
  - Informasi Kesehatan yang Dilindungi (PHI)
  - Informasi Identitas Pribadi (PII)
  - Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS),
  - Ditandai sebagai Rahasia
- Non-sensitif

Untuk informasi lebih lanjut tentang konsep dan fitur kebijakan alur data, lihat Panduan fundamental.

Struktur aturan

Setiap aturan kebijakan terdiri dari elemen-elemen berikut.

- **Kategori sensitivitas**
  - **Informasi Kesehatan yang Dilindungi (PHI)**
  - **Informasi Identitas Pribadi (PII)**
  - **Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)**
  - **Ditandai sebagai Rahasia**

    Lihat "Definisi data sensitif" (hlm. 878)
- **Pengirim** - menentukan inisiator dari transfer data yang dikontrol oleh aturan ini. Ia dapat berupa pengguna tunggal, sejumlah pengguna, atau kelompok pengguna.
  - **Pengguna Internal** - pengguna kelompok yang mencakup seluruh pengguna internal organisasi.
  - **Kontak / Dari organisasi** - Akun Windows di dalam organisasi, yang dikenali oleh Advanced Data Loss Prevention, serta semua akun lainnya (termasuk yang digunakan oleh aplikasi komunikasi pihak ketiga) yang telah digunakan akun Windows tertentu sebelumnya.
  - **Kontak / Identitas kustom** - pengidentifikasi dari pengguna internal yang ditentukan dalam salah satu format berikut: surel, ID Skype, pengidentifikasi ICQ, pengidentifikasi IRC, surel Jabber, surel Agen Mail.ru, nomor telepon Viber, surel Zoom.
    Wildcard berikut dapat digunakan untuk menentukan sekelompok kontak:
    - ***** - menggantikan berapa pun jumlah simbol
    - **?** - menggantikan simbol tunggal apa pun
- **Penerima** - menentukan tujuan dari transfer data yang dikontrol oleh aturan ini. Ia dapat berupa pengguna tunggal, sejumlah pengguna, atau kelompok pengguna, juga jenis tujuan lainnya yang dijelaskan di bawah.
  - **Apa pun** - penerima jenis apa pun yang didukung oleh Advanced DLP.
  - **Kontak / Kontak apa pun** - kontak internal atau eksternal apa pun.
  - **Kontak / Kontak internal apa pun** - kontak pengguna internal apa pun (lihat "Deteksi tujuan mandiri" (hlm. 877)).
  - **Kontak / Kontak eksternal apa pun** - kontak pengguna eksternal atau entitas apa pun.

© Acronis International GmbH, 2003-2024

- **Kontak / Dari organisasi** - prinsip yang sama seperti yang dijelaskan di dalam bidang Pengirim.
- **Kontak / Identitas kustom** - prinsip yang sama seperti yang dijelaskan di dalam bidang Pengirim.
- **Layanan berbagi file** - pengidentifikasi dari layanan berbagi file yang dikontrol.
- **Jejaring sosial** - pengidentifikasi dari jaringan sosial yang dikontrol.
- **Host / Host apa pun** - komputer apa pun yang dikenali oleh Advanced DLP sebagai internal atau eksternal.
- **Host / Host internal apa pun** - komputer apa pun yang dikenali oleh Advanced DLP sebagai internal.
- **Host / Host eksternal apa pun** - komputer apa pun yang dikenali oleh Advanced DLP sebagai eksternal.
- **Host / Host khusus** - pengidentifikasi komputer khusus sebagai nama host (mis. FQDN) atau Alamat IP (IPv4 atau IPv6).
- **Perangkat / Perangkat apa pun** - perangkat periferal apa pun yang terkoneksi dengan beban kerja.
- **Perangkat / eksternal** - penyimpanan yang dapat dilepas atau drive terpetakan yang dialihkan yang terkoneksi ke beban kerja.
- **Perangkat / Dapat dilepas terenkripsi** - perangkat penyimpanan yang dapat dilepas yang dienkripsi dengan BitLocker To Go.
- **Perangkat / Papan klip yang dialihkan** - papan klip yang dialihkan yang terkoneksi ke beban kerja.
- **Printer** - printer lokal atau printer jaringan apa pun yang terkoneksi ke beban kerja.

- **Izin** - kontrol pencegah yang diterapkan atas transfer data yang dikontrol oleh aturan ini. Dijelaskan dengan lebih detail dalam topik Izin dalam aturan kebijakan alur data.
- **Tindakan** - tindakan non-pencegahan yang dilakukan saat aturan ini dipicu. Secara default bidang ini diatur ke "Tidak ada tindakan". Opsinya adalah:
  - **Tulis dalam log** - menyimpan rekaman peristiwa dalam log audit saat aturan dipicu.
  - **Beri tahukan pengguna akhir jika transfer data ditolak** - memberitahukan pengguna dengan peringatan di layar secara waktu nyata saat mereka memicu aturan.
  - **Buat peringatan** - memperingatkan administrator saat aturan dipicu.

Peringatan!
Saat **Tidak ada tindakan** dipilih dan aturan dipicu:

- catatan tidak ada peristiwa ditambahkan ke log audit;
- tidak ada peringatan dikirim ke administrator;
- tidak ada notifikasi layar ditampilkan ke pengguna akhir.

Apa yang memicu aturan kebijakan?

Transfer data cocok dengan aturan kebijakan alur data jika semua kondisi berikut bernilai benar:

© Acronis International GmbH, 2003-2024

- Semua pengirim transfer data ini tercantum atau merupakan bagian dari kelompok pengguna yang ditentukan di dalam bidang **Pengirim** aturan.
- Semua penerima transfer data ini tercantum atau merupakan bagian dari kelompok pengguna yang ditentukan di dalam bidang **Penerima** aturan.
- Data yang sedang ditransfer cocok dengan **Kategori sensitivitas** aturan.

Menyesuaikan izin dalam aturan kebijakan alur data

Advanced Data Loss Prevention mendukung tiga jenis izin dalam aturan kebijakan alur data. Izin dikonfigurasi secara mandiri untuk setiap aturan kebijakan.

Izinkan (permisif)	Transfer data yang cocok dengan kombinasi kategori sensitivitas, pengirim dan penerima ditentukan dalam aturan yang diizinkan.
Pengecualian (larangan)	Transfer data yang cocok dengan kombinasi kategori sensitivitas, pengirim dan penerima yang ditentukan dalam aturan yang tidak diizinkan, tapi pengirim dapat mengirimkan pengecualian ke aturan untuk mengizinkan transfer tertentu. **Penting** Semua transfer data setelahnya antara pengirim ini dan penerima untuk kategori sensitivitas ini akan diizinkan selama lima menit setelah pengecualian dikirimkan.
Tolak (larangan)	Transfer data yang cocok dengan kombinasi kategori sensitivitas, pengirim dan penerima ditentukan dalam aturan tidak diizinkan, dan pengirim tidak memiliki opsi untuk mengirimkan pengecualian.

Selain itu, sebuah bendera prioritas dapat ditetapkan ke izin **Izinkan** dan **Pengecualian** untuk meningkatkan fleksibilitas manajemen kebijakan. Dengan pengaturan ini, Anda dapat menimpa izin yang diatur untuk kelompok tertentu di aturan alur data lainnya dalam kebijakan. Anda dapat menggunakannya untuk menerapkan aturan alur data kelompok hanya untuk beberapa anggota. Untuk mencapai ini, Anda harus membuat aturan alur data untuk pengguna tertentu yang ingin Anda kecualikan dalam aturan kelompok, dan kemudian memprioritaskan izin mereka atas pembatasan alur data yang dikonfigurasikan di dalam aturan kelompok tempat pengguna ini berada. Untuk informasi tentang prioritas izin saat menggabungkan aturan, lihat "Menggabungkan aturan kebijakan alur data" (hlm. 870).

Penting
Sebelum mengalihkan perusahaan atau kebijakan unit dari mode Observasi ke mode Penerapan, penting untuk menyesuaikan aturan default untuk setiap kategori data sensitif dari permisif ke tahap larangan. Aturan default ditandai dengan tanda bintang (*) dalam tampilan **Kebijakan alur data**. Baca lebih lanjut tentang jenis aturan kebijakan di Panduan fundamental.

Untuk mengedit izin di aturan kebijakan

© Acronis International GmbH, 2003-2024

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Navigasi ke **Proteksi** > **Kebijakan alur data**.
3. Pilih aturan kebijakan yang ingin Anda edit lalu klik **Edit** di atas daftar aturan.
   Jendela **Edit aturan alur data** terbuka.
4. Di bagian **Izin**, pilih **Izinkan**, **Pengecualian**, atau **Tolak**.
5. (Opsional) Untuk memprioritaskan izin **Izinkan** atau **Pengecualian** aturan ini atas izin dalam aturan yang lain, klik kotak centang **Prioritaskan**.
   Anda tidak perlu menggunakan kotak centang ini untuk memprioritaskan alur data atas aturan default Apa Pun > Lainnya, karena aturan tersebut selalu memiliki prioritas terendah dalam kebijakan secara default.
   Untuk informasi tentang prioritas izin saat menggabungkan aturan, lihat "Menggabungkan aturan kebijakan alur data" (hlm. 870).
6. (Opsional) Pilih tindakan yang harus dieksekusi saat aturan dipicu.
7. Simpan perubahan ke aturan kebijakan.

Menggabungkan aturan kebijakan alur data

Saat transfer data memiliki kecocokan lebih dari satu aturan, izin dan tindakan yang dikonfigurasikan untuk semua aturan digabungkan dan diterapkan seperti berikut.

Izin

Jika transfer data memiliki kecocokan lebih dari satu aturan dan aturan-aturan ini memiliki izin yang berbeda untuk kategori data yang sama, aturan yang berlaku adalah yang memiliki izin dengan prioritas yang lebih tinggi, berdasarkan daftar prioritas izin berikut (dalam urutan yang menurun):

1. Pengecualian dengan bendera **Diprioritaskan**
2. Izinkan dengan bendera **Diprioritaskan**
3. Tolak
4. Pengecualian
5. Izinkan

Jika transfer data memiliki kecocokan lebih dari satu aturan dan aturan-aturan ini memiliki izin yang berbeda untuk kategori data yang berbeda, logika berikut diterapkan untuk aturan yang berlaku:

1. Izin aturan yang paling terlarang ditentukan untuk setiap kategori sensitivitas yang cocok dengan transfer data.
2. Izin aturan yang paling terlarang yang ditentukan dalam poin 1 diterapkan.

Contoh

Transfer file cocok dengan tiga aturan dalam kategori sensitivitas yang berbeda seperti berikut:

© Acronis International GmbH, 2003-2024

Kategori sensitivitas	Izin
PII	Izinkan - Diprioritaskan
PHI	Pengecualian - Diprioritaskan
PCI	Tolak

Izin yang akan diterapkan adalah Ditolak.

Tindakan

Jika transfer data memiliki kecocokan lebih dari satu aturan dan aturan-aturan ini memiliki opsi berbeda yang diterapkan dalam bidang **Tindakan**, semua tindakan yang dikonfigurasi dalam semua aturan yang terpicu dilaksanakan.

Tinjauan dan manajemen kebijakan

Sebelum kebijakan alur data dasar yang dibuat secara otomatis diterapkan, kebijakan itu perlu ditinjau, divalidasi, dan disetujui oleh klien, karena klien yang pada dasarnya mengetahui seluruh kekhususan proses bisnis mereka dan dapat menilai apakah kebijakan tersebut ditafsirkan secara konsisten di dalam kebijakan dasar. Juga, klien dapat mengidentifikasi ketidakakuratan, yang kemudian diperbaiki oleh administrator mitra.

Selama peninjauan kebijakan, administrator mitra menyajikan kebijakan alur data dasar ke klien, yang meninjau setiap alur data di dalam kebijakan dan memvalidasi konsistensinya dengan proses bisnis mereka. Validasi tidak memerlukan keterampilan teknis, karena representasi aturan kebijakan di konsol Cyber Protect jelas secara intuitif: setiap aturan menjelaskan siapa pengirim dan penerima aliran data sensitif.

Berdasarkan instruksi klien, administrator mitra secara manual menyesuaikan kebijakan dasar dengan mengedit, menghapus dan membuat aturan kebijakan alur data. Setelah persetujuan klien, kebijakan yang ditinjau diterapkan untuk memproteksi beban kerja dengan mengalihkan rencana proteksi yang diaplikasi ke berbagai beban kerja ini ke dalam mode Penerapan.

Sebelum menerapkan kebijakan yang ditinjau, penting untuk mengubah izin **Izinkan** di dalam seluruh aturan kebijakan default yang dibuat secara otomatis untuk kategori data sensitif menjadi **Tolak** atau **Pengecualian**. Izin **Tolak** tidak dapat ditimpa oleh pengguna, sementara izin **Pengecualian** memblokir transfer yang cocok dengan aturan tapi mengizinkan pengguna untuk menimpa pemblokiran di dalam situasi darurat dengan mengirimkan pengecualian terkait bisnis.

Pembaruan kebijakan alur data

Saat proses bisnis perusahaan atau unitnya berubah signifikan, kebijakan DLP-nya harus diperbarui untuk membuatnya konsisten terhadap perubahan dalam alur data sensitif dari proses bisnis yang diperbarui. Pembaruan kebijakan juga diperlukan jika peran jabatan karyawan berubah - dalam hal ini, bagian kebijakan unit digunakan untuk memproteksi beban kerja karyawan juga perlu diperbarui.

© Acronis International GmbH, 2003-2024

Alur kerja manajemen kebijakan Advanced DLP memungkinkan administrator untuk melakukan otomatisasi pembaruan kebijakan terhadap keseluruhan perusahaan, unit, pengguna, atau bagian dari pengguna dalam unit.

Memperbarui kebijakan untuk perusahaan atau unit

Semua opsi dari mode Observasi dapat digunakan untuk memperbarui kebijakan perusahaan atau keseluruhan unit, serta bagian dari kebijakan unit untuk satu atau lebih pengguna di dalam unit.

Untuk memperbarui kebijakan untuk perusahaan atau unit

Proses pembaruan terdiri dari langkah-langkah berikut yang harus dilakukan oleh administrator Perusahaan atau Mitra yang mengelola beban kerja perusahaan.

1. Hapus semua aturan non-default dalam kebijakan yang diterapkan.
2. Untuk memulai pembaruan, alihkan rencana proteksi dengan Advanced DLP yang diaplikasikan pada perusahaan atau unit ke salah satu opsi mode observasi, bergantung mana yang optimal untuk perusahaan atau unit tertentu ini, lalu aplikasikan rencana terhadap semua beban kerja di dalam perusahaan atau unit.
3. Saat periode pembaruan berakhir, tinjau kebijakan perusahaan atau unit baru bersama klien, sesuaikan jika diperlukan, dan dapatkan persetujuan dari klien.
4. Alihkan rencana proteksi yang diaplikasikan pada beban kerja perusahaan atau unit ke opsi mode penerapan yang sesuai, yang klien anggap sebagai optimal untuk mencegah kebocoran data dari beban kerja unit.

Memperbarui kebijakan untuk salah satu atau lebih pengguna di dalam perusahaan atau unit

Kebijakan tingkat pengguna dapat diperbarui dengan menggunakan opsi mana pun dari mode Observasi, begitu juga dalam mode penerapan adaptif.

Menggunakan mode Observasi untuk memperbarui kebijakan pengguna

Menggunakan mode observasi untuk memperbarui kebijakan untuk pengguna atau bagian pengguna di dalam perusahaan (atau unit) memiliki kekhususan berikut: kebijakan alur data yang diterapkan untuk seluruh perusahaan (atau unit) tidak diterapkan atas transfer data pengguna selama periode pembaruan. Akibatnya, aturan tersendiri untuk pengguna dapat dibuat selama pembaruan, yang dapat bertolak belakang atau cocok dengan aturan kelompok yang sudah ada di dalam kebijakan penerapan untuk perusahaan (atau unit). Setelah pembaruan selesai dan kebijakan diterapkan kembali atas transfer data pengguna, apakah aturan tersendiri ini dibuat untuk pengguna akan diaplikasi secara aktual atau tidak pada transfer data pengguna bergantung pada prioritasnya masing-masing, dibandingkan dengan aturan lain di dalam kebijakan yang cocok dengan berbagai transfer data ini.

Untuk memperbarui kebijakan untuk pengguna melalui mode Observasi

© Acronis International GmbH, 2003-2024

Proses pembaruan terdiri dari langkah-langkah berikut yang harus dilakukan oleh administrator Perusahaan atau Mitra yang mengelola beban kerja perusahaan.

1. Hapus semua aturan non-default di dalam kebijakan yang diterapkan untuk perusahaan (atau unit) yang memiliki pengguna sebagai pengirim tunggal mereka.
2. Hapus pengguna dari daftar pengirim dari semua aturan alur data non-default di dalam kebijakan yang diterapkan.
3. Buat rencana proteksi baru dengan Advanced DLP di dalam mode Observasi dan aplikasikan ke beban kerja pengguna untuk mulai periode pembaruan (observasi).
   Durasi periode pembaruan bergantung seberapa lama itu dilakukan untuk pengguna agar dapat melakukan seluruh atau 90-95% aktivitas bisnis reguler mereka yang melibatkan transfer data sensitif dari beban kerja mereka.
4. Saat periode pembaruan berakhir, tinjau aturan baru yang terkait dengan pengguna ini yang telah ditambahkan ke kebijakan yang diterapkan, sesuaikan jika diperlukan, dan dapatkan persetujuan dari klien.
5. Alihkan rencana proteksi yang diaplikasikan pada beban kerja ke mode **Penerapan ketat** atau mode **Penerapan adaptif** - bergantung pada opsi mana yang klien anggap sebagai optimal untuk mencegah kebocoran data dari beban kerja pengguna.
   Jika tidak, Anda dapat mengaplikasikan ulang rencana proteksi yang diaplikasikan ke perusahaan (atau unit) ke beban kerja pengguna.

Menggunakan Mode penerapan adaptif untuk memperbarui kebijakan pengguna

Pembaruan kebijakan untuk pengguna tunggal atau bagian dari seluruh pengguna di dalam perusahaan (atau unit) dapat dilakukan dengan menggunakan Mode penerapan adaptif dari rencana proteksi dengan Advanced DLP yang diaplikasikan pada beban kerja pengguna.

Catatan
Metode pembaruan kebijakan ini memiliki kekhusuan berikut: Aturan kebijakan yang diterapkan pada perusahaan (unit) untuk kelompok pengirim dengan keanggotaan pengguna (mis. Pengguna Internal) juga diterapkan atas transfer data dari pengguna ini selama pembaruan. Akibatnya, pembaruan tidak akan membuat aturan tersendiri baru untuk pengguna yang mungkin bertolak belakang atau cocok dengan aturan kebijakan yang sudah ada ini untuk kelompok pengirim. Salah satu dari dua metode ini lebih efektif untuk pembaruan kebijakan pengguna untuk klien tertentu bergantung kepada kebutuhan keamanan IT khususnya

Untuk memperbarui kebijakan bagi pengguna melalui Mode penerapan adaptif

Proses pembaruan terdiri dari langkah-langkah berikut yang harus dilakukan oleh administrator Perusahaan atau Mitra yang mengelola beban kerja perusahaan.

1. Hapus semua aturan non-default di dalam kebijakan yang diterapkan untuk perusahaan (unit) yang memiliki pengguna sebagai pengirim tunggal mereka.
2. Hapus pengguna dari daftar pengirim dari semua aturan alur data non-default di dalam kebijakan yang diterapkan.

© Acronis International GmbH, 2003-2024

3. Untuk semua aturan default di dalam kebijakan yang diterapkan untuk perusahaan (atau unit), atur izinnya ke **Pengecualian**, lalu pilih tindakan **Tulis dalam log** di bidang **Tindakan**.
4. Jika rencana proteksi yang saat ini diaplikasikan ke beban kerja pengguna diatur ke mode **Penerapan ketat**, buat rencana proteksi baru dengan Advanced DLP dan aplikasikan ke beban kerja pengguna di dalam mode **Penerapan adaptif** untuk memulai periode pembaruan.
   Durasi periode pembaruan bergantung seberapa lama itu dilakukan untuk pengguna agar dapat melakukan seluruh atau 90-95% aktivitas bisnis reguler mereka yang melibatkan transfer data sensitif dari beban kerja mereka.
5. Saat periode pembaruan berakhir, tinjau aturan baru yang terkait dengan pengguna ini yang telah ditambahkan ke kebijakan yang diterapkan, sesuaikan jika diperlukan, dan dapatkan persetujuan dari klien.
6. Alihkan rencana proteksi yang diaplikasikan pada beban kerja ke mode **Penerapan ketat** atau tetap biarkan dalam mode **Penerapan adaptif** - bergantung pada opsi mana yang klien anggap optimal untuk mencegah kebocoran data dari beban kerja pengguna.
   Jika tidak, Anda dapat mengaplikasikan ulang rencana proteksi yang diaplikasikan ke perusahaan (atau unit) ke beban kerja pengguna.

Mengaktifkan Advanced Data Loss Prevention di rencana proteksi

Fitur Advanced Data Loss Prevention dapat disertakan di dalam rencana proteksi mana pun untuk penyewa pelanggan jika paket layanan Proteksi dan Advanced Data Loss Prevention diaktifkan untuk pelanggan ini.

Advanced DLP adalah modul lanjutan dari grup fitur pencegahan kehilangan data. Fitur Advanced DLP dan Kontrol perangkat dapat digunakan secara independen atau bersamaan (dalam satu rencana proteksi, atau dalam dua rencana yang melindungi beban kerja yang sama). Jika digunakan bersamaan, kemampuan fungsional keduanya diselaraskan sebagai berikut.

- Kontrol perangkat berhenti mengendalikan akses pengguna ke saluran lokal di mana Advanced DLP menginspeksi isi data yang ditransfer. Namun, Kontrol perangkat tetap mempertahankan kontrol atas jenis perangkat berikut jika mereka dikonfigurasi untuk hanya baca atau akses ditolak:
  - Yang dapat dilepas
  - Dapat dilepas yang terenkripsi
  - Drive yang dipetakan

  Sebagai contoh, jika Anda memiliki Kontrol perangkat dan Advanced DLP yang diaktifkan dalam satu rencana proteksi atau dalam dua rencana yang melindungi beban kerja yang sama, dan Anda memiliki akses hanya baca yang dikonfigurasi untuk perangkat USB dalam Kontrol perangkat, akses hanya baca akan diterapkan ke semua perangkat USB, kecuali untuk perangkat USB yang ada di dalam daftar izin, terlepas dari pengaturan akses dalam modul Advanced DLP. Jika pengaturan default Pengaktifan akses dikonfigurasi dalam Kontrol perangkat, pengaturan akses dalam Advanced DLP akan diterapkan.
- Akses pengguna ke saluran lokal dan periferal dalam daftar izin berikut ini diterapkan oleh Kontrol Perangkat:

© Acronis International GmbH, 2003-2024

- Drive optik
- Drive flopi
- Perangkat seluler terkoneksi MTP
- Adaptor Bluetooth
- Papan klip Windows
- Tangkapan layar
- Jenis perangkat USB dan perangkat (kecuali penyimpanan Dapat Dilepas dan Terenkripsi)

Untuk membuat rencana proteksi dengan Advanced DLP

1. Navigasi ke **Manajemen** > **Rencana proteksi**.
2. Klik **Buat rencana**.
3. Perluas bagian **Pencegahan Kehilangan Data** lalu klik baris **Mode**.
   Dialog **Mode** terbuka.
   - Untuk memulai pembuatan atau pembaruan kebijakan alur data, pilih **Mode Observasi**, lalu pilih cara memproses transfer data:

Opsi	Deskripsi
Izinkan semua	Seluruh transfer data sensitif dari beban kerja pengguna diperlakukan sebagaimana mestinya untuk proses dan keamanan bisnis. Aturan baru dibuat untuk setiap alur data terdeteksi yang tidak cocok dengan aturan yang telah ditentukan dalam kebijakan.
Benarkan semua	Seluruh transfer data sensitif dari beban kerja pengguna diperlakukan sebagaimana mestinya untuk proses bisnis, namun berisiko. Oleh karena itu, untuk setiap transfer data sensitif yang dicegat ke penerima atau tujuan mana pun baik yang di dalam dan luar organisasi yang tidak cocok dengan aturan alur data yang dibuat sebelumnya, pengguna harus memasukkan pembenaran bisnis satu-waktu. Saat pembenaran dikirimkan, aturan alur data baru dibuat dalam kebijakan alur data.
Gabungan	Logika Izinkan semua diaplikasikan untuk seluruh transfer data sensitif internal, dan logika Benarkan semua diaplikasikan untuk seluruh transfer data sensitif eksternal. Untuk definisi tujuan internal, lihat "Deteksi tujuan mandiri" (hlm. 877)

Peringatan!
- Pilih **Mode Observasi** saja jika Anda tidak memiliki kebijakan alur data yang dibuat sebelumnya atau jika Anda memperbarui kebijakan. Sebelum Anda memulai pembaruan kebijakan, lihat "Pembaruan kebijakan alur data" (hlm. 871).
- Kebocoran data tidak dicegah dalam mode Observasi. Lihat Mode Observasi di panduan Fundamental.

   - Untuk menerapkan kebijakan alur data yang sudah ada, pilih **Mode penerapan**, lalu pilih seberapa ketat penerapan aturan kebijakan alur data:

© Acronis International GmbH, 2003-2024

Opsi	Deskripsi
Penerapan ketat	Kebijakan alur data diterapkan sebagaimana mestinya dan tidak akan diperluas dengan aturan kebijakan permisif baru saat alur data sensitif yang tidak terobservasi sebelumnya terdeteksi. Lihat Penerapan ketat di panduan Fundamental.
Penerapan adaptif (Penerapan dengan pembelajaran)	Kebijakan yang diterapkan meneruskan adaptasi otomatisnya untuk operasi bisnis yang tidak dilakukan selama periode observasi atau untuk perubahan di dalam proses bisnis. Mode ini memungkinkan kebijakan alur data yang diterapkan untuk diperluas berdasarkan alur data yang baru dipelajari yang terdeteksi dalam beban kerja. Lihat Penerapan adaptif di panduan Fundamental.

Penting
Sebelum mengalihkan perusahaan atau kebijakan unit dari mode Observasi ke mode Penerapan, penting untuk menyesuaikan aturan default untuk setiap kategori data sensitif dari permisif ke tahap larangan. Aturan default ditandai dengan tanda bintang (*) dalam tampilan **Kebijakan alur data**. Baca lebih lanjut tentang jenis aturan kebijakan di Panduan fundamental.

4. Klik **Selesai** untuk menutup dialog Mode.
5. (Opsional) Untuk mengonfigurasi pengenalan karakter optik, daftar izin, dan opsi perlindungan lainnya, klik **Pengaturan Lanjutan**.
   Untuk informasi dalam opsi yang tersedia, lihat "Pengaturan lanjutan" (hlm. 876).
6. Simpan rencana proteksi dan terapkan ke beban kerja yang Anda ingin lindungi.

Pengaturan lanjutan

Anda dapat menggunakan pengaturan lanjutan di rencana proteksi dengan Advanced Data Loss Prevention untuk meningkatkan kualitas pemeriksaan konten data di saluran yang dikontrol oleh Advanced Data Loss Prevention, juga meniadakan kontrol pencegahan transfer data ke jenis perangkat periferal dalam daftar izin, kategori komunikasi jaringan, host tujuan, juga transfer data yang dimulai oleh aplikasi dalam daftar izin. Anda dapat mengonfigurasi pengaturan lanjutan berikut ini:

- **Pengenalan karakter optik**
  Pengaturan ini untuk mengaktifkan atau menonaktifkan pengenalan karakter optik (OCR) untuk mengekstrak bagian dari teks dalam 31 bahasa untuk pemeriksaan konten lebih lanjut dari file grafis dan gambar dalam dokumen, pesan, hasil pindaian, tangkapan layar, dan objek lain.
- **Transfer data yang dilindungi kata sandi**
  Isi arsip dan dokumen yang dilindungi kata sandi tidak dapat diperiksa. Dengan pengaturan ini, Advanced DLP memungkinkan administrator untuk memilih apakah transfer keluar dari data yang dilindungi kata sandi akan diizinkan atau diblokir.

© Acronis International GmbH, 2003-2024

- **Mencegah transfer data mengalami kesalahan**
  Analisis konten yang sedang dikirim terkadang gagal atau kesalahan kontrol lainnya terjadi dalam operasi agen DLP. Jika opsi ini diaktifkan, transfer akan diblokir. Jika opsi dinonaktifkan, transfer akan diperbolehkan meskipun terjadi kesalahan.
- **Daftar izin untuk jenis perangkat dan komunikasi jaringan**
  Transfer data ke jenis perangkat periferal dan dalam ditentukan dalam komunikasi jaringan yang dicentang dalam daftar ini diperbolehkan, terlepas dari sensitivitas data dan kebijakan alur data yang diterapkan.

  Peringatan!
  Opsi ini digunakan jika terjadi masalah dengan jenis Perangkat atau Protokol tertentu. Jangan aktifkan opsi ini kecuali disarankan oleh perwakilan Dukungan.

- **Daftar izin untuk host jarak jauh**
  Transfer data ke host tujuan yang ditentukan dalam daftar ini diperbolehkan, terlepas dari sensitivitas data dan kebijakan alur data yang diterapkan.
- **Daftar izin untuk aplikasi**
  Transfer data yang dilakukan oleh aplikasi yang ditentukan dalam daftar ini diperbolehkan, terlepas dari sensitivitas data dan kebijakan alur data yang diterapkan.

Indikator **Tingkat keamanan** dari pengaturan Lanjutan ditampilkan di tampilan **Buat rencana proteksi**, dan di tampilan "Perincian" rencana proteksi terdapat indikasi tingkat logika berikut:

- **Dasar** mengindikasikan bahwa tidak ada pengaturan lanjutan yang diaktifkan.
- **Sedang** mengindikasikan bahwa satu atau lebih pengaturan telah diaktifkan, tetapi kombinasi dari **OCR**, **Transfer data yang dilindungi kata sandi**, dan **Mencegah transfer data mengalami kesalahan** tidak diaktifkan.
- **Ketat** mengindikasikan bahwa setidaknya kombinasi dari **OCR**, **Transfer data yang dilindungi kata sandi**, dan **Pengaturan pencegahan transfer data dari kesalahan** telah diaktifkan.

Deteksi tujuan mandiri

Dalam mode Observasi Gabungan, Advanced Data Loss Prevention menerapkan berbagai aturan yang berbeda pada tujuan dari transfer data yang terdeteksi - internal atau eksternal. Logika untuk menentukan sebuah tujuan sebagai internal digambarkan seperti di bawah ini. Seluruh tujuan lain dianggap eksternal.

Untuk setiap transfer data yang dicegat, Advanced Data Loss Prevention mendeteksi secara otomatis jika tujuan server HTTP, FTP atau SMB adalah internal dengan melakukan permintaan DNS dan membandingkan nama-nama FQDN mesin tempat agen Pencegahan Kehilangan Data berjalan dan server jarak jauh. Jika permintaan DNS gagal, ia juga memeriksa apakah beban kerja terproteksi dan server jarak jauh berada dalam jaringan yang sama. Beberapa server yang memiliki nama domain yang sama (atau berada dalam subjaringan yang sama) sebagai mesin tempat agen Pencegahan Kehilangan Data berjalan dianggap sebagai internal.

© Acronis International GmbH, 2003-2024

Untuk komunikasi surel, Advanced Data Loss Prevention menganggap semua surel yang dikirim dari alamat surel perusahaan dengan menggunakan server surat perusahaan sebagai transfer internal jika surel penerima berada pada domain yang sama seperti surel pengirim, dan nama server surat penerima mirip.

Email non-korporat dianggap sebagai komunikasi eksternal kecuali akun penerima dikenal. Alamat email yang dikenal diperbarui saat Pencegahan Kehilangan Data memantau aktivitas pengguna pada jaringan dan memperbarui database di back end bersama data untuk alamat email yang terkait dengan pengguna.

Komunikasi melalui pengirim pesan dianggap sebagai komunikasi eksternal kecuali akun penerima dikenal. Akun dikenal diperbarui saat Pencegahan Kehilangan Data memantau aktivitas pengguna pada jaringan dan memperbarui database di back end bersama data untuk akun yang terkait dengan pengguna.

Definisi data sensitif

Topik ini menjelaskan logika dari identifikasi data sensitif selama analisis konten.

Untuk mengurangi jumlah false positive, kecocokan identik dihitung sebagai satu kecocokan untuk seluruh kelompok dari ekspresi logika yang dijelaskan.

Penting
Ekspresi logika yang digunakan untuk identifikasi konten disediakan sebagai informasi saja dan tidak menjelaskan solusi dalam detail penuh.

Informasi Kesehatan yang Dilindungi (PHI)

Bahasa yang didukung

- AS, Inggris Raya, Bahasa Inggris-Internasional
- Bahasa Finlandia
- Bahasa Italia
- Bahasa Prancis
- Bahasa Polandia
- Bahasa Rusia
- Bahasa Hungaria
- Bahasa Norwegia
- Bahasa Spanyol

Data yang dianggap Informasi Kesehatan yang Dilindungi

Data berikut dianggap sebagai informasi kesehatan yang dilindungi.

© Acronis International GmbH, 2003-2024

- Nama depan dan nama belakang
- Alamat (jalan, kota, negara, precinct, kode pos, dan kode geografis yang sesuai dengannya)
- Nomor telepon
- Alamat surel
- Nomor Jaminan Sosial
- Nomor penerima program kesehatan
- Nomor Rekening Bank
- URL
- Nomor alamat IP
- Kode ICD-10-CM
- ICD-10-PCS-and-GEMs
- HIPAA
- Perawatan terkait kesehatan lainnya
- Nomor Kartu Kredit

Ekspresi logika yang digunakan untuk deteksi konten

Ekspresi logika terdiri dari string berikut yang digabungkan dengan operator logika OR. Operator OR digunakan untuk menggabungkan kelompok data yang berbeda dalam daftar di atas jika operator logika AND tidak ditentukan secara eksplisit. Jumlah dalam kurung mewakili jumlah instans yang terdeteksi yang akan menampilkan hasil deteksi positif.

- **Nomor Jaminan Sosial** (5)
- (Nama depan dan nama belakang (3) OR Alamat (3) OR Nomor Telepon (3) OR Alamat Email (3) OR Nomor Rekening Bank (3) OR Nomor Kartu Kredit (3)) AND (Nomor Jaminan Sosial (3) OR Nomor penerima jaminan kesehatan (3) OR kode ICD-10-CM (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR Perawatan kesehatan terkait lainnya (3))

Informasi Identitas Pribadi (PII)

Bahasa yang didukung

- AS, Inggris Raya, Bahasa Inggris-Internasional
- Bahasa Bulgaria
- Bahasa Mandarin
- Bahasa Ceko
- Bahasa Denmark
- Bahasa Belanda
- Bahasa Finlandia

© Acronis International GmbH, 2003-2024

- Bahasa Prancis
- Bahasa Jerman
- Bahasa Hungaria
- Bahasa Indonesia
- Bahasa Italia
- Bahasa Korea
- Bahasa Melayu
- Bahasa Norwegia
- Bahasa Polandia
- Bahasa Portugis (Brasil)
- Bahasa Portugis (Portugal)
- Bahasa Rumania
- Bahasa Rusia
- Bahasa Serbia
- Singapura
- Bahasa Spanyol
- Bahasa Swedia
- Taiwan
- Bahasa Turki
- Bahasa Thailand
- Bahasa Jepang

Data yang dianggap Informasi Identitas Pribadi (PII)

- Nama depan dan nama belakang
- Alamat (jalan, kota, county, kode pos)
- Nomor Rekening Bank
- Nomor ID pribadi dan fiskal
- Nomor Paspor
- Nomor Jaminan Sosial
- Nomor telepon
- Nomor plat mobil
- Nomor SIM
- Pengidentifikasi dan nomor seri
- Alamat IP

© Acronis International GmbH, 2003-2024

- Alamat surel
- Nomor Kartu Kredit

Ekspresi logika yang digunakan untuk deteksi konten

Ekspresi logika untuk semua bahasa yang didukung kecuali Bahasa Jepang

Ekspresi logika terdiri dari string berikut digabungkan dengan operator logika OR atau AND. Jumlah dalam kurung mewakili jumlah instans yang terdeteksi yang akan menampilkan hasil deteksi positif.

- Nomor ID pribadi dan fiskal (5)
- Nama depan dan nama belakang (3) AND **(**Nomor Kartu Kredit (3) OR Nomor Jaminan Sosial (3) OR Nomor Rekening Bank (3) OR Nomor ID pribadi dan fiskal (3) OR Nomor SIM (3) OR Nomor Paspor (3) OR Nomor Jaminan Sosial (3) OR Alamat IP (3) OR Plat nomor seri mobil (3) OR Pengidentifikasi dan nomor seri**)**
- Nomor telepon (3) AND **(**Nomor Kartu Kredit (3) OR Nomor Jaminan Sosial (3) OR Nomor Rekening Bank (3) OR Alamat (3) OR Nomor ID pribadi dan fiskal (3) OR Nomor SIM (3) OR Nomor Paspor (3) OR Nomor Jaminan Sosial (3) OR Plat nomor mobil (3) OR Pengidentifikasi dan Pengidentifikasi dan nomor seri (3)**)**
- **(**Nama depan dan Nama belakang (30) OR Alamat (30)**)** AND **(**Alamat Email (30) OR Nomor Telepon (30) OR Alamat IP (30)**)**
- Alamat Email (3) AND **(**Nomor Kartu Kredit (3) OR Nomor Jaminan Sosial (3) OR Nomor Rekening Bank (3) OR Nomor ID pribadi dan fiskal (3) OR Nomor SIM (3) OR Nomor Paspor (3) OR Nomor jaminan sosial (3) OR Plat nomor mobil (3) OR Pengenal dan nomor seri (3)**)**
- Alamat Email (30) AND **(**Alamat (30) OR Nomor Telepon (30)**)**
- Nama depan dan nama belakang (30) AND Alamat (30)
- Nomor Telepon (30) AND Alamat (30)
- Nama depan dan nama belakang (3) AND Nomor Rekening Bank (3)
- Nomor Telepon (3) AND **(**Nomor Kartu Kredit (3) OR Nomor Rekening Bank (3) OR Nomor jaminan sosial (3) OR Nomor ID pribadi dan fiskal (3) OR Nomor SIM (3) OR Nomor Paspor (3)**)**

Ekspresi logika untuk Bahasa Jepang

Catatan
Hanya cocok unik yang dihitung oleh deteksi konten.

Ekspresi logika terdiri dari string berikut digabungkan dengan operator logika OR. Operator OR digunakan untuk menggabungkan kelompok berbeda jika operator logika AND tidak ditentukan secara eksplisit.

- Nomor jaminan sosial (5)
- Nama depan dan Nama belakang (3) AND **(**Nomor Kartu Kredit (3) OR Nomor Rekening Bank (3) OR Nomor SIM (3) OR Nomor Paspor (3) OR Nomor jaminan sosial (3)**)**

© Acronis International GmbH, 2003-2024

- Nama depan dan Nama belakang (30) AND **(**Alamat Email (30) OR Nomor Telepon (30) OR Alamat IP (30) OR Alamat (30)**)**
- Alamat (3) AND **(**Nomor Kartu Kredit (3) OR Nomor Rekening Bank (3) OR Nomor SIM (3) OR Nomor Paspor (3) OR Nomor jaminan sosial (3)**)**
- Alamat Email (3) AND **(**Nomor Kartu Kredit (3) OR Nomor Rekening Bank (3) OR Nomor jaminan sosial (3) OR Nomor SIM (3)**)**
- Alamat (5) AND **(**Alamat Email (5) OR Nama depan dan Nama belakang (5) OR Nomor Telepon (5) OR Alamat IP (5)**)**
- Nama depan dan nama belakang (3) AND Nomor Rekening Bank (3)
- Nomor Telepon (3) AND **(**Nomor Kartu Kredit (3) OR Nomor Rekening Bank (3) OR Alamat (3) OR Nomor jaminan sosial (3) OR Nomor SIM (3)**)**

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)

Bahasa yang didukung

Grup sensitif ini adalah bahasa - independen. Data PCI DSS dalam Bahasa Inggris di semua negara.

Data yang dianggap PCI DSS

- Data pemegang kartu
  - Primary Account Number (PAN)
  - Nama pemegang kartu
  - Tanggal kedaluwarsa
  - Kode layanan
- Data Autentikasi Sensitif
  - Data full track (data strip magnetis atau setaranya di sebuah cip)
  - CAV2/CVC2/CVV2/CID
  - PIN/Blok PIN

Ekspresi logika yang digunakan untuk deteksi konten

Ekspresi logika terdiri dari string berikut digabungkan dengan operator logika OR. Jumlah dalam kurung mewakili jumlah instans yang terdeteksi yang akan menampilkan hasil deteksi positif.

- Nomor Kartu Kredit (5)
- Nomor Kartu Kredit (3) AND (Nama Amerika (Ex) (3) OR Nama Amerika (3) OR Kata Kunci PCI DSS (3) OR Tanggal (bulan/tahun) (3))
- Sampah Kartu Kredit (5)

Ditandai sebagai Rahasia

Data ditandai sebagai rahasia terdeteksi melalui kelompok kata kunci.

© Acronis International GmbH, 2003-2024

Kondisi Kecocokan berdasarkan bobot, dan setiap kata memiliki bobot == 1. Deteksi konten dianggap positif saat Cocok jika bobot > 3.

Bahasa yang didukung

- Bahasa Inggris
- Bahasa Bulgaria
- Bahasa Mandarin - Disederhanakan
- Bahasa Mandarin - Tradisional
- Bahasa Ceko
- Bahasa Denmark
- Bahasa Belanda
- Bahasa Finlandia
- Bahasa Prancis
- Bahasa Jerman
- Bahasa Hungaria
- Bahasa Indonesia
- Bahasa Italia
- Bahasa Jepang
- Bahasa Korea
- Bahasa Melayu
- Bahasa Norwegia
- Bahasa Polandia
- Bahasa Portugis - Brasil
- Bahasa Portugis - Portugal
- Bahasa Rusia
- Bahasa Serbia
- Bahasa Spanyol
- Bahasa Swedia
- Bahasa Turki

Grup kata kunci

Grup kata kunci untuk setiap bahasa berisi kata khusus-negara yang sesuai dengan kata kunci berikut yang digunakan untuk Bahasa Inggris (sensitif huruf besar/kecil).

- rahasia
- distribusi internal

© Acronis International GmbH, 2003-2024

- bukan untuk distribusi
- jangan didistribusikan
- bukan untuk publik
- bukan untuk distribusi eksternal
- hanya untuk penggunaan internal
- dokumentasi berkualifikasi tinggi
- pribadi
- informasi istimewa
- hanya untuk penggunaan internal
- hanya untuk penggunaan resmi

Peristiwa Pencegahan Kehilangan Data

Advanced Data Loss Prevention membuat peristiwa dalam tampilan peristiwa DLP seperti berikut.

- Selama mode observasi, peristiwa dibuat untuk semua transfer data yang dibenarkan.
- Selama mode penerapan, peristiwa dibuat berdasarkan tindakan **Tulis dalam log** yang dikonfigurasi untuk setiap aturan kebijakan yang dipicu.

Untuk melihat peristiwa untuk sebuah aturan dalam kebijakan alur data

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Navigasi ke **Proteksi** > **Kebijakan alur data**.
3. Temukan aturan yang ingin Anda lihat peristiwanya dan klik elipsis di ujung baris aturan.
4. Pilih **Lihat peristiwa**.

Untuk melihat detail tentang peristiwa dalam tampilan peristiwa DLP

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Navigasi ke **Proteksi** > **Peristiwa DLP**.
3. Klik peristiwa dalam daftar untuk melihat lebih banyak detail.
   Panel detail Peristiwa diperluas ke sebelah kanan.
4. Gulir ke bawah dan ke atas di panel detail Peristiwa untuk melihat informasi yang tersedia.
   Detail yang ditampilkan dalam panel bergantung kepada jenis aturan dan pengaturan aturan yang terpicu peristiwa tersebut.

Untuk memfilter peristiwa dalam daftar peristiwa DLP

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Navigasi ke **Proteksi** > **Peristiwa DLP**.
3. Di kiri atas, klik **Filter**.

© Acronis International GmbH, 2003-2024

4. Pilih kategori sensitivitas, beban kerja, jenis tindakan, pengguna, dan saluran dari menu drop-down.
   Anda dapat memilih lebih dari satu item dalam menu drop-down. Pemfilteran menerapkan operator logis ATAU di antara item dalam menu yang sama, tetapi operator logis DAN digunakan di antara item dari menu yang berbeda.
   Misalnya, jika Anda memilih kategori sensitivitas **PHI** dan **PII**, hasilnya akan mengembalikan semua peristiwa yang berisi PHI atau PII, atau keduanya. Jika Anda memilih kategori sensitivitas **PHI** dan tindakan **Akses tulis**, hanya peristiwa yang cocok dengan kedua kategori yang akan muncul dalam hasil filter.
5. Klik **Terapkan**.
6. Untuk melihat semua peristiwa lagi, klik **Filter**, lalu **Atur ulang ke default**, dan terakhir klik **Terapkan**.

Untuk mencari peristiwa dalam daftar peristiwa DLP

1. Ulangi langkah 1-2 dari prosedur di atas.
2. Dari daftar drop-down ke sebelah kanan Filter, pilih kategori yang ingin Anda cari: **Pengirim**, **Destinasi**, **Process**, **Subjek pesan**, atau **Alasan**.
3. Dalam kotak teks, masukkan frasa yang Anda minati lalu konfirmasikan dengan menekan Enter di keyboard.
   Hanya peristiwa yang cocok dengan frasa yang Anda masukkan akan muncul dalam daftar.
4. Untuk mengatur ulang daftar peristiwa, klik tanda **X** dalam kotak teks pencarian lalu tekan Enter.

Untuk melihat daftar peristiwa yang terkait dengan aturan tertentu dalam kebijakan alur data

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Navigasi ke **Proteksi** > **Kebijakan alur data**.
3. Pilih kotak centang di depan nama aturan kebijakan yang Anda minati.
   Anda dapat memilih beberapa aturan kebijakan jika diperlukan.
4. Klik **Lihat peristiwa**.
   Tampilan beralih ke **Proteksi** > **Peristiwa DLP** dan peristiwa terkait aturan kebijakan yang Anda pilih muncul dalam daftar.

Widget Advanced Data Loss Prevention dalam dasbor Ikhtisar

Dasbor **Ikhtisar** menyediakan sejumlah widget kustom yang memberikan ikhtisar operasi terkait dengan layanan Cyber Protection, termasuk Advanced Data Loss Prevention. Anda dapat menemukan widget Advanced Data Loss Prevention berikut dalam dasbor **Ikhtisar** di **Pemantauan**.

- **Transfer data sensitif** - menampilkan jumlah total operasi transfer data sensitif kepada penerima internal dan eksternal. Grafik dibagi berdasarkan jenis izin: diizinkan, dibenarkan atau diblokir. Anda dapat menyesuaikan widget ini dengan memilih rentang waktu yang diinginkan (1 hari, 7 hari, 30 hari, atau bulan ini).

© Acronis International GmbH, 2003-2024

- **Kategori data sensitif keluar** - menampilkan jumlah total operasi transfer data sensitif kepada penerima eksternal. Diagram dibagi berdasarkan kategori sensitif: Informasi Kesehatan yang Dilindungi (PHI), Informasi Identitas Pribadi (PII), PCI DSS, dan Ditandai sebagai Rahasia (Rahasia).
- **Pengirim terbanyak data sensitif keluar** - menampilkan jumlah total transfer data sensitif dari organisasi kepada penerima eksternal dan daftar lima pengguna dengan jumlah transfer terbanyak (bersama dengan jumlah ini). Statistik ini mencakup transfer yang diizinkan dan yang dibenarkan. Anda dapat menyesuaikan widget ini dengan memilih rentang waktu yang diinginkan (1 hari, 7 hari, 30 hari, atau bulan ini).
- **Pengirim terbanyak data sensitif keluar yang diblokir** - menampilkan jumlah total transfer data sensitif yang diblokir dan daftar lima pengguna dengan jumlah percobaan transfer terbanyak (bersama dengan jumlah ini). Anda dapat menyesuaikan widget ini dengan memilih rentang waktu yang diinginkan (1 hari, 7 hari, 30 hari, atau bulan ini).
- **Peristiwa DLP terbaru** - menampilkan detail peristiwa pencegahan kehilangan data terbaru untuk rentang waktu yang dipilih. Anda dapat menyesuaikan widget ini menggunakan opsi berikut:
  - **Rentang (tanggal diposting)** (1 hari, 7 hari, 30 hari atau bulan).
  - Nama **beban kerja**
  - **Status operasi** (diizinkan, dibenarkan, atau diblokir)
  - **Sensitivitas** (PHI, PII, Rahasia, PCI DSS)
  - **Jenis tujuan** (eksternal, internal)
  - **Pengelompokan** (beban kerja, pengguna, jenis tujuan)

Widget diperbarui setiap lima menit. Widget memiliki elemen yang dapat diklik sehingga memungkinkan Anda untuk menyelidiki dan menyelesaikan masalah. Anda dapat mengunduh status dasbor saat ini atau mengirimnya melalui email dalam format .pdf atau/dan .xlsx.

Kategori sensitivitas kustom

Kategori data sensitif kustom dapat membantu organisasi untuk melindungi kekayaan intelektual dan data rahasia khusus untuk organisasi tersebut dengan memperluas katalog bawaan Advanced DLP tentang definisi konten terkait peraturan kepatuhan.

Untuk membuat kategori sensitif kustom

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Navigasikan ke **Proteksi** > **Pencegahan kehilangan data** > **Pengklasifikasi data**.
3. Pilih **Kategori sensitivitas**.
4. Anda akan melihat daftar sensitivitas, baik bawaan (seperti Informasi kesehatan yang dilindungi atau Informasi Identifikasi Pribadi) dan yang dikustomisasi.
5. Klik **Buat Sensitivitas** di pojok kanan atas jendela.
6. Masukkan namanya di jendela berikutnya.

© Acronis International GmbH, 2003-2024

7. Sensitivitas kustom baru selalu dinonaktifkan secara default. Anda dapat mengaktifkannya setelah mengonfigurasi semua parameternya.
8. Setelah membuat sensitivitas baru, Anda harus menyiapkan pendeteksi kontennya. Klik panah untuk memperluas konten sensitivitas baru Anda dan pilih **Tambahkan pendeteksi konten**.
9. Di jendela berikutnya, Anda dapat menggunakan salah satu pendeteksi konten yang ada (dengan mengeklik tanda centang di samping namanya, lalu mengeklik **Tambah** di pojok kanan bawah) atau mendefinisikan yang baru.
10. Alih-alih membuat sensitivitas baru dari awal, Anda juga dapat menggunakan kembali sensitivitas yang sudah ada (baik sensitivitas bawaan atau kustom yang sudah ada) dengan membuat klona dan menyesuaikan parameternya.
    - Untuk membuat klona sensitivitas yang ada, klik tanda centang di sebelah namanya, lalu pilih **Klona** dari menu drop-down Tindakan (ditunjukkan dengan elipsis) di pojok kiri atas. Anda dapat memilih beberapa item sekaligus untuk membuat klona pada lebih dari satu sensitivitas.
    - Di jendela berikutnya, Anda dapat memilih parameter sensitivitas yang ada yang ingin Anda pertahankan dengan mengeklik tanda centang di sebelah setiap parameter.

Catatan
Menyalin sensitivitas bawaan di dalam satu penyewa akan membuat sensitivitas baru yang terdiri dari pendeteksi yang sama (menjadi Kustom setelah disalin)

Untuk membuat pendeteksi konten baru

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Navigasikan ke **Proteksi** > **Pencegahan kehilangan data** > **Pengklasifikasi data**.
3. Pilih **Pendeteksi konten**.
4. Anda akan melihat daftar pendeteksi konten, baik bawaan maupun khusus.
5. Klik **Buat pendeteksi konten** di pojok kanan atas jendela.
6. Menu drop-down akan terbuka, di mana Anda dapat memilih jenis pendeteksi yang ingin Anda buat – saat ini, hanya pendeteksi konten **Jenis file** yang tersedia, akan ada lebih banyak pembaruan yang akan tersedia di masa mendatang.
7. Di jendela berikut, Anda dapat mengonfigurasi pendeteksi konten.

Jenis pendeteksi konten	Deskripsi
Pendeteksi konten jenis file	a. Terdapat dua daftar: **Jenis file yang didukung** dan **Jenis file yang dipilih**. Dengan mengeklik ikon "plus" di sebelah kanan jenis file yang didukung, Anda akan memindahkannya ke daftar Jenis file yang dipilih. Anda juga dapat memilih beberapa jenis file yang didukung dengan mengeklik tanda centang di sebelah namanya, lalu menggunakan tombol **Tambahkan yang dipilih** di pojok kanan atas.

© Acronis International GmbH, 2003-2024

Jenis pendeteksi konten	Deskripsi
	b. Untuk menghapus jenis file dari daftar Jenis file yang dipilih, klik ikon tempat sampah di sebelah kanan namanya. Anda juga dapat menghapus beberapa jenis file sekaligus menggunakan tanda centang dan tombol **Hapus yang dipilih**.
Pendeteksi konten kata kunci	a. Saat membuat pendeteksi konten kata kunci baru, Anda perlu mengimpor kata kunci dari file. Setelah berhasil mengimpor, Anda dapat menggabungkan kata kunci baru dengan daftar yang sudah ada atau mengganti daftar yang sudah ada dengan kata kunci yang diimpor. b. Anda juga perlu menentukan apakah Anda ingin pendeteksi konten cocok dengan semua kata kunci dari daftar, kata kunci apa pun dari daftar atau sejumlah kata kunci kustom.

8. Alih-alih membuat pendeteksi konten baru dari awal, Anda juga dapat menggunakan kembali yang sudah ada (baik sensitivitas bawaan atau kustom yang ada) dengan membuat klona dan menyesuaikan parameternya.
   - Untuk membuat klona pendeteksi konten, klik tanda centang di sebelah namanya, lalu pilih **Klona** dari menu drop-down Tindakan (ditunjukkan dengan elipsis) di pojok kiri atas. Anda dapat memilih beberapa item sekaligus untuk membuat klona pada lebih dari satu pendeteksi konten.

Catatan
Menyalin pendeteksi konten bawaan akan mengubahnya menjadi kustom.

Peta organisasi

Catatan
Fungsionalitas ini hanya dapat diakses oleh pengguna Administrator Perusahaan.

Peta organisasi adalah basis data yang berisi data untuk pengguna dan semua akun pengguna yang digunakan untuk mentransfer data melalui pesan instan, email, atau cara lainnya, yang telah diintersepsi oleh Advanced DLP.

Peta organisasi menyediakan cara untuk membuat dan mengelola grup pengguna di Advanced DLP, dan untuk mengelola pengguna dan akun yang terkait dengan pengguna di Advanced DLP. Grup pengguna kemudian dapat digunakan untuk manajemen kebijakan DLP berbasis grup.

Untuk menemukan peta Organisasi

- Di konsol Cyber Protect Cloud, buka **Perlindungan** > **Pencegahan kehilangan data** > **Peta organisasi**.

© Acronis International GmbH, 2003-2024

Bagaimana cara kerjanya?

Catatan
Peta organisasi diisi saat modul Advanced DLP beroperasi dalam mode Observasi.

Untuk setiap transfer data yang diintersepsi oleh Agen DLP, atribut berikut dikumpulkan di back end.

Atribut	Deskripsi	Label di Antarmuka Pengguna
Unit Organisasi	Sebuah grup yang dibuat secara manual. Unit organisasi dapat memiliki satu atau lebih Unit Organisasi yang bersarang.	Nama grup, seperti yang didefinisikan
ID Keamanan	Sebuah pengenal keamanan unik.	Di halaman detail pengguna > **SID**
	Nama tampilan ramah pengguna yang diambil dari nama akun untuk pengguna. Nama ini tidak selalu tersedia dalam pemetaan organisasi.	**Nama**
PC\UserName	Nama pengguna dari titik akhir (beban kerja). Nama pengguna hanya dapat diberikan ke satu Unit Organisasi saja.	**Nama pengguna**
Perangkat (Beban Kerja)	Nama dari titik akhir (beban kerja).	**Beban kerja**
Akun	Akun yang digunakan oleh pengguna untuk komunikasi melalui pesan instan dan email, dan telah diintersepsi oleh Agen DLP. Misalnya, jika agen mendeteksi bahwa nama pengguna 'PC\John' menggunakan john@gmail.com untuk mengirim email - akun ini terhubung dengan nama pengguna PC\John.	**Akun**

Dalam peta organisasi, Anda dapat melihat dan mencari akun, pengguna, dan grup, serta membuat, mengedit, dan menghapus grup.

Untuk mencari akun tertentu

Sebagai bagian dari investigasi insiden, pengguna Administrator mungkin perlu menemukan pemilik dari akun tertentu yang terlibat dalam potensi pelanggaran data.

1. Di konsol Cyber Protect Cloud, buka **Perlindungan** > **Pencegahan kehilangan data** > **Peta organisasi**.
2. Dalam kotak teks **Pencarian** di atas daftar pengguna, mulailah mengetik atau tempelkan akun. Daftar ini disaring saat Anda mengetik.

Untuk mencari nama pengguna tertentu

© Acronis International GmbH, 2003-2024

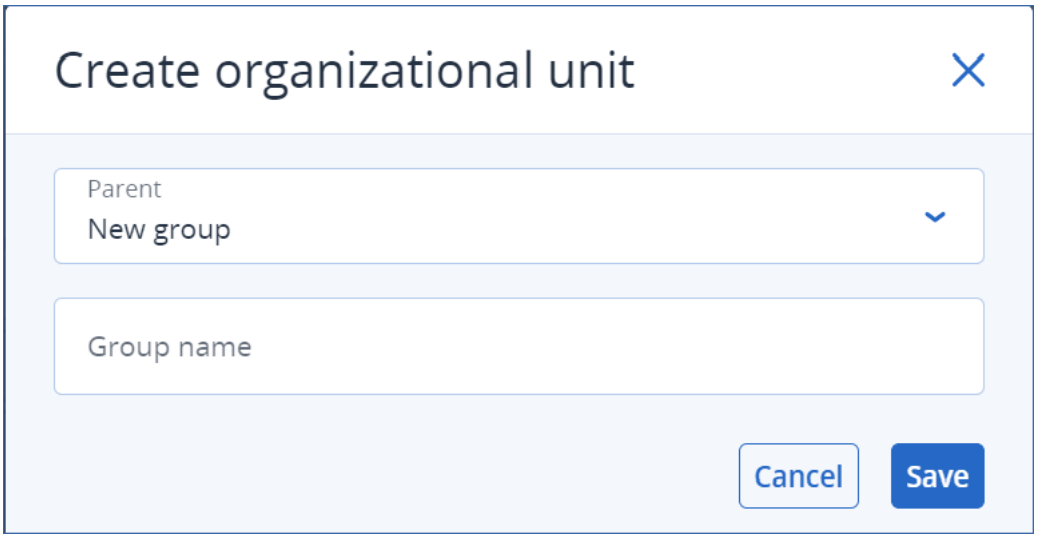
1. Di konsol Cyber Protect Cloud, buka **Perlindungan** > **Pencegahan kehilangan data** > **Peta organisasi**.
2. Untuk mencari dalam grup tertentu, klik nama grup di dalam daftar.
3. Dalam kotak teks **Pencarian** di atas daftar pengguna, mulailah mengetik atau tempelkan nama pengguna.
   Daftar ini disaring saat Anda mengetik.

Untuk melihat akun yang digunakan oleh nama pengguna tertentu

1. Temukan pengguna dalam daftar pengguna.
2. Klik tiga titik di akhir baris pengguna dan pilih **Lihat**.
3. Dalam dialog detail pengguna, temukan bagian **Akun terkait**.
4. Anda dapat menambahkan komentar di dalam kotak teks Deskripsi.

Untuk membuat grup pengguna

1. Di konsol Cyber Protect Cloud, buka **Perlindungan** > **Pencegahan kehilangan data** > **Peta organisasi**.
2. Di bagian kiri bawah dari daftar grup, klik **Buat grup**.
   Dialog Membuat unit organisasi terbuka.



3. Dari menu drop-down Orang Tua, pilih konteks untuk grup baru.

   Catatan
   Anda tidak dapat mengubah induk nanti. Grup akan tetap bersarang dalam konteks ini.

4. Masukkan nama grup dan klik **Simpan**.

Untuk menambahkan pengguna ke dalam grup

1. Di konsol Cyber Protect Cloud, buka **Perlindungan** > **Pencegahan kehilangan data** > **Peta organisasi**.

© Acronis International GmbH, 2003-2024

2. Dalam daftar pengguna, temukan pengguna yang ingin Anda tambahkan dan pilih kotak centang di awal baris pengguna.
   Tombol **Pindahkan yang dipilih** dan **Hapus yang dipilih** muncul di atas daftar pengguna.

3. Klik **Pindahkan yang dipilih**.
   Dialog Pindah pengguna terbuka.
4. Pilih induk baru untuk pengguna yang dipilih dan klik **Simpan**.

Catatan
Satu pengguna hanya bisa menjadi anggota dari satu grup saja.

Untuk menghapus akun yang terkait dengan pengguna

1. Temukan pengguna dalam daftar pengguna.
2. Klik tiga titik di akhir baris pengguna dan pilih **Lihat**.
3. Dalam dialog detail pengguna, temukan bagian **Akun terkait**.
4. Temukan akun yang ingin Anda hapus dan klik tiga titik di sebelahnya.
5. Dari daftar drop-down, pilih **Hapus**.

Untuk mengubah nama grup pengguna

1. Di konsol Cyber Protect Cloud, buka **Perlindungan** > **Pencegahan kehilangan data** > **Peta organisasi**.
2. Klik tiga titik di sebelah nama grup dan klik **Ubah Nama**.

Untuk menghapus grup pengguna

1. Di konsol Cyber Protect Cloud, buka **Perlindungan** > **Pencegahan kehilangan data** > **Peta organisasi**.
2. Klik tiga titik di sebelah nama grup dan klik **Hapus**.
   Semua pengguna dari grup dipindahkan ke entitas induk.

Masalah dan batasan yang diketahui

- [DEVLOCK-4028] Tidak ada kontrol untuk obrolan grup di agen desktop Zoom.
- [DEVLOCK-4016] Nama yang ramah dan ID pengirim tidak diambil untuk GMX Web Mail dan Web.de Mail jika draf dibuat.
- [DEVLOCK-4447] Tidak ada dialog Pembenaran untuk naver.com WebMail dalam hal pembuatan draf.
- [DEVLOCK-1033] DeviceLockDriver: pemeriksaan bug potensial DRIVER_POWER_STATE_FAILURE disebabkan oleh kebuntuan selama pemrosesan IRP_MN_QUERY_DEVICE_RELATIONS.

© Acronis International GmbH, 2003-2024

Deteksi dan Tanggapan Titik Akhir (EDR)

Catatan
Fungsionalitas ini adalah bagian dari paket perlindungan Advanced Security + EDR, yang pada gilirannya merupakan bagian dari layanan Perlindungan cyber. Perhatikan bahwa saat menambahkan fungsionalitas EDR ke rencana proteksi, Anda mungkin akan dikenakan biaya tambahan.

EDR mendeteksi aktivitas mencurigakan pada beban kerja, termasuk serangan yang luput dari perhatian. EDR kemudian menciptakan insiden, yang memberikan ikhtisar langkah demi langkah dari setiap serangan, untuk membantu Anda memahami bagaimana serangan terjadi dan cara mencegahnya terjadi lagi. Dengan interpretasi yang mudah dipahami dari setiap tahap serangan, waktu yang dihabiskan untuk menyelidiki serangan dapat dikurangi menjadi hitungan menit.

Alasan Anda memerlukan Deteksi dan Tanggapan Titik Akhir (EDR)

Ketika ancaman cyber dan serangan berbahaya terus berkembang hingga saat ini, pencegahan tidak lagi dapat menjamin perlindungan 100%. Sebagian serangan akan selalu bisa membobol lapisan pencegahan dan berhasil menembus jaringan. Solusi konvensional tidak akan bisa melihat waktu terjadinya serangan, sehingga pihak penyerang bisa dengan bebas berada di lingkungan Anda selama berhari-hari, berminggu-minggu, hingga berbulan-bulan.

Solusi EDR yang sudah ada dapat membantu mencegah "kegagalan senyap" tersebut dengan menemukan dan menyingkirkan pelaku penyerangan secara cepat. Namun, solusi tersebut umumnya memerlukan keahlian tingkat tinggi di bidang keamanan atau analis Pusat Operasi Keamanan (SOC) yang mahal, dan proses analisis insidennya bisa memerlukan waktu yang sangat lama.

Fungsionalitas Keamanan Tingkat Lanjut + EDR Acronis dapat mengatasi hambatan-hambatan itu, dengan cara mengidentifikasi serangan yang tidak terdeteksi, dan membantu Anda memahami proses terjadinya suatu serangan serta cara mencegahnya agar tidak terjadi lagi. Dengan demikian, waktu yang diperlukan untuk menginvestigasi serangan akan jauh berkurang.

Berikut alasan mengapa Anda memerlukan EDR:

- **Visibilitas penuh**: Pahami apa yang terjadi dan cara terjadinya, bahkan untuk serangan yang tidak terdeteksi. Evolusi setiap serangan juga dipetakan secara visual, langkah demi langkah (mulai dari titik masuk awal hingga menampilkan data yang ditarget dan/atau diambil), memungkinkan Anda memahami cakupan dan dampak insiden dengan cepat. Untuk informasi lebih lanjut, lihat "Cara menginvestigasi insiden di rantai cyber kill" (hlm. 906).
- **Meminimalkan waktu investigasi**: Kurangi waktu investigasi insiden yang biasanya memerlukan waktu berjam-jam hingga menjadi beberapa menit. EDR memberikan detail setiap langkah penyerangan dalam bahasa yang mudah dipahami, sehingga mampu mengurangi

© Acronis International GmbH, 2003-2024

kebutuhan akan ahli yang mahal atau karyawan tambahan. Untuk informasi lebih lanjut, lihat "Menyelidiki insiden" (hlm. 905)

- **Periksa ancaman yang diketahui di beban kerja Anda**: Anda dapat secara otomatis mencari ancaman malware, kerentanan, dan jenis peristiwa global lainnya pada beban kerja Anda yang mungkin dapat memengaruhi perlindungan data Anda. Ancaman tersebut disebut sebagai Insiden Penyusupan (IOC), dan ditentukan berdasarkan data ancaman yang diperoleh dari Pusat Operasi Perlindungan Cyber (CPOC). Untuk informasi lebih lanjut, lihat "Periksa indikator penyusupan (IOC) dari serangan terhadap beban kerja Anda yang diketahui secara publik" (hlm. 917).
- **Tanggapi insiden lebih cepat**: Dengan akses ke semua aktivitas pasca-pembobolan dan uraian setiap langkah di rantai kill, Anda dapat melakukan sejumlah tindakan untuk meremediasi setiap titik serangan. Di antaranya, Anda dapat menginvestigasi menggunakan kontrol jarak jauh dan cadangan forensik (fitur ini tidak tersedia di versi Akses Awal), mengarantina beban kerja, dan menghentikan proses malware. Anda juga dapat memulihkan operasi bisnis menggunakan Cyber Disaster Recovery Cloud. Untuk informasi lebih lanjut, lihat "Remediasi insiden" (hlm. 920).
- **Laporkan postur keamanan Anda dengan percaya diri**: Dengan mengaktifkan EDR, Anda dapat menghilangkan kekhawatiran dan ketakutan akan dampak serangan cyber terhadap bisnis Anda. Selain itu, informasi yang berkaitan dengan insiden disimpan selama 180 hari, yang nantinya dapat digunakan untuk audit.

Fitur

Deteksi dan Tanggapan Titik Akhir (EDR) mencakup beberapa fitur berikut:

- Terima pemberitahuan peringatan saat terjadi pelanggaran
- Kelola insiden Anda di halaman Insiden
- Visualisasi alur cerita penyerangan yang mudah dipahami
- Rekomendasi dan langkah remediasi
- Periksa serangan yang diungkapkan secara publik pada beban kerja Anda menggunakan umpan ancaman
- Sekilas pembahasan tentang dasbor
- Simpan peristiwa keamanan selama 180 hari

Terima pemberitahuan peringatan saat terjadi pelanggaran

EDR memberikan pemberitahuan peringatan setiap kali terjadi insiden. Lansiran ini disorot di menu utama konsol Cyber Protect. Anda kemudian dapat menyelidiki peringatan dengan mengeklik tombol **Investigasi insiden**, yang mengarahkan Anda ke layar investigasi insiden (atau dikenal sebagai rantai cyber kill).

Untuk informasi lebih lanjut, lihat "Meninjau insiden" (hlm. 897).

© Acronis International GmbH, 2003-2024

Kelola insiden Anda di halaman Insiden

EDR memungkinkan Anda mengelola semua insiden Anda di halaman Insiden (diakses dari menu Perlindungan di konsol Cyber Protect). Halaman Insiden, yang dapat difilter menurut kebutuhan Anda, memastikan Anda dapat dengan cepat dan mudah memahami status insiden saat ini, termasuk tingkat keparahan, beban kerja yang terpengaruh, dan level kepositifan. Anda juga dapat menavigasi langsung ke rantai cyber kill untuk melihat alur cerita serangan simpul demi simpul.

Untuk informasi selengkapnya tentang halaman Insiden, lihat "Meninjau insiden" (hlm. 897).

Visualisasi alur cerita penyerangan yang mudah dipahami

EDR menyediakan representasi visual dari serangan dalam format yang mudah dibaca. Ini memastikan bahwa personel non-keamanan pun dapat memahami tujuan dan tingkat keparahan serangan apa pun. Benar-benar tidak perlu layanan Pusat Operasi Keamanan (SOC) atau menyewa pakar keamanan; EDR merinci bagaimana tepatnya serangan terjadi, termasuk:

- Cara penyerang masuk
- Cara penyerang menyembunyikan jejaknya
- Kerugian yang ditimbulkan
- Cara serangan menyebar

Untuk informasi lebih lanjut, lihat "Cara menginvestigasi insiden di rantai cyber kill" (hlm. 906).

Rekomendasi dan langkah remediasi

EDR memberikan rekomendasi yang jelas dan mudah diterapkan untuk menyelesaikan serangan pada beban kerja. Untuk mengatasi serangan dengan cepat, klik tombol **Remediasi keseluruhan insiden** untuk melihat dan mengikuti langkah-langkah yang direkomendasikan untuk mengurangi insiden tersebut. Langkah-langkah yang disarankan ini memungkinkan Anda untuk melanjutkan operasi yang terpengaruh oleh serangan dengan cepat. Namun, jika Anda ingin melakukan langkah remediasi yang lebih terperinci, Anda dapat menavigasi ke setiap simpul dan memulihkannya dengan tindakan yang relevan.

Untuk informasi lebih lanjut, lihat "Remediasi insiden" (hlm. 920).

Periksa serangan yang diungkapkan secara publik pada beban kerja Anda menggunakan umpan ancaman

EDR menyertakan kemampuan untuk meninjau serangan yang ada dan diketahui dalam umpan ancaman terhadap beban kerja Anda. Umpan ancaman ini dibuat secara otomatis berdasarkan data ancaman yang diterima dari Pusat Operasi Perlindungan Cyber (CPOC); EDR memungkinkan Anda memverifikasi apakah ancaman memengaruhi beban kerja Anda atau tidak, lalu mengambil langkah yang diperlukan untuk meniadakan ancaman tersebut.

© Acronis International GmbH, 2003-2024

Untuk informasi lebih lanjut, lihat "Periksa indikator penyusupan (IOC) dari serangan terhadap beban kerja Anda yang diketahui secara publik" (hlm. 917).

Sekilas pembahasan tentang dasbor

EDR menyediakan berbagai statistik dalam dasbor konsol Cyber Protect. Anda dapat melihat:

- Status ancaman saat ini, termasuk jumlah insiden yang perlu diselidiki.
- Evolusi serangan berdasarkan tingkat keparahan, menunjukkan kemungkinan kampanye serangan.
- Tingkat efisiensi penutupan insiden.
- Taktik paling bertarget yang digunakan untuk menyerang pelanggan Anda.
- Status jaringan beban kerja, apakah terisolasi atau terhubung.

Simpan peristiwa keamanan selama 180 hari

EDR mengumpulkan beban kerja dan kejadian aplikasi dan menyimpannya selama 180 hari. Peristiwa sebelum periode 180 hari akan dihapus (penghapusan acara didasarkan pada usia dan bukan menurut ruang penyimpanan). Perhatikan bahwa meskipun EDR dinonaktifkan, semua peristiwa yang dikumpulkan sebelumnya untuk suatu beban kerja akan dipertahankan, dan akan tersedia untuk penyelidikan insiden.

Persyaratan perangkat lunak

Deteksi dan Tanggapan Titik Akhir (EDR) mendukung sistem operasi berikut:

- Microsoft Windows 7 Service Pack 1 dan versi lebih baru
- Microsoft Windows Server 2008 R2 dan versi lebih baru

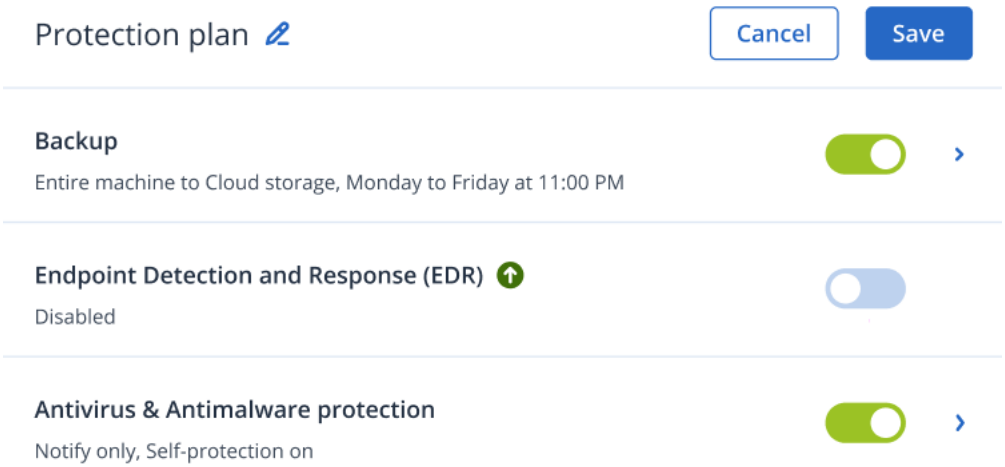
Mengaktifkan fungsionalitas Deteksi dan Tanggapan Titik Akhir (EDR)

Anda dapat mengaktifkan EDR dalam rencana proteksi apa pun.

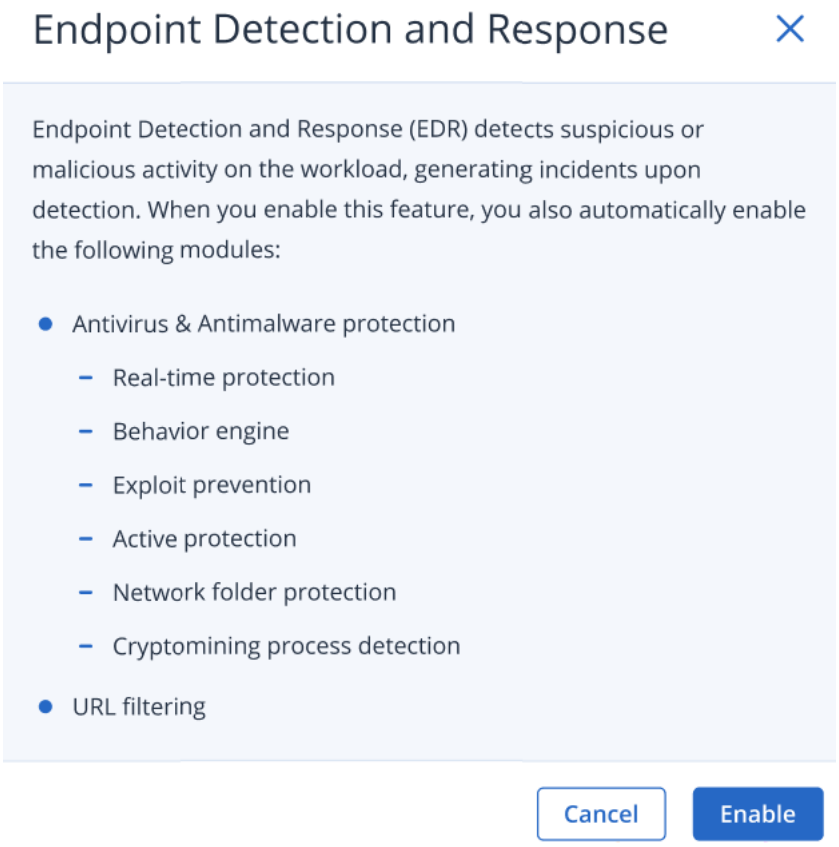
Untuk mengaktifkan EDR

1. Di konsol Cyber Protect, buka **Manajemen > Rencana proteksi**.
2. Pilih rencana proteksi yang relevan dari daftar yang ditampilkan, dan di panel samping kanan, klik **Edit**.
   Cara lainnya, Anda dapat membuat rencana proteksi baru dan melanjutkan ke langkah berikutnya. Untuk informasi lebih lanjut tentang bekerja dengan rencana proteksi, lihat "Modul dan rencana proteksi" (hlm. 213).
3. Di panel samping rencana proteksi, aktifkan modul **Deteksi dan Tanggapan Titik Akhir (EDR)** dengan mengeklik tombol alih di sebelah nama modul.

© Acronis International GmbH, 2003-2024



4. Di dialog yang ditampilkan, klik **Aktifkan**. Ingat bahwa ketika EDR diaktifkan, modul proteksi lain juga diaktifkan, seperti yang terlihat pada dialog yang tampil.



Catatan
Jika salah satu dari **Active protection**, **Mesin perilaku**, **Pencegahan eksploit**, atau **pemfilteran URL Dimatikan**, **Deteksi dan Tanggapan Titik Akhir (EDR)** juga **Dimatikan**.

5. Ikon paket **Keamanan Tingkat Lanjut + EDR**, seperti yang ditunjukkan di bawah, ditambahkan ke daftar paket proteksi yang diperlukan untuk penerapan rencana proteksi, tergantung pada paket tambahan yang Anda pilih.

© Acronis International GmbH, 2003-2024

ADVANCED SECURITY + EDR

Cara menggunakan Deteksi dan Tanggapan Titik Akhir (EDR)

EDR memungkinkan Anda untuk mendeteksi serangan yang tidak diketahui, sekaligus membantu Anda memahami bagaimana serangan terjadi dan cara mencegahnya terjadi lagi. Dengan interpretasi yang mudah dipahami dari setiap tahap serangan, waktu yang dihabiskan untuk menyelidiki serangan dapat dikurangi menjadi hitungan menit.

Tabel di bawah menjelaskan alur kerja umum saat bekerja dengan EDR. Awalnya, Anda akan meninjau dan memprioritaskan setiap insiden baru, menyelidikinya lebih lanjut dalam rantai cyber kill, lalu mengambil tindakan remediasi yang relevan.

Langkah	Cara menggunakan EDR
LANGKAH 1: Tinjau insiden	Dalam daftar insiden EDR: • Pahami postur keamanan suatu organisasi: berapa banyak insiden yang perlu diselidiki? • Pahami insiden mana yang paling kritis, dan prioritaskan penyelidikannya menurut tingkat keparahannya. • Pahami insiden mana yang baru atau sedang berlangsung.
LANGKAH 2: Investigasi insiden	Dalam rantai cyber kill EDR: • Pahami tujuan penyerang dan lihat teknik serangan yang digunakan. • Verifikasi seberapa besar kemungkinan insiden merupakan serangan jahat yang sebenarnya. • Verifikasi apakah umpan ancaman memengaruhi beban kerja Anda atau tidak. • Lihat tindakan respons apa yang telah diterapkan pada insiden.
LANGKAH 3: Remediasi insiden	Di bagian perbaikan EDR yang relevan: • Remediasi seluruh insiden dengan cepat dan mudah dengan menerapkan tindakan respons global. • Remediasi poin serangan individu dalam suatu insiden. • Terapkan tindakan untuk mencegah serangan (atau serangan di masa mendatang) agar tidak menyebar atau memengaruhi beban kerja yang belum ditargetkan oleh penyerang.

Meninjau insiden

Deteksi dan Tanggapan Titik Akhir (EDR) menyediakan daftar insiden yang menyertakan pencegahan (atau malware) dan deteksi yang mencurigakan pada beban kerja. Daftar insiden memberi Anda ringkasan serangan atau ancaman yang memengaruhi beban kerja Anda, termasuk ancaman yang mungkin belum dimitigasi.

Dari daftar insiden, Anda dapat mengetahui hal-hal berikut dengan cepat:

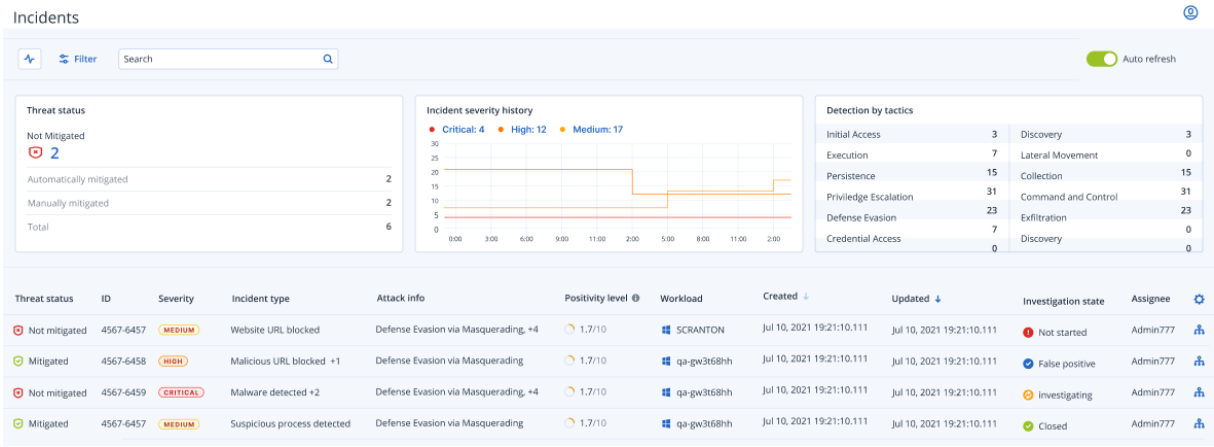
© Acronis International GmbH, 2003-2024

- Postur keamanan organisasi: berapa jumlah insiden yang perlu diinvestigasi?
- Insiden mana saja yang paling kritis, dan prioritaskan investigasinya berdasarkan tingkat keparahan insiden.
- Insiden apa saja yang masih baru atau yang belum terselesaikan.

Catatan
Ketika masuk sebagai administrator mitra, Anda dapat melihat semua insiden EDR dalam satu layar yang mengkonsolidasikan insiden dari semua pelanggan Anda, tanpa perlu mengakses tampilan insiden individu setiap pelanggan. Sebuah kolom **Pelanggan** tambahan ditampilkan, yang mencakup nama pelanggan yang menjadi milik setiap insiden. Selain itu, widget yang ditampilkan pada dasbor **Ikhtisar** menampilkan data metrik yang diagregasikan dari semua pelanggan.

Daftar insiden, seperti yang ditunjukkan di bawah ini, diakses dari menu **Perlindungan** di konsol Cyber Protect. Untuk informasi lebih lanjut tentang peninjauan insiden di daftar insiden, lihat "Melihat insiden mana yang saat ini tidak dimitigasi" (hlm. 901) Untuk mempelajari selengkapnya tentang waktu pembuatan insiden, lihat Apa itu insiden?.

Catatan
Jika Managed Detection and Response (MDR) diaktifkan pada beban kerja Anda, kolom tambahan **tiket MDR** ditampilkan. Kolom ini menampilkan nomor tiket yang disediakan oleh vendor MDR.



Catatan
Konsol Cyber Protect harus terbuka agar Anda dapat menerima pemberitahuan insiden.

Apa itu insiden?

Insiden, atau insiden keamanan, bisa diartikan sebagai *kontainer* yang setidaknya berisi satu titik deteksi pencegahan atau mencurigakan (atau perpaduannya), dan berisi semua peristiwa dan deteksi terkait dari satu serangan. Insiden keamanan ini juga dapat menyertakan peristiwa tambahan yang memberikan konteks yang lebih terperinci.

© Acronis International GmbH, 2003-2024

Ini akan memungkinkan Anda melihat beberapa peristiwa serangan dalam satu insiden, dan memahami langkah-langkah logis yang telah diambil oleh penyerang. Selain itu, ini juga dapat membantu memangkas waktu investigasi serangan.

Saat EDR diaktifkan di rencana proteksi, insiden keamanan akan dibuat ketika:

- **Lapisan pencegahan menghentikan sesuatu:** Insiden ini akan ditutup oleh sistem secara otomatis, sesuai dengan pengaturan rencana proteksi. Namun, Anda dapat menginvestigasi apa yang dilakukan oleh malware sebelum dihentikan. Misalnya, ransomware berhasil dihentikan saat mulai mengenkripsi file, tetapi sebelum berhasil dihentikan, ransomware tersebut bisa saja mencuri kredensial atau menginstal layanan.
- **Aktivitas mencurigakan terdeteksi oleh EDR:** Ini adalah deteksi yang perlu diinvestigasi dan diremediasi. Dengan meninjau rantai cyber kill yang ditingkatkan secara visual (untuk informasi lebih lanjut, lihat "Cara menginvestigasi insiden di rantai cyber kill" (hlm. 906)), Anda akan dapat menerapkan tindakan remediasi yang relevan dengan mudah.

Memprioritaskan insiden yang membutuhkan perhatian segera

Daftar insiden konsol Cyber Protect dapat diakses kapan saja dari menu **Perlindungan** di konsol Cyber Protect. Daftar insiden memberi Anda gambaran umum sekilas tentang setiap serangan atau ancaman dan memungkinkan Anda memprioritaskan insiden yang memerlukan perhatian.

Penting
Untuk memastikan beban kerja Anda tetap aman, *pastikan selalu* menganalisis dan memprioritaskan insiden yang sedang berlangsung atau tidak dimitigasi.

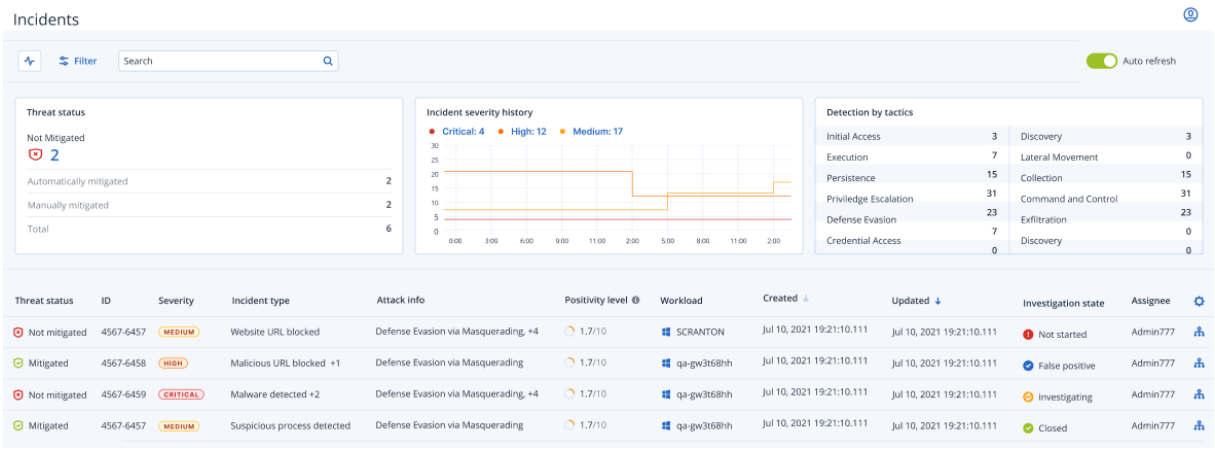
Cara menganalisis insiden keamanan yang membutuhkan perhatian segera

Daftar insiden memungkinkan Anda menganalisis dan memprioritaskan insiden terdaftar yang memerlukan perhatian. Anda dapat:

- Lihat insiden yang saat ini tidak dimitigasi: Pahami dengan cepat dari daftar insiden jika ada serangan yang sedang berlangsung. Setiap insiden yang tidak dimitigasi, seperti yang ditunjukkan dalam kolom **Status ancaman**, harus segera dilihat (secara default, daftar insiden difilter untuk menampilkan insiden ini).
- Pahami ruang lingkup dan dampak insiden: Berdasarkan pemfilteran Anda terhadap serangan yang baru dibuka atau yang sedang berlangsung, pahami tingkat keparahan insiden yang difilter serta dampaknya terhadap bisnis Anda.

Setelah memiliki daftar insiden yang paling penting, Anda kemudian dapat menganalisis detail insiden untuk mendapatkan pemahaman yang lebih baik tentang insiden tertentu, serta teknik yang digunakan oleh penyerang untuk mencapai tujuannya. Untuk informasi lebih lanjut, lihat "Analisis detail insiden" (hlm. 903).

© Acronis International GmbH, 2003-2024



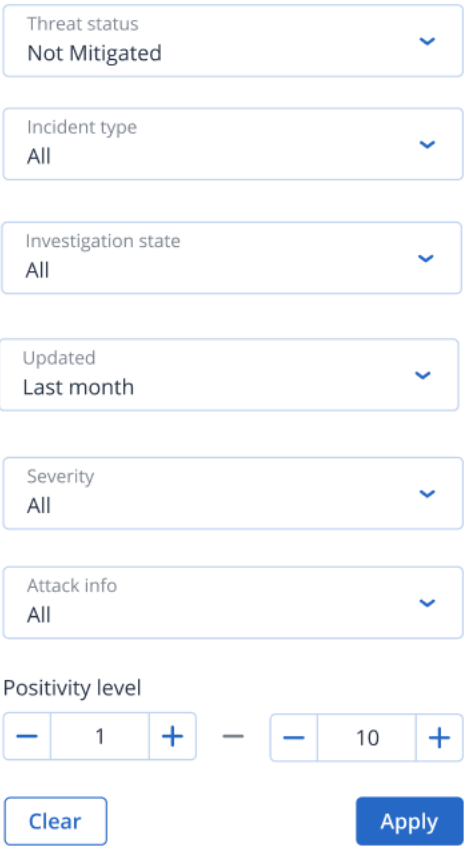
Catatan

Secara default, daftar insiden diurutkan menurut kolom **Diperbarui**, yang memberikan detail tanggal dan waktu insiden terakhir diperbarui dengan deteksi baru yang direkam di dalam insiden tersebut. Perhatikan bahwa setiap insiden yang ada dapat diperbarui kapan saja, meskipun sebelumnya insiden tersebut telah ditutup. Anda juga dapat memfilter daftar untuk menampilkan serangan yang baru dibuka atau yang sedang berlangsung sesuai dengan kebutuhan Anda, seperti yang dijelaskan dalam prosedur di bawah ini.

Untuk memfilter daftar insiden

1. Di bagian atas daftar Insiden, klik **Filter** untuk memfilter daftar insiden yang ditampilkan. Misalnya, jika Anda memilih tanggal mulai dan selesai pada bidang **Dibuat**, daftar insiden dan widget menampilkan insiden relevan yang dibuat selama periode waktu yang ditentukan.

© Acronis International GmbH, 2003-2024



2. Setelah selesai, klik **Terapkan**.

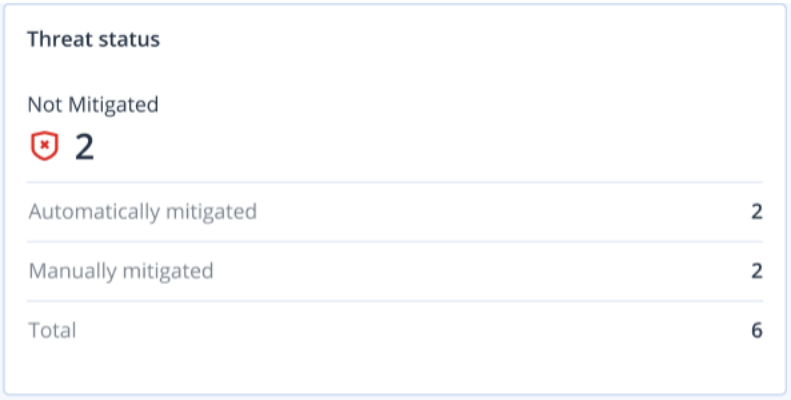
Melihat insiden mana yang saat ini tidak dimitigasi

Anda dapat melihat status ancaman saat ini untuk insiden di kolom **Status ancaman**, yang menunjukkan apakah insiden tersebut **Dimitigasi** atau **Tidak dimitigasi**. Status ancaman ditentukan secara otomatis oleh EDR; setiap insiden yang tidak dimitigasi harus diinvestigasi sesegera mungkin.

Kemudian, Anda dapat menyempurnakan daftar insiden yang ditampilkan lebih lanjut dengan menerapkan filter. Misalnya, jika Anda ingin memfilter daftar berdasarkan status ancaman *dan* tingkat keparahan tertentu, pilih opsi filter yang relevan. Setelah memfilter insiden yang menarik bagi Anda, Anda kemudian dapat menginvestigasinya, seperti yang dijelaskan di "Menyelidiki insiden" (hlm. 905).

Anda juga dapat menggunakan widget **Status ancaman**, seperti yang ditunjukkan di bawah ini, untuk ikhtisar sekilas tentang status ancaman saat ini. Perhatikan bahwa data yang ditampilkan di widget ini mencerminkan filter yang Anda terapkan; lihat "Untuk memfilter daftar insiden" (hlm. 900).

© Acronis International GmbH, 2003-2024



Memahami ruang lingkup dan dampak insiden

Anda dapat dengan cepat memahami ruang lingkup dan dampak insiden dengan meninjau kolom **Keparahan**, **Info serangan**, dan **Level kepositifan**. Seperti disebutkan di atas, setelah menentukan insiden yang sedang berlangsung, Anda dapat memfilter kolom tambahan ini untuk melakukan hal berikut:

- Tinjau insiden mana yang lebih kritis dalam kolom **Keparahan**. Tingkat keparahan suatu insiden bisa dikategorikan menjadi **Kritis**, **Tinggi**, atau **Sedang**.
  - **Kritis**: Ada risiko tinggi aktivitas cyber berbahaya dengan risiko membahayakan host penting di lingkungan Anda.
  - **Tinggi**: Ada risiko tinggi aktivitas cyber berbahaya dengan risiko kerusakan parah di lingkungan Anda.
  - **Sedang**: Ada peningkatan risiko aktivitas cyber yang berbahaya.

    Catatan
    Saat menentukan tingkat keparahan, algoritme EDR mempertimbangkan jenis beban kerja serta cakupan setiap langkah serangan. Misalnya, insiden yang mencakup langkah-langkah terkait pencurian kredensial diatur ke **Kritis**.

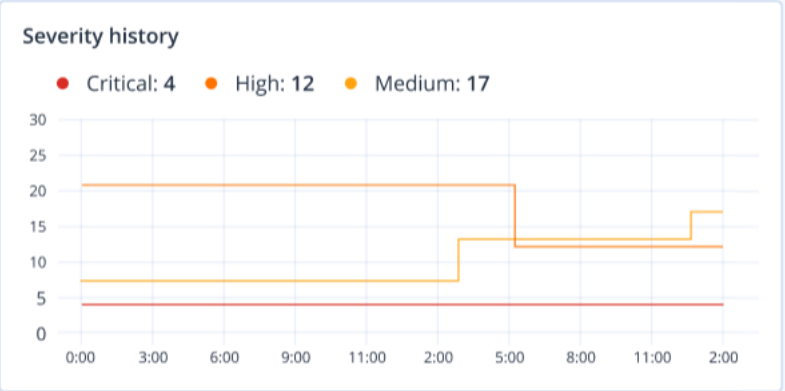
- Pahami mengapa insiden dibuat dalam kolom **Jenis Insiden**. Jenis insiden dapat mencakup satu atau lebih dari yang berikut:
  - **Ransomware terdeteksi**
  - **Malware terdeteksi**
  - **Proses mencurigakan terdeteksi**
  - **Proses berbahaya terdeteksi**
  - **URL mencurigakan diblokir**
  - **URL berbahaya diblokir**
- Tentukan teknik serangan yang digunakan dalam kolom **Info serangan**, dan lihat jika ada tema atau pola umum pada serangan tersebut.

© Acronis International GmbH, 2003-2024

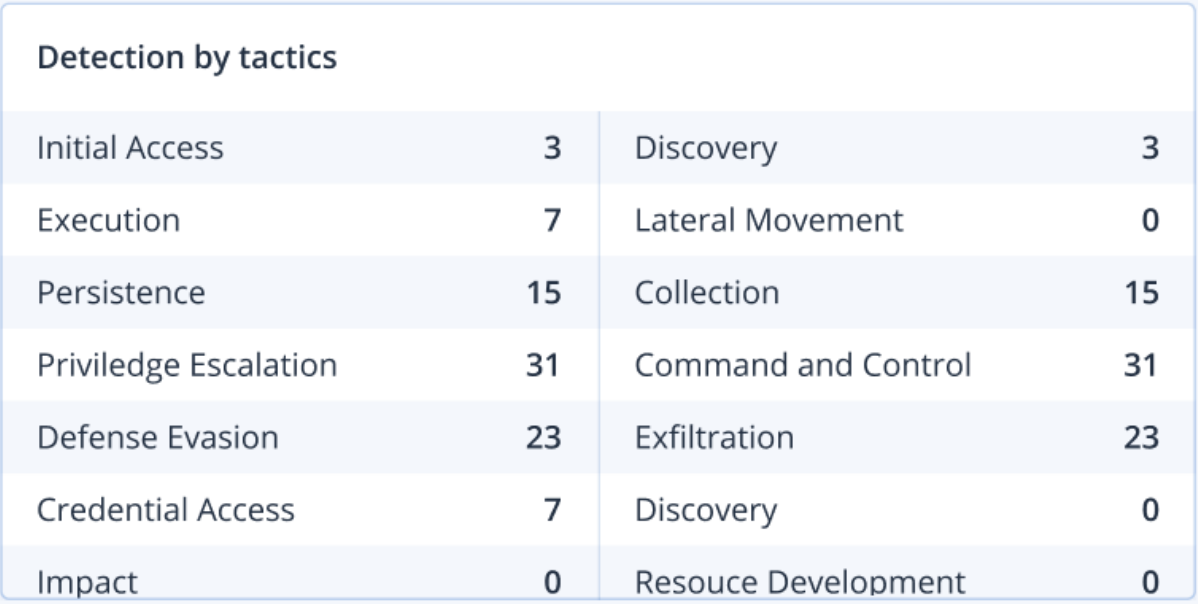
- Konfirmasi seberapa besar kemungkinan suatu insiden merupakan serangan jahat yang sebenarnya; kolom **Level kepositifan** mencakup skor antara 1-10 (semakin tinggi skornya, semakin besar kemungkinan serangan tersebut benar-benar berbahaya).

Setelah menemukan insiden yang memerlukan perhatian segera, Anda kemudian dapat menyelidikinya, seperti yang dijelaskan di "Menyelidiki insiden" (hlm. 905)

Anda juga dapat menggunakan widget **Riwayat keparahan** dan **Deteksi dengan taktik** untuk gambaran umum sekilas tentang tingkat keparahan dan teknik serangan.



Widget **Deteksi dengan taktik** menampilkan berbagai teknik serangan yang digunakan, dengan nilai berwarna hijau atau merah yang menunjukkan kenaikan atau penurunan selama rentang waktu yang ditentukan sebelumnya. Widget ini memberikan tampilan gabungan dari semua tujuan dalam insiden yang difilter, memberi Anda ikhtisar singkat tentang dampaknya terhadap pelanggan Anda.



Analisis detail insiden

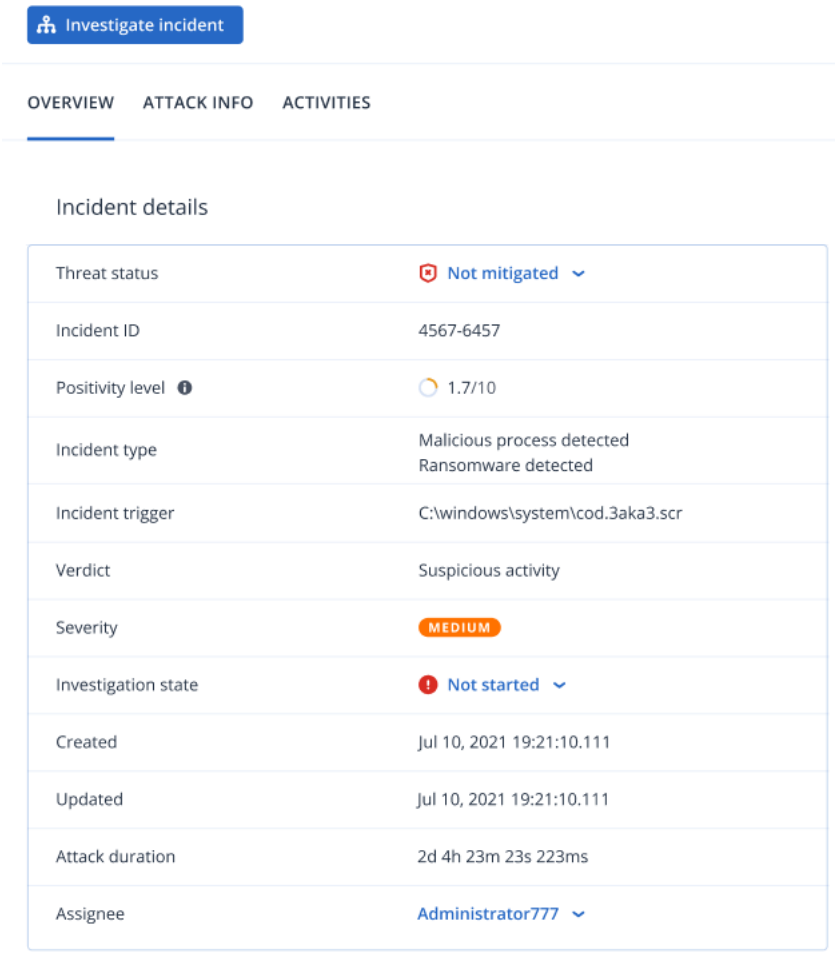
Pada tahap peninjauan insiden, Anda juga dapat menganalisis detail setiap insiden dari daftar insiden Deteksi dan Tanggapan Titik Akhir (EDR). Detail ini memungkinkan Anda memeriksa seluruh

© Acronis International GmbH, 2003-2024

insiden serta memahami proses dan waktu kejadiannya. Selain itu, Anda dapat menetapkan suatu insiden ke pengguna tertentu untuk investigasi, dan menetapkan status investigasi.

Untuk menganalisis detail insiden

1. Di konsol Cyber Protect, buka **Perlindungan > Insiden**. Daftar Insiden akan ditampilkan.
2. Klik insiden yang ingin Anda tinjau. Detail insiden yang dipilih akan ditampilkan.
3. Di tab **Ikhtisar**, Anda dapat meninjau detail insiden dan beban kerja, termasuk status dan tingkat keparahan ancaman saat ini. Anda juga dapat menentukan **Status investigasi** (pilih salah satu dari opsi **Menginvestigasi**, **Belum mulai** (status default), **Positif palsu**, atau **Ditutup**), dan pilih pengguna untuk penetapan insidennya (di daftar drop-down **Penerima tugas**, pilih pengguna yang relevan).



4. Klik tab **Info Serangan** untuk meninjau detail serangan dan teknik yang digunakan dalam serangan tersebut. Klik tautan di samping tiap teknik serangan yang tercantum untuk meninjau informasi lebih lanjut tentang tekniknya di MITRE.org.
5. Klik tab **Aktivitas** untuk meninjau tindakan apa pun yang diambil dalam rantai cyber kill untuk memitigasi insiden. Untuk informasi lebih lanjut, lihat "Cara menginvestigasi insiden di rantai cyber kill" (hlm. 906).

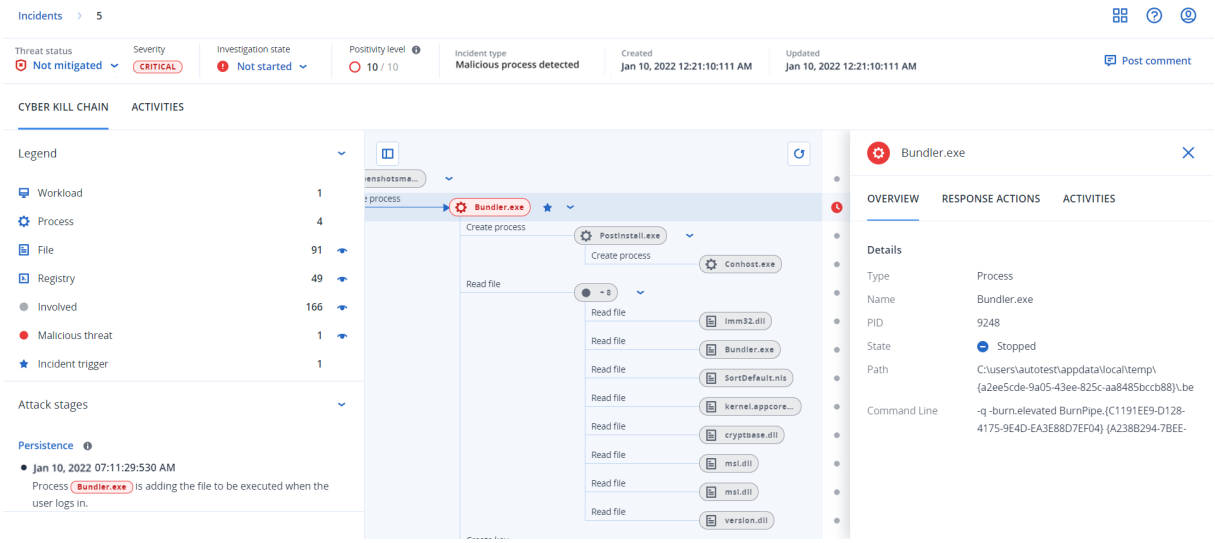
© Acronis International GmbH, 2003-2024

Misalnya, jika ada patch yang dijalankan pada beban kerja, Anda dapat melihat siapa yang memasang patch tersebut, berapa lama prosesnya, dan kesalahan apa saja yang mungkin timbul pada saat memasang patch itu.

6. Klik **Investigasi insiden** untuk mengakses rantai cyber kill, yang memungkinkan Anda menginvestigasi insiden simpul demi simpul. Untuk informasi lebih lanjut, lihat "Cara menginvestigasi insiden di rantai cyber kill" (hlm. 906).

Menyelidiki insiden

Deteksi dan Tanggapan Titik Akhir (EDR) memungkinkan Anda menyelidiki seluruh insiden, termasuk semua tahapan serangan dan objek (proses, pendaftar, tugas terjadwal, dan domain) yang terkena dampak serangan. Objek-objek ini diwakili oleh simpul dalam rantai cyber kill yang mudah dipahami, seperti yang ditunjukkan di bawah ini. Gunakan rantai cyber kill untuk memahami kejadian dan waktu terjadinya.



Setiap langkah serangan dilihat dalam rantai cyber kill, yang memberi Anda interpretasi mendetail tentang cara dan alasan insiden itu terjadi. Rantai cyber kill menggunakan kalimat dan grafik yang mudah dipahami yang membantu menjelaskan setiap langkah serangan, yang pada gilirannya membantu meminimalkan waktu penyelidikan.

Anda dapat dengan cepat memahami ruang lingkup dan dampak dari suatu insiden, dengan evolusi serangan yang dipetakan ke kerangka kerja MITRE. Ini memungkinkan Anda menganalisis apa yang terjadi di setiap langkah serangan, termasuk:

- Titik masuk awal
- Cara serangan dilakukan
- Eskalasi hak istimewa
- Teknik deteksi penghindaran
- Gerakan lateral ke beban kerja lainnya

© Acronis International GmbH, 2003-2024

- Pencurian kredensial
- Upaya eksfiltrasi

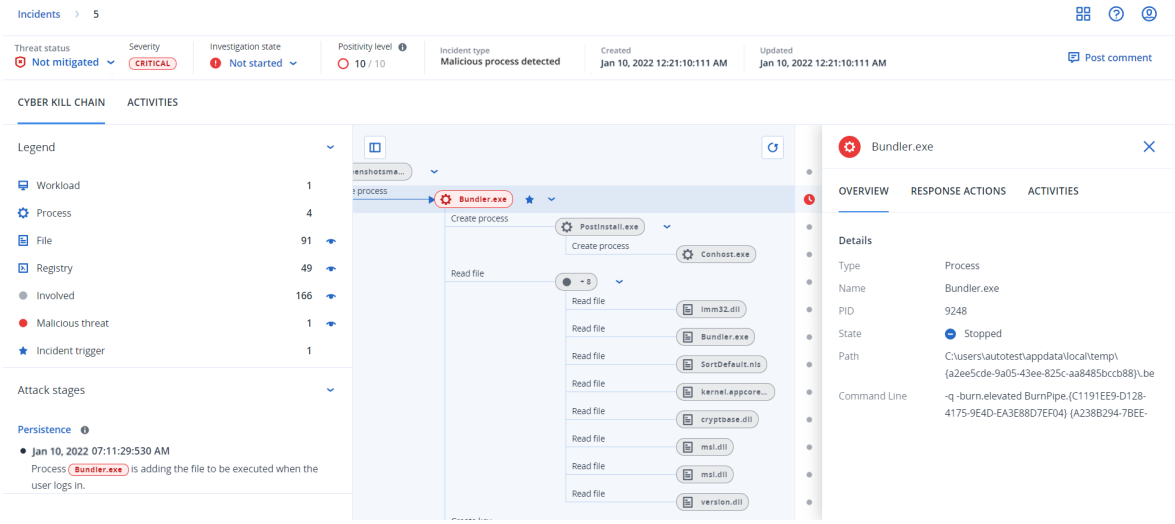
Catatan
Setiap objek yang terkena dampak serangan, baik itu proses, registri, tugas terjadwal, atau domain, diwakili oleh sebuah simpul dalam rantai cyber kill.

Cara menginvestigasi insiden di rantai cyber kill

Anda dapat menginvestigasi setiap langkah serangan di rantai cyber kill. Ikuti kalimat dan grafik rantai cyber kill untuk memahami setiap langkah serangan, yang nantinya dapat membantu Anda memangkas waktu investigasi.

Untuk memulai investigasi di rantai cyber kill

1. Di konsol Cyber Protect, buka **Perlindungan > Insiden**.
2. Di daftar insiden yang ditampilkan, klik di kolom ujung kanan insiden yang ingin Anda investigasi. Rantai cyber kill untuk insiden yang dipilih akan ditampilkan.



3. Tampilkan ringkasan insiden di panel status ancaman di atas halaman. Panel status ancaman menyertakan informasi berikut:
   - Status ancaman saat ini: Status ancaman ditentukan oleh sistem secara otomatis. Insiden yang **Tidak dimitigasi** akan diinvestigasi sesegera mungkin.

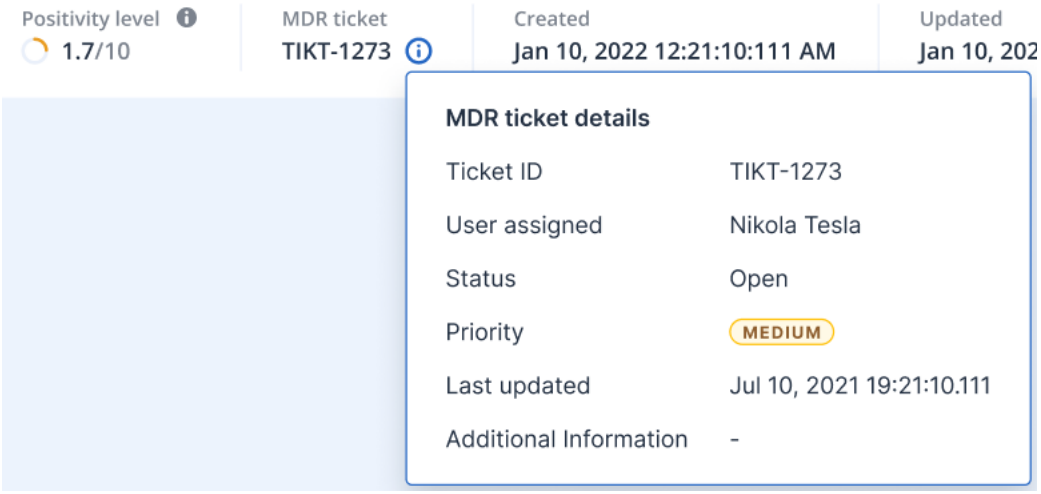
© Acronis International GmbH, 2003-2024

Penting
Insiden ditetapkan menjadi **Dimitigasi** ketika proses pemulihan dari cadangan telah berhasil diselesaikan atau ketika semua deteksi telah berhasil diremediasi dengan proses penghentian, karantina, atau tindakan pembatalan.

Insiden ditetapkan menjadi **Tidak dimitigasi** ketika proses pemulihan dari cadangan tidak berhasil diselesaikan atau ketika setidaknya ada satu deteksi yang gagal diremediasi dengan proses penghentian, karantina, atau tindakan pembatalan.

Anda juga bisa mengatur status ancaman ke **Termitigasi** atau **Tidak dimitigasi** secara manual. Saat memilih status apapun, Anda diminta untuk mengisi komentar. This komentar disimpan sebagai bagian dari aktivitas investigasi, dan dapat dilihat di tab **Aktivitas**. Perhatikan bahwa EDR masih bisa mengembalikan status ancama ke **Termigitasi** atau **Tidak dimitigasi** jika deteksi baru ditemukan untuk tindakan respons atau insiden berjalan dan berhasil dengan baik.

- Tingkat keparahan insiden: **Kritis**, **Tinggi**, atau **Sedang**. Untuk informasi lebih lanjut, lihat "Meninjau insiden" (hlm. 897).
- Status investigasi saat ini: **Menginvestigasi**, **Belum mulai** (status default), **Positif palsu**, atau **Ditutup**. Anda perlu mengubah status saat mulai menginvestigasi insidennya, sehingga rekan kerja lainnya dapat mengetahui perubahan pada insiden.
- Level kepositifan: Menandakan seberapa besar kemungkinan suatu insiden merupakan serangan yang benar-benar berbahaya, dengan rentang nilai 1-10. Untuk informasi lebih lanjut, lihat "Meninjau insiden" (hlm. 897).
- Jenis insiden: Satu atau lebih dari **Ransomware terdeteksi**, **Malware terdeteksi**, **Proses mencurigakan terdeteksi**, **Proses berbahaya terdeteksi**, **URL mencurigakan diblokir**, dan **URL berbahaya diblokir**.
- Jika Managed Detection and Response (MDR) diaktifkan pada beban kerja, bidang **tiket MDR** ditampilkan. Anda dapat melihat detail tiket MDR yang dibuat untuk insiden tersebut, dan analis keamanan MDR yang ditugaskan untuk insiden tersebut.



© Acronis International GmbH, 2003-2024

- Saat insiden dibuat dan diperbarui: Tanggal dan waktu insiden dideteksi, atau saat insiden terakhir diperbarui dengan deteksi baru yang direkam di dalam insiden tersebut.

4. Klik tab **Legenda** untuk menampilkan beragam simpul yang ada di grafik rantai kill, dan tentukan simpul yang akan dilihat. Untuk informasi lebih lanjut, lihat "Memahami dan menyesuaikan tampilan rantai cyber kill" (hlm. 908).
5. Investigasi dan remediasi insiden dengan melakukan langkah-langkah berikut. Perhatikan bahwa ini adalah alur kerja pada umumnya untuk menginvestigasi dan meremediasi insiden, yang mungkin berbeda berdasarkan setiap insiden dan kebutuhan Anda.
   a. Investigasi setiap tahap serangan di tab **Tahapan serangan**. Untuk informasi lebih lanjut, lihat "Cara menavigasi tahapan serangan" (hlm. 911).
   b. Klik **Remediasi keseluruhan insiden** untuk menerapkan tindakan remediasi. Untuk informasi lebih lanjut, lihat "Remediasi seluruh insiden" (hlm. 921).

      Anda juga dapat melakukan remediasi simpul individu di rantai cyber kill, sebagaimana dijelaskan di "Tindakan untuk merespons simpul rantai cyber kill individu" (hlm. 926).
   c. Tinjau tindakan yang diambil untuk memitigasi insiden di tab **Aktivitas**. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Memahami dan menyesuaikan tampilan rantai cyber kill

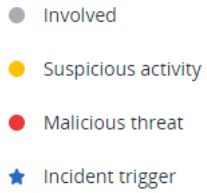
Untuk memahami simpul yang terdampak di rantai cyber kill, akses legenda. Legenda menampilkan semua simpul yang ada dalam suatu insiden, sehingga memungkinkan Anda memahami dampak di setiap simpul yang diakibatkan oleh tindakan penyerang. Anda juga dapat menentukan simpul yang ingin Anda sembunyikan atau tampilkan di rantai cyber kill.

Untuk mengakses legenda

1. Klik ikon panah di sebelah kanan bagian Legenda.
   Bagian Legenda akan diperluas, sebagaimana ditampilkan di bawah.

© Acronis International GmbH, 2003-2024

2. Terdapat empat warna utama di legenda yang membantu memudahkan Anda dalam memahami apa yang terjadi pada setiap simpul di rantai cyber kill, sebagaimana ditampilkan di bawah. Simpul berkode warna tersebut juga diikutsertakan di dalam tahapan serangan, sebagaimana dijelaskan di "Cara menavigasi tahapan serangan" (hlm. 911).



Untuk menyembunyikan atau menampilkan simpul di rantai cyber kill

1. Di bagian Legenda yang diperluas, pastikan ditampilkan di samping simpul yang ingin Anda tampilkan di rantai cyber kill. Jika ikon yang ditampilkan adalah , klik ikon untuk mengubahnya menjadi .
2. Untuk menyembunyikan simpul di rantai cyber kill, klik . Ikon berubah menjadi dan simpul tidak ditampilkan di rantai cyber kill.

Investigasi tahapan serangan insiden

Tahapan serangan insiden memberikan interpretasi yang mudah dipahami untuk setiap insiden.

Setiap tahapan serangan merangkum apa yang terjadi, dan apa saja objek (disebut sebagai *simpul* di rantai cyber kill) yang menjadi target. Misalnya, jika file yang diunduh ternyata menyamar sebagai file lain, tahapan serangan akan menunjukkan hal tersebut, dan tautan ke simpul yang relevan akan

© Acronis International GmbH, 2003-2024

disertakan di rantai cyber kill yang bisa Anda selidiki, serta tautan ke teknik MITRE ATT&CK yang relevan.

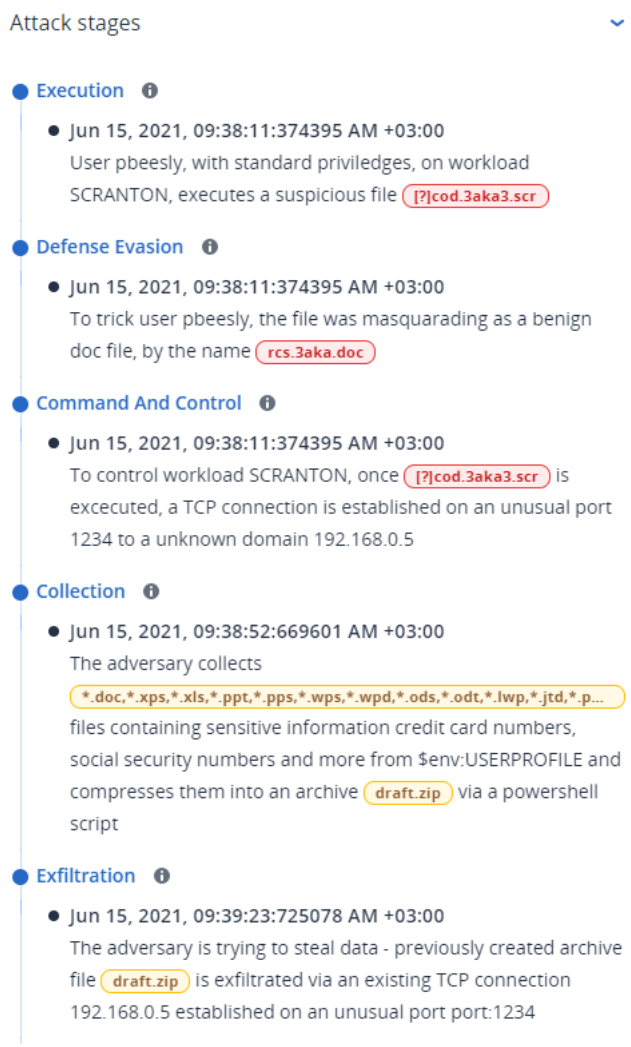
Setiap tahapan serangan memberi Anda informasi yang diperlukan untuk menjawab tiga pertanyaan penting:

- Apa tujuan penyerang?
- Bagaimana cara penyerang mencapai tujuan tersebut?
- Simpul mana yang menjadi target?

Yang tidak kalah pentingnya, interpretasi yang diberikan memastikan waktu yang diperlukan untuk menginvestigasi insiden menjadi berkurang drastis, karena Anda tidak perlu lagi memeriksa setiap peristiwa keamanan dari kronologi atau simpul grafik dan mencoba membuat interpretasi serangannya secara mandiri.

Tahapan serangan juga menyertakan informasi tentang file yang disusupi yang berisi informasi sensitif, misalnya nomor kartu kredit dan nomor jaminan sosial, sebagaimana ditampilkan di tahap **Koleksi** di contoh di bawah.

Untuk informasi lebih lanjut, lihat "Informasi apa yang termasuk dalam tahap serangan?" (hlm. 911).



© Acronis International GmbH, 2003-2024

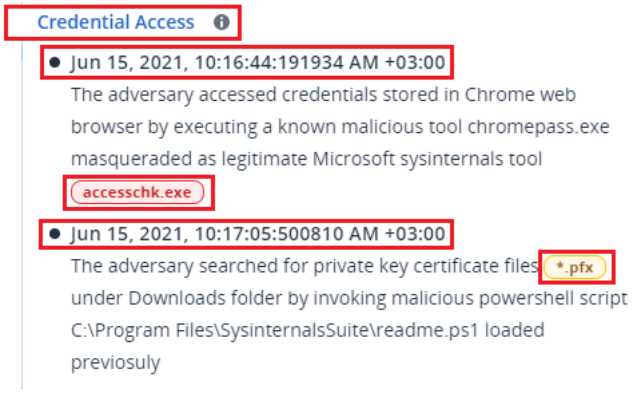
Cara menavigasi tahapan serangan

Tahapan serangan ditampilkan dalam urutan kronologis. Gulir ke bawah untuk melihat daftar lengkap tahapan serangan insiden.

Untuk menginvestigasi tahapan serangan tertentu secara lebih mendetail, klik tahapan serangan untuk menavigasi ke simpul yang relevan di grafik rantai cyber kill. Untuk informasi lebih lanjut tentang navigasi grafik rantai cyber kill dan simpul tertentu, lihat "Investigasi simpul individu di rantai cyber kill" (hlm. 913).

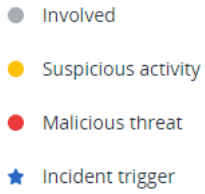
Informasi apa yang termasuk dalam tahap serangan?

Setiap tahap serangan memberikan interpretasi serangan yang mudah dipahami dalam bahasa manusia yang mudah dibaca. Interpretasi ini terdiri dari beberapa elemen, seperti yang ditunjukkan di bawah ini dan dijelaskan dalam tabel berikut.



Elemen tahap serangan	Deskripsi
Header	Menjelaskan apa yang coba dilakukan penyerang, dan tujuan mereka (dalam contoh di atas, **Akses Kredensial**), dengan tautan ke teknik MITRE ATT&CK yang dikenal. Klik tautan untuk mempelajari lebih lanjut tentang situs web MITRE ATT&CK. **Catatan** Jika tahap serangan bukan teknik MITRE ATT&CK yang diketahui, teks header tidak akan ditautkan. Ini relevan untuk teknik umum seperti file yang terdeteksi di folder acak.
Stempel waktu	Waktu tahap serangan terjadi.
Teknik	Cara penyerang mencapai tujuannya secara teknis, dan objek apa (entri registri, file, atau

© Acronis International GmbH, 2003-2024

Elemen tahap serangan	Deskripsi
	tugas terjadwal) yang terpengaruh. Dalam deskripsi teks teknik serangan disertakan tautan dengan kode warna untuk setiap simpul yang terdampak di rantai cyber kill, seperti yang ditunjukkan dalam contoh di atas. Tautan berkode warna ini memungkinkan Anda menavigasi dengan cepat ke simpul yang terpengaruh dan menyelidiki apa yang sebenarnya terjadi. Warna yang digunakan dalam tahap serangan menunjukkan hal berikut:  Melihat legenda di atas, kita dapat melihat bahwa tahap serangan contoh Akses Kredensial memiliki tautan ke simpul malware accesschk.exe dan simpul file yang mencurigakan *.pfx (klik tautan untuk melompat ke simpul yang sesuai dalam rantai cyber kill). Untuk informasi selengkapnya tentang menavigasi simpul ini dan tindakan yang tersedia, lihat "Investigasi simpul individu di rantai cyber kill" (hlm. 913). Perhatikan bahwa tahapan serangan juga menyertakan tautan ke simpul file yang memiliki informasi tentang file yang disusupi yang berisi informasi sensitif, seperti informasi kesehatan yang dilindungi (PHI), nomor kartu kredit, dan nomor jaminan sosial.

Catatan

Setiap tahap serangan adalah peristiwa deteksi tunggal. Konten yang terdaftar di setiap tahap (header, stempel waktu, teknik) dihasilkan sesuai dengan parameter tertentu dalam kejadian deteksi, dan yang didasarkan pada templat tahap serangan yang disimpan oleh Deteksi dan Tanggapan Titik Akhir (EDR).

© Acronis International GmbH, 2003-2024

Investigasi simpul individu di rantai cyber kill

Selain meninjau tahapan serangan, Anda juga dapat menavigasi setiap simpul serangan di rantai cyber kill. Ini memungkinkan Anda untuk memeriksa simpul tertentu di rantai cyber kill untuk menginvestigasi dan meremediasi setiap simpul.

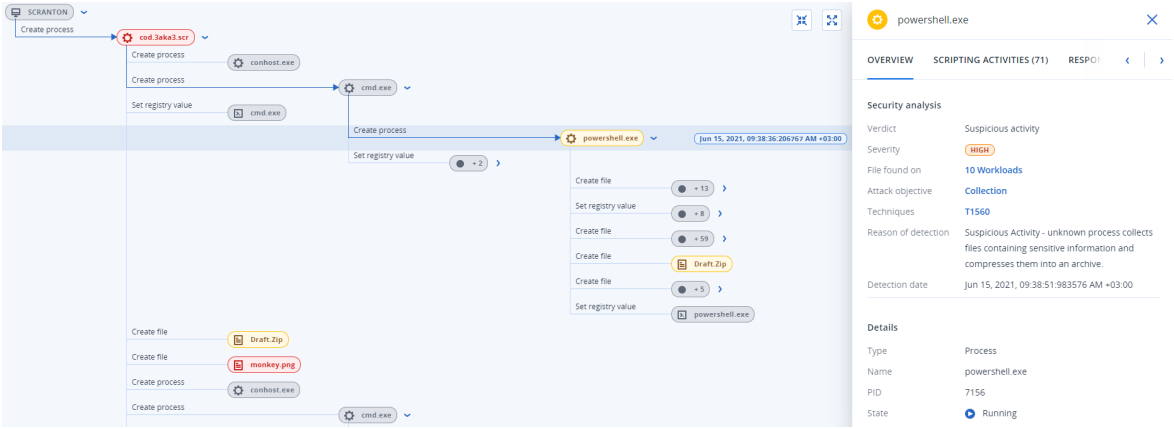
Misalnya, Anda dapat menentukan seberapa besar kemungkinan suatu insiden merupakan serangan yang benar-benar berbahaya. Berdasarkan investigasi Anda, Anda juga dapat menerapkan sejumlah tindakan respons pada simpul, yang meliputi isolasi beban kerja atau karantina file yang mencurigakan.

Untuk menginvestigasi simpul individu di rantai cyber kill

1. Di konsol Cyber Protect, buka **Perlindungan > Insiden**.
2. Di daftar insiden yang ditampilkan, klik di kolom ujung kanan insiden yang ingin Anda investigasi. Rantai cyber kill untuk insiden yang dipilih akan ditampilkan.
3. Navigasi ke simpul yang relevan, lalu klik untuk menampilkan panel samping simpul.

   Catatan
   Klik simpul untuk memperluas dan menampilkan simpul yang berkaitan.

   Misalnya, dengan mengeklik simpul **powershell.exe** pada contoh di bawah akan membuka panel samping simpulnya. Anda juga dapat mengeklik ikon panah di samping simpul untuk melihat simpul lain yang berhubungan, termasuk file dan nilai registri, yang mungkin terpengaruh oleh simpul **powershell.exe**. Anda dapat mengeklik simpul yang berkaitan ini untuk menginvestigasi lebih jauh.



4. Investigasi informasi yang diikutsertakan dalam tab panel samping:
   - **Ikhtisar**: Menyertakan dua bagian utama yang memberikan ringkasan keamanan dari simpul yang diserang.
     - **Analisis keamanan**: Memberikan analisis tentang simpul yang diserang, termasuk putusan EDR perihal ancaman (misalnya aktivitas mencurigakan), tujuan serangan berdasarkan teknik serangan MITRE (klik tautan untuk membuka situs web MITRE), alasan di balik deteksi, dan jumlah beban kerja yang mungkin terdampak oleh serangan (klik tautan **Beban Kerja n** untuk melihat beban kerja yang terdampak).

© Acronis International GmbH, 2003-2024

Catatan
Tautan **Beban Kerja n** menandakan bahwa ada objek berbahaya atau mencurigakan yang *ditemukan* di beban kerja lainnya. Ini tidak berarti bahwa ada serangan yang terjadi di beban kerja lainnya, tetapi ada indikator penyusupan di beban kerja tersebut. Serangan mungkin telah terjadi (dan menciptakan insiden lain), atau penyerang bersiap untuk menyerang beban kerja lainnya menggunakan "perlengkapan" serangan mereka.

  - **Detail**: Menyertakan detail tentang simpul, termasuk jenisnya, nama dan statusnya saat ini, jalur ke simpul, serta file hash dan tanda tangan digital yang mungkin ada (misalnya MD5 dan nomor seri sertifikat).
- **Aktivitas Pembuatan Skrip**: Menyertakan detail tentang skrip apa pun yang dipanggil atau dimuat dalam serangan. Klik untuk menyalin skrip ke papan klip Anda untuk investigasi lebih lanjut.

  Catatan
  Tab **Aktivitas Pembuatan Skrip** hanya ditampilkan untuk simpul proses yang menjalankan perintah atau skrip (misalnya cmd atau perintah PowerShell).

- **Tindakan untuk Merespons**: Menyertakan sejumlah bagian yang memberikan tindakan investigasi, remediasi, dan pencegahan tambahan sesuai jenis simpul.
  Misalnya, untuk simpul beban kerja, Anda dapat menentukan sejumlah respons yang menyertakan cadangan forensik dan pemulihan dari cadangan. Alternatifnya, untuk simpul berbahaya atau mencurigakan, Anda dapat menghentikan atau mengarantina simpulnya, membatalkan perubahan yang dibuat oleh serangan, dan menambahkannya ke daftar izin atau daftar blokir rencana proteksi.
  Untuk informasi lebih lanjut tentang penerapan tindakan respons pada simpul tertentu, lihat "Tindakan untuk merespons simpul rantai cyber kill individu" (hlm. 926).
- **Aktivitas**: Menampilkan tindakan yang diterapkan pada insiden dalam urutan kronologis. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Memahami tindakan yang diambil untuk memitigasi insiden

Setelah Anda meninjau insiden dan menginvestigasi cara terjadinya serangan, Anda akan perlu menerapkan tindakan respons. Setelah menerapkan tindakan respons, tindakan tersebut akan dapat dilihat di beberapa tempat, sehingga Anda dapat memahami langkah apa saja yang telah diambil untuk memitigasi insidennya.

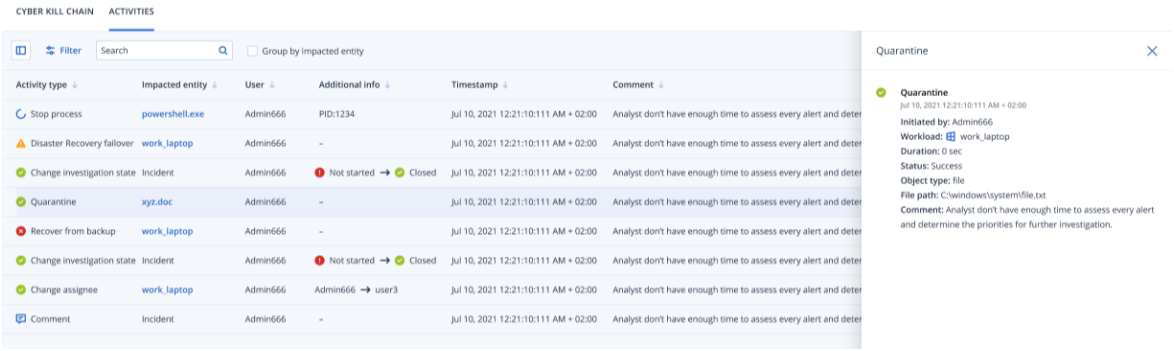
Catatan
Insiden yang dibuat oleh lapisan pencegahan akan menerapkan tindakan yang dikonfigurasi di rencana proteksi secara otomatis. Untuk titik deteksi, Anda perlu menentukan tindakan respons yang relevan untuk memitigasi setiap skenario serangan.

© Acronis International GmbH, 2003-2024

Untuk memahami tindakan respons yang telah diambil, Anda dapat melihat semua tindakan respons yang diterapkan pada seluruh insiden, atau melihat tindakan yang telah diterapkan pada simpul tertentu di rantai cyber kill insiden.

Untuk melihat semua tindakan respons yang diterapkan pada insiden

1. Di konsol Cyber Protect, buka **Perlindungan > Insiden**.
2. Di daftar insiden yang ditampilkan, klik di kolom ujung kanan insiden yang ingin Anda investigasi. Rantai cyber kill untuk insiden yang dipilih akan ditampilkan.
3. Klik tab **Aktivitas**.
   Daftar tindakan respons yang sudah diterapkan pada insiden akan ditampilkan.



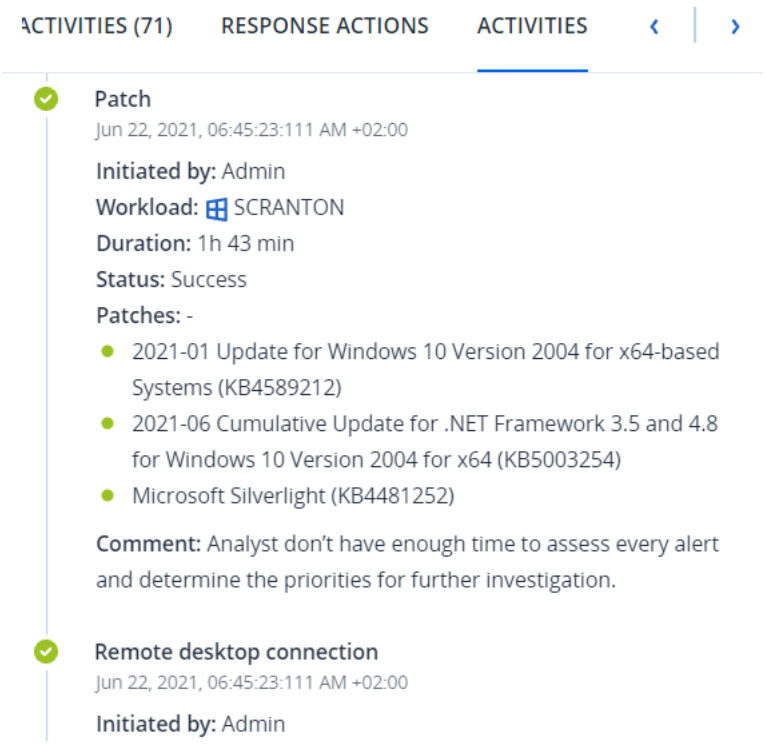
4. Anda dapat melakukan sejumlah tindakan pada daftar yang ditampilkan:
   - Klik baris jenis aktivitas untuk menampilkan informasi selengkapnya tentang aktivitas yang dipilih. Informasi ditampilkan di panel samping, sebagaimana ditampilkan di Langkah 3, dan menyertakan detail tentang siapa yang memulai tindakan, status, jalur file, dan komentar apa pun yang ditambahkan oleh pihak yang memulai tindakan.
   - Gunakan kotak **Pencarian** untuk mencari tindakan tertentu.
   - Klik **Filter** untuk menerapkan filter pada daftar.
   - Pilih kotak centang **Kelompokkan berdasarkan entitas terdampak** untuk mengelompokkan tindakan yang relevan berdasarkan entitas.
   - Klik untuk menampilkan / menyembunyikan daftar tindakan yang telah diselesaikan. Pastikan ditampilkan di samping tindakan yang ingin Anda tampilkan. Jika Anda ingin menyembunyikan tindakan di daftar yang ditampilkan, klik lagi untuk mengubahnya menjadi .

© Acronis International GmbH, 2003-2024

Untuk melihat tindakan yang diterapkan pada simpul tertentu

© Acronis International GmbH, 2003-2024

1. Dalam rantai cyber kill, klik simpul untuk menampilkan panel samping simpul tersebut.
2. Klik tab **Aktivitas**.



3. Untuk mendapatkan pemahaman menyeluruh tentang tindakan yang diambil dan alasan pengambilan tindakannya, Anda mungkin perlu menggulir ke tindakan respons yang diterapkan untuk simpul yang bersangkutan. Misalnya, untuk tindakan koneksi desktop jarak jauh, Anda dapat melihat siapa yang memulai tindakan dan waktunya, durasi tindakan, dan status secara keseluruhan (berhasil, gagal, atau berhasil dengan kesalahan).

Periksa indikator penyusupan (IOC) dari serangan terhadap beban kerja Anda yang diketahui secara publik

Deteksi dan Tanggapan Titik Akhir (EDR) menyertakan kemampuan untuk meninjau serangan yang sudah dikenal di umpan ancaman dengan beban kerja Anda. Umpan ancaman ini dibuat secara otomatis berdasarkan data ancaman yang diterima dari Pusat Operasi Perlindungan Cyber (CPOC); EDR memungkinkan Anda memverifikasi apakah ancaman memengaruhi beban kerja Anda atau tidak, lalu mengambil langkah yang diperlukan untuk meniadakan ancaman tersebut.

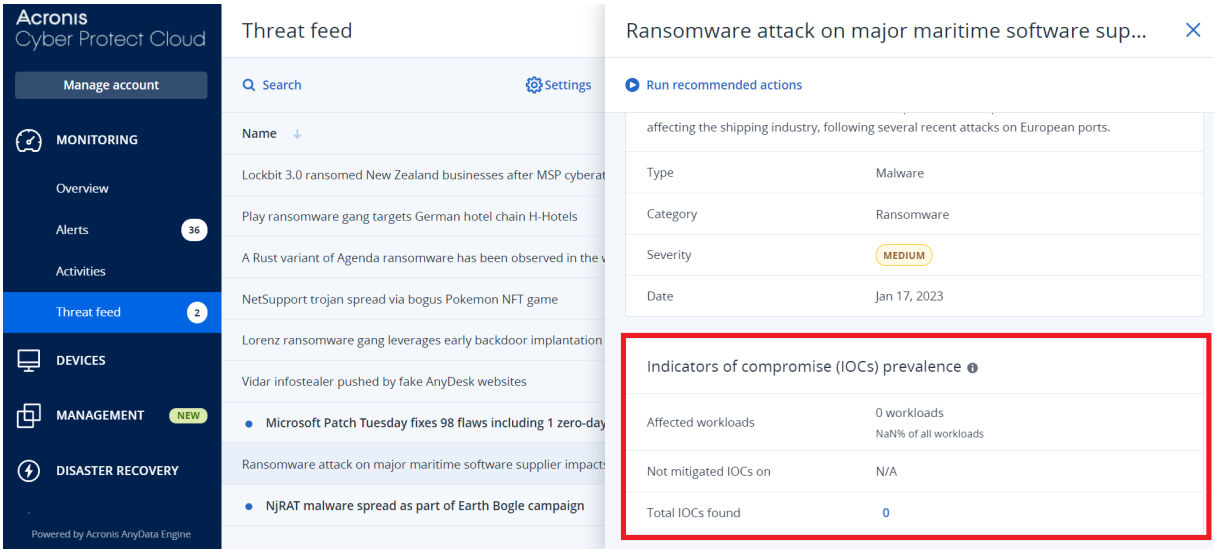
Anda dapat mengakses umpan ancaman dari menu **Pemantauan** di konsol Cyber Protect. Untuk informasi lebih lanjut, lihat "Umpan ancaman" (hlm. 301).

Untuk meninjau detail ancaman tertentu dan mengonfirmasi potensi dampaknya pada beban kerja Anda, klik umpan ancaman. Anda dapat melihat jumlah IOC yang terdeteksi dan beban kerja yang terpengaruh, dan periksa beban kerja yang memiliki IOC yang tidak termitigasi.

© Acronis International GmbH, 2003-2024

Catatan

Jika rencana proteksi tidak mengaktifkan EDR, fungsionalitas umpan ancaman tambahan ini tidak akan ditampilkan, sebagaimana terlihat di bawah.



Menentukan pengaturan umpan ancaman

Anda dapat menentukan sejumlah pengaturan umpan ancaman untuk dapat mencari lokasi dan memitigasi ancaman yang dikenal secara otomatis.

Untuk menentukan pengaturan umpan ancaman

1. Di konsol Cyber Protect, buka **Pemantauan > Umpan ancaman**.
2. Di halaman Umpan ancaman yang ditampilkan, klik **Pengaturan**.

© Acronis International GmbH, 2003-2024

3. Di dialog yang ditampilkan, pilih opsi berikut:

Opsi	Deskripsi
Cari indikator penyusupan (IOC)	Klik tombol untuk mengaktifkan pencarian otomatis untuk IOC di beban kerja Anda. Saat opsi ini diaktifkan, opsi **Tindakan saat deteksi** dan **Buat peringatan** juga akan ditampilkan.
Tindakan saat deteksi	Dari daftar dropdown, pilih tindakan yang akan dilakukan pada file yang relevan ketika ditemukan adanya ancaman di beban kerja: • **Tidak ada tindakan** • **Karantina** • **Hapus** • **Isolasi beban kerja**
Buat peringatan	Pilih kotak centang untuk membuat peringatan jika IOC ditemukan di beban kerja. Peringatan akan ditampilkan di halaman Peringatan.

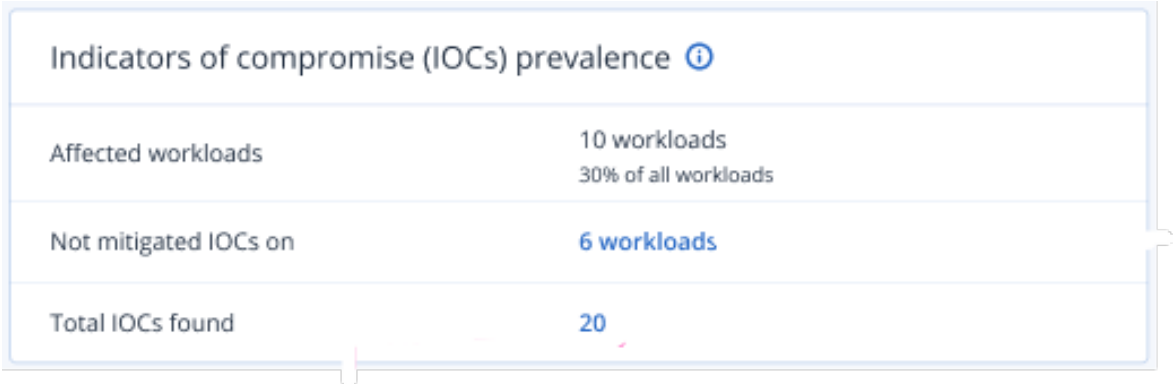
4. Klik **Terapkan**.

Meninjau dan memitigasi IOC pada beban kerja yang terdampak

Saat Deteksi dan Tanggapan Titik Akhir (EDR) diaktifkan di rencana proteksi, Anda dapat melihat ancaman yang memengaruhi beban kerja di rencana proteksi. Anda juga dapat memitigasi sisa indikator penyusupan (IOC) yang tidak dimitigasi secara otomatis. Untuk informasi tentang cara memitigasi IOC secara otomatis, lihat "Menentukan pengaturan umpan ancaman" (hlm. 918).

Untuk meninjau dan memitigasi beban kerja yang terdampak

1. Di konsol Cyber Protect, buka **Pemantauan > Umpan ancaman**.
2. Klik thread untuk menampilkan detail ancaman tersebut.
3. Di bagian **Prevalensi indikator penyusupan (IOC)**, klik tautan **beban kerja *n*** untuk menampilkan beban kerja dengan IOC yang tidak termitigasi.



4. Di halaman Beban kerja yang ditampilkan, klik beban kerja yang relevan dan tinjau detailnya. Anda dapat menjalankan fungsionalitas tertentu pada beban kerja, termasuk menentukan URL

© Acronis International GmbH, 2003-2024

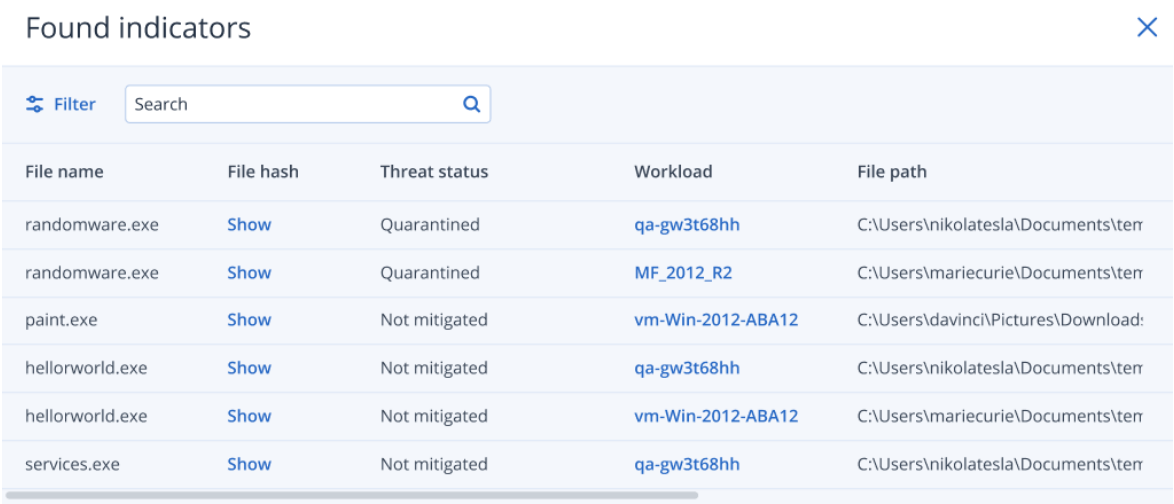
tambahan untuk filter (lihat "Pemfilteran URL" (hlm. 842)), dan memblokir proses berbahaya (lihat bagian Pengecualian di "Pengaturan perlindungan Antivirus dan antimalware" (hlm. 819)). Misalnya, jika umpan ancaman menunjukkan bahwa ada beban kerja yang terpengaruh oleh IOC, pertama-tama cari lokasi IOC dan lakukan analisis sebagaimana dijelaskan di "Meninjau dan menganalisis IOC yang ditemukan" (hlm. 920). Selanjutnya, buka rencana proteksi untuk beban kerja dan tentukan proteksi tambahan, misalnya memblokir file hash atau proses berbahaya.

Meninjau dan menganalisis IOC yang ditemukan

Selain meninjau beban kerja yang terpengaruh oleh ancaman yang diketahui, Anda juga dapat meninjau dan menganalisis indikator penyusupan (IOC) tertentu. Ini memungkinkan Anda meninjau beban kerja individu yang terdampak oleh IOC, dan memitigasi IOC tersebut.

Untuk meninjau dan menganalisis IOC

1. Di konsol Cyber Protect, buka **Pemantauan > Umpan ancaman**.
2. Klik thread untuk menampilkan detail ancaman tersebut.
3. Di bagian **Prevalensi indikator penyusupan (IOC)**, klik tautan **Total IOC ditemukan**. Halaman Indikator yang ditemukan akan ditampilkan.



4. (Opsional) Gunakan opsi **Filter** untuk memfilter daftar IOC berdasarkan statusnya. Anda juga dapat menggunakan opsi **Pencarian** untuk mencari IOC tertentu.
5. Untuk melihat beban kerja yang terdampak oleh IOC, klik tautan di kolom **Beban kerja**. Selanjutnya Anda dapat melakukan beragam tindakan pada beban kerja, misalnya menjalankan manajemen patch, atau mengubah rencana proteksi.
6. (Opsional) Di kolom **File hash**, klik **Tampilkan** untuk menampilkan hash file yang ditemukan untuk IOC tertentu. Di dialog yang ditampilkan, klik untuk menyalin file hash IOC ke editor teks.

Remediasi insiden

Deteksi dan Tanggapan Titik Akhir (EDR) memungkinkan Anda meremediasi seluruh insiden, atau titik serangan individu suatu insiden.

© Acronis International GmbH, 2003-2024

Dengan meremediasi seluruh insiden, Anda dapat memilih remediasi insiden yang ingin Anda jalankan secara global. Jika Anda perlu mengelola insiden secara lebih mendetail, Anda dapat meremediasi titik serangan individu yang diperlukan. Misalnya, Anda mungkin ingin mengisolasi jaringan beban kerja untuk menghentikan pergerakan lateral atau aktivitas perintah dan kontrol (C&C); cara ini akan memastikan bahwa sekalipun beban kerja sudah diisolasi, semua teknologi Acronis Cyber Protect masih tetap berfungsi, dan investigasi dapat dilakukan.

EDR memastikan remediasi yang efektif dengan:

- Mitigasi - untuk memastikan ancaman dapat dihentikan.
- Pemulihan - untuk memastikan layanan dapat segera kembali online.
- Pencegahan - untuk memastikan teknik yang digunakan dalam serangan dapat dicegah pada waktu mendatang.

Remediasi seluruh insiden

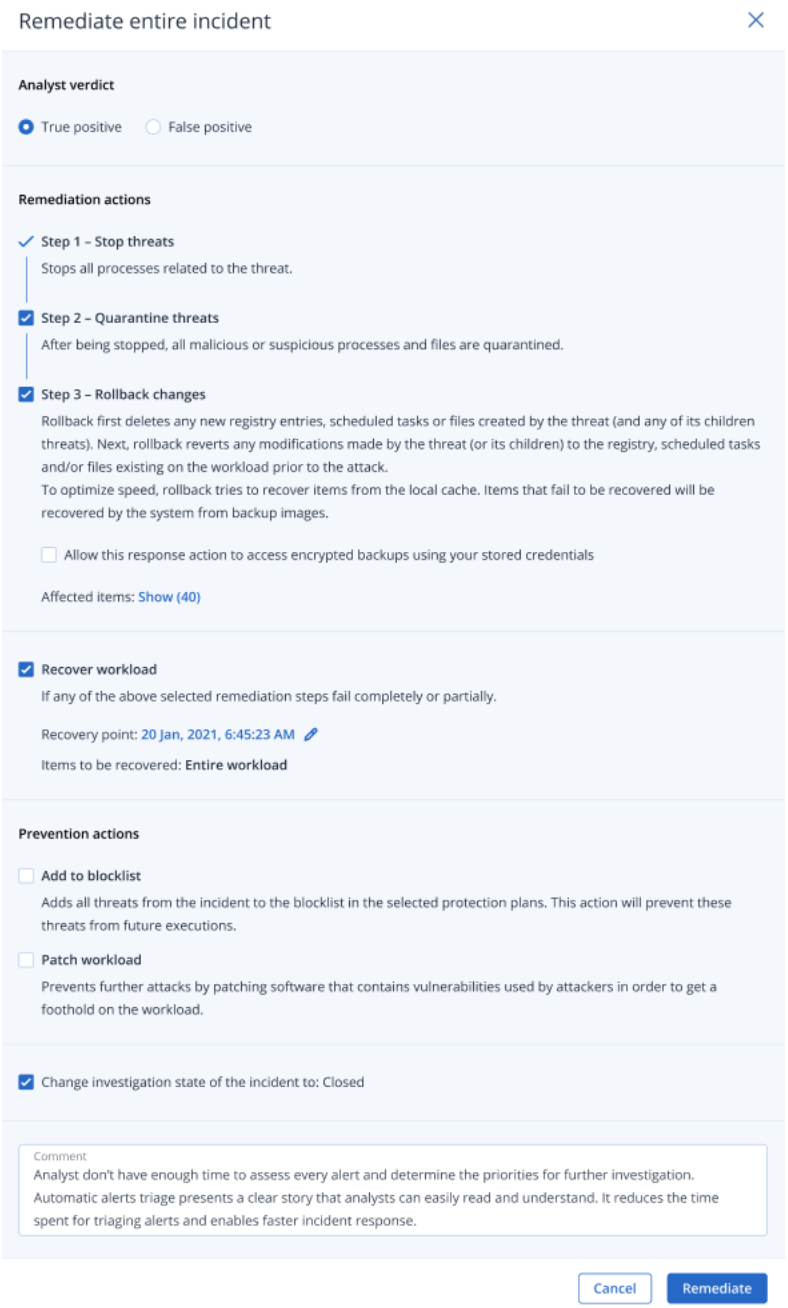
Dengan remediasi seluruh insiden, Anda dapat memilih remediasi yang ingin dijalankan secara global pada insiden tersebut dengan cepat dan mudah. Deteksi dan Tanggapan Titik Akhir (EDR) memandu Anda melalui proses remediasinya, langkah demi langkah.

Jika Anda perlu mengelola jaringan dan insidennya secara lebih mendetail, lihat "Tindakan untuk merespons simpul rantai cyber kill individu" (hlm. 926).

Untuk remediasi seluruh insiden

1. Di konsol Cyber Protect, buka **Perlindungan > Insiden**.
2. Di daftar insiden yang ditampilkan, klik di kolom ujung kanan insiden yang ingin Anda investigasi. Rantai cyber kill untuk insiden yang dipilih akan ditampilkan.
3. Klik **Remediasi seluruh insiden**. Dialog Remediasi seluruh insiden akan ditampilkan.

© Acronis International GmbH, 2003-2024



4. Di bagian **Putusan analis**, berdasarkan investigasi insiden Anda, pilih salah satu pilihan berikut:
   - **Positif benar**: Pilih jika Anda yakin serangannya merupakan serangan asli. Setelah dipilih, Anda kemudian dapat menambahkan tindakan remediasi dan pencegahan, sebagaimana dijelaskan dalam langkah-langkah berikutnya.
   - **Positif palsu**: Pilih jika Anda yakin serangannya bukan merupakan serangan asli. Dalam mode ini, Anda dapat menentukan cara mencegah terulangnya kembali insiden ini, misalnya dengan menambahkan insiden ke daftar izin rencana proteksi.

     Catatan
     Setelah memilih **Positif palsu**, Anda hanya akan dapat menentukan tindakan pencegahan. Untuk informasi lebih lanjut, lihat "Remediasi insiden positif palsu" (hlm. 925).

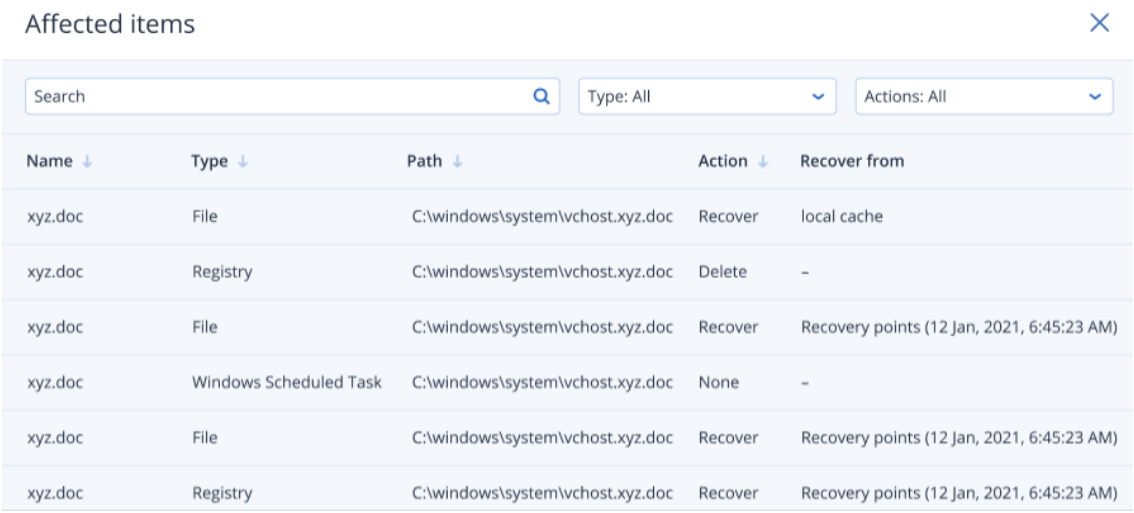
© Acronis International GmbH, 2003-2024

5. Di bagian **Tindakan remediasi**, ikuti langkah-langkah remediasi berikut. Perhatikan bahwa langkah-langkahnya harus diikuti secara berurutan; misalnya, Anda tidak boleh melakukan Langkah 2 sebelum menyelesaikan Langkah 1.
   a. **Langkah 1 - Hentikan ancaman**: Pilih kotak centang untuk menghentikan semua proses yang terkait dengan ancaman.
   b. **Langkah 2 - Karantina ancaman**: Setelah ancaman dihentikan, pilih kotak centang untuk mengarantina semua proses dan file yang berbahaya maupun mencurigakan.
   c. **Langkah 3 - Batalkan perubahan**: Setelah ancaman dikarantina, pilih kotak centang untuk menghapus entri registri baru, tugas terjadwal, atau file yang dibuat oleh ancaman (dan semua ancaman anaknya). Proses pembatalan perubahan akan membatalkan semua modifikasi yang dibuat oleh ancaman (atau anaknya) pada registri, tugas terjadwal, dan/atau file yang ada pada beban kerja sebelum serangan. Untuk mengoptimalkan kecepatan, proses pembatalan akan mencoba memulihkan item dari cache lokal. Item yang gagal dipulihkan akan dipulihkan oleh sistem dari gambar cadangan.

      Catatan
      Proses pembatalan hanya memulihkan dari item di cache lokal saja. Pembatalan dari arsip cadangan hanya akan tersedia di rilis mendatang.

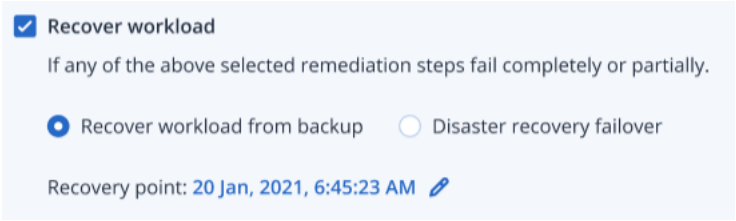
      Pilih kotak centang **Izinkan tindakan respons ini mengakses cadangan terenkripsi menggunakan kredensial tersimpan** jika akses ke cadangan terkait terenkripsi. EDR mengakses kredensial pengguna yang tersimpan untuk mendekripsi arsip terenkripsi dan mencari file yang relevan.

      Anda juga dapat mengklik **Item yang terpengaruh** untuk melihat semua item (file, registri, atau tugas terjadwal) yang terpengaruh oleh pembatalan, tindakan yang dilakukan (**Hapus**, **Pulihkan**, atau **Tidak ada**), dan apakah item dikembalikan dari cache lokal atau citra cadangan.

   d. **Pulihkan beban kerja**: Pilih kotak centang untuk memulihkan beban kerja jika langkah-langkah remediasi di atas gagal dilakukan, baik sebagian atau seluruhnya.

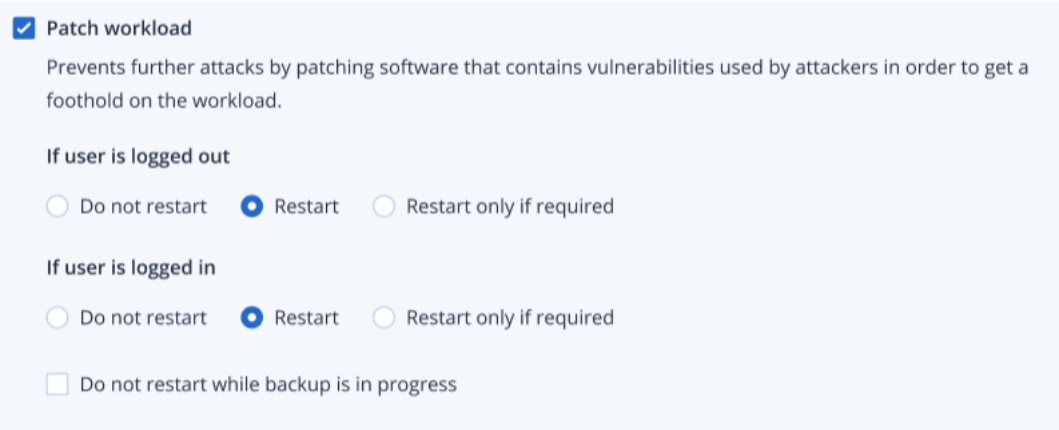
© Acronis International GmbH, 2003-2024



Pilih salah satu opsi pemulihan berikut:

- **Pulihkan beban kerja dari cadangan**: Memungkinkan Anda memulihkan beban kerja dari titik pemulihan tertentu. Klik ikon edit titik pemulihan untuk memilih opsi cadangan pemulihan dari daftar yang ada.
- **Failover pemulihan bencana**: Memungkinkan Anda menjalankan pemulihan bencana, jika fungsionalitas ini diaktifkan di rencana proteksi Anda. Kami menyarankan Anda menggunakan opsi ini untuk beban kerja penting, seperti server AD, atau server database. Untuk informasi lebih lanjut, lihat "Menerapkan pemulihan bencana" (hlm. 730).

6. Di bagian **Tindakan pencegahan**, pilih langkah remediasi yang relevan:
   - **Tambah ke daftar blokir**: Pilih kotak centang dan pilih rencana proteksi yang relevan dari daftar rencana proteksi yang ditampilkan. Tindakan pencegahan ini memastikan semua deteksi insiden tidak akan dijalankan untuk rencana proteksi yang dipilih.
   - **Patch beban kerja**: Pilih kotak centang untuk memasang patch pada perangkat lunak yang rentan dan mencegah penyerang mendapatkan akses ke beban kerja. Anda kemudian dapat memilih tindakan yang relevan untuk dilakukan setelah pemasangan patch selesai (**Jangan mulai ulang**, **Mulai ulang**, atau **Mulai ulang hanya jika perlu**), tergantung masuk tidaknya pengguna.
     Anda juga dapat memilih kotak centang **Jangan mulai ulang saat pencadangan sedang dalam proses** untuk memastikan beban kerja tidak dimulai ulang pada saat proses pencadangan.



7. Pilih kotak centang **Ubah status investigasi insiden menjadi: Ditutup**. Jika tidak dipilih, status investigasi akan tetap sama seperti status sebelumnya.
8. Klik **Remediasi**. Tindakan remediasi yang Anda pilih akan dijalankan langkah demi langkah, dan proses setiap langkah remediasinya ditampilkan di dialog Remediasi seluruh insiden.

© Acronis International GmbH, 2003-2024

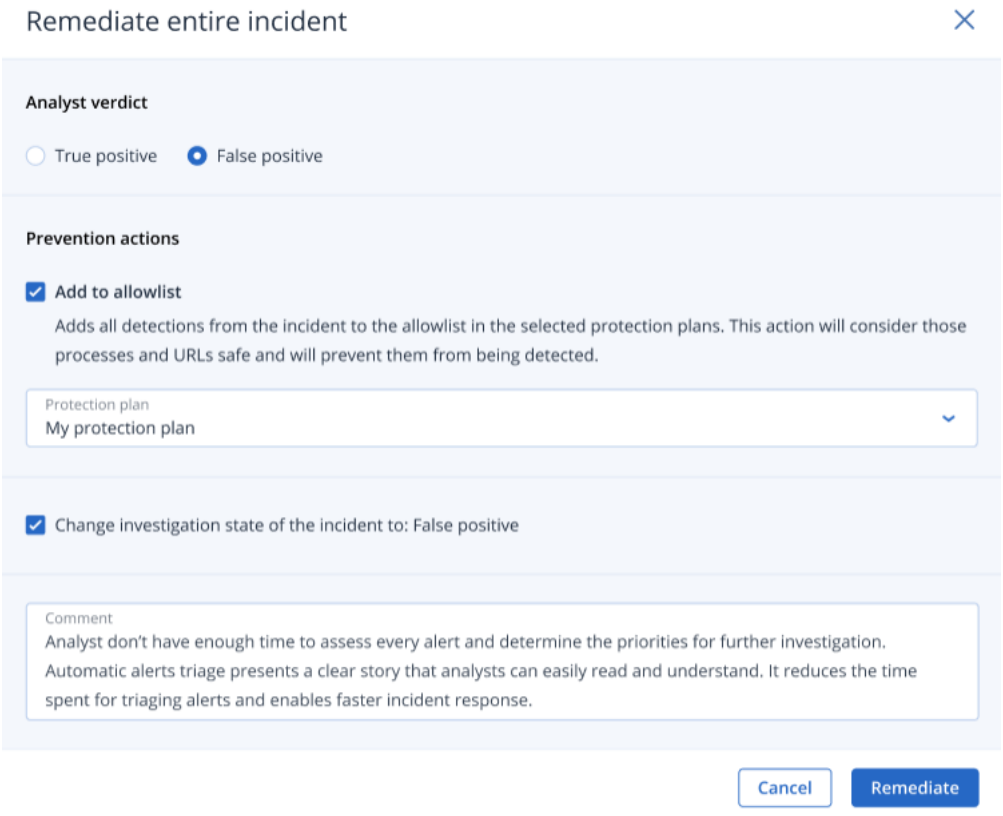
Setelah diklik, tombol akan menampilkan **Buka aktivitas**. Klik **Buka aktivitas** untuk meninjau semua tindakan respons yang diterapkan pada insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Remediasi insiden positif palsu

Jika Anda yakin suatu serangan bukanlah serangan asli, dengan kata lain positif palsu, Anda dapat menentukan cara mencegah insiden tersebut terjadi lagi. Misalnya, Anda dapat menambahkan insiden ke daftar izin rencana proteksi.

Untuk memulihkan insiden positif palsu

1. Di rantai cyber kill untuk insiden yang dipilih, klik **Remediasi seluruh kejadian**. Dialog Remediasi seluruh insiden akan ditampilkan.
2. Di bagian **Putusan analis**, pilih **Positif palsu**.



3. Di bagian **Tindakan pencegahan**, pilih kotak centang **Tambah ke daftar izin**. Dari daftar rencana perlindungan yang ditampilkan, pilih rencana proteksi yang relevan.
   Tindakan pencegahan ini memastikan semua deteksi insiden akan dicegah agar tidak terdeteksi untuk rencana proteksi yang dipilih.
4. Pilih kotak centang **Ubah status investigasi insiden menjadi: Positif palsu**.
5. Klik **Remediasi**.
   Setelah diklik, tombol akan menampilkan **Buka aktivitas**. Klik **Buka aktivitas** untuk meninjau tindakan respons yang diterapkan pada insiden tersebut. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

© Acronis International GmbH, 2003-2024

Tindakan untuk merespons simpul rantai cyber kill individu

Jika Anda perlu mengelola insiden secara lebih mendetail, Anda dapat menerapkan beragam tindakan respons pada simpul rantai cyber kill individu. Tindakan untuk merespons ini memungkinkan Anda meremediasi simpul secara cepat dan mudah.

Catatan
Untuk menerapkan tindakan respons global pada keseluruhan insiden, lihat "Remediasi seluruh insiden" (hlm. 921).

Tindakan untuk merespons dibagi menjadi beberapa kategori berikut, tetapi tidak semua simpul menyertakan semua kategori berikut:

- **Remediasi**: Tindakan di kategori ini memungkinkan Anda menerapkan respons cepat terhadap serangan, termasuk mengelola isolasi jaringan untuk beban kerja, serta penghapusan dan karantina file, proses, dan nilai registri.
- **Investigasi**: Tindakan di kategori ini (hanya berlaku untuk beban kerja) memungkinkan Anda menjalankan cadangan Forensik atau koneksi desktop jarak jauh untuk investigasi yang lebih mendalam.
- **Investigasi**: Tindakan di kategori ini (hanya berlaku untuk beban kerja saja) memungkinkan Anda untuk menjalankan koneksi desktop jarak jauh untuk investigasi yang lebih menyeluruh.
- **Pemulihan**: Tindakan di kategori ini (hanya berlaku untuk beban kerja) memungkinkan Anda merespons serangan yang intensif dengan menjalankan pemulihan dari cadangan atau failover Pemulihan Bencana.
- **Cegah**: Tindakan di kategori ini memungkinkan Anda mencegah terjadinya ancaman atau positif palsu pada waktu mendatang dengan menambahkannya ke daftar izin atau daftar blokir rencana proteksi.

Catatan
Jika insiden ditutup, Anda tidak akan dapat menerapkan tindakan respons pada simpul. Akan tetapi, Anda dapat membuka kembali insiden yang sudah ditutup dengan mengubah status investigasinya menjadi **Menginvestigasi**. Saat dibuka kembali, Anda kemudian dapat menerapkan tindakan respons.

Tabel berikut menjelaskan setiap jenis simpul di rantai cyber kill, kategori yang berlaku untuk setiap simpul, dan tindakan respons yang tersedia.

Simpul	Kategori	Tindakan untuk Merespons
Beban kerja	Remediasi	• Kelola isolasi jaringan • Mulai ulang beban kerja

© Acronis International GmbH, 2003-2024

Simpul	Kategori	Tindakan untuk Merespons
	Investigasi	• Cadangan forensik • Koneksi desktop jarak jauh
	Investigasi	• Koneksi desktop jarak jauh
	Pemulihan	• Memulihkan dari cadangan • Failover Pemulihan Bencana
	Cegah	• Patch
Proses	Remediasi	• Hentikan proses • Karantina
	Cegah	• Tambah ke daftar izin • Tambah ke daftar blokir
File	Remediasi	• Hapus • Karantina
	Cegah	• Tambah ke daftar izin • Tambah ke daftar blokir
Registri	Remediasi	• Hapus
Jaringan	Cegah	• Tambah ke daftar izin • Tambah ke daftar blokir

Tetapkan tindakan respons untuk beban kerja yang terpengaruh

Sebagai bagian dari respons terhadap serangan, Anda dapat menerapkan tindakan berikut ke beban kerja yang terpengaruh:

© Acronis International GmbH, 2003-2024

- **Kelola isolasi jaringan**: Memungkinkan Anda mengelola isolasi jaringan dari beban kerja untuk menghentikan gerakan lateral atau aktivitas Perintah dan Kontrol (C&C). Untuk informasi lebih lanjut, lihat "Mengelola isolasi jaringan dari beban kerja" (hlm. 928).
- **Patch**: Memungkinkan Anda menambal beban kerja untuk mencegah eksploitasi kerentanan di masa mendatang dalam potensi serangan di masa mendatang. Untuk informasi lebih lanjut, lihat "Patch beban kerja" (hlm. 932).
- **Mulai ulang beban kerja**: Memungkinkan Anda untuk segera memulai ulang beban kerja, atau memulai ulang beban kerja sesuai dengan periode batas waktu yang telah ditentukan. Untuk informasi lebih lanjut, lihat "Mulai kembali beban kerja" (hlm. 933).
- **Cadangan forensik**: Memungkinkan Anda untuk melakukan pencadangan forensik sesuai permintaan untuk audit atau tujuan penyelidikan lebih lanjut. Untuk informasi lebih lanjut, lihat "Jalankan pencadangan forensik pada beban kerja sesuai permintaan" (hlm. 934).
- **Koneksi desktop jarak jauh**: Memungkinkan Anda untuk mengakses beban kerja yang sedang diselidiki dari jarak jauh. Untuk informasi lebih lanjut, lihat "Koneksi jarak jauh ke beban kerja" (hlm. 936).
- **Memulihkan dari cadangan**: Memungkinkan Anda untuk memulihkan seluruh mesin Anda dari cadangan atau file atau folder tertentu. Untuk informasi lebih lanjut, lihat "Memulihkan dari cadangan" (hlm. 936).
- **Kegagalan Pemulihan Bencana**: Memungkinkan Anda menjalankan "Menerapkan pemulihan bencana" (hlm. 730). Perhatikan bahwa beban kerja Anda harus memiliki langganan Pemulihan Bencana Tingkat Lanjut. Untuk informasi lebih lanjut, lihat "Failover Pemulihan Bencana" (hlm. 937).

Mengelola isolasi jaringan dari beban kerja

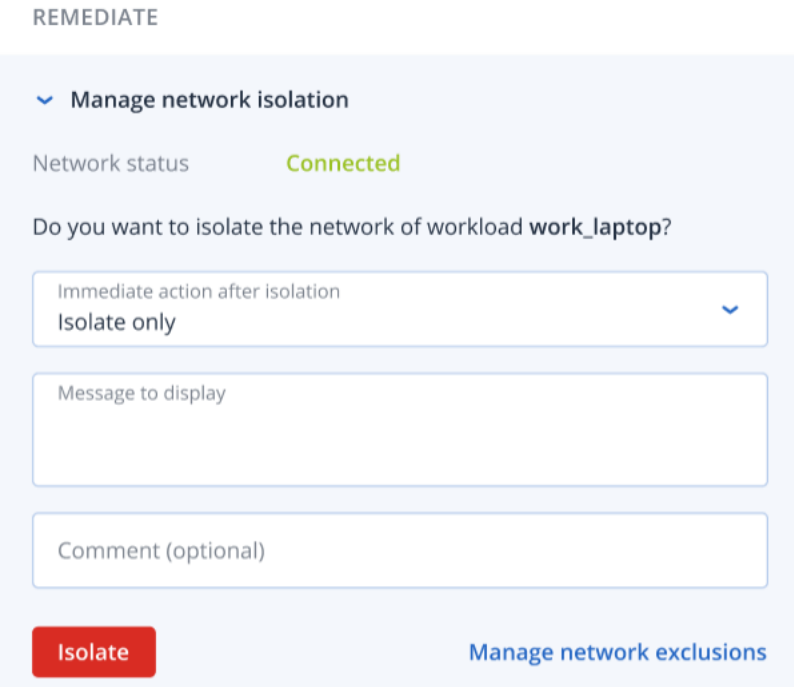
EDR memungkinkan Anda mengelola isolasi jaringan dari suatu beban kerja untuk menghentikan gerakan lateral atau aktivitas Perintah dan Kontrol (C&C). Ada sejumlah opsi isolasi yang dapat dipilih sesuai dengan kebutuhan Anda. Perhatikan bahwa semua teknologi Acronis Cyber Protect berfungsi meskipun beban kerja diisolasi dan memastikan bahwa penyelidikan dapat dilakukan sepenuhnya.

Untuk mengisolasi beban kerja dari jaringan

1. Di rantai cyber kill, klik simpul beban kerja yang ingin Anda remediasi.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.

© Acronis International GmbH, 2003-2024

3. Di bagian **Remediasi**, klik **Kelola isolasi jaringan**.



Catatan
Nilai **Status Jaringan** menunjukkan apakah beban kerja saat ini terhubung atau tidak. Jika nilai menampilkan **Terisolasi**, Anda dapat menghubungkan kembali beban kerja yang terisolasi ke jaringan, seperti yang dijelaskan dalam prosedur di bawah ini. Jika beban kerja offline, Anda masih dapat mengisolasi beban kerja; ketika kembali online, status beban kerja secara otomatis berubah menjadi **Terisolasi**.

4. Di daftar drop-down **Tindakan segera setelah isolasi**, pilih salah satu opsi berikut:
   - **Hanya isolasi**
   - **Isolasi dan cadangkan beban kerja**
   - **Isolasi dan cadangkan beban kerja dengan data forensik**
   - **Isolasi dan nonaktifkan beban kerja**

   Untuk informasi lebih lanjut tentang cara menentukan tempat mencadangkan beban kerja dan opsi enkripsi, lihat "Mengelola pencadangan serta pemulihan beban kerja dan file" (hlm. 395).
5. [Opsional] Di bidang **Pesan untuk ditampilkan**, tambahkan pesan untuk ditampilkan kepada pengguna akhir saat mereka mengakses beban kerja yang terisolasi. Misalnya, Anda dapat memberi tahu pengguna bahwa beban kerja sekarang diisolasi dan akses jaringan masuk dan keluar dari beban kerja saat ini tidak tersedia. Perhatikan bahwa pesan ini juga ditampilkan sebagai pemberitahuan monitor tray, dan tetap ditampilkan hingga pengguna menutup pesan tersebut.
6. [Opsional] Di bidang **Komentar**, tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.

© Acronis International GmbH, 2003-2024

7. Klik **Kelola pengecualian jaringan** untuk menambahkan port, URL, nama host, dan alamat IP yang akan memiliki akses ke beban kerja selama isolasi. Untuk informasi lebih lanjut, lihat cara mengelola pengecualian jaringan.
8. Klik **Isolasi**.
   Beban kerja terisolasi. Tindakan ini juga dapat dilihat di tab **Aktivitas** simpul individu maupun seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Catatan
Beban kerja juga ditampilkan sebagai **Terisolasi** di bawah menu **Beban kerja** di konsol Cyber Protect. Anda juga dapat mengisolasi satu atau beberapa beban kerja dari menu **Beban kerja > Beban kerja dengan agen**; pilih beban kerja yang relevan dan di panel samping kanan pilih **Kelola isolasi jaringan**. Dalam dialog yang ditampilkan, Anda dapat mengelola pengecualian jaringan dan mengeklik **Isolasi** atau **Isolasi semua** untuk mengisolasi beban kerja yang dipilih.

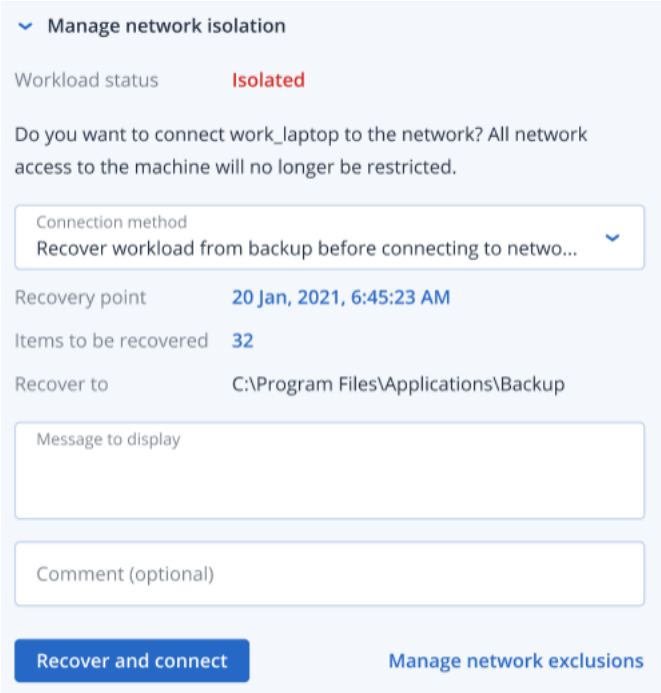
Untuk menghubungkan beban kerja terisolasi ke jaringan lagi

1. Di rantai cyber kill, klik simpul beban kerja yang ingin Anda hubungkan kembali.

Catatan
Jika beban kerja terisolasi sedang offline, Anda masih dapat menghubungkannya kembali ke jaringan; ketika kembali online status beban kerja secara otomatis berubah menjadi **Terhubung**.

2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.
3. Di bagian **Remediasi**, klik **Kelola isolasi jaringan**.
4. Pilih salah satu opsi berikut:
   - **Terhubung ke jaringan segera**: Beban kerja dihubungkan kembali ke jaringan.
   - **Pulihkan beban kerja dari cadangan sebelum terhubung ke jaringan**: Pilih titik pemulihan untuk memulihkan beban kerja.
     a. Di bidang **Titik pemulihan**, klik **Pilih**.
     b. Di panel samping yang ditampilkan, pilih titik pemulihan yang relevan.
     c. Klik **Pulihkan > Seluruh beban kerja** untuk memulihkan semua file dan folder pada beban kerja.
     Atau
     Klik **Pulihkan > File/folder** untuk memulihkan file dan folder tertentu pada beban kerja. Anda kemudian diminta untuk memilih file atau folder yang relevan. Setelah dipilih, Anda dapat melihat daftar item dengan mengeklik nilai yang relevan di bidang **Item yang akan dipulihkan**.

© Acronis International GmbH, 2003-2024



Catatan
Jika titik pemulihan yang Anda pilih dienkripsi, Anda akan diminta memasukkan kata sandi.

5. [Opsional] Pilih kotak centang **Mulai ulang beban kerja secara otomatis jika diperlukan**. Opsi ini hanya relevan jika Anda memilih **Pulihkan > Seluruh beban kerja** di Langkah 4.
6. [Opsional] Di bidang **Pesan untuk ditampilkan**, tambahkan pesan untuk ditampilkan kepada pengguna akhir saat mereka mengakses beban kerja yang terhubung. Misalnya, Anda dapat memberi tahu pengguna bahwa cadangan telah dipulihkan ke beban kerja dan akses jaringan masuk dan keluar dari beban kerja dilanjutkan.
7. [Opsional] Di bidang **Komentar**, tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
8. Klik **Hubungkan** jika Anda memilih **Hubungkan ke jaringan segera** di Langkah 4.
   Atau
   Klik **Pulihkan dan hubungkan** jika Anda memilih **Pulihkan beban kerja dari cadangan sebelum terhubung ke jaringan** di Langkah 4.
   Beban kerja terhubung kembali ke jaringan dan semua akses jaringan ke beban kerja tidak lagi dibatasi.

Catatan
Anda juga dapat menyambungkan satu atau beberapa beban kerja terisolasi dari menu **Beban kerja > Beban kerja agen** di konsol Cyber Protect; pilih beban kerja yang relevan dan di sidebar kanan pilih **Mengelola isolasi jaringan**. Dalam dialog yang ditampilkan, klik **Hubungkan** atau **Hubungkan semua** untuk menghubungkan kembali beban kerja yang dipilih ke jaringan.

Untuk mengelola pengecualian jaringan

© Acronis International GmbH, 2003-2024

Catatan
Bahkan jika semua teknologi Acronis Cyber Protect berfungsi saat beban kerja dalam isolasi, mungkin ada skenario ketika Anda memerlukan koneksi jaringan tambahan untuk dibuat (misalnya, Anda mungkin perlu mengunggah file dari beban kerja ke direktori bersama). Dalam skenario ini, Anda dapat menambahkan pengecualian jaringan, tetapi pastikan semua ancaman telah dihapus sebelum menambahkan pengecualian.

1. Di bagian **Remediasi** dari tab **Tindakan untuk merespons**, klik **Kelola pengecualian jaringan**.
2. Di panel samping Pengecualian jaringan, tambahkan pengecualian yang relevan. Untuk setiap opsi yang tersedia (Port, alamat URL, dan Nama host/alamat IP), lakukan hal berikut:
   a. Klik **Tambah** lalu masukkan port yang relevan, alamat URL, atau Nama host/alamat IP.
   b. Di daftar drop-down **Arah lalu lintas**, pilih salah satu dari **Koneksi masuk dan keluar**, **Koneksi masuk saja**, atau **Koneksi keluar saja**.
   c. Klik **Tambah**.
3. Klik **Simpan**.

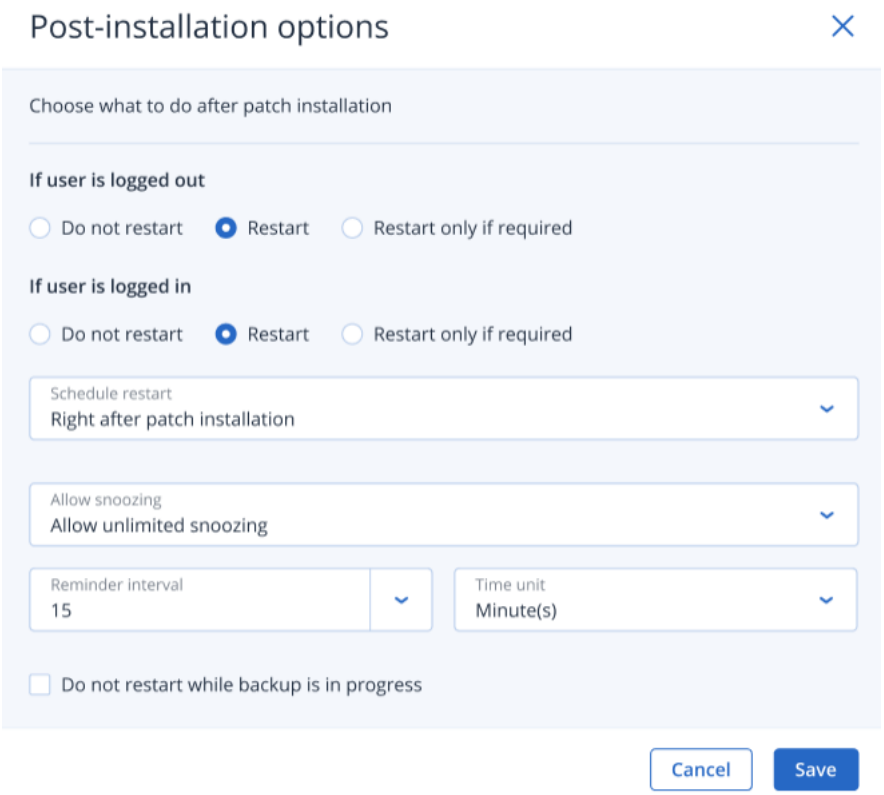
Patch beban kerja

EDR secara otomatis mendeteksi jika beban kerja memerlukan patch, dan memungkinkan Anda memasang patch beban kerja untuk mencegah eksploitasi kerentanan pada potensi serangan di masa mendatang. Perhatikan bahwa fitur ini hanya tersedia jika beban kerja mitra memiliki langganan Manajemen Tingkat Lanjut.

Untuk memasang patch beban kerja

1. Di rantai cyber kill, klik simpul beban kerja yang ingin Anda beri patch.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.
3. Di bagian **Remediasi**, klik **Patch**.
4. Di bidang **Patch yang akan diinstal**, klik **Pilih**. Dalam dialog yang ditampilkan, pilih patch yang relevan lalu klik **Pilih**.
5. Di bidang **Opsi pasca-instalasi**, klik tautan yang ditampilkan. Dialog Opsi pasca-instalasi ditampilkan.

© Acronis International GmbH, 2003-2024



6. Pilih tindakan yang akan dilakukan setelah patch diinstal:
   - **Jika pengguna keluar**: Pilih salah satu dari **Jangan mulai ulang**, **Mulai ulang**, atau **Mulai ulang hanya jika diperlukan**.
   - **Jika pengguna masuk**: Pilih salah satu dari **Jangan mulai ulang**, **Mulai ulang**, atau **Mulai ulang hanya jika diperlukan**.
     Saat memilih **Mulai ulang**, Anda juga dapat menentukan yang berikut ini:
     - Jadwalkan mulai ulang.
     - Izinkan penundaan, termasuk interval yang ditentukan di antara penundaan.
7. [Opsional] Pilih kotak centang **Jangan mulai ulang saat pencadangan sedang berlangsung** untuk memastikan beban kerja tidak dimulai ulang jika pencadangan sedang berlangsung.
8. Klik **Simpan**.
9. Di tab **Tindakan untuk Merespons**, klik **Patch**.
   Patch yang dipilih dijalankan. Tindakan ini juga dapat dilihat di tab **Aktivitas** simpul individu maupun seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

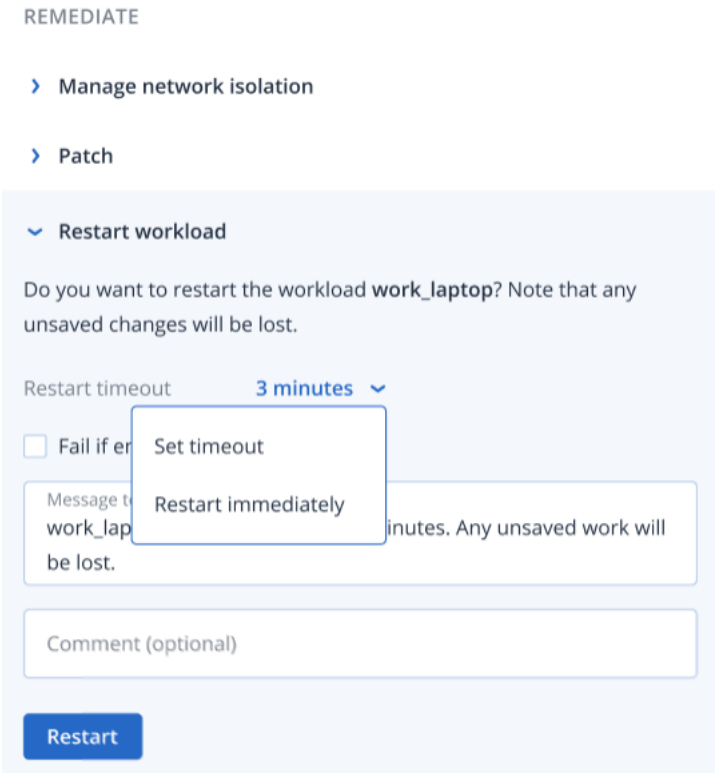
Mulai kembali beban kerja

Sebagai bagian dari respons remediasi Anda terhadap serangan, EDR memungkinkan Anda langsung memulai kembali beban kerja, atau memulai ulang beban kerjanya sesuai periode batas waktu yang ditentukan sebelumnya.

Untuk memulai ulang beban kerja

© Acronis International GmbH, 2003-2024

1. Di rantai cyber kill, klik simpul beban kerja yang ingin Anda tetapkan jadwal mulai ulangnya.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.
3. Di bagian **Remediasi**, klik **Mulai ulang beban kerja**.



4. Di bidang **Batas waktu mulai ulang**, klik tautan yang ditampilkan, lalu pilih salah satu opsi berikut:
   - **Tetapkan batas waktu**: Di dialog Batas waktu mulai ulang, tetapkan periode batas waktu untuk beban kerja, lalu klik **Simpan**.
   - **Langsung mulai ulang**: Pilih untuk langsung memulai ulang beban kerja.
5. [Opsional] Pilih kotak centang **Gagal jika pengguna akhir masuk** untuk memastikan beban kerja tidak dimulai ulang jika pengguna masuk.
6. Di bidang **Pesan yang akan ditampilkan**, tambahkan pesan untuk ditampilkan ke pengguna saat mengakses beban kerja yang diisolasi.
7. [Opsional] Di bidang **Komentar**, tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
8. Klik **Mulai ulang**.
   Beban kerja ditetapkan untuk dimulai ulang sesuai jadwal yang ditentukan. Tindakan ini juga dapat dilihat di tab **Aktivitas** simpul individu maupun seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Jalankan pencadangan forensik pada beban kerja sesuai permintaan

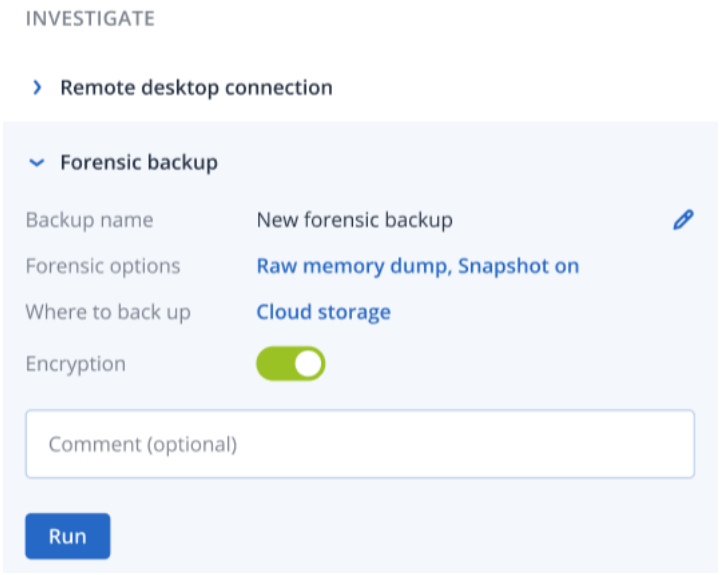
Sebagai bagian dari penyelidikan serangan, EDR memungkinkan Anda untuk melakukan pencadangan forensik sesuai permintaan untuk audit atau tujuan penyelidikan lebih lanjut.

© Acronis International GmbH, 2003-2024

Perhatikan bahwa fitur ini hanya tersedia jika beban kerja mitra memiliki langganan Cadangan Tingkat Lanjut.

Untuk menjalankan pencadangan forensik

1. Di rantai cyber kill, klik simpul beban kerja tempat Anda ingin menjalankan pencadangan forensik.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.
3. Di bagian **Investigasi**, klik **Pencadangan forensik**.



4. [Opsional] Di bidang **Nama cadangan**, klik ikon edit untuk mengedit nama cadangan.
5. Di bidang **Opsi forensik**, klik tautan yang ditampilkan. Di dialog opsi Forensik yang ditampilkan, pilih salah satu dari opsi berikut:
   - **Kumpulkan sampah memori mentah**
   - **Kumpulkan sampah memori kernel**

   Anda juga dapat memilih kotak centang **Snapshot proses yang sedang berjalan** untuk menambahkan informasi tentang proses yang dijalankan saat pencadangan dimulai. Informasi ini disimpan di citra cadangan.

   Klik **Simpan** untuk menutup dialog opsi Forensik.
6. Di bidang **Tempat menyimpan cadangan**, klik tautan yang ditampilkan untuk mendefinisikan lokasi pencadangan.
7. [Opsional] Klik opsi **Enkripsi** untuk mengaktifkan enkripsi. Di dialog yang ditampilkan, masukkan kata sandi untuk cadangan yang dienkripsi dan pilih algoritme enkripsi yang relevan.
8. [Opsional] Di bidang **Komentar**, tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
9. Klik **Jalankan**.

© Acronis International GmbH, 2003-2024

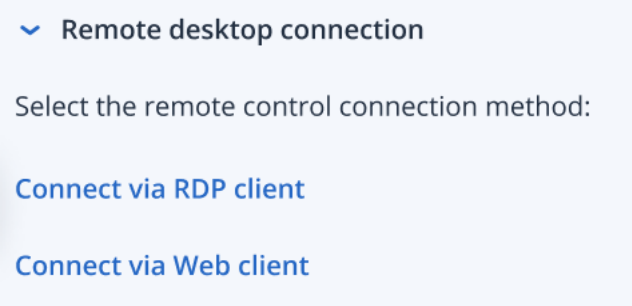
Pencadangan forensik dimulai. Tindakan ini juga dapat dilihat di tab **Aktivitas** simpul individu maupun seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Koneksi jarak jauh ke beban kerja

Sebagai bagian dari penyelidikan serangan, EDR memungkinkan Anda untuk mengakses beban kerja yang sedang diselidiki dari jarak jauh.

Untuk terhubung ke beban kerja dari jarak jauh

1. Di rantai cyber kill, klik simpul beban kerja yang ingin Anda hubungkan secara jarak jauh.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.
3. Di bagian **Investigasi**, klik **Koneksi desktop jarak jauh**.



4. Pilih salah satu dari metode koneksi jarak jauh berikut:
   - **Sambungkan melalui klien RDP**: Metode ini akan meminta Anda untuk mengunduh dan menginstal Klien Koneksi Desktop Jarak Jauh. Anda kemudian dapat jarak jauh terhubung ke beban kerja dari konsol Cyber Protect.
   - **Sambungkan melalui klien Web**: Metode ini tidak memerlukan instalasi klien RDP di beban kerja Anda. Anda akan diarahkan ke layar login untuk memasukkan kredensial ke mesin jarak jauh.

   Saat koneksi jarak jauh dimulai, tindakan ini dapat dilihat di tab **Aktivitas** simpul individu dan seluruh insident. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Memulihkan dari cadangan

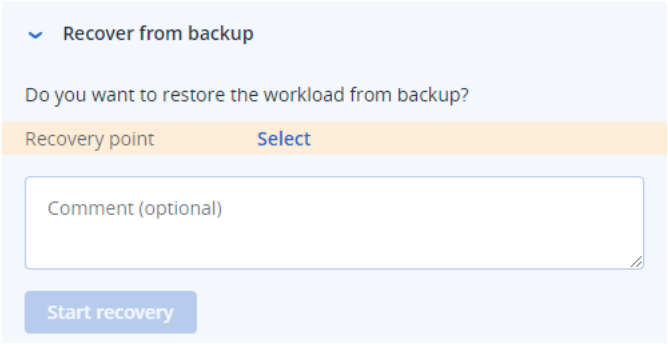
Sebagai bagian dari respons pemulihan Anda terhadap serangan, EDR memungkinkan Anda memulihkan seluruh mesin dari cadangan atau file atau folder tertentu.

Untuk memulihkan beban kerja Anda dari cadangan

1. Di rantai cyber kill, klik simpul beban kerja yang ingin Anda pulihkan.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.

© Acronis International GmbH, 2003-2024

3. Di bagian **Pemulihan**, klik **Memulihkan dari cadangan**.



4. Di bidang **Titik pemulihan**, klik **Pilih** kemudian lakukan langkah-langkah berikut:
   a. Di panel samping yang ditampilkan, pilih titik pemulihan yang relevan.
   b. Klik **Pulihkan > Seluruh beban kerja** untuk memulihkan semua file dan folder pada beban kerja.
      Atau
      Klik **Pulihkan > File/folder** untuk memulihkan file dan folder tertentu pada beban kerja. Anda kemudian diminta untuk memilih file atau folder yang relevan. Setelah dipilih, Anda dapat melihat item yang dipilih untuk pemulihan dengan mengeklik nilai yang relevan di bidang **Item yang akan dipulihkan**.

      Catatan
      Jika titik pemulihan yang Anda pilih dienkripsi, Anda akan diminta memasukkan kata sandi.

5. [Opsional] Pilih kotak centang **Mulai ulang beban kerja secara otomatis**. Opsi ini hanya relevan jika Anda memilih **Pulihkan > Seluruh beban kerja** di Langkah 4.
6. [Opsional] Di bidang **Komentar**, tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
7. Klik **Mulai pemulihan**.
   Proses untuk memulihkan beban kerja dimulai. Kemajuan tindakan ini dapat dilihat di tab **Aktivitas** dari kedua simpul individu dan seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Failover Pemulihan Bencana

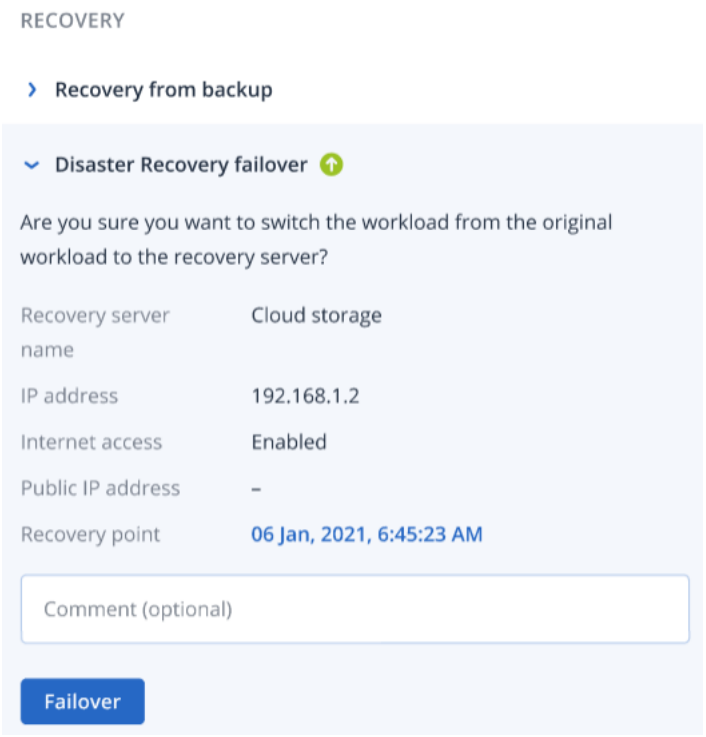
Sebagai bagian dari respons pemulihan Anda terhadap serangan, EDR memungkinkan Anda untuk menjalankan "Menerapkan pemulihan bencana" (hlm. 730), yang memungkinkan Anda mengalihkan beban kerja ke server pemulihan. Perhatikan bahwa beban kerja Anda harus memiliki langganan Pemulihan Bencana Tingkat Lanjut.

Untuk menjalankan failover Pemulihan Bencana

1. Di rantai cyber kill, klik simpul beban kerja yang ingin Anda pulihkan.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.

© Acronis International GmbH, 2003-2024

3. Di bagian **Pemulihan**, klik **kegagalan Pemulihan Bencana**.



4. Di bidang **Titik pemulihan**, lakukan langkah-langkah berikut:
   a. Klik tanggal titik pemulihan saat ini untuk memilih titik pemulihan.
   b. Di panel samping yang ditampilkan, pilih titik pemulihan yang relevan.

   Catatan
   Jika memiliki langganan Pemulihan Bencana Tingkat Lanjut, Anda dapat memilih server pemulihan yang relevan (VM offline) yang dibuat di Pemulihan Bencana. Jika tidak memiliki langganan, Anda akan diminta untuk mengonfigurasi Pemulihan Bencana.

5. [Opsional] Di bidang **Komentar**, tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
6. Klik **Failover**.
   Beban kerja dialihkan ke server pemulihan. Tindakan ini dapat dilihat di tab **Aktivitas** dari kedua simpul individu dan seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Menentukan tindakan respons untuk proses yang mencurigakan

Sebagai bagian dari respons perbaikan terhadap serangan, Anda dapat menerapkan tindakan berikut ke proses yang mencurigakan:

- Hentikan proses (lihat di bawah)
- Karantina proses (lihat di bawah)
- Batalkan perubahan yang dibuat dengan proses (lihat di bawah)

© Acronis International GmbH, 2003-2024

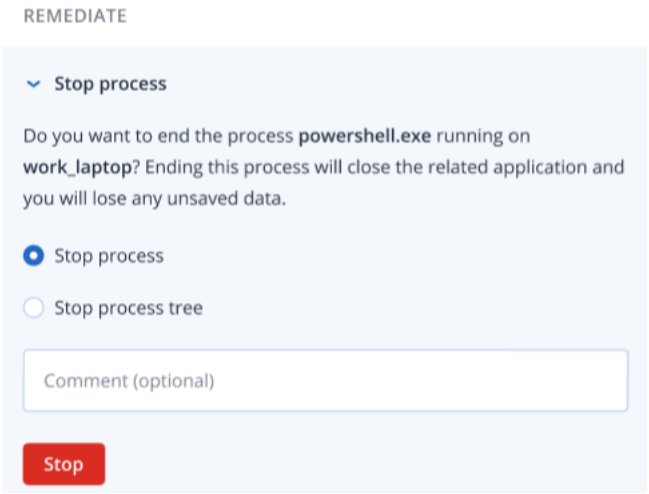
- Tambahkan proses ke daftar izin atau daftar blokir rencana proteksi (lihat "Tambahkan atau hapus proses, file, atau jaringan dalam daftar blokir atau daftar izin rencana proteksi" (hlm. 944))

Untuk menghentikan proses yang mencurigakan

1. Di rantai cyber kill, klik simpul proses yang ingin Anda remediasi.

   Catatan
   Proses Windows yang kritis atau proses yang tidak berjalan tidak dapat dihentikan dan dinonaktifkan dalam rantai cyber kill.

2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.
3. Di bagian **Remediasi**, klik **Hentikan proses**.



4. Pilih salah satu dari opsi berikut:
   - **Hentikan proses** (menghentikan proses tertentu)
   - **Hentikan hierarki proses** (menghentikan proses spesifik dan semua proses anak)
5. [Opsional] Tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
6. Klik **Stop**. Proses akan dihentikan.

   Catatan
   Aplikasi terkait ditutup dan semua data yang belum disimpan akan hilang.

   Tindakan ini juga dapat dilihat di tab **Aktivitas** simpul individu maupun seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

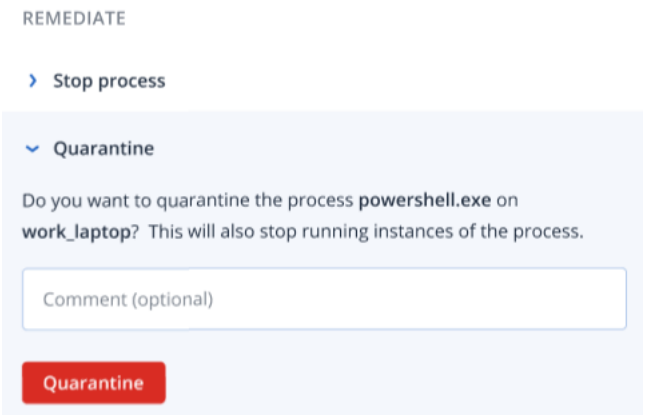
Untuk mengarantina proses yang mencurigakan

© Acronis International GmbH, 2003-2024

1. Di rantai cyber kill, klik simpul proses yang ingin Anda karantina.

Catatan
Proses kritis Windows tidak dapat dikarantina dan dinonaktifkan dalam rantai cyber kill.

2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.
3. Di bagian **Remediasi**, klik **Karantina**.



4. [Opsional] Tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
5. Klik **Karantina**. Prosesnya dihentikan dan kemudian dikarantina.

Catatan
Proses ditambahkan dan dikelola di bagian karantina yang tersedia di bawah proteksi antimalware.

Tindakan ini juga dapat dilihat di tab **Aktivitas** simpul individu maupun seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Untuk membatalkan perubahan

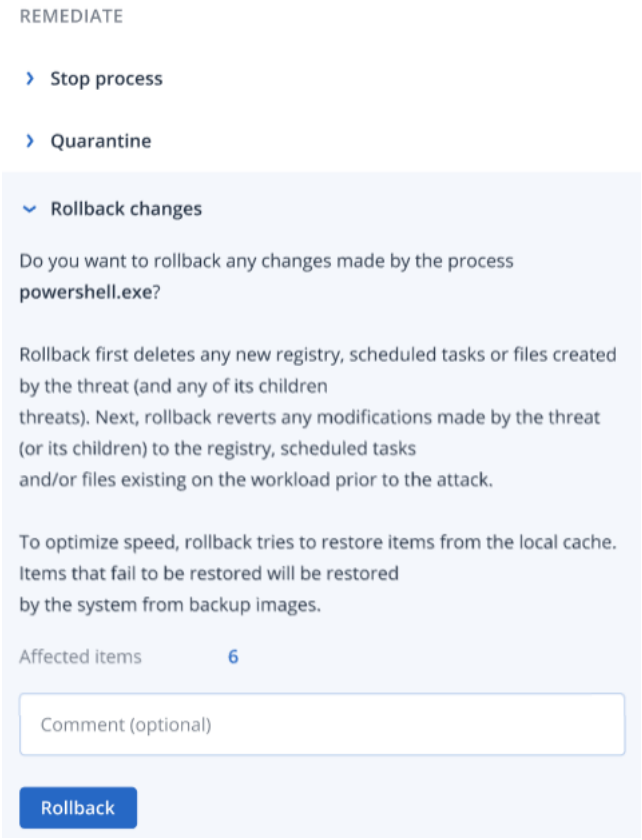
1. Di rantai cyber kill, klik simpul proses yang ingin Anda batalkan perubahannya.

Catatan
Tindakan ini hanya tersedia untuk simpul deteksi (ditampilkan sebagai simpul merah atau kuning).

2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.

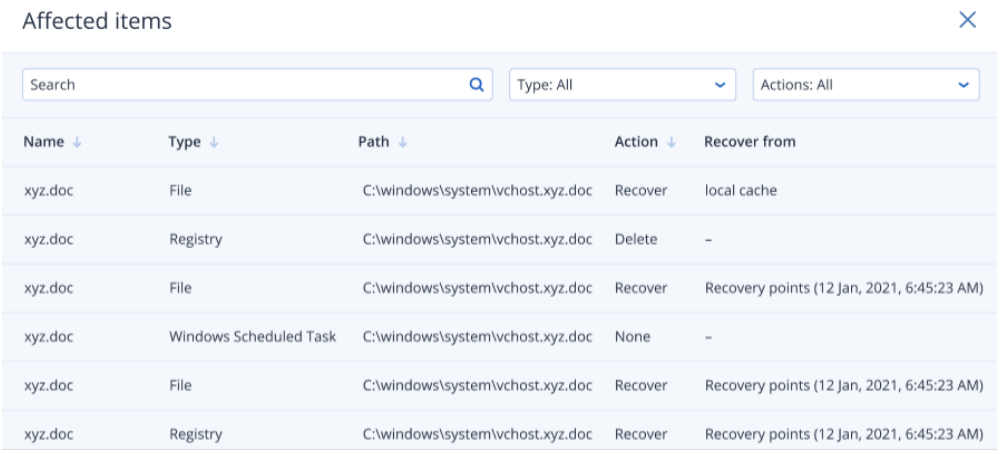
© Acronis International GmbH, 2003-2024

3. Di bagian **Remediasi**, klik **Batalkan perubahan**.



Catatan
Proses pembatalan hanya memulihkan dari item di cache lokal saja. Pembatalan dari arsip cadangan hanya akan tersedia di rilis mendatang.

4. Untuk melihat item yang terpengaruh oleh pembatalan perubahan, klik tautan **Item yang terpengaruh**. Dialog yang ditampilkan menunjukkan semua item (file, registri, tugas terjadwal) yang akan dikembalikan oleh pembatalan dan tindakan yang dilakukan (**Hapus**, **Pulihkan**, atau **Tidak Ada**). Selain itu, Anda dapat melihat apakah item yang dikembalikan akan dipulihkan dari cache lokal atau titik pemulihan cadangan.



© Acronis International GmbH, 2003-2024

5. [Opsional] Tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
6. Klik **Batalkan**. Fungsi pembatalan mengembalikan semua perubahan registri, file, atau tugas terjadwal yang dibuat oleh proses dalam langkah-langkah berikut:
   a. Setiap entri baru (registri, tugas terjadwal, file) yang dibuat oleh ancaman (dan ancaman anaknya) akan dihapus.
   b. Modifikasi apa pun yang dilakukan ancaman (dan ancaman anaknya) pada registri, tugas terjadwal, dan/atau file yang ada pada beban kerja sebelum serangan dikembalikan.
   c. Pembatalan mencoba memulihkan item dari cache lokal. Untuk item yang tidak dapat dipulihkan, EDR akan secara otomatis memulihkannya dari citra cadangan bersih.

   Tindakan pembatalan juga dapat dilihat di tab **Aktivitas** dari kedua simpul individu dan seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

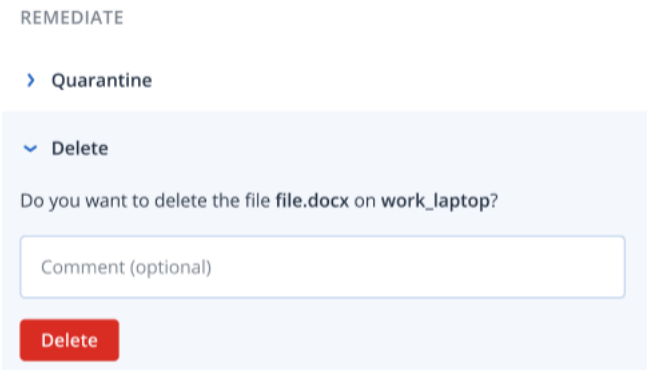
Tetapkan tindakan respons untuk file yang mencurigakan

Sebagai bagian dari respons perbaikan terhadap serangan, Anda dapat menerapkan tindakan berikut ke file yang mencurigakan:

- Hapus file (lihat di bawah)
- Karantina file (lihat di bawah)
- Tambahkan file ke daftar izin atau daftar blokir rencana proteksi (lihat "Tambahkan atau hapus proses, file, atau jaringan dalam daftar blokir atau daftar izin rencana proteksi" (hlm. 944))

Untuk menghapus file yang mencurigakan

1. Di rantai cyber kill, klik simpul file yang ingin Anda pulihkan.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.
3. Di bagian **Remediasi**, klik **Hapus**.



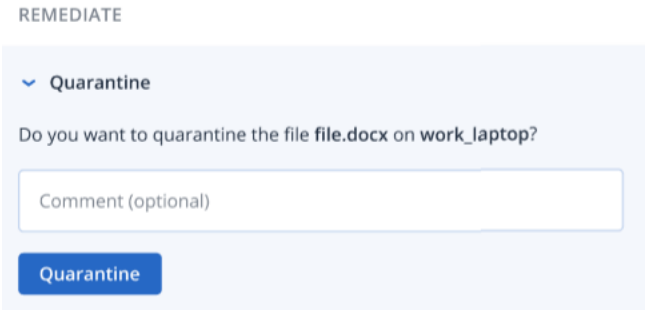
4. [Opsional] Tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.

© Acronis International GmbH, 2003-2024

5. Klik **Hapus**.
   File dihapus. Tindakan ini juga dapat dilihat di tab **Aktivitas** simpul individu maupun seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Untuk mengarantina file yang mencurigakan

1. Di rantai cyber kill, klik simpul file yang ingin Anda pulihkan.
2. Di panel samping yang ditampilkan, buka **Tindakan untuk Merespons**.
3. Di bagian **Remediasi**, klik **Karantina**.



4. [Opsional] Tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
5. Klik **Karantina**.
   File dikarantina. Tindakan ini juga dapat dilihat di tab **Aktivitas** simpul individu maupun seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Menetapkan tindakan respons untuk entri registri yang mencurigakan

Sebagai bagian dari respons perbaikan Anda terhadap serangan, Anda dapat menghapus entri registri yang mencurigakan.

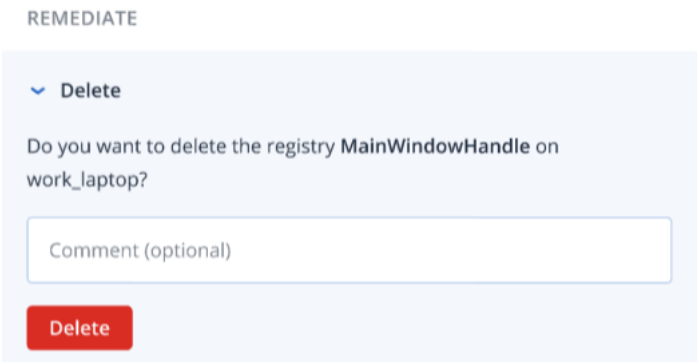
Opsi ini tersedia untuk simpul rantai cyber kill registri.

Untuk menghapus entri registri yang mencurigakan

1. Di rantai cyber kill, klik simpul yang ingin Anda pulihkan.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.

© Acronis International GmbH, 2003-2024

3. Di bagian **Remediasi**, klik **Hapus**.



4. [Opsional] Tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
5. Klik **Hapus**.
   Entri registri dihapus. Tindakan ini juga dapat dilihat di tab **Aktivitas** simpul individu maupun seluruh insiden. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Tambahkan atau hapus proses, file, atau jaringan dalam daftar blokir atau daftar izin rencana proteksi

Sebagai bagian dari respons pencegahan terhadap serangan, Anda dapat menambahkan simpul ke daftar izin atau daftar blokir rencana proteksi.

Anda dapat menambahkan simpul ke daftar izin jika menganggap simpul tersebut aman dan ingin mencegah pendeteksiannya di masa mendatang. Tambahkan simpul ke daftar blokir untuk menghentikan simpul agar tidak berjalan di masa mendatang.

Anda juga dapat menghapus simpul dari daftar izin atau daftar blokir untuk mengizinkan atau mencegah akses di masa mendatang ke simpul tersebut.

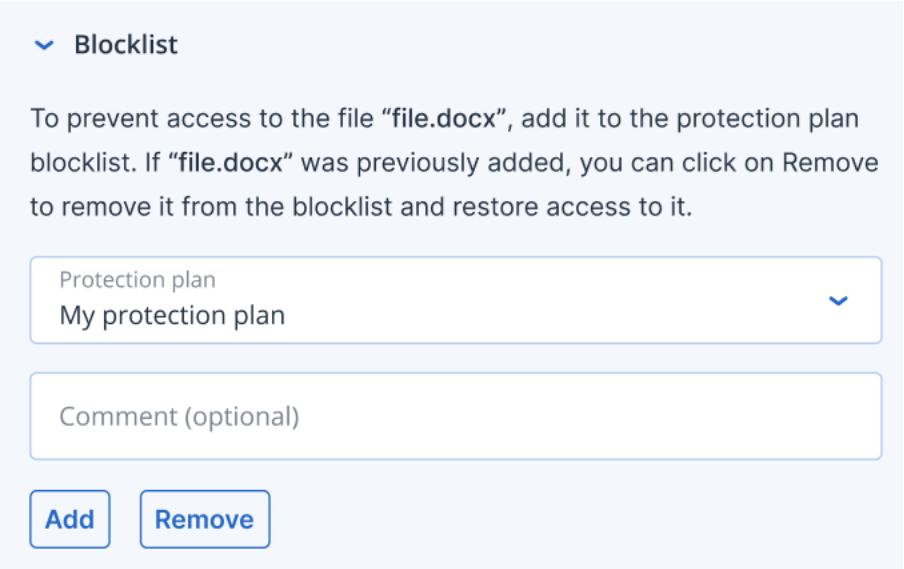
Opsi ini tersedia untuk simpul rantai cyber kill berikut:

- Proses
- File
- Jaringan

Untuk menambahkan atau menghapus proses, file, atau jaringan dalam daftar blokir rencana proteksi

1. Di rantai cyber kill, klik proses, file, atau simpul domain yang ingin Anda pulihkan.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.
3. Di bagian **Prevent**, klik ikon panah di sebelah **Blocklist**.

© Acronis International GmbH, 2003-2024

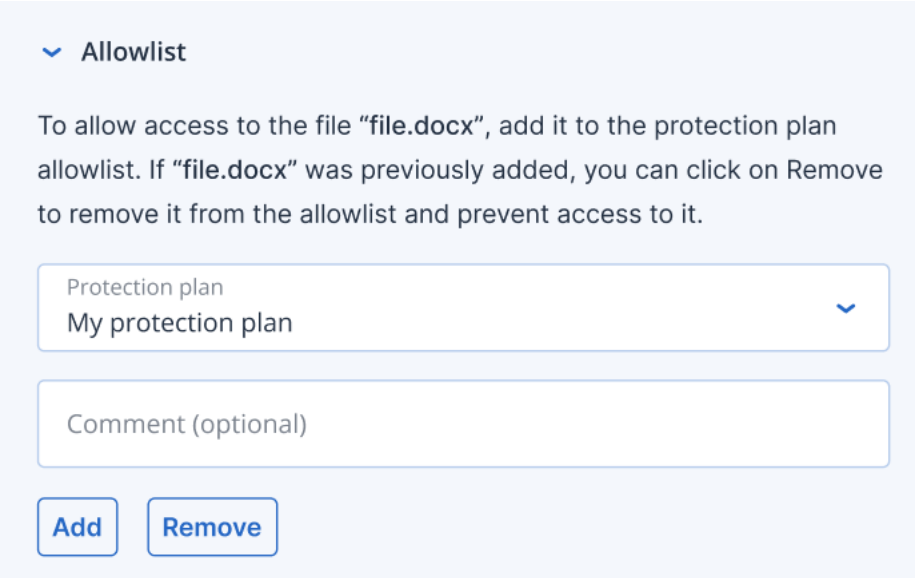


4. Pilih rencana proteksi relevan yang ingin Anda terapkan tindakan ini.
5. [Opsional] Tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
6. Klik **Tambah**.
   Tindakan telah diimplementasikan, dan peluncuran proses, file, atau jaringan akan dicegah di masa mendatang.
   Alternatifnya, jika proses, file, atau jaringan sebelumnya telah ditambahkan ke daftar blokir dan sekarang Anda ingin menghapusnya dari daftar blokir, klik **Hapus**. Ini akan memungkinkan simpul dapat diakses di masa mendatang.
   Tindakan menambah atau menghapus juga dapat dilihat di tab **Aktivitas** baik dari simpul individu maupun insiden keseluruhan. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Untuk menambahkan atau menghapus proses, file, atau jaringan dalam daftar izin rencana proteksi

1. Di rantai cyber kill, klik proses, file, atau simpul domain yang ingin Anda pulihkan.
2. Di panel samping yang ditampilkan, klik tab **Tindakan untuk Merespons**.
3. Di bagian **Prevent**, klik ikon panah di sebelah **Allowlist**.

© Acronis International GmbH, 2003-2024



4. Pilih rencana proteksi relevan yang ingin Anda terapkan tindakan ini.
5. [Opsional] Tambahkan komentar. Komentar ini dapat dilihat di tab **Aktivitas** (untuk simpul tunggal atau seluruh insiden), dan dapat membantu Anda (atau rekan kerja Anda) mengingat alasan mengambil suatu tindakan saat melihat kembali insidennya.
6. Klik **Tambah**.
   Tindakan telah diimplementasikan dan deteksi proses, file, atau jaringan akan dicegah di masa mendatang.
   Alternatifnya, jika proses, file, atau jaringan sebelumnya telah ditambahkan ke daftar izin dan sekarang Anda ingin menghapusnya dari daftar izin, klik **Hapus**. Ini akan mencegah simpul dapat akses di masa mendatang.
   Tindakan menambah atau menghapus juga dapat dilihat di tab **Aktivitas** baik dari simpul individu maupun insiden keseluruhan. Untuk informasi lebih lanjut, lihat "Memahami tindakan yang diambil untuk memitigasi insiden" (hlm. 914).

Mengaktifkan mode monitoring untuk Endpoint Detection and Response (EDR)

Mode monitoring di Cyber Protection memungkinkan Anda untuk menggunakan EDR dalam lingkungan produksi. Sebagai gantinya, mode ini memungkinkan Anda untuk memeriksa adanya positif palsu, dan membuat pengecualian yang diperlukan sebelum menyebarkan EDR sepenuhnya.

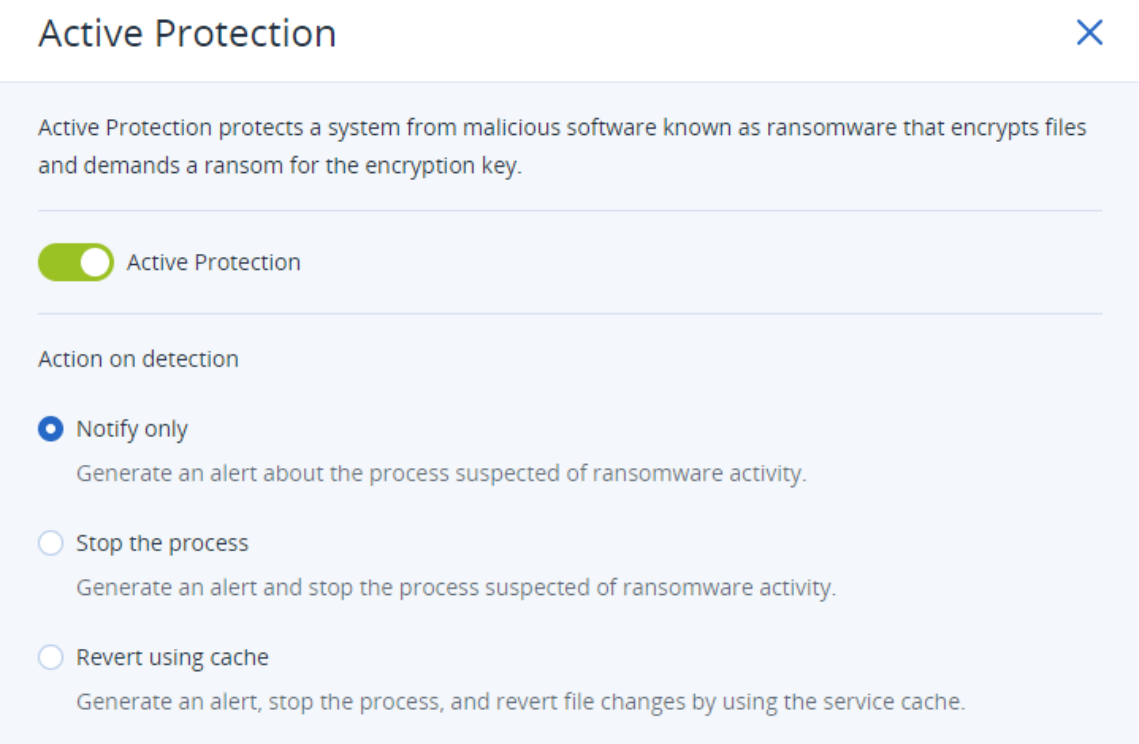
Dalam mode monitoring, tidak ada yang diblok atau dihentikan, dan insiden dibuat, tetapi tidak ada respons yang dimulai.

Untuk mengaktifkan mode monitoring untuk EDR

1. Dalam rencana proteksi yang relevan, pastikan bahwa EDR diaktifkan. Untuk informasi lebih lanjut, lihat "Mengaktifkan fungsionalitas Deteksi dan Tanggapan Titik Akhir (EDR)" (hlm. 895).

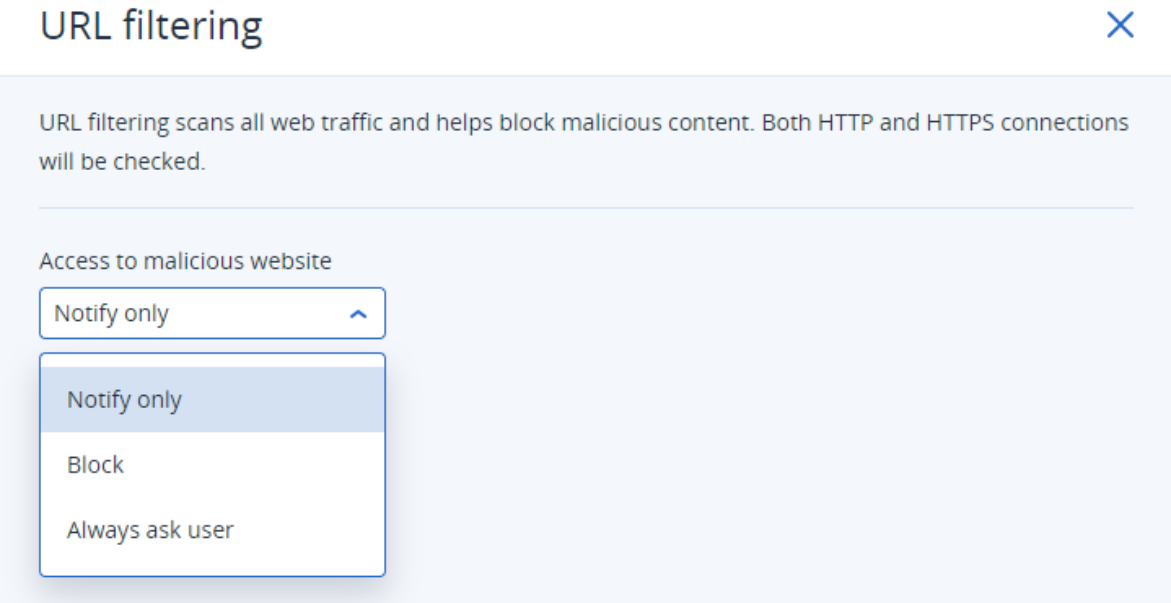
© Acronis International GmbH, 2003-2024

2. Perluas modul **Antivirus & Proteksi Antimalware**, dan kemudian tetapkan hal berikut:
   - Klik **Proteksi Aktif**, dan di bagian **Tindakan saat mendeteksi**, pilih **Hanya kirim notifikasi**. Kemudian klik **Selesai**. Untuk informasi lebih lanjut, lihat "Active Protection" (hlm. 820).



   - Klik **Mesin perilaku**, dan di bagian **Tindakan saat mendeteksi**, pilih **Hanya kirim notifikasi**. Kemudian klik **Selesai**. Untuk informasi lebih lanjut, lihat "Mesin perilaku" (hlm. 824).
   - Klik **Pencegahan eksploitasi**, dan di bagian **Tindakan saat mendeteksi**, pilih **Hanya kirim notifikasi**. Kemudian klik **Selesai**. Untuk informasi lebih lanjut, lihat "Pencegahan eksploit" (hlm. 825).
   - Klik **Proteksi Real-time**, dan di bagian **Tindakan saat mendeteksi**, pilih **Hanya kirim notifikasi**. Kemudian klik **Selesai**. Untuk informasi lebih lanjut, lihat "Perlindungan waktu nyata" (hlm. 827).
   - Klik **Jadwal pindai**, dan di bagian **Tindakan saat mendeteksi**, pilih **Hanya kirim notifikasi**. Kemudian klik **Selesai**. Untuk informasi lebih lanjut, lihat "Jadwalkan pemindaian" (hlm. 828).
3. Perluas modul **Penyaringan URL**, dan dalam daftar drop-down **Akses ke situs web berbahaya**, pilih **Hanya kirim notifikasi**. Kemudian klik **Selesai**. Untuk informasi lebih lanjut, lihat "Pemfilteran URL" (hlm. 842).

© Acronis International GmbH, 2003-2024



Cara menguji apakah Deteksi dan Tanggapan Titik Akhir (EDR) bekerja dengan baik

Untuk memastikan EDR diterapkan dan bekerja, Anda dapat menjalankan beberapa perintah yang memicu deteksi EDR.

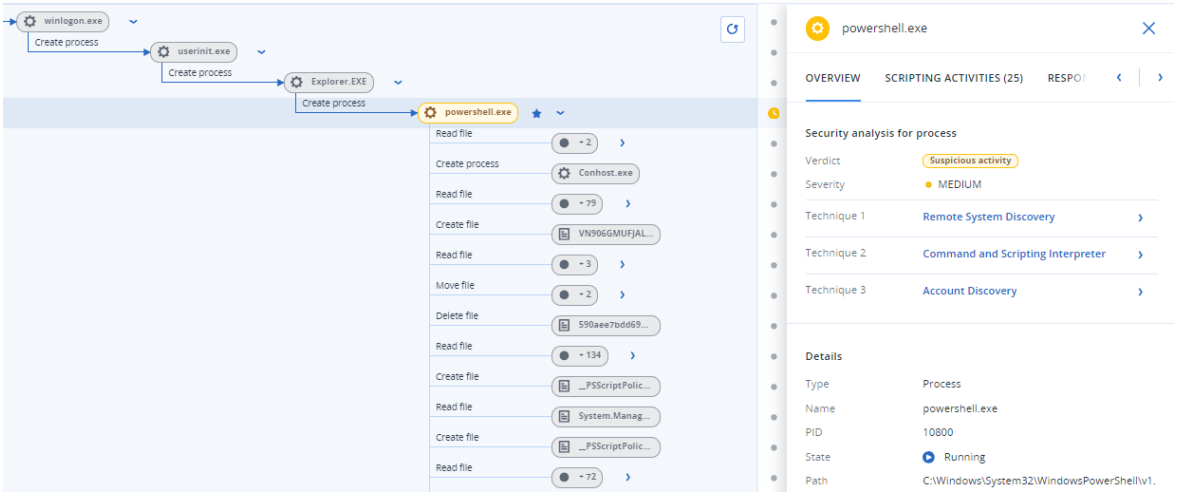
Catatan
Ketika EDR diterapkan, Anda bisa melihat insidennya dengan cepat jika aktivitas mencurigakan terjadi. Langkah di bawah memungkinkan Anda memeriksa apakah EDR bekerja jika tidak ada insiden baru yang terpicu selama beberapa hari.

Untuk menguji apakah EDR telah disebarkan dan berfungsi dengan benar

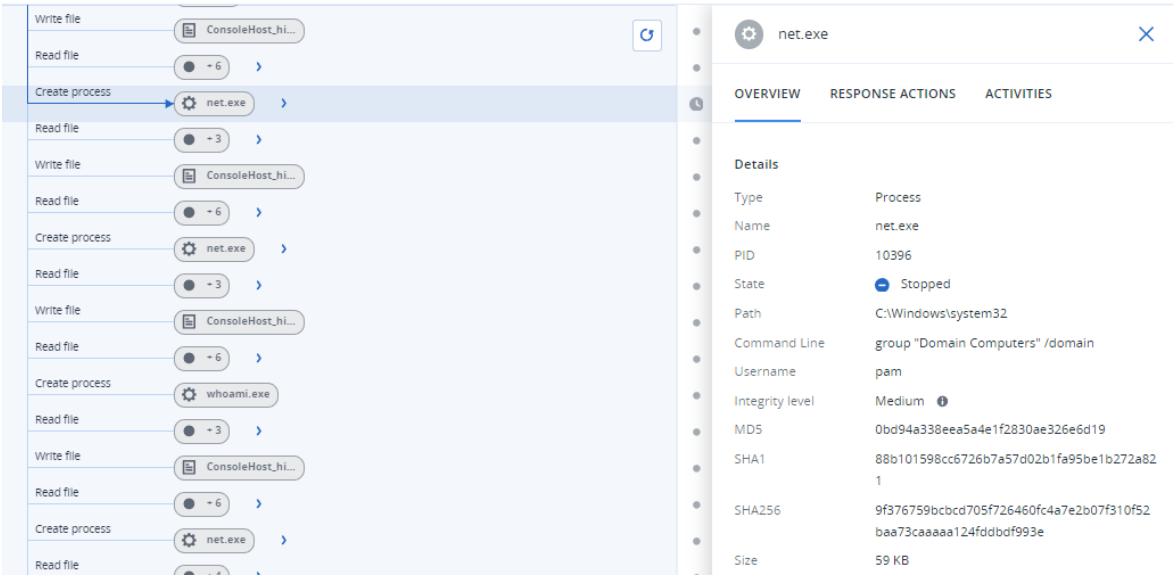
1. Masuk ke dalam akun pengguna Active Directory yang diikuti domain yang relevan.
2. Jalankan perintah berikut Windows PowerShell:
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. Di konsol Cyber Protect, buka **Perlindungan > Insiden** untuk melihat insiden yang dibuat.

   Anda juga dapat mengklik tipe insiden tipe keparahan **Medium** yang terpicu untuk menampilkannya di rantai cyber kill EDR dan memastikan perintah PowerShell yang Anda eksekusi dalam langkah sebelumnya, seperti yang ditunjukkan pada contoh di bawah.

© Acronis International GmbH, 2003-2024



4. Jalankan perintah berikut dalam Windows PowerShell:
   - `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. Dalam rantai cyber kill EDR, klik node yang dapat dieksekusi (contohnya, **net.exe** atau **whoami.exe**) untuk menunjukkan perintah PowerShell yang dieksekusi pada baris perintah. Perintah berikut ditampilkan dalam bagian **Detail** pada tab **Ikhtisar** pada contoh di bawah.



6. Setelah Anda mengonfirmasi insiden EDR telah dibuat, atur **status Ancaman** untuk insiden ke keadaan **Termigitasi** dan **Investigasi** ke **Ditutup** secara manual. Untuk informasi lebih lanjut, lihat "Cara menginvestigasi insiden di rantai cyber kill" (hlm. 906). Anda juga bisa memasukkan komentar untuk insiden untuk menunjukkan bahwa ini merupakan insiden pengujian.

© Acronis International GmbH, 2003-2024

Menilai kerentanan dan mengelola patch

Penilaian kerentanan (VA) adalah proses mengidentifikasi, mengukur, dan memprioritaskan kerentanan yang ditemukan dalam sistem. Dalam modul penilaian kerentanan, Anda dapat memindai mesin untuk mencari kerentanan, dan memeriksa apakah sistem operasi dan aplikasi yang diinstal sudah mutakhir dan berfungsi dengan baik.

Pemindaian penilaian kerentanan didukung untuk mesin dengan sistem operasi berikut:

- Windows. Untuk informasi lebih lanjut, lihat "Produk Microsoft dan produk pihak ketiga yang didukung" (hlm. 951).
- macOS. Untuk informasi lebih lanjut, lihat "Produk Apple dan pihak ketiga yang didukung" (hlm. 952).
- Mesin Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Untuk informasi lebih lanjut, lihat "Produk Linux yang didukung" (hlm. 953).

Gunakan fungsi **Manajemen patch** (PM) untuk mengelola patch (pembaruan) pada aplikasi dan sistem operasi yang diinstal pada mesin Anda, dan selalu perbarui sistem Anda. Dalam modul manajemen patch, Anda dapat secara otomatis atau manual menyetujui instalasi pembaruan pada mesin Anda.

Manajemen patch didukung untuk mesin dengan sistem operasi Windows. Untuk informasi lebih lanjut, lihat "Produk Microsoft dan produk pihak ketiga yang didukung" (hlm. 951).

Penilaian kerentanan

Proses penilaian kerentanan terdiri dari langkah-langkah berikut:

1. Anda membuat rencana proteksi dengan modul penilaian kerentanan yang diaktifkan, menentukan Pengaturan penilaian kerentanan, dan menetapkan rencana ke mesin.
2. Sistem, berdasarkan jadwal atau sesuai permintaan, mengirimkan perintah untuk menjalankan pemindaian penilaian kerentanan ke agen perlindungan yang diinstal pada mesin.
3. Agen mendapatkan perintah, mulai memindai kerentanan pada mesin, dan menjalankan aktivitas pemindaian.
4. Setelah pemindaian penilaian kerentanan selesai, agen membuat hasil dan mengirimkannya ke layanan pemantauan.
5. Layanan pemantauan memproses data dari agen dan menampilkan hasilnya dalam widget penilaian kerentanan dan daftar kerentanan yang ditemukan.
6. Saat memperoleh daftar kerentanan yang ditemukan, Anda dapat memprosesnya dan menentukan yang mana dari kerentanan tersebut yang harus diperbaiki.

Anda dapat memantau hasil pemindaian penilaian kerentanan di widget **Pemantauan**> **Ikhtisar** > **Kerentanan / Kerentanan yang ada**.

© Acronis International GmbH, 2003-2024

Produk Microsoft dan produk pihak ketiga yang didukung

Produk Microsoft dan produk pihak ketiga untuk sistem operasi Windows berikut didukung untuk penilaian kerentanan dan manajemen patch:

Produk Microsoft yang didukung

Windows OS

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server OS

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office dan komponen terkait

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Komponen terkait Windows OS

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studio dan Aplikasi
- Komponen sistem operasi

Aplikasi 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

Produk pihak ketiga yang didukung untuk Windows OS

Bekerja jarak jauh menjadi semakin populer di seluruh dunia, karenanya alat bantu kolaborasi dan komunikasi, klien VPN saat ini harus selalu diperbarui dan diperiksa untuk mengetahui adanya kemungkinan kerentanan. Layanan Cyber Protection mendukung penilaian kerentanan dan manajemen patch untuk aplikasi semacam ini.

Alat bantu kolaborasi dan komunikasi, klien VPN

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

Untuk informasi lebih lanjut mengenai produk pihak ketiga yang didukung untuk Windows OS, lihat Daftar produk pihak ketiga yang didukung Manajemen Patch (62853).

Produk Apple dan pihak ketiga yang didukung

Produk Apple dan produk pihak ketiga berikut untuk macOS didukung untuk penilaian kerentanan:

Produk Apple yang didukung

macOS

- macOS 10.13.x dan versi yang lebih baru

Aplikasi bawaan macOS

© Acronis International GmbH, 2003-2024

- Safari, iTunes, dan lainnya.

Produk pihak ketiga yang didukung untuk macOS

- Microsoft Office (Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC media player

Produk Linux yang didukung

Distribusi dan versi Linux berikut ini didukung untuk VA:

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

Pengaturan penilaian kerentanan

Untuk mempelajari cara membuat rencana proteksi dengan modul penilaian Kerentanan, lihat "Membuat rencana proteksi". Anda dapat melakukan pemindaian VA berdasarkan jadwal atau sesuai permintaan (dengan menggunakan tindakan **Jalankan sekarang** dalam rencana proteksi).

Anda dapat menentukan pengaturan berikut di modul penilaian Kerentanan.

Apa yang dipindai

Tentukan produk perangkat lunak mana yang ingin Anda pindai kerentanannya:

- Mesin Windows:
  - **Produk Microsoft**
  - **Produk pihak ketiga Windows** (untuk informasi lebih lanjut mengenai produk pihak ketiga yang didukung untuk Windows OS, lihat Daftar produk pihak ketiga yang didukung Manajemen Patch (62853))
- Mesin macOS:
  - **Produk Apple**
  - **Produk pihak ketiga macOS**

© Acronis International GmbH, 2003-2024

- Mesin Linux:
  - **Pindai paket Linux**

Jadwal

Tentukan jadwal yang sesuai untuk melakukan pemindaian penilaian kerentanan pada mesin yang dipilih:

Bidang	Deskripsi
Jadwalkan operasi tugas menggunakan peristiwa berikut	Pengaturan ini menentukan kapan tugas akan dijalankan. Nilai berikut tersedia: • **Jadwalkan berdasarkan waktu** – Ini adalah pengaturan default. Tugas akan berjalan sesuai waktu yang ditentukan. • **Saat pengguna masuk ke sistem** – Secara default, akses masuk (login) pengguna mana pun akan memicu tugas. Anda dapat mengubah pengaturan ini agar hanya akun pengguna tertentu yang dapat memicu tugas. • **Saat pengguna keluar dari sistem** – Secara default, akses keluar (logoff) pengguna mana pun akan memicu tugas. Anda dapat mengubah pengaturan ini agar hanya akun pengguna tertentu yang dapat memicu tugas. **Catatan** Tugas tidak akan berjalan saat sistem dimatikan. Mematikan dan keluar adalah peristiwa berbeda di konfigurasi penjadwalan. • **Pada startup sistem** – Tugas akan berjalan saat sistem operasi dimulai. • **Pada shutdown sistem** – Tugas akan berjalan saat sistem operasi dimatikan.
Jenis jadwal	Bidang ini muncul jika di **Jadwalkan operasi tugas menggunakan peristiwa berikut** Anda telah memilih **Jadwalkan berdasarkan waktu**. Nilai berikut tersedia: • **Bulanan** – Pilih bulan dan minggu atau hari dalam sebulan saat tugas akan berjalan. • **Harian** – Ini adalah pengaturan default. Pilih hari dalam seminggu saat tugas akan dijalankan. • **Per jam** – Pilih hari dalam pekan, jumlah pengulangan, dan interval waktu tugas akan berjalan.
Mulai pada	Bidang ini muncul jika di **Jadwalkan operasi tugas menggunakan peristiwa berikut** Anda telah memilih **Jadwalkan berdasarkan waktu** Pilih waktu yang tepat kapan tugas akan dijalankan.

© Acronis International GmbH, 2003-2024

Bidang	Deskripsi
Jalankan dalam rentang tanggal	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Jadwalkan berdasarkan waktu**. Atur periode waktu ketika jadwal yang sudah dikonfigurasi akan berlaku.
Tentukan akun pengguna yang akses masuknya ke sistem operasi akan memulai tugas	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Saat pengguna masuk ke sistem**. Nilai berikut tersedia: • **Semua pengguna** - Gunakan opsi ini jika Anda ingin akses masuk pengguna mana pun memicu tugas. • **Pengguna berikut** - Gunakan opsi ini jika Anda hanya ingin akses masuk akun pengguna tertentu yang memicu tugas.
Tentukan akun pengguna yang logout-nya dari sistem operasi akan memulai tugas	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Saat pengguna keluar dari sistem**. Nilai berikut tersedia: • **Pengguna mana pun** - Gunakan opsi ini jika Anda ingin logout pengguna mana pun memicu tugas. • **Pengguna berikut** - Gunakan opsi ini jika Anda hanya ingin logout akun pengguna tertentu yang memicu tugas.
Persyaratan untuk memulai	Mendefinisikan semua kondisi yang harus dipenuhi secara bersamaan agar tugas dapat dijalankan. Kondisi awal untuk pemindaian antimalware serupa dengan kondisi awal untuk **Modul cadangan** yang dijelaskan dalam "Persyaratan untuk memulai". Anda dapat menetapkan persyaratan awal tambahan berikut: • **Distribusikan waktu mulai tugas dalam rentang waktu** – Opsi ini memungkinkan Anda menentukan jangka waktu tugas untuk menghindari kemacetan jaringan. Anda dapat menentukan penundaan dalam jam atau menit. Misalnya, jika waktu mulai default adalah pukul 10.00 dan penundaannya adalah 60 menit, tugas akan dimulai antara pukul 10.00 sampai 11.00. • **Jika mesin dimatikan, jalankan tugas yang tertinggal pada saat mesin dinyalakan** • **Cegah mode tidur atau hibernasi selama menjalankan tugas** – Opsi ini hanya berlaku untuk mesin yang menjalankan Windows. • **Jika persyaratan awal tidak terpenuhi, tetap jalankan tugas setelahnya** – Tentukan periode waktu dalam jam saat tugas akan dijalankan setelahnya, terlepas dari kondisi awal lainnya.

© Acronis International GmbH, 2003-2024

Bidang	Deskripsi
	Catatan Persyaratan awal tidak didukung untuk Linux.

Penilaian kerentanan untuk mesin Windows

Anda dapat memindai mesin Windows dan produk pihak ketiga untuk Windows guna menemukan kerentanan.

Untuk mengonfigurasi penilaian kerentanan untuk mesin Windows

1. Di konsol Cyber Protect, buat rencana proteksi dan aktifkan modul **Penilaian kerentanan**.
2. Tetapkan pengaturan penilaian kerentanan:
   - **Apa yang dipindai** – pilih **produk Microsoft**, **produk pihak ketiga Windows**, atau keduanya.
   - **Jadwal** – tentukan jadwal untuk melakukan penilaian kerentanan.

   Untuk informasi lebih lanjut tentang opsi **Jadwal**, lihat "Pengaturan penilaian kerentanan" (hlm. 953).
3. Menetapkan rencana ke mesin Windows.

Setelah pemindaian penilaian kerentanan, Anda dapat melihat daftar kerentanan yang ditemukan. Anda dapat memproses informasi dan memutuskan kerentanan yang mana yang harus diperbaiki.

Untuk memantau hasil penilaian kerentanan, lihat widget **Pemantauan** > **Ikhtisar** > **Kerentanan / Kerentanan yang Ada** widgets.

Penilaian kerentanan untuk mesin Linux

Anda dapat memindai mesin Linux untuk kerentanan tingkat aplikasi dan tingkat kernel.

Mengonfigurasi penilaian kerentanan untuk mesin Linux

1. Di konsol Cyber Protect, buat rencana proteksi dan aktifkan modul **Penilaian kerentanan**.
2. Tetapkan pengaturan penilaian kerentanan:
   - **Apa yang dipindai** – pilih **Pindai paket Linux**.
   - **Jadwal** – tentukan jadwal untuk melakukan penilaian kerentanan.

   Untuk informasi lebih lanjut tentang opsi **Jadwal**, lihat "Pengaturan penilaian kerentanan" (hlm. 953).
3. Tetapkan rencana ke mesin Linux.

Setelah pemindaian penilaian kerentanan, Anda dapat melihat daftar kerentanan yang ditemukan. Anda dapat memproses informasi dan memutuskan kerentanan yang mana yang harus diperbaiki.

Untuk memantau hasil penilaian kerentanan, lihat widget **Pemantauan** > **Ikhtisar** > **Kerentanan / Kerentanan yang Ada** widgets.

© Acronis International GmbH, 2003-2024

Penilaian kerentanan untuk perangkat macOS

Anda dapat memindai perangkat macOS untuk mencari kerentanan tingkat sistem operasi dan tingkat aplikasi.

Untuk mengonfigurasi penilaian kerentanan untuk perangkat macOS

1. Di konsol Cyber Protect, buat rencana proteksi dan aktifkan modul **Penilaian kerentanan**.
2. Tetapkan pengaturan penilaian kerentanan:
   - **Apa yang dipindai** – pilih **produk Apple**, **produk pihak ketiga macOS**, atau keduanya.
   - **Jadwal** – tentukan jadwal untuk melakukan penilaian kerentanan.

   Untuk informasi lebih lanjut tentang opsi **Jadwal**, lihat "Pengaturan penilaian kerentanan" (hlm. 953).
3. Tetapkan rencana ke perangkat macOS.

Setelah pemindaian penilaian kerentanan, Anda dapat melihat daftar kerentanan yang ditemukan. Anda dapat memproses informasi dan memutuskan kerentanan yang mana yang harus diperbaiki.

Untuk memantau hasil penilaian kerentanan, lihat widget **Pemantauan** > **Ikhtisar** > **Kerentanan / Kerentanan yang Ada** widgets.

Mengelola kerentanan yang ditemukan

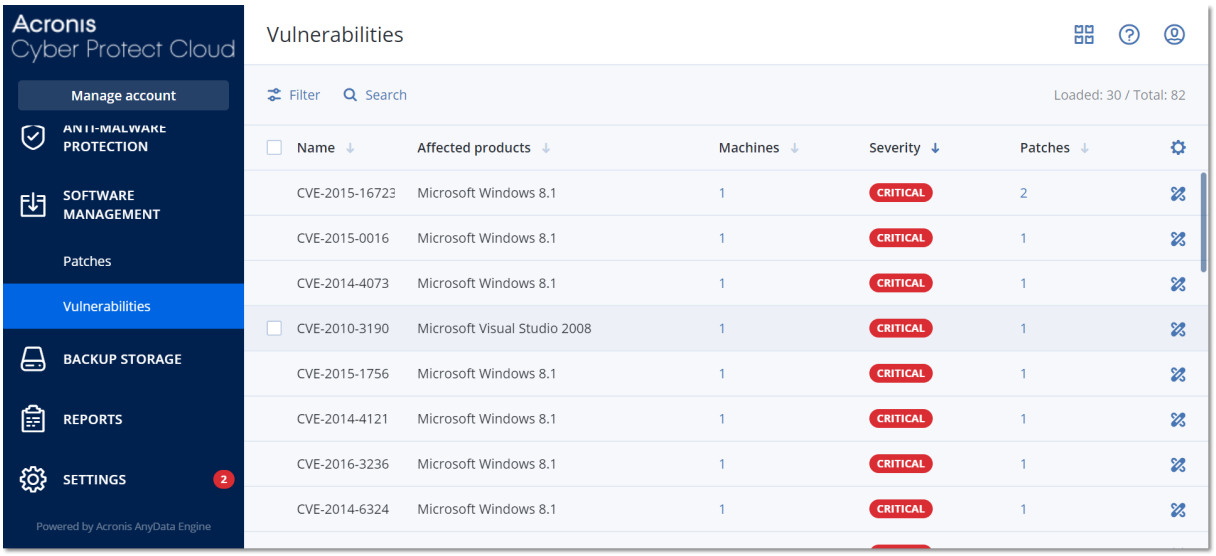
Jika penilaian kerentanan dilakukan setidaknya sekali dan beberapa kerentanan ditemukan, Anda dapat melihatnya di **Manajemen perangkat lunak** > **Kerentanan**. Daftar kerentanan menunjukkan kedua kerentanan yang memiliki patch untuk diinstal dan yang tidak memiliki patch yang disarankan. Anda dapat menggunakan filter untuk menampilkan kerentanan dengan patch saja.

Nama	Deskripsi
Nama	Nama kerentanan.
Produk yang terdampak	Produk perangkat lunak di mana kerentanan ditemukan.
Mesin	Jumlah mesin yang terdampak.
Tingkat keparahan	Tingkat keparahan yang ditemukan. Tingkat-tingkat berikut ini dapat ditetapkan berdasarkan Sistem Penilaian Kerentanan Umum (CVSS): • **Kritis**: 9 - 10 CVSS • **Tinggi**: 7 - 9 CVSS • **Sedang**: 3 - 7 CVSS • **Rendah**: 0 - 3 CVSS • **Tidak ada**

© Acronis International GmbH, 2003-2024

Patch	Jumlah patch yang sesuai.
Diterbitkan	Tanggal dan waktu ketika kerentanan diterbitkan dalam Kerentanan dan Pembukaan Umum (CVE).
Terdeteksi	Tanggal pertama saat kerentanan pertama terdeteksi pada mesin.

Anda dapat menemukan deskripsi kerentanan yang ditemukan dengan mengeklik namanya dalam daftar.



Untuk memulai proses perbaikan kerentanan

1. Di konsol Cyber Protect, buka **Manajemen perangkat lunak** > **Kerentanan**.
2. Pilih kerentanan dalam daftar, lalu klik **Instal patch**. Wizard perbaikan kerentanan akan terbuka.
3. Pilih patch yang akan diinstal pada mesin yang dipilih, lalu klik **Berikutnya**.
4. Pilih beberapa mesin tempat Anda ingin menginstal patch.
5. Pilih opsi boot ulang.
   a. Pilih apakah Anda ingin mesin di-boot ulang setelah patch diinstal.

Opsi	Deskripsi
Tidak	Mesin tidak akan di-boot ulang secara otomatis setelah patch diinstal.
Jika diperlukan	Mesin akan di-boot ulang hanya jika diperlukan untuk menerapkan patch.
Ya	Mesin akan di-boot ulang secara otomatis setelah patch diinstal. Anda juga dapat menentukan penundaan boot ulang.

   b. [Opsional] Jika Anda ingin menunda boot ulang mesin saat pencadangan mesin sedang berlangsung, pilih **Jangan boot ulang hingga pencadangan selesai**.
6. Klik **Instal patch**.

Hasilnya, patch yang dipilih akan diinstal pada mesin yang dipilih.

© Acronis International GmbH, 2003-2024

Manajemen patch

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Untuk informasi lebih lanjut mengenai produk pihak ketiga yang didukung untuk Windows OS, lihat Daftar produk pihak ketiga yang didukung Manajemen Patch (62853).

Gunakan fungsionalitas manajemen patch untuk:

- menginstal pembaruan tingkat OS dan tingkat aplikasi
- menyetujui patch secara manual atau otomatis
- menginstal patch sesuai permintaan atau berdasarkan jadwal
- menentukan secara tepat patch mana yang akan diinstal berdasarkan kriteria yang berbeda: tingkat keparahan, kategori, dan status persetujuan
- melakukan pencadangan pra-pembaruan untuk mencegah kemungkinan pembaruan yang tidak berhasil
- menentukan tindakan reboot setelah penginstalan patch

Catatan
Untuk bekerja dengan pembaruan Windows, fitur manajemen patch membutuhkan pembaruan Windows diaktifkan pada beban kerja.

Cyber Protection memperkenalkan teknologi rekan-ke-rekan untuk meminimalkan lalu lintas bandwidth jaringan. Anda dapat memilih satu atau beberapa agen khusus yang akan mengunduh pembaruan dari internet dan mendistribusikannya di antara agen-agen lain dalam jaringan. Semua agen juga akan saling berbagi pembaruan sebagai agen rekan-ke-rekan.

Alur kerja manajemen patch

Alur kerja manajemen patch mencakup langkah-langkah untuk mengonfigurasi dan menerapkan rencana proteksi, menjalankan pemindaian penilaian kerentanan, mengonfigurasi pengaturan patch, menyetujui patch, dan terakhir, menginstal patch yang disetujui. Langkah-langkah alur kerja yang tepat adalah sebagai berikut.

1. Konfigurasikan rencana proteksi yang mengaktifkan modul **Penilaian kerentanan** dan **Manajemen patch**.
2. Konfigurasikan pengaturan penilaian kerentanan. Untuk informasi lebih lanjut tentang pengaturan ini, lihat "Pengaturan penilaian kerentanan" (hlm. 953).
3. Konfigurasikan pengaturan manajemen patch. Untuk informasi lebih lanjut tentang pengaturan ini, lihat "Pengaturan manajemen patch dalam rencana proteksi" (hlm. 960)
4. Terapkan rencana proteksi pada satu atau beberapa mesin.

© Acronis International GmbH, 2003-2024

5. Tunggu hingga penilaian kerentanan selesai dipindai. Pemindaian akan dimulai secara otomatis, sesuai dengan jadwal yang dikonfigurasi dalam rencana proteksi. Alternatifnya, Anda dapat memulai pemindaian sesuai permintaan secara manual dengan mengeklik ikon **Jalankan sekarang** di modul **Penilaian kerentanan** dalam rencana proteksi.
6. Setujui patch tersebut. Anda dapat menentukan pengaturan untuk persetujuan patch otomatis, yang mencakup instalasi otomatis patch pada mesin uji. Untuk informasi lebih lanjut, lihat "Persetujuan patch otomatis" (hlm. 967). Cara lainnya, Anda dapat menyetujui patch secara manual dengan menetapkan status persetujuannya ke **Disetujui**. Untuk informasi lebih lanjut, lihat "Menyetujui patch secara manual" (hlm. 972).
7. Instal patch-nya. Patch yang disetujui dapat diinstal secara otomatis, sesuai dengan jadwal yang dikonfigurasi dalam rencana proteksi. Cara lainnya, Anda dapat menginstal patch secara manual sesuai permintaan. Untuk informasi lebih lanjut, lihat "Menginstal patch sesuai permintaan" (hlm. 972).

Anda dapat memantau hasil instalasi patch di widget **Pemantauan**> **Ikhtisar** > **Riwayat instalasi patch**.

Pengaturan manajemen patch dalam rencana proteksi

Dalam modul **Manajemen patch** pada rencana proteksi, Anda dapat mengonfigurasi pengaturan manajemen patch berikut:

- Pembaruan apa yang harus diinstal untuk Microsoft dan produk pihak ketiga untuk OS Windows.
- Kapan menjalankan instalasi patch otomatis.
- Apakah akan menjalankan cadangan pra-pembaruan.

Untuk informasi selengkapnya tentang membuat rencana proteksi dan mengaktifkan modul **Manajemen patch**, lihat "Membuat rencana proteksi" (hlm. 214).

Catatan
Ketersediaan fitur ini bergantung pada kuota layanan yang diaktifkan untuk akun Anda.

Produk Microsoft

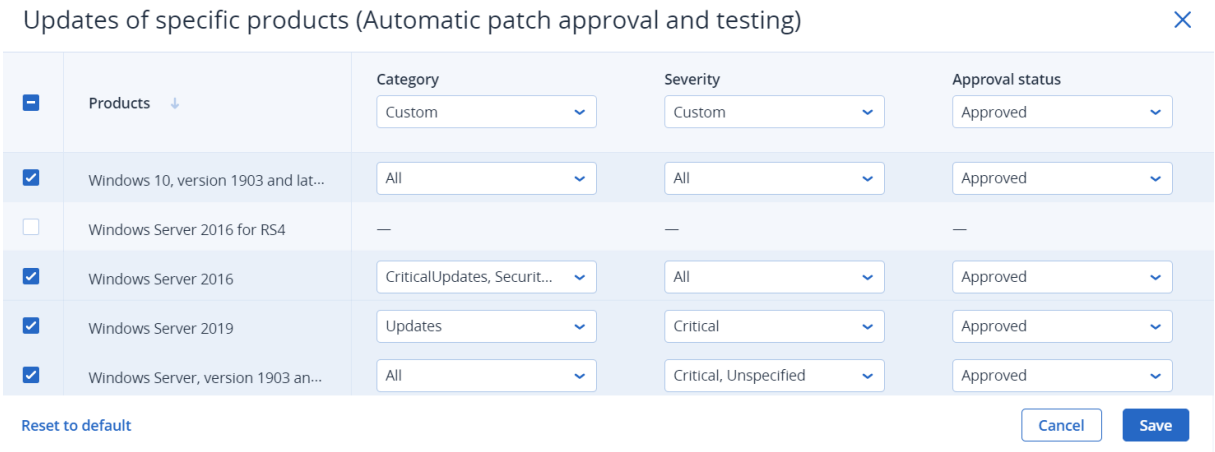
Untuk menginstal pembaruan Microsoft di mesin yang dipilih, aktifkan opsi **Perbarui produk Microsoft**.

Pilih opsi instalasi:

Opsi	Deskripsi
Semua pembaruan	Gunakan opsi ini jika Anda ingin menginstal semua pembaruan yang disetujui.
Hanya pembaruan Penting dan Keamanan	Gunakan opsi ini jika Anda ingin menginstal semua keamanan dan pembaruan penting yang disetujui.

© Acronis International GmbH, 2003-2024

Opsi	Deskripsi
Pembaruan produk tertentu (Persetujuan dan pengujian patch otomatis)	Gunakan opsi ini jika Anda ingin menentukan pengaturan kustom untuk produk yang berbeda. Jika Anda ingin memperbarui produk spesifik, Anda dapat menetapkan pembaruan mana yang akan diinstal untuk setiap produk berdasarkan kategori, keparahan, atau status persetujuan. Jika Anda ingin mengonfigurasi persetujuan uji otomatis dan pengujian patch, pilih opsi ini.



Untuk produk Microsoft, distribusi patch menggunakan layanan Windows API. Patch dan pembaruan tidak diunduh atau disimpan secara internal atau pada agen distribusi. Sebagai gantinya, mereka diunduh dari Microsoft CDN. Dengan demikian, bahkan dengan peran Updater yang ditetapkan, agen tidak dapat mengunduh dan mendistribusikan patch.

Produk pihak ketiga Windows

Untuk menginstal pembaruan pihak ketiga untuk Windows OS di mesin yang dipilih, aktifkan opsi **Produk pihak ketiga Windows**.

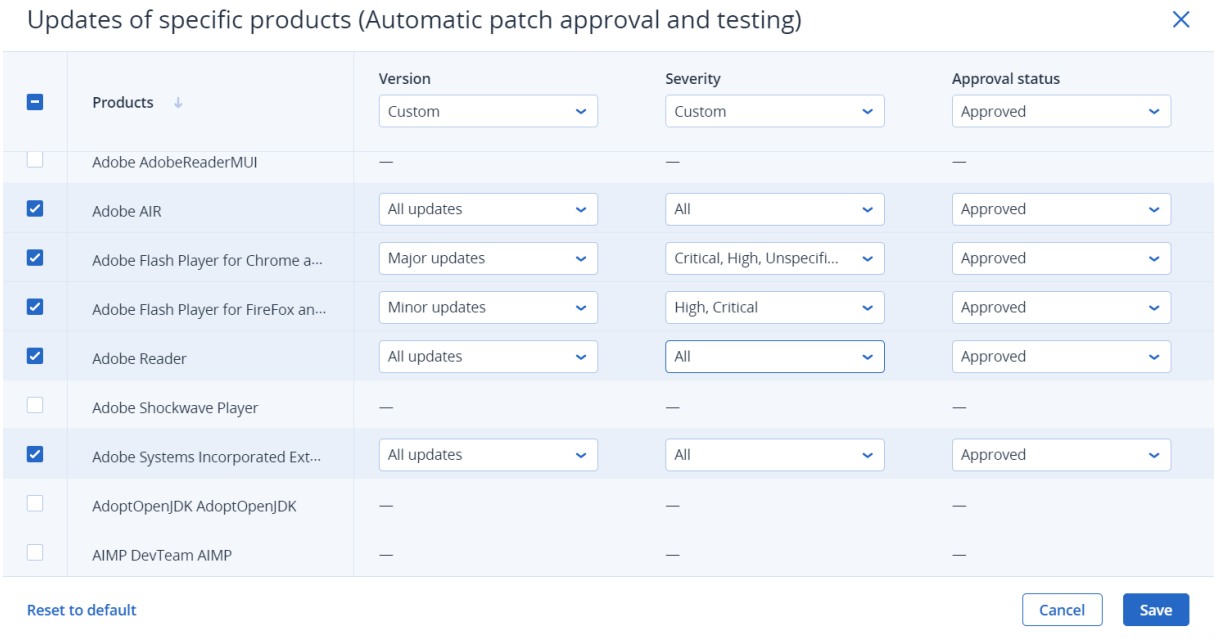
Pilih opsi instalasi:

Opsi	Deskripsi
Semua pembaruan	Gunakan opsi ini jika Anda ingin menginstal semua pembaruan yang disetujui. *
Hanya pembaruan berat	Gunakan opsi ini jika Anda ingin menginstal semua pembaruan yang disetujui.
Hanya pembaruan ringan	Gunakan opsi ini jika Anda ingin menginstal pembaruan ringan yang disetujui.
Pembaruan produk	Gunakan opsi ini jika Anda ingin menentukan pengaturan kustom

© Acronis International GmbH, 2003-2024

Opsi	Deskripsi
tertentu (Persetujuan dan pengujian patch otomatis)	untuk produk yang berbeda. Jika Anda ingin memperbarui produk tertentu, maka untuk setiap produk, Anda dapat menentukan pembaruan mana yang akan diinstal berdasarkan kategori, tingkat keparahan, atau status persetujuan. Jika Anda ingin mengonfigurasi persetujuan uji otomatis dan pengujian patch, pilih opsi ini.
Instal versi terbaru hanya untuk aplikasi yang terdeteksi rentan	Pilih kotak centang ini jika Anda ingin menginstal pembaruan terbaru hanya untuk aplikasi yang terdeteksi rentan. *

* Opsi ini memerlukan agen Cyber Protect versi 23.11.36772 atau yang lebih baru.



Untuk produk pihak ketiga Windows, patch didistribusikan secara langsung ke beban kerja yang dikelola dari basis data Acronis internal. Jika peran Updater ditugaskan ke agen, agen ini akan digunakan untuk mengunduh dan mendistribusikan patch.

Jadwal

Tentukan jadwal dan kondisi yang sesuai dengan pembaruan yang akan diinstal pada mesin yang dipilih.

Bidang	Deskripsi
Jadwalkan operasi tugas	Pengaturan ini menentukan kapan tugas akan dijalankan. Nilai berikut tersedia:

© Acronis International GmbH, 2003-2024

Bidang	Deskripsi
menggunakan peristiwa berikut	• **Jadwalkan berdasarkan waktu** – Ini adalah pengaturan default. Tugas akan berjalan sesuai waktu yang ditentukan. • **Ketika pengguna masuk ke sistem** – Secara default, akses masuk setiap pengguna akan menjalankan tugas. Anda dapat mengubah pengaturan ini agar hanya akun pengguna tertentu yang dapat memicu tugas. • **Ketika pengguna keluar dari sistem** – Secara default, akses keluar pengguna mana pun akan menjalankan tugas. Anda dapat mengubah pengaturan ini agar hanya akun pengguna tertentu yang dapat memicu tugas. **Catatan** Tugas tidak akan berjalan saat sistem dimatikan. Mematikan dan keluar adalah peristiwa berbeda di konfigurasi penjadwalan. • **Pada startup sistem** – Tugas akan berjalan saat sistem operasi dimulai. • **Pada shutdown sistem** – Tugas akan berjalan saat sistem operasi dimatikan.
Jenis jadwal	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Jadwalkan berdasarkan waktu**. Nilai berikut tersedia: • **Bulanan** – Pilih bulan dan minggu atau hari dalam sebulan saat tugas akan berjalan. • **Harian** – Ini adalah pengaturan default. Pilih hari dalam seminggu saat tugas akan dijalankan. • **Per jam** – Pilih hari dalam pekan, jumlah pengulangan, dan interval waktu tugas akan berjalan.
Mulai pada	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Jadwalkan berdasarkan waktu** Pilih waktu yang tepat kapan tugas akan dijalankan.
Konfigurasi periode pemeliharaan untuk patch	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Jadwalkan berdasarkan waktu**. Pilih pengaturan ini jika Anda ingin instalasi patch berjalan hanya selama interval waktu yang akan Anda tentukan. Jika proses instalasi patch belum selesai pada waktu berakhir yang ditentukan oleh periode pemeliharaan patch, maka proses tersebut akan dihentikan secara otomatis.
Jalankan dalam rentang tanggal	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Jadwalkan berdasarkan waktu**. Atur periode waktu ketika jadwal yang sudah dikonfigurasi akan berlaku.

© Acronis International GmbH, 2003-2024

Bidang	Deskripsi
Tentukan akun pengguna yang akses masuknya ke sistem operasi akan memulai tugas	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Saat pengguna masuk ke sistem**. Nilai berikut tersedia: • **Semua pengguna** - Gunakan opsi ini jika Anda ingin akses masuk pengguna mana pun memicu tugas. • **Pengguna berikut** - Gunakan opsi ini jika Anda hanya ingin akses masuk akun pengguna tertentu yang memicu tugas.
Tentukan akun pengguna yang logout-nya dari sistem operasi akan memulai tugas	Bidang ini muncul jika, di **Jadwalkan operasi tugas menggunakan peristiwa berikut**, Anda telah memilih **Saat pengguna keluar dari sistem**. Nilai berikut tersedia: • **Pengguna mana pun** - Gunakan opsi ini jika Anda ingin logout pengguna mana pun memicu tugas. • **Pengguna berikut** - Gunakan opsi ini jika Anda hanya ingin logout akun pengguna tertentu yang memicu tugas.
Persyaratan untuk memulai	Mendefinisikan semua kondisi yang harus dipenuhi secara bersamaan agar tugas dapat dijalankan. Kondisi awal untuk pemindaian antimalware serupa dengan kondisi awal untuk **Modul cadangan** yang dijelaskan dalam "Persyaratan untuk memulai". Anda dapat menetapkan persyaratan awal tambahan berikut: • **Distribusikan waktu mulai tugas dalam rentang waktu** – Opsi ini memungkinkan Anda menentukan jangka waktu tugas untuk menghindari kemacetan jaringan. Anda dapat menentukan penundaan dalam jam atau menit. Misalnya, jika waktu mulai default adalah pukul 10.00 dan penundaannya adalah 60 menit, tugas akan dimulai antara pukul 10.00 sampai 11.00. • **Jika mesin dimatikan, jalankan tugas yang tertinggal pada saat mesin dinyalakan** • **Cegah mode tidur atau hibernasi selama menjalankan tugas** – Opsi ini hanya berlaku untuk mesin yang menjalankan Windows. • **Jika persyaratan awal tidak terpenuhi, tetap jalankan tugas setelahnya** – Tentukan periode waktu dalam jam saat tugas akan dijalankan setelahnya, terlepas dari kondisi awal lainnya. **Catatan** Persyaratan awal tidak didukung untuk Linux.
Mulai ulang	Tentukan apakah boot ulang mesin akan dilakukan secara otomatis

© Acronis International GmbH, 2003-2024

Bidang	Deskripsi
setelah pembaruan	setelah penginstalan pembaruan selesai. Nilai berikut tersedia: • **Tidak Pernah** – Boot ulang tidak akan pernah dimulai setelah pembaruan. • **Jika diperlukan** – Boot ulang akan dimulai hanya jika diperlukan untuk menerapkan pembaruan. • **Selalu** – Boot ulang akan selalu dimulai setelah pembaruan. Anda dapat menentukan penundaan boot ulang.
Jangan boot ulang hingga pencadangan selesai	Jika Anda memilih opsi ini, dan proses pencadangan sedang berjalan, boot ulang mesin akan ditunda hingga pencadangan selesai.

Pencadangan prapembaruan

Jalankan pencadangan sebelum menginstal pembaruan perangkat lunak – sistem akan membuat pencadangan bertahap dari suatu mesin sebelum menginstal pembaruan apa pun pada mesin tersebut. Jika tidak ada cadangan yang dibuat sebelumnya, maka cadangan penuh dari suatu mesin akan dibuat. Hal ini memungkinkan Anda untuk mencegah kasus kegagalan instalasi pembaruan dan Anda harus kembali ke keadaan sebelumnya. Agar opsi **Pencadangan prapembaruan** dapat berfungsi, mesin yang terkait harus memiliki manajemen patch dan modul pencadangan yang aktif dalam rencana proteksi dan item untuk dicadangkan – keseluruhan mesin atau volume boot+sistem. Jika Anda memilih item yang tidak sesuai untuk dicadangkan, maka sistem tidak akan mengizinkan Anda untuk mengaktifkan opsi **Pencadangan prapembaruan**.

Melihat daftar patch yang tersedia

Setelah pemindaian penilaian kerentanan selesai, Anda dapat melihat informasi tentang patch yang tersedia di **Manajemen perangkat lunak** > **Patch**.

Untuk melihat perincian tentang patch tertentu, dalam daftar patch, klik patch yang sesuai.

Tabel berikut menjelaskan informasi patch yang dapat Anda lihat di layar.

Bidang	Deskripsi
Status persetujuan	Status persetujuan terutama diperlukan untuk skenario persetujuan otomatis. Anda dapat menentukan salah satu status berikut untuk patch: • **Disetujui** – patch diinstal setidaknya pada satu mesin dan divalidasi sebagai ok • **Ditolak** – patch tidak aman dan dapat merusak sistem mesin • **Menunggu persetujuan** – status patch tidak jelas dan harus divalidasi
Perjanjian	• Disetujui

© Acronis International GmbH, 2003-2024

lisensi	• Tidak disetujui. Jika Anda tidak menyetujui perjanjian lisensi, status patch menjadi **Ditolak** dan tidak akan diinstal
Tingkat keparahan	Tingkat keparahan patch: • **Kritis** • **Tinggi** • **Sedang** • **Rendah** • **Tidak ada**
Penjual	Vendor patch
Produk yang terpengaruh	Produk di mana patch dapat diterapkan
Versi yang diinstal	Versi produk yang sudah diinstal
Versi	Versi patch
Kategori	Kategori patch: • **Pembaruan penting** – perbaikan yang dirilis secara luas untuk masalah spesifik guna menangani bug kritis dan tidak terkait keamanan. • **Pembaruan keamanan** – perbaikan yang dirilis secara luas untuk produk spesifik guna menangani masalah keamanan. • **Pembaruan definisi** – pembaruan untuk virus atau file definisi lainnya. • **Rollup pembaruan** – set kumulatif hotfix, pembaruan keamanan, pembaruan penting, dan pembaruan yang digabungkan untuk kemudahan penyebaran. Rollup biasanya menargetkan aspek tertentu, seperti keamanan, atau komponen tertentu, seperti Layanan Informasi Internet (IIS). • **Service pack** – set kumulatif semua hotfix, pembaruan keamanan, pembaruan penting, dan pembaruan yang dibuat sejak rilis produk. Service pack mungkin juga berisi perubahan desain atau fitur dalam jumlah terbatas yang diminta pelanggan. • **Alat** – utilitas atau fitur yang membantu pelaksanaan tugas atau sekumpulan tugas. • **Paket fitur** – rilis fitur baru, biasanya dilanjutkan ke produk pada rilis berikutnya. • **Pembaruan** – perbaikan yang dirilis secara luas untuk masalah spesifik guna menangani bug non-kritis dan tidak terkait keamanan. • **Aplikasi** – memasang patch untuk aplikasi.
Tanggal rilis	Tanggal saat patch dirilis
Terakhir dilaporkan	Tanggal terakhir kali patch dilaporkan
Pertama kali dipasang	Tanggal instalasi patch pertama yang berhasil pada mesin
Microsoft KB	Jika patch ditujukan untuk produk Microsoft, bidang tersebut menampilkan ID artikel KB

© Acronis International GmbH, 2003-2024

Mesin	Jumlah mesin yang terdampak
Kerentanan	Jumlah kerentanan. Jika mengeklik jumlah kerentanan, Anda akan diarahkan ke daftar kerentanan.
Ukuran	Ukuran rata-rata patch
Bahasa	Bahasa yang didukung patch
Situs vendor	Situs resmi vendor

Mengonfigurasi masa pakai patch dalam daftar

Anda dapat terus memperbarui daftar patch dengan mengonfigurasi masa pakai patch dalam daftar di layar **Patch**. Pengaturan ini menentukan berapa lama patch terdeteksi yang tersedia akan terlihat di daftar patch. Patch akan dihapus dari daftar setelah berhasil diinstal pada semua mesin yang diindikasikan hilang, atau setelah masa pakai dalam daftar berlalu.

Untuk mengonfigurasi masa pakai patch dalam daftar

1. Di konsol Cyber Protect, buka **Manajemen perangkat lunak** > **Patch**.
2. Klik **Pengaturan**.
3. Di **Masa pakai dalam daftar**, pilih opsi yang sesuai.

Opsi	Deskripsi
Selamanya	Patch akan selalu ada dalam daftar.
7 hari	Patch akan dihapus dari daftar tujuh hari setelah instalasi pertama. Sebagai contoh, mari kita asumsikan bahwa Anda memiliki dua mesin yang patchnya harus diinstal. Salah satunya sedang online, dan yang lainnya offline. Patch diinstal di mesin pertama. Setelah 7 hari, patch akan dihapus dari daftar patch, meskipun tidak diinstal pada mesin kedua (karena sedang offline).
30 hari	Patch akan dihapus dari daftar 30 hari setelah instalasi pertama.

Persetujuan patch otomatis

Persetujuan patch otomatis mempermudah proses instalasi pembaruan pada mesin. Dengan persetujuan patch otomatis, instalasi patch tidak tertunda oleh proses persetujuan patch manual. Pembaruan dan perbaikan penting diinstal lebih cepat, sehingga keandalan sistem Anda pun semakin tinggi.

Anda dapat menggunakan persetujuan patch otomatis dalam skenario uji untuk instalasi patch otomatis. Jika patch berhasil diinstal pada mesin uji, patch tersebut juga akan diinstal secara otomatis pada mesin produksi. Untuk informasi selengkapnya tentang skenario ini, lihat "Kasus penggunaan untuk persetujuan dan pengujian patch otomatis" (hlm. 968).

© Acronis International GmbH, 2003-2024

Anda juga dapat menggunakan persetujuan patch otomatis dalam skenario instalasi patch otomatis di lingkungan produksi, sehingga tidak perlu mengikuti fase pengujian. Untuk informasi selengkapnya tentang skenario ini, lihat "Kasus penggunaan untuk persetujuan patch otomatis tanpa pengujian" (hlm. 971).

Mengonfigurasi persetujuan patch otomatis

Anda dapat mengonfigurasi persetujuan patch otomatis dan memastikan bahwa instalasi patch tidak tertunda karena proses persetujuan patch manual.

Untuk mengonfigurasi persetujuan patch otomatis

1. Di konsol Cyber Protect, buka **Manajemen perangkat lunak** > **Patch**.
2. Klik **Pengaturan**.
3. Aktifkan **Persetujuan patch otomatis**.
4. Konfigurasikan pengaturan untuk persetujuan patch otomatis.
   a. Pilih opsi persetujuan patch otomatis.

Opsi	Deskripsi
Persetujuan dan pengujian patch otomatis	Status persetujuan patch akan berubah menjadi **Disetujui** bila jumlah hari yang dipilih telah berlalu setelah instalasi patch berhasil. Anda sebaiknya menggunakan pengaturan ini jika Anda ingin menguji patch dengan menginstalnya pada mesin uji terlebih dahulu, memastikan semuanya berfungsi sesuai harapan, lalu menginstal patch di lingkungan produksi Anda.
Persetujuan patch otomatis tanpa pengujian	Status persetujuan patch akan berubah menjadi **Disetujui** bila jumlah hari yang dipilih telah berlalu sejak patch ditemukan.

   b. Pilih jumlah hari yang harus dilewati setelah kondisi dari opsi persetujuan patch otomatis terpenuhi. Setelah jangka waktu ini, status persetujuan patch akan otomatis berubah dari **Menunggu persetujuan** menjadi **Disetujui**.
5. Pilih **Secara otomatis menerima perjanjian lisensi**.
6. Klik **Terapkan**.

Kasus penggunaan untuk persetujuan dan pengujian patch otomatis

Jika Anda ingin menguji patch baru pada mesin uji sebelum menginstalnya pada mesin produksi, Anda dapat mengonfigurasi dua rencana proteksi - rencana instalasi patch untuk tujuan uji, dan rencana instalasi patch yang diuji pada mesin produksi. Dengan demikian, Anda akan memastikan bahwa patch yang Anda instal di lingkungan produksi Anda aman dan mesin produksi Anda berfungsi dengan benar setelah instalasi patch.

Kasus penggunaan terdiri dari tahap berikut:

© Acronis International GmbH, 2003-2024

1. Konfigurasikan pengaturan untuk Persetujuan patch otomatis. Pilih opsi **Persetujuan dan pengujian patch otomatis**. Untuk informasi lebih lanjut, lihat "Mengonfigurasi persetujuan patch otomatis" (hlm. 968).
2. Konfigurasikan rencana proteksi untuk tujuan uji (misalnya, 'Uji proses patch') dengan modul **Manajemen patch** yang diaktifkan dan terapkan hal tersebut pada mesin di lingkungan uji. Tentukan kondisi instalasi patch berikut: status persetujuan patch harus **Menunggu persetujuan**. Langkah ini diperlukan untuk memvalidasi patch dan memeriksa apakah mesin bekerja dengan benar setelah instalasi patch. Untuk informasi lebih lanjut, lihat "Mengonfigurasi rencana proteksi pada proses patch Uji" (hlm. 969).
3. Konfigurasikan rencana proteksi untuk lingkungan produksi (misalnya, 'Patch produksi') dengan modul **Manajemen patch** yang diaktifkan dan terapkan pada mesin di lingkungan produksi. Tentukan kondisi instalasi patch berikut: status persetujuan patch harus **Disetujui**. Untuk informasi lebih lanjut, lihat "Mengonfigurasi rencana proteksi patch Produksi" (hlm. 970).
4. Jalankan Rencana patch uji dan periksa hasilnya. Biarkan status persetujuan mesin yang tidak mengalami masalah sebagai **Menunggu persetujuan**, namun ubah status persetujuan mesin yang tidak berfungsi dengan benar menjadi **Ditolak**. Sesuai dengan jumlah hari yang ditetapkan dalam pengaturan **Persetujuan patch otomatis**, status patch akan otomatis berubah dari **Menunggu persetujuan** menjadi **Disetujui**. Saat Anda menjalankan rencana patch Produksi, hanya patch **Disetujui** yang akan diinstal pada mesin produksi. Untuk informasi lebih lanjut, lihat "Menjalankan Rencana proteksi patch uji dan menolak patch yang tidak aman" (hlm. 971).
5. Jalankan Rencana patch produksi.

Mengonfigurasi rencana proteksi pada proses patch Uji

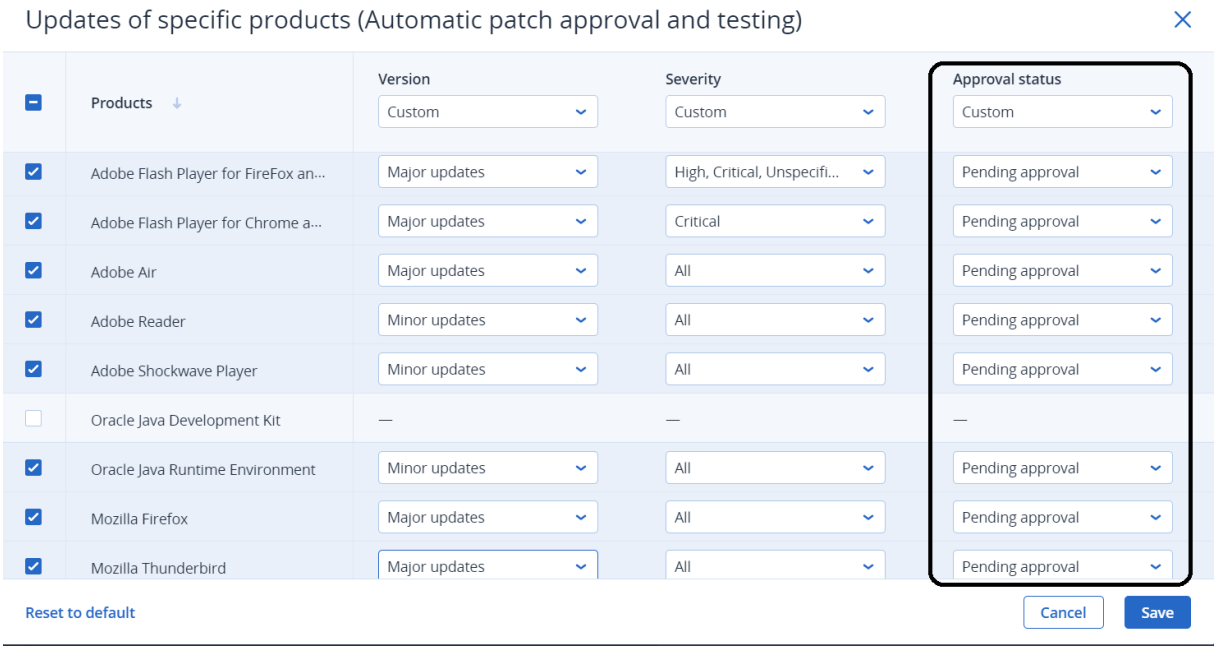
Anda dapat mengonfigurasi rencana proteksi dengan pengaturan instalasi patch untuk mesin Anda di lingkungan uji.

Untuk mengonfigurasi rencana proteksi pada proses patch Uji

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana proteksi**.
2. Klik **Buat rencana**.
3. Aktifkan modul **Manajemen patch**.
4. Tentukan pembaruan mana yang akan diinstal untuk Microsoft dan produk pihak ketiga, jadwal, dan cadangan pra-pembaruan. Untuk perincian lebih lanjut tentang pengaturan ini, lihat "Pengaturan manajemen patch dalam rencana proteksi" (hlm. 960).

Penting
Agar semua produk diperbarui, pilih status persetujuan **Menunggu persetujuan**. Oleh karenanya, agen hanya akan menginstal patch **Menunggu persetujuan** pada mesin yang dipilih di lingkungan uji.

© Acronis International GmbH, 2003-2024



Mengonfigurasi rencana proteksi patch Produksi

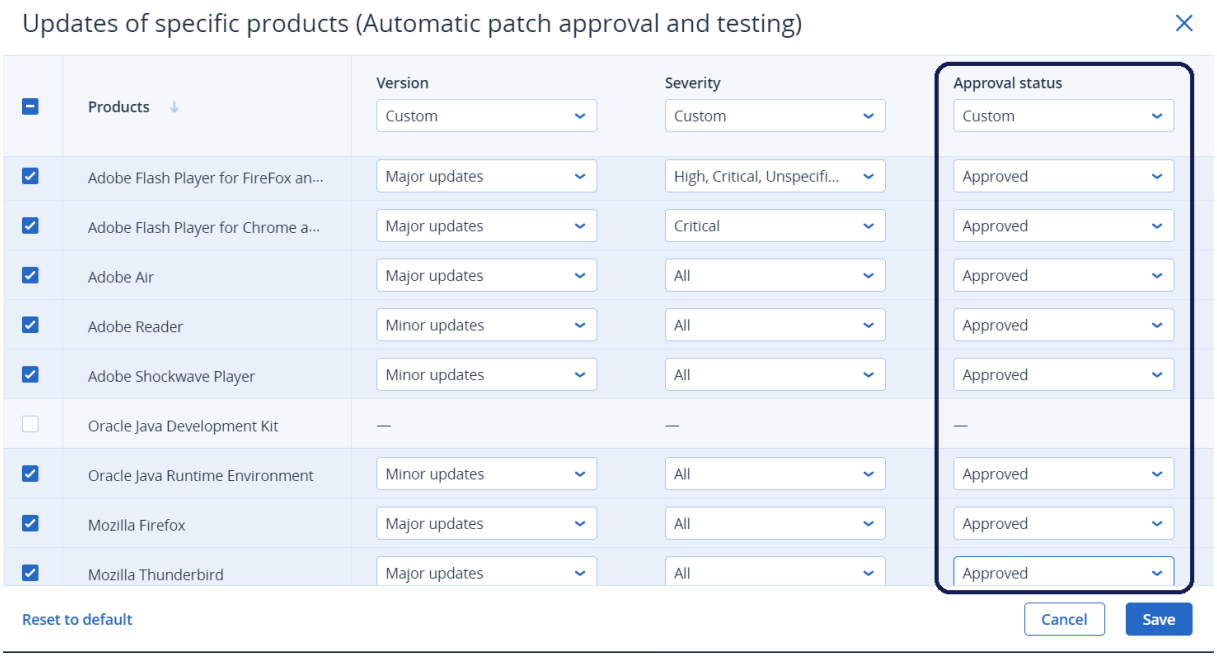
Anda dapat mengonfigurasi rencana proteksi dengan pengaturan instalasi patch untuk mesin Anda di lingkungan produksi.

Untuk mengonfigurasi rencana proteksi pada proses patch Produksi

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana proteksi**.
2. Klik **Buat rencana**.
3. Aktifkan modul **Manajemen patch**.
4. Tentukan pembaruan mana yang akan diinstal untuk Microsoft dan produk pihak ketiga, jadwal, dan cadangan pra-pembaruan. Untuk perincian lebih lanjut tentang pengaturan ini, lihat "Pengaturan manajemen patch dalam rencana proteksi" (hlm. 960).

Penting
Agar semua produk diperbarui, atur **Status persetujuan** ke **Disetujui**. Oleh karenanya, agen hanya akan menginstal patch **Disetujui** pada mesin yang dipilih di lingkungan produksi.

© Acronis International GmbH, 2003-2024



Menjalankan Rencana proteksi patch uji dan menolak patch yang tidak aman

Setelah patch diinstal pada mesin di lingkungan uji Anda, Anda dapat memeriksa apakah semuanya berfungsi sesuai harapan. Anda dapat membiarkan status persetujuan mesin yang tidak mengalami masalah sebagai **Menunggu persetujuan**, namun mengubah status persetujuan mesin yang tidak berfungsi dengan benar menjadi **Ditolak**.

Untuk menjalankan Rencana proteksi uji patch dan menolak patch yang tidak aman

1. Jalankan Rencana proteksi uji patch (sesuai jadwal atau secara manual).
2. Tergantung pada hasilnya, lihat patch terinstal mana yang aman.
3. Buka **Manajemen perangkat lunak** > **Patch** dan setel **Status persetujuan** ke **Ditolak** untuk patch yang tidak aman.

Kasus penggunaan untuk persetujuan patch otomatis tanpa pengujian

Jika Anda ingin menginstal patch baru secara otomatis pada mesin produksi Anda sesegera mungkin, tanpa menginstalnya pada mesin uji terlebih dahulu, Anda hanya dapat mengonfigurasi satu rencana proteksi.

Kasus penggunaan terdiri dari tahap berikut:

1. Konfigurasikan pengaturan untuk Persetujuan patch otomatis. Pilih opsi **Persetujuan patch otomatis tanpa pengujian**. Untuk informasi lebih lanjut, lihat "Mengonfigurasi persetujuan patch otomatis" (hlm. 968).
2. Konfigurasikan rencana proteksi untuk lingkungan produksi (misalnya, 'Patch produksi') dengan modul **Manajemen patch** yang diaktifkan dan terapkan pada mesin di lingkungan produksi. Tentukan kondisi instalasi patch berikut: status persetujuan patch harus **Disetujui**. Untuk

© Acronis International GmbH, 2003-2024

informasi lebih lanjut, lihat "Mengonfigurasi rencana proteksi patch Produksi" (hlm. 970).

3. Jalankan Rencana patch produksi.

Menyetujui patch secara manual

Anda dapat menyetujui patch secara manual dan mempercepat instalasinya tanpa mengikuti fase pengujian.

Prasyarat

- Rencana proteksi yang mengaktifkan modul **Manajemen patch** diterapkan pada setidaknya satu mesin Windows.
- Ada patch yang masih belum diinstal pada satu atau beberapa mesin yang menerapkan rencana proteksi.

Untuk menyetujui patch secara manual

1. Di konsol Cyber Protect, buka **Manajemen perangkat lunak** > **Patch**.
2. Pilih patch yang ingin Anda instal, lalu terima perjanjian lisensinya.
3. Tetapkan **Status persetujuan** patch ke **Disetujui**.
   Status persetujuan patch ditetapkan ke **Disetujui**. Patch akan diinstal secara otomatis pada mesin berdasarkan jadwal yang ditentukan dalam rencana proteksi. Jika Anda ingin segera menginstal patch, ikuti prosedur yang dijelaskan di "Menginstal patch sesuai permintaan" (hlm. 972).

Menginstal patch sesuai permintaan

Anda dapat menginstal patch secara manual sesuai permintaan ketika Anda tidak ingin menunggu waktu instalasi yang dijadwalkan.

Anda dapat memulai instalasi patch manual dari tiga layar: **Patch**, **Kerentanan**, dan **Semua perangkat**.

Untuk menginstal patch secara manual

Dari Patch

1. Di konsol Cyber Protect, buka **Manajemen perangkat lunak** > **Patch**.
2. Terima perjanjian lisensi untuk patch yang ingin Anda instal.
3. Dalam wizard **Instal patch**, pilih patch yang ingin Anda instal, lalu klik **Instal**.
4. Pilih beberapa mesin tempat Anda ingin menginstal patch.
5. Pilih opsi boot ulang.

© Acronis International GmbH, 2003-2024

a. Pilih apakah Anda ingin mesin di-boot ulang setelah patch diinstal.

Opsi	Deskripsi
Tidak	Mesin tidak akan di-boot ulang secara otomatis setelah patch diinstal.
Jika diperlukan	Mesin akan di-boot ulang hanya jika diperlukan untuk menerapkan patch.
Ya	Mesin akan di-boot ulang secara otomatis setelah patch diinstal. Anda juga dapat menentukan penundaan boot ulang.

b. [Opsional] Jika Anda ingin menunda boot ulang mesin saat pencadangan mesin sedang berlangsung, pilih **Jangan boot ulang hingga pencadangan selesai**.

6. Klik **Instal patch**.

Dari Kerentanan

1. Di konsol Cyber Protect, buka **Manajemen perangkat lunak** > **Kerentanan**.
2. Lakukan proses remediasi seperti dijelaskan pada "Mengelola kerentanan yang ditemukan" (hlm. 957).

Dari Semua perangkat

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih mesin tempat Anda ingin menginstal patch.
3. Klik **Patch**.
4. Pilih patch yang ingin Anda instal, lalu klik **Berikutnya**.
5. Pilih opsi boot ulang.
   a. Pilih apakah Anda ingin mesin di-boot ulang setelah patch diinstal.

Opsi	Deskripsi
Tidak	Mesin tidak akan di-boot ulang secara otomatis setelah patch diinstal.
Jika diperlukan	Mesin akan di-boot ulang hanya jika diperlukan untuk menerapkan patch.
Ya	Mesin akan di-boot ulang secara otomatis setelah patch diinstal. Anda juga dapat menentukan penundaan boot ulang.

   b. [Opsional] Jika Anda ingin menunda boot ulang mesin saat pencadangan mesin sedang berlangsung, pilih **Jangan boot ulang hingga pencadangan selesai**.
6. Klik **Instal patch**.

© Acronis International GmbH, 2003-2024

Mengelola inventaris perangkat keras dan perangkat lunak Anda

Inventaris perangkat lunak

Fitur inventaris perangkat lunak tersedia untuk perangkat yang mengaktifkan paket Tingkat Lanjut, atau yang memiliki lisensi Cyber Protect (Lama). Fitur ini memungkinkan Anda untuk menampilkan semua aplikasi perangkat lunak yang diinstal pada semua perangkat Windows dan macOS.

Untuk mendapatkan data inventaris perangkat lunak, Anda dapat menjalankan pemindaian otomatis atau manual pada perangkat.

Anda dapat menggunakan data inventaris perangkat lunak untuk:

- menjelajahi dan membandingkan informasi tentang semua aplikasi yang diinstal pada perangkat perusahaan
- menentukan apakah aplikasi perlu diperbarui
- menentukan apakah aplikasi yang tidak digunakan perlu dihapus
- memastikan versi perangkat lunak pada beberapa perangkat perusahaan sama
- memantau perubahan dalam status perangkat lunak antara pemindaian yang berurutan.

Mengaktifkan pemindaian inventaris perangkat lunak

Ketika pemindaian inventaris perangkat lunak diaktifkan pada perangkat, sistem secara otomatis mengumpulkan data perangkat lunak setiap 12 jam.

Fitur pemindaian inventaris Perangkat Lunak diaktifkan secara default untuk semua perangkat dengan lisensi yang diperlukan, tetapi Anda dapat mengubah pengaturan tersebut bila perlu.

Catatan
Penyewa pelanggan dapat mengaktifkan atau menonaktifkan pemindaian inventaris perangkat lunak. Penyewa unit hanya dapat melihat pengaturan pemindaian inventaris perangkat lunak, tetapi tidak dapat mengubahnya.

Untuk mengaktifkan pemindaian inventaris perangkat lunak

1. Di konsol Cyber Protect, buka **Pengaturan**.
2. Klik **Perlindungan**.
3. Klik **Pemindaian inventaris**.
4. Aktifkan modul **Pemindaian inventaris perangkat lunak** dengan mengeklik switch di sebelah nama modul.

Untuk menonaktifkan pemindaian inventaris perangkat lunak

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Pengaturan**.
2. Klik **Perlindungan**.
3. Klik **Pemindaian inventaris**.
4. Nonaktifkan modul **Pemindaian inventaris perangkat lunak** dengan mengeklik switch di sebelah nama modul.

Menjalankan pemindaian inventaris perangkat lunak secara manual

Anda dapat menjalankan pemindaian inventaris perangkat lunak secara manual dari layar **Inventaris perangkat lunak**, atau dari tab **Perangkat Lunak** di layar **Inventaris**.

Prasyarat

- Perangkat menggunakan sistem operasi Windows atau macOS.
- Perangkat memiliki lisensi Cyber Protect (Lama) yang diperlukan atau memiliki paket Manajemen Tingkat Lanjut yang aktif.

Untuk menjalankan pemindaian inventaris perangkat lunak dari layar Inventaris perangkat lunak

1. Di konsol Cyber Protect, buka **Manajemen perangkat lunak**.
2. Klik **Inventaris perangkat lunak**.
3. Di bidang drop-down **Kelompokkan berdasarkan:** , pilih **Perangkat**.
4. Temukan perangkat yang ingin Anda pindai, dan klik **Pindai sekarang**.

Untuk menjalankan pemindaian inventaris perangkat lunak dari tab Perangkat Lunak di layar Inventaris

1. Di konsol Cyber Protect, buka **Perangkat**.
2. Klik perangkat yang ingin Anda pindai, dan klik **Inventaris**.
3. Di tab **Perangkat Lunak**, klik **Pindai sekarang**.

Menjelajahi inventaris perangkat lunak

Anda dapat menampilkan dan menelusuri data untuk semua aplikasi perangkat lunak yang tersedia pada semua perangkat perusahaan.

Prasyarat

- Perangkat menggunakan sistem operasi Windows atau macOS.
- Perangkat memiliki lisensi Cyber Protect (Lama) yang diperlukan atau memiliki paket Manajemen Tingkat Lanjut yang aktif.
- Pemindaian inventaris perangkat lunak pada perangkat berhasil diselesaikan.

© Acronis International GmbH, 2003-2024

Untuk menampilkan semua aplikasi perangkat lunak yang tersedia di semua perangkat perusahaan Windows dan macOS

1. Di konsol Cyber Protect, buka **Manajemen Perangkat Lunak**.
2. Klik **Inventaris perangkat lunak**.

   Secara default, data dikelompokkan berdasarkan perangkat. Tabel berikut menjelaskan data yang terlihat di layar **Inventaris perangkat lunak**.

Kolom	Deskripsi
Nama	Nama aplikasi.
Versi	Versi aplikasi.
Status	Status aplikasi. • **Baru**. • **Diperbarui**. • **Dihapus**. • **Tidak Ada Perubahan**.
Penjual	Vendor aplikasi.
Tanggal diinstal	Tanggal dan waktu saat aplikasi diinstal.
Dijalankan terakhir	Hanya untuk perangkat macOS. Tanggal dan waktu saat aplikasi terakhir kali aktif.
Lokasi	Direktori tempat aplikasi diinstal.
Pengguna	Pengguna yang menginstal aplikasi.
Jenis sistem	Hanya untuk perangkat Windows. Jenis aplikasi bit. • **X86** untuk aplikasi 32-bit. • **X64** untuk aplikasi 64-bit.

3. Untuk mengelompokkan data berdasarkan aplikasi, di bidang drop-down **Kelompokkan berdasarkan:**, pilih **Aplikasi**.
4. Untuk mempersempit informasi yang ditampilkan pada layar, gunakan satu atau kombinasi filter.
   a. Klik **Filter**.
   b. Pilih satu atau kombinasi dari beberapa filter.

      Tabel berikut menjelaskan filter pada layar **Inventaris perangkat lunak**.

Filter	Deskripsi
Nama Perangkat	Nama perangkat. Pilihan ganda memungkinkan. Gunakan filter ini jika Anda ingin membandingkan perangkat lunak pada perangkat tertentu.

© Acronis International GmbH, 2003-2024

Filter	Deskripsi
Aplikasi	Nama aplikasi. Pilihan ganda memungkinkan. Gunakan filter ini jika Anda ingin membandingkan data untuk aplikasi tertentu pada perangkat tertentu atau pada semua perangkat.
Penjual	Vendor aplikasi. Pilihan ganda memungkinkan. Gunakan filter ini jika Anda ingin menampilkan semua aplikasi dari vendor tertentu pada perangkat tertentu atau pada semua perangkat.
Status	Status aplikasi. Pilihan ganda memungkinkan. Gunakan filter ini jika Anda ingin menampilkan semua aplikasi dalam status yang dipilih pada perangkat tertentu atau pada semua perangkat.
Tanggal diinstal	Tanggal saat aplikasi diinstal. Gunakan filter ini jika Anda ingin menampilkan semua aplikasi yang diinstal di tanggal tertentu pada perangkat tertentu atau pada semua perangkat.
Tanggal pemindaian	Tanggal pemindaian inventaris perangkat lunak. Gunakan filter ini jika Anda ingin menampilkan informasi tentang perangkat lunak pada perangkat tertentu atau pada semua perangkat yang dipindai pada tanggal tersebut.

c. Klik **Terapkan**.

5. Untuk menjelajahi seluruh daftar inventaris perangkat lunak, gunakan penomoran halaman di bagian kiri bawah layar.

- Klik nomor halaman yang ingin Anda buka.
- Di bidang drop-down, pilih nomor halaman dari halaman yang ingin Anda buka.

Menampilkan inventaris perangkat lunak dari satu perangkat

Anda dapat menampilkan daftar semua aplikasi perangkat lunak yang diinstal pada satu perangkat, serta informasi terperinci tentang aplikasi tersebut, seperti status, versi, vendor, tanggal penginstalan, dijalankan terakhir, dan lokasi.

Prasyarat

- Perangkat menggunakan sistem operasi Windows atau macOS.
- Perangkat memiliki lisensi Cyber Protect (Lama) yang diperlukan atau memiliki paket Manajemen Tingkat Lanjut yang aktif.
- Pemindaian inventaris perangkat lunak pada perangkat berhasil diselesaikan.

© Acronis International GmbH, 2003-2024

Untuk menampilkan inventaris perangkat lunak dari satu perangkat dari layar Inventaris Perangkat Lunak

1. Di konsol Cyber Protect, buka **Manajemen perangkat lunak**.
2. Klik **Inventaris perangkat lunak**.
3. Di bidang drop-down **Kelompokkan berdasarkan:** , pilih **Perangkat**.
4. Temukan perangkat yang ingin Anda periksa menggunakan salah satu opsi berikut.
   - Temukan perangkat menggunakan **Filter**:
     a. Klik **Filter**.
     b. Di bidang **Nama perangkat** , pilih nama perangkat yang ingin Anda tampilkan.
     c. Klik **Terapkan**.
   - Temukan perangkat menggunakan **Pencarian** dinamis:
     a. Klik **Pencarian**.
     b. Ketik nama lengkap perangkat atau sebagian dari nama perangkat.

Untuk melihat inventaris perangkat lunak dari satu perangkat dari layar Perangkat Lunak

1. Di konsol Cyber Protect, buka **Perangkat**.
2. Klik perangkat yang ingin Anda tampilkan, dan klik **Inventaris**.
3. Klik tab **Perangkat Lunak**.

Inventaris perangkat keras

Fitur inventaris perangkat keras memungkinkan Anda untuk melihat semua komponen perangkat keras yang tersedia di:

- perangkat fisik Windows dan macOS dengan lisensi yang mendukung fitur inventaris Perangkat Keras.
- mesin virtual Windows dan macOS yang berjalan pada platform virtualisasi berikut: VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo, dan Virtuozzo Hybrid Infrastructure. Untuk informasi lebih lanjut tentang versi yang didukung dari platform virtualisasi, lihat "Platform virtualisasi yang didukung" (hlm. 32).

Catatan
Fitur inventaris Perangkat Keras untuk mesin virtual tidak didukung di Cyber Protect edisi legasi.

Fitur inventaris perangkat keras hanya didukung untuk perangkat yang menginstal agen perlindungan.

Untuk mendapatkan data inventaris perangkat keras, Anda dapat menjalankan pemindaian otomatis atau manual pada perangkat.

Anda dapat menggunakan data inventaris perangkat keras untuk:

© Acronis International GmbH, 2003-2024

- menemukan semua aset perangkat keras organisasi
- menjelajahi inventaris perangkat keras dari semua perangkat di organisasi Anda
- membandingkan komponen perangkat keras pada beberapa perangkat perusahaan
- menampilkan informasi terperinci tentang komponen perangkat keras.

Mengaktifkan pemindaian inventaris perangkat keras

Jika pemindaian inventaris perangkat keras diaktifkan pada perangkat fisik dan mesin virtual, sistem secara otomatis mengumpulkan data perangkat keras setiap 12 jam.

Fitur pemindaian inventaris perangkat keras diaktifkan secara default, tetapi Anda dapat mengubah pengaturan tersebut bila perlu.

Catatan
Penyewa pelanggan dapat mengaktifkan atau menonaktifkan pemindaian inventaris perangkat keras. Penyewa unit hanya dapat melihat pengaturan pemindaian inventaris perangkat keras, tetapi tidak dapat mengubahnya.

Untuk mengaktifkan pemindaian inventaris perangkat keras

1. Di konsol Cyber Protect, buka **Pengaturan**.
2. Klik **Perlindungan**.
3. Klik **Pemindaian inventaris**.
4. Aktifkan modul **Pemindaian inventaris perangkat keras** dengan mengeklik switch di sebelah nama modul.

Untuk menonaktifkan pemindaian inventaris perangkat keras

1. Di konsol Cyber Protect, buka **Pengaturan**.
2. Klik **Perlindungan**.
3. Klik **Pemindaian inventaris**.
4. Nonaktifkan modul **Pemindaian inventaris perangkat keras** dengan mengeklik switch di sebelah nama modul.

Menjalankan pemindaian inventaris perangkat keras secara manual

Anda dapat menjalankan pemindaian inventaris perangkat keras untuk satu perangkat secara manual, dan melihat data terkini untuk komponen perangkat keras dari perangkat tersebut.

© Acronis International GmbH, 2003-2024

Catatan
Pemindaian inventaris perangkat keras mesin virtual hanya didukung jika tanggal dan waktu saat ini dari mesin virtual sesuai dengan tanggal dan waktu saat ini dalam UTC. Untuk memastikan bahwa mesin virtual menggunakan pengaturan waktu yang benar, nonaktifkan opsi **Sinkronisasi waktu** dari mesin virtual, atur tanggal, waktu, dan zona waktu saat ini, lalu mulai ulang **Acronis Agent Core Service** dan **Acronis Managed Machine Service**.

Prasyarat

- (Untuk semua perangkat) Perangkat menggunakan sistem operasi Windows atau macOS.
- (Untuk semua perangkat) Perangkat memiliki lisensi yang mendukung fitur inventaris Perangkat Keras. Perhatikan bahwa fitur inventaris Perangkat Keras untuk mesin virtual tidak didukung di edisi Cyber Protect (Lama).
- (Untuk semua perangkat) Agen perlindungan diinstal di perangkat.
- (Untuk mesin virtual) Mesin berjalan pada salah satu platform virtualisasi yang didukung. Untuk informasi lebih lanjut, lihat "Inventaris perangkat keras" (hlm. 978).

Untuk menjalankan pemindaian inventaris perangkat keras pada satu perangkat

1. Di konsol Cyber Protect, buka **Perangkat**.
2. Klik perangkat yang ingin Anda pindai, dan klik **Inventaris**.
3. Di tab **Perangkat keras**, klik **Pindai sekarang**.

Menjelajahi inventaris perangkat keras

Anda dapat menampilkan dan menjelajahi data untuk semua komponen perangkat keras yang tersedia pada semua perangkat perusahaan.

Prasyarat

- (Untuk semua perangkat) Perangkat menggunakan sistem operasi Windows atau macOS.
- (Untuk semua perangkat) Perangkat memiliki lisensi yang mendukung fitur inventaris Perangkat Keras. Perhatikan bahwa fitur inventaris Perangkat Keras untuk mesin virtual tidak didukung di Cyber Protect edisi legasi.
- (Untuk semua perangkat) Agen perlindungan diinstal di perangkat.
- (Untuk semua perangkat) Pemindaian inventaris perangkat keras pada perangkat telah berhasil diselesaikan.
- (Untuk mesin virtual) Mesin berjalan pada salah satu platform virtualisasi yang didukung. Untuk informasi lebih lanjut, lihat "Inventaris perangkat keras" (hlm. 978).

Untuk melihat semua komponen perangkat keras yang tersedia di perangkat perusahaan Windows dan macOS

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Perangkat**.
2. Di bidang drop-down **Tampilan:**, pilih **Perangkat keras**.

Catatan
Tampilan adalah sekumpulan kolom yang menentukan data mana yang terlihat di layar. Tampilan yang ditetapkan adalah **Standar** dan **Perangkat keras**. Anda dapat membuat dan menyimpan tampilan kustom yang mencakup kumpulan kolom yang berbeda, dan lebih nyaman untuk kebutuhan Anda.

Tabel berikut menjelaskan data yang terlihat pada tampilan **Perangkat keras**.

Kolom	Deskripsi
Nama	Nama perangkat.
Status pemindaian perangkat keras	Status pemindaian perangkat keras. • **Selesai**. • **Belum mulai**. • **Tidak didukung**. status ditampilkan untuk beban kerja yang fungsi inventaris perangkat kerasnya tidak didukung, yaitu mesin virtual, perangkat seluler, perangkat Linux. • **Perbarui agen**. ditampilkan jika versi agen yang kedaluwarsa terinstal pada perangkat. Mengeklik tindakan ini akan mengarahkan ke halaman Pengaturan> Agen, di mana admin dapat melakukan pembaruan agen. • **Tingkatkan kuota**. Mengekliknya akan membuka dialog di mana admin dapat mengalihkan lisensi saat ini ke salah satu lisensi penyewa lain yang tersedia
Prosesor	Model semua prosesor perangkat.
Inti prosesor	Jumlah inti dari semua prosesor perangkat.
Penyimpanan disk	Penyimpanan yang digunakan, dan penyimpanan total dari semua disk perangkat.
Memori	Kapasitas RAM total dari perangkat.
Tanggal pemindaian	Tanggal dan waktu pemindaian inventaris perangkat keras terakhir.
Motherboard	Motherboard perangkat.
Nomor seri motherboard	Nomor seri motherboard.
Versi BIOS	Versi BIOS sistem.

© Acronis International GmbH, 2003-2024

Kolom	Deskripsi
Organisasi	Organisasi tempat perangkat berada.
Pemilik	Pemilik perangkat.
Domain	Domain perangkat.
Sistem operasi	Sistem operasi perangkat.
Build sistem operasi	Build sistem operasi perangkat.

3. Untuk menambahkan kolom di tabel, klik ikon opsi kolom, dan pilih kolom yang Anda inginkan agar terlihat di tabel.
4. Untuk mempersempit informasi yang ditampilkan pada layar, gunakan satu atau beberapa filter.
   a. Klik **Pencarian**.
   b. Klik tanda panah, lalu klik **Perangkat keras**.
   c. Pilih satu atau kombinasi dari beberapa filter.
      Tabel berikut menjelaskan tentang filter **Perangkat keras**.

Filter	Deskripsi
Model prosesor	Pilihan ganda memungkinkan. Gunakan filter ini jika Anda ingin menampilkan data perangkat keras dari perangkat yang memiliki model prosesor yang ditentukan.
Inti prosesor	Gunakan filter ini jika Anda ingin menampilkan data perangkat keras dari perangkat yang memiliki jumlah inti prosesor yang ditentukan.
Ukuran total disk	Gunakan filter ini jika Anda ingin menampilkan data perangkat keras dari perangkat yang memiliki ukuran penyimpanan total yang ditentukan.
Kapasitas memori	Gunakan filter ini jika Anda ingin menampilkan data perangkat keras dari perangkat yang memiliki kapasitas RAM yang ditentukan.

   d. Klik **Terapkan**.
5. Untuk mengurutkan data dalam urutan naik, klik nama kolom.

Menampilkan perangkat keras dari satu perangkat

Anda dapat melihat informasi rinci tentang motherboard, prosesor, memori, grafik, drive penyimpanan, jaringan, dan sistem perangkat tertentu.

Prasyarat

- (Untuk semua perangkat) Perangkat menggunakan sistem operasi Windows atau macOS.
- (Untuk semua perangkat) Perangkat memiliki lisensi yang mendukung fitur inventaris Perangkat Keras. Perhatikan bahwa fitur inventaris Perangkat Keras untuk mesin virtual tidak didukung di Cyber Protect edisi legasi.

© Acronis International GmbH, 2003-2024

- (Untuk semua perangkat) Agen perlindungan diinstal di perangkat.
- (Untuk semua perangkat) Pemindaian inventaris perangkat keras pada perangkat telah berhasil diselesaikan.
- (Untuk mesin virtual) Mesin berjalan pada salah satu platform virtualisasi yang didukung. Untuk informasi lebih lanjut, lihat "Inventaris perangkat keras" (hlm. 978).

Untuk melihat informasi rinci tentang perangkat keras pada perangkat tertentu

1. Di konsol Cyber Protect, buka **Perangkat**->**Semua Perangkat**.
2. Di bidang drop-down **Tampilan:**, pilih **Perangkat keras**.
3. Temukan perangkat yang ingin Anda periksa menggunakan salah satu metode yang dijelaskan di bawah ini.
   - Temukan perangkat menggunakan **Filter**:
     a. Klik **Filter**.
     b. Pilih satu atau kombinasi dari beberapa parameter filter untuk menemukan perangkat.
     c. Klik **Terapkan**.
   - Temukan perangkat menggunakan **Pencarian**:
     a. Klik **Pencarian**.
     b. Ketik nama lengkap perangkat atau sebagian dari nama perangkat, dan klik **Enter**.
4. Klik baris yang mencantumkan perangkat, dan klik **Inventaris**.
5. Klik tab **Perangkat keras**.
   Data perangkat keras berikut tersedia.

Komponen perangkat keras	Informasi yang ditampilkan
Motherboard	Nama, produsen, model, dan nomor seri dari motherboard perangkat.
Prosesor	Produsen, model, kecepatan jam maks, dan jumlah inti dari setiap prosesor perangkat.
Memori	Kapasitas, produsen, dan nomor seri memori dari perangkat.
Grafis	Produsen dan model GPU perangkat.
Drive penyimpanan	Model, jenis media, ruang yang tersedia, dan ukuran drive penyimpanan dari perangkat.
Jaringan	Alamat Mac, alamat IP, dan jenis adaptor jaringan perangkat.
Sistem	ID produk, tanggal penginstalan asli, waktu boot sistem, produsen sistem, model sistem, versi BIOS, perangkat boot, lokal sistem, dan zona waktu sistem.

© Acronis International GmbH, 2003-2024

Menghubungkan ke beban kerja untuk desktop jarak jauh atau bantuan jarak jauh

Fungsi desktop dan bantuan jarak jauh adalah cara mudah untuk terhubung ke beban kerja di organisasi Anda untuk kontrol jarak jauh atau bantuan jarak jauh. Mulai Desember 2022, fungsi ini mendukung protokol NEAR, RDP, dan Berbagi Layar Apple. Untuk informasi lebih lanjut, lihat "Protokol koneksi jarak jauh" (hlm. 989).

Anda dapat menggunakan fungsi desktop jarak jauh untuk melakukan tugas-tugas berikut.

- Terhubung ke beban kerja Windows, macOS, dan Linux jarak jauh dengan menggunakan NEAR dalam mode hanya lihat.
- Terhubung ke beban kerja Windows jarak jauh dengan menggunakan RDP.
- Terhubung ke beban kerja macOS jarak jauh dengan menggunakan Berbagi Layar Apple dalam mode hanya lihat atau tutup.
- Terhubung ke beban kerja terkelola dan mengendalikannya dari jarak jauh menggunakan koneksi jarak jauh awan.
- Terhubung ke beban kerja yang tidak terkelola dan mengendalikannya dari jarak jauh menggunakan koneksi jarak jauh langsung.
- Terhubung ke beban kerja jarak jauh yang tidak terkelola dengan menggunakan Acronis Bantuan Cepat.
- Terhubung ke beban kerja jarak jauh dengan menggunakan metode autentikasi yang berbeda: dengan kredensial beban kerja jarak jauh, dengan meminta izin untuk mengamati atau mengontrol, atau dengan kode akses (untuk Bantuan Cepat).
- Mengamati beberapa monitor dalam satu waktu menggunakan multi-tampilan.
- Merekam sesi jarak jauh (ketika terhubung melalui NEAR).
- Melihat laporan riwayat sesi.

Untuk informasi lebih lanjut tentang fitur yang merupakan bagian dari paket Standar dan Manajemen Tingkat Lanjut, lihat "Fitur desktop dan bantuan jarak jauh yang didukung" (hlm. 986).

Anda dapat menggunakan fungsi bantuan jarak jauh untuk melakukan tugas-tugas berikut.

- Terhubung ke beban kerja Windows, macOS, dan Linux jarak jauh dengan menggunakan NEAR dalam mode kontrol.
- Terhubung ke beban kerja macOS jarak jauh dengan menggunakan Berbagi Layar Apple dalam mode kontrol.
- Memberikan bantuan jarak jauh untuk beban kerja menggunakan koneksi jarak jauh awan.
- Transfer file antara beban kerja lokal dan jarak jauh.
- Melakukan tindakan manajemen dasar pada beban kerja jarak jauh: memulai ulang, mematikan, tidur, mengosongkan keranjang sampah, dan mengeluarkan pengguna jarak jauh.

© Acronis International GmbH, 2003-2024

- Memantau beban kerja jarak jauh dengan mengambil tangkapan layar desktop-nya secara berkala.

Untuk informasi lebih lanjut tentang fitur yang merupakan bagian dari proteksi Standar dan Manajemen Tingkat Lanjut, lihat "Fitur desktop dan bantuan jarak jauh yang didukung" (hlm. 986).

Penting
Untuk mengaktifkan fungsionalitas desktop jarak jauh dan bantuan yang lengkap untuk beban kerja terkelola, Anda harus mengonfigurasi dan menerapkan rencana manajemen jarak jauh pada beban kerja. Meskipun Anda hanya dapat menerapkan satu rencana manajemen jarak jauh pada beban kerja, tergantung pada kebutuhan Anda, Anda dapat mengonfigurasi rencana manajemen jarak jauh yang berbeda dan menerapkannya pada beban kerja yang berbeda.

Sebagai contoh, Anda bisa membuat rencana manajemen jarak jauh yang hanya mengaktifkan protokol RDP dan menerapkannya pada beberapa beban kerja. Dengan demikian, Anda akan dapat terhubung dari jarak jauh ke beban kerja ini tanpa mengaktifkan lisensi Manajemen Tingkat Lanjut per beban kerja, dan tanpa membayar biaya tambahan apa pun.

Di sisi lain, Anda dapat membuat rencana manajemen jarak jauh lain yang mengaktifkan protokol NEAR dan Berbagi Layar Apple. Dalam hal ini, lisensi Manajemen Tingkat Lanjut per beban kerja akan diaktifkan, dan Anda akan dikenai biaya untuk setiap beban kerja yang menerapkan rencana manajemen jarak jauh ini.

Untuk informasi lebih lanjut tentang rencana manajemen jarak jauh dan cara menggunakannya, lihat "Rencana manajemen jarak jauh" (hlm. 992).

Catatan
Fungsi desktop dan bantuan jarak jauh mensyaratkan:

- instalasi Hubungkan Klien satu kali pada beban kerja pengelola (host). Sistem akan menyarankan Anda untuk mengunduh klien ketika Anda mencoba melakukan tindakan jarak jauh (kontrol jarak jauh atau bantuan jarak jauh) pada beban kerja target untuk pertama kalinya. Selain itu, Anda dapat mengunduh Hubungkan Klien dari jendela **Unduhan** di konsol Perlindungan. Untuk mengetahui informasi lebih lanjut tentang pengaturan yang dapat Anda konfigurasi, lihat "Mengonfigurasi pengaturan Hubungkan Klien" (hlm. 1023).
- instalasi Connect Agent pada beban kerja terkelola. Connect Agent adalah modul yang merupakan bagian dari agen Perlindungan, mulai dari versi 15.0.31266.
- untuk beban kerja jarak jauh macOS, izin sistem yang diperlukan harus diberikan pada Connect Agent. Untuk informasi lebih lanjut, lihat "Menginstal agen proteksi di macOS" (hlm. 81).
- menjalankan aplikasi Acronis Bantuan Cepat pada beban kerja tidak terkelola. Anda dapat mengunduh Acronis Bantuan Cepat dari situs web.

Untuk informasi lebih lanjut tentang platform yang didukung oleh setiap desktop dan komponen bantuan jarak jauh, lihat "Platform yang didukung" (hlm. 988).

© Acronis International GmbH, 2003-2024

Fitur desktop dan bantuan jarak jauh yang didukung

Tabel berikut memberikan informasi lebih lanjut tentang perubahan fitur fungsi desktop dan bantuan jarak jauh yang didukung yang diperkenalkan pada Desember 2022.

Fitur	Perlindungan standar sebelum Desember 2022	Manajemen Tingkat Lanjut sebelum Desember 2022	Perlindungan standar setelah Desember 2022	Manajemen Tingkat Lanjut setelah Desember 2022
Bantuan jarak jauh melalui RDP untuk Windows	Iya	Tidak	Tidak	Tidak
Berbagi koneksi jarak jauh dengan pengguna	Tidak	Iya	Tidak	Tidak
Koneksi jarak jauh				
Tindakan jarak jauh	Tidak	Tidak	Iya	Iya
Memilih sesi untuk menghubungkan Windows/macOS/Linux	Tidak	Tidak	Tidak	Iya
Koneksi langsung melalui RDP dan Berbagi Layar Apple	Tidak	Tidak	Tidak	Iya
Kontrol multi-jendela	Tidak	Tidak	Tidak	Iya
Mode koneksi: Kontrol/Hanya lihat/Tutup	Tidak	Tidak	Tidak	Iya
Dukungan kredensial umum untuk koneksi jarak jauh	Tidak	Tidak	Iya	Iya
Koneksi bersamaan per teknisi				
melalui RDP	Iya	Iya	Iya	Iya
melalui NEAR	Tidak	Tidak	Tidak	Iya
Transfer dan berbagi file				
dari Windows ke Windows/macOS/Linux	Tidak	Tidak	Tidak	Iya

© Acronis International GmbH, 2003-2024

Fitur	Perlindungan standar sebelum Desember 2022	Manajemen Tingkat Lanjut sebelum Desember 2022	Perlindungan standar setelah Desember 2022	Manajemen Tingkat Lanjut setelah Desember 2022
dari macOS ke Windows/macOS/Linux	Tidak	Tidak	Tidak	Iya
dari Linux ke Windows/macOS/Linux	Tidak	Tidak	Tidak	Iya
Koneksi melalui aplikasi Quick Assist				
dari Windows ke Windows/macOS/Linux	Tidak	Tidak	Tidak	Iya
dari macOS ke Windows/macOS/Linux	Tidak	Tidak	Tidak	Iya
dari Linux ke Windows/macOS/Linux	Tidak	Tidak	Tidak	Iya
Koneksi jarak jauh melalui protokol				
Koneksi jarak jauh melalui NEAR				
dari Windows ke Windows/macOS/Linux	Tidak	Tidak	Tidak	Iya
dari macOS ke Windows/macOS/Linux	Tidak	Tidak	Tidak	Iya
dari Linux ke Windows/macOS/Linux	Tidak	Tidak	Tidak	Iya
Koneksi jarak jauh melalui RDP (klien desktop)				
dari Windows ke Windows	Iya	Iya	Iya	Iya
dari macOS ke Windows	Iya	Iya	Iya	Iya
dari Linux ke Windows	Tidak	Tidak	Iya	Iya
Koneksi jarak jauh melalui RDP (klien web)				
dari Windows ke Windows	Iya	Iya	Iya	Iya
dari macOS ke Windows	Iya	Iya	Iya	Iya

© Acronis International GmbH, 2003-2024

Fitur	Perlindungan standar sebelum Desember 2022	Manajemen Tingkat Lanjut sebelum Desember 2022	Perlindungan standar setelah Desember 2022	Manajemen Tingkat Lanjut setelah Desember 2022
dari Linux ke Windows	Tidak	Tidak	Iya	Iya
Koneksi jarak jauh melalui Berbagi Layar Apple				
dari Windows/macOS/Linux ke macOS	Tidak	Tidak	Tidak	Iya
Manajemen sesi				
Perekaman sesi	Tidak	Tidak	Tidak	Iya
Pelaporan dan pemantauan				
Riwayat dan pencarian sesi	Tidak	Tidak	Tidak	Iya
Transmisi tangkapan layar	Tidak	Tidak	Tidak	Iya

Platform yang didukung

Tabel berikut mencantumkan sistem operasi yang didukung oleh setiap komponen fungsi desktop dan bantuan jarak jauh.

Komponen desktop jarak jauh	Platform yang didukung
Hubungkan Klien	• Windows 7 atau versi lebih baru • macOS 10.13 atau versi lebih baru • 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 Manjaro 20
Connect Agent	• Windows 7 atau versi lebih baru

© Acronis International GmbH, 2003-2024

Komponen desktop jarak jauh	Platform yang didukung
	• Windows Server 2008 R2 atau versi lebih baru • macOS 10.13 atau versi lebih baru • 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 Bantuan Cepat	• Windows 7 atau versi lebih baru • Windows Server 2008 R2 atau versi lebih baru • macOS 10.13 atau versi lebih baru • 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

Protokol koneksi jarak jauh

Fungsi desktop jarak jauh menggunakan protokol berikut untuk koneksi jarak jauh.

NEAR

NEAR adalah protokol yang sangat aman yang dikembangkan oleh Acronis yang memiliki karakteristik sebagai berikut.

- ### H.264

  NEAR mengimplementasikan tiga mode kualitas: **Halus**, **Seimbang**, dan **Tajam**. Dalam mode **Halus**, NEAR menggunakan pengodean H.264 perangkat keras di macOS dan Windows untuk mengodekan gambar desktop, dan kembali ke pengode perangkat lunak jika pengode perangkat keras tidak tersedia. Ukuran gambar saat ini dibatasi hingga resolusi Full HD (1920x1080).

- ### Codec Adaptif

  Dalam mode kualitas **Seimbang** dan **Tajam**, NEAR menggunakan codec Adaptif, yang memberikan kualitas gambar penuh dalam 32 bit dibandingkan mode 'video' yang digunakan oleh H.264.

© Acronis International GmbH, 2003-2024

Dalam mode **Seimbang**, kualitas gambar otomatis disesuaikan menurut kondisi jaringan saat ini dan mempertahankan kecepatan frame saat ini.

Dalam mode **Tajam**, gambar memiliki kualitas penuh, tetapi kecepatan frame mungkin berkurang jika jaringan, prosesor, atau kartu video kelebihan beban.

Codec Adaptif menggunakan OpenCL di Windows dan macOS jika tersedia pada driver grafisnya.

- ### Transfer suara

  NEAR dapat menangkap suara komputer jarak jauh dan mentransfernya ke host. Untuk informasi selengkapnya tentang mengaktifkan pengalihan suara jarak jauh di Windows, macOS, dan Linux, lihat "Pengalihan suara jarak jauh" (hlm. 990).

- ### Opsi masuk yang berbeda

  Anda dapat menggunakan metode berikut untuk masuk ke beban kerja jarak jauh.

  Kode akses: pengguna yang masuk ke beban kerja jarak jauh menjalankan Bantuan Cepat dan memberi tahu Anda kode aksesnya. Dengan metode ini, Anda selalu terhubung ke sesi pengguna yang masuk saat ini.

  Kredensial beban kerja: masuk ke beban kerja jarak jauh menggunakan kredensial administrator yang terdaftar di beban kerja.

  Minta izin untuk mengamati atau mengontrol: pengguna yang masuk ke beban kerja jarak jauh akan diminta mengizinkan atau menolak koneksi.

- ### Keamanan

  Data Anda selalu dienkripsi dua arah dengan enkripsi AES di NEAR.

RDP

Protokol Desktop Jarak Jauh (RDP) adalah protokol berpemilik yang dikembangkan oleh Microsoft yang memungkinkan untuk terhubung ke komputer Windows jarak jauh melalui koneksi jaringan.

Berbagi Layar Apple

Berbagi Layar Apple adalah klien VNC dari Apple yang disertakan sebagai bagian dari macOS versi 10.5 dan versi lebih baru.

Pengalihan suara jarak jauh

Hubungkan Klien mendukung streaming audio melalui protokol koneksi NEAR. Untuk informasi lebih lanjut tentang NEAR, lihat "Protokol koneksi jarak jauh" (hlm. 989).

Mengalihkan suara dari beban kerja Windows jarak jauh

Untuk beban kerja Windows, suara jarak jauh seharusnya ditransmisikan secara otomatis. Pastikan bahwa ada perangkat keluaran suara (speaker atau headphone) yang terhubung ke beban kerja

© Acronis International GmbH, 2003-2024

jarak jauh.

Mengalihkan suara dari beban kerja macOS jarak jauh

Untuk mengaktifkan pengalihan suara dari beban kerja macOS, pastikan bahwa:

- Beban kerja telah menginstal agen Perlindungan.
- Beban kerja telah terinstal driver penangkap suara.
- Beban kerja menggunakan protokol NEAR untuk koneksi jarak jauh.

Catatan
Untuk macOS 10.15 Catalina, izin Mikrofon harus diberikan kepada Connect Agent. Untuk informasi lebih lanjut tentang pemberian izin Mikrofon ke Connect Agent, lihat "Memberikan izin sistem yang diperlukan kepada Connect Agent" (hlm. 82).

Agen berfungsi dengan driver penangkap suara berikut: Soundflower atau Blackhole.

Proses instalasi pada versi terbaru dijelaskan di halaman wiki Blackhole: https://github.com/ExistentialAudio/BlackHole/wiki/Installation.

Catatan
Saat ini Hubungkan Klien hanya mendukung versi Blackhole 2 saluran.

Sebagai alternatif, jika Homebrew diinstal pada beban kerja, Anda dapat menginstal Blackhole dengan menjalankan perintah berikut:

```
brew install --cask blackhole-2ch
```

Catatan
Ketika suara beban kerja macOS jarak jauh dialihkan, pengguna yang masuk ke beban kerja jarak jauh tidak akan mendengar suara tersebut.

Mengalihkan suara dari beban kerja Linux jarak jauh

Pengalihan suara jarak jauh seharusnya berfungsi otomatis dengan sebagian besar distribusi Linux. Jika pengalihan suara jarak jauh tidak berfungsi secara default, instal driver PulseAudio dengan menjalankan perintah berikut:

```
sudo apt-get install pulseaudio
```

Koneksi ke beban kerja jarak jauh untuk desktop jarak jauh atau bantuan jarak jauh

Fungsi desktop dan bantuan jarak jauh menyediakan beberapa cara untuk membuat koneksi langsung jarak jauh atau awan ke beban kerja Anda.

© Acronis International GmbH, 2003-2024

Koneksi langsung dibuat melalui TCP/IP di jaringan area lokal (LAN) antara Hubungkan Klien dan beban kerja jarak jauh yang tidak memiliki agen terpasang. Berbagai koneksi ini tidak memerlukan akses Internet.

Koneksi awan dibuat antara Hubungkan Klien dan agen atau Bantuan Cepat di beban kerja melalui Acronis Cloud.

Tabel berikut memberikan info lebih lanjut mengenai opsi koneksi awan.

Koneksi awan	Opsi koneksi awan	Mode tampilan	Tindakan jarak jauh yang didukung	Tersedia untuk
melalui NEAR	dari Hubungkan Klien ke Connect Agent dari Hubungkan Klien ke Bantuan Cepat	Kontrol Hanya lihat	Desktop jarak jauh Bantuan jarak jauh	beban kerja terkelola
melalui RDP	dari Hubungkan Klien ke Connect Agent dari klien web ke Connect Agent	Kontrol	Desktop jarak jauh	beban kerja terkelola
via Berbagi Layar Apple	dari Hubungkan Klien ke Connect Agent	Kontrol Hanya lihat Tutup	Desktop jarak jauh Bantuan jarak jauh	beban kerja terkelola

Tabel berikut memberikan info lebih lanjut mengenai opsi koneksi langsung.

Koneksi langsung	Opsi koneksi langsung	Tindakan jarak jauh yang didukung	Tersedia untuk
melalui RDP	dari Hubungkan Klien ke server RDP	Desktop jarak jauh	beban kerja tidak terkelola
via Berbagi Layar Apple	dari Hubungkan Klien ke server Berbagi Layar Apple	Desktop jarak jauh Bantuan jarak jauh	beban kerja tidak terkelola

Rencana manajemen jarak jauh

Rencana manajemen jarak jauh adalah rencana yang Anda terapkan pada agen Perlindungan untuk mengaktifkan dan mengonfigurasi desktop jarak jauh dan fungsionalitas bantuan pada beban kerja terkelola Anda.

Jika tidak ada rencana manajemen jarak jauh yang diterapkan pada beban kerja, fungsionalitas desktop jarak jauh dan bantuan akan terbatas pada tindakan jarak jauh (mulai ulang, matikan, tidur, kosongkan tempat sampah, dan keluar dari pengguna jarak jauh).

© Acronis International GmbH, 2003-2024

Catatan
Ketersediaan pengaturan yang dapat Anda konfigurasikan dalam rencana manajemen jarak jauh tergantung pada rencana layanan yang diterapkan pada penyewa. Untuk mengakses semua pengaturan, aktifkan paket Manajemen Tingkat Lanjut. Untuk informasi lebih lanjut tentang fitur yang merupakan bagian dari paket Standar dan Manajemen Tingkat Lanjut, lihat "Fitur desktop dan bantuan jarak jauh yang didukung" (hlm. 986).

Membuat rencana manajemen jarak jauh

Anda dapat membuat rencana agen, lalu menetapkannya ke beban kerja untuk mengonfigurasi fungsi desktop dan bantuan jarak jauh pada beban kerja terkelola.

Catatan
Ketersediaan pengaturan rencana manajemen jarak jauh tergantung pada kuota layanan yang diberikan kepada penyewa. Jika menggunakan fungsi standar, Anda hanya dapat mengonfigurasi koneksi melalui RDP.

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Untuk membuat rencana manajemen jarak jauh

Dari rencana manajemen Jarak Jauh

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana manajemen jarak jauh**.
2. Buat rencana manajemen jarak jauh dengan menggunakan salah satu dari dua opsi.
   - Jika tidak terdapat rencana pengelolaan jarak jauh dalam daftar, klik **Buat**.
   - Jika ada rencana manajemen jarak jauh dalam daftar, klik **Buat rencana**.
3. [Opsional] Untuk mengubah nama default rencana, klik ikon pensil, masukkan nama rencana, lalu klik **Lanjutkan**.
4. Klik **Protokol koneksi**, dan aktifkan protokol yang ingin disediakan dalam rencana manajemen jarak jauh ini untuk koneksi jarak jauh - NEAR, RDP, atau Berbagi Layar Apple.
5. [Opsional] Untuk protokol NEAR, di bagian **Pengaturan keamanan**, pilih atau hapus kotak centang untuk mengaktifkan atau menonaktifkan pengaturan terkait, lalu klik **Selesai**.

Pengaturan	Deskripsi	Tersedia untuk
Kunci beban kerja ketika pengguna terputus dari sesi konsol	Jika memilih pengaturan ini, beban kerja jarak jauh akan dikunci ketika Anda terputus dari sesi konsol.	Windows, macOS
Hanya izinkan satu pengguna pada satu	Jika Anda memilih pengaturan ini, koneksi	Windows, macOS, Linux

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi	Tersedia untuk
waktu untuk terhubung menggunakan NEAR atau untuk mentransfer file	menggunakan NEAR dan transfer file tidak akan dapat dilakukan ketika ada koneksi jarak jauh yang aktif ke beban kerja.	
Izinkan administrator beban kerja terhubung ke semua sesi pengguna non-admin	Jika Anda memilih pengaturan ini, administrator akan diizinkan terhubung ke semua sesi pengguna standar pada beban kerja. Jika **Izinkan administrator beban kerja terhubung ke semua sesi pengguna non-admin** dan **Izinkan pembuatan sesi sistem** sudah selesai, Anda hanya akan dapat terhubung ke sesi administrator aktif pada beban kerja macOS jarak jauh.	Windows, macOS
Izinkan pembuatan sesi sistem	Jika Anda memilih pengaturan ini, ketika membuat koneksi jarak jauh, administrator akan terhubung ke sesi baru, bukan salah satu dari sesi aktif yang sudah ada.	macOS
Izinkan sinkronisasi papan klip	Jika memilih pengaturan ini, Anda akan dapat mentransfer data antara papan klip dan papan klip beban kerja jarak jauh. Misalnya, Anda akan dapat menyalin teks dari file pada beban kerja jarak jauh dan menempelnya di file pada beban kerja, dan sebaliknya.	Windows, macOS, Linux

6. Klik **Pengaturan keamanan**, pilih atau hapus kotak centang untuk mengaktifkan atau menonaktifkan pengaturan terkait, lalu klik **Selesai**.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
Tampilkan jika beban kerja dikontrol secara jarak jauh	Jika Anda memilih pengaturan ini, pemberitahuan akan ditampilkan di desktop dari beban kerja jarak jauh saat ada koneksi desktop jarak jauh yang aktif ke beban kerja.
Minta izin pengguna untuk mengambil tangkapan layar beban kerja	Jika Anda memilih pengaturan ini, pengguna beban kerja jarak jauh akan diberi tahu ketika administrator meminta transmisi tangkapan layar dari beban kerja.

7. Klik **Manajemen beban kerja**, pilih fitur yang ingin Anda sediakan pada beban kerja jarak jauh, lalu klik **Selesai**.

Pengaturan	Deskripsi	Tersedia di
Transfer file	Memungkinkan transfer file antara beban kerja lokal dan jarak jauh.	Windows, macOS, Linux
Transmisi tangkapan layar	Memungkinkan transmisi tangkapan layar desktop beban kerja jarak jauh ke konsol Cyber Protect.	Windows, macOS, Linux

8. Klik **Pengaturan tampilan**, pilih atau hapus kotak centang untuk mengaktifkan atau menonaktifkan pengaturan terkait, lalu klik **Selesai**.

Catatan
Pengaturan tampilan hanya tersedia untuk koneksi melalui NEAR.

Pengaturan	Deskripsi	Tersedia di
Gunakan Deduplikasi Desktop untuk menangkap desktop	Duplikasi desktop adalah salah satu metode tangkapan layar pada Windows. Di beberapa lingkungan, metode ini mungkin tidak stabil. Jika Anda tidak menggunakan Deduplikasi desktop, Anda akan menggunakan metode dasar (BitBlt) yang jauh lebih lambat, tetapi lebih stabil.	Windows
Gunakan akselerasi OpenCL	Akselerasi OpenCL dapat mempercepat codec Adaptif,	Linux

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi	Tersedia di
	yang bertanggung jawab untuk mode kualitas **Seimbang** dengan menjalankan beberapa komputasi di unit pemrosesan grafis (GPU). Hal ini memerlukan instalasi driver OpenCL di Linux jarak jauh. Codec Adaptif menggunakan OpenCL di macOS dan Windows jika tersedia pada driver grafis.	
Gunakan enkode H.264 perangkat keras	NEAR mendukung tiga mode kualitas: **Halus**, **Seimbang**, dan **Tajam**. Mode **Halus** menggunakan pengodean H.264 perangkat keras untuk mengodekan gambar desktop. Mode **Seimbang** menggunakan codec Adaptif, yang memberikan kualitas gambar penuh dalam 32 bit dibandingkan mode 'video' yang digunakan oleh H.264. Kualitas gambar otomatis disesuaikan menurut kondisi jaringan saat ini dan mempertahankan kecepatan frame saat ini. Mode **Tajam** menggunakan codec Adaptif, yang memberikan kualitas gambar penuh dalam 32 bit dibandingkan mode 'video' yang digunakan oleh H.264. Kualitas gambar selalu penuh, tetapi mungkin dengan frame per detik yang berkurang jika jaringan atau prosesor/kartu video Anda kelebihan beban.	Windows, macOS

© Acronis International GmbH, 2003-2024

9. Jika Anda ingin informasi tentang pengguna yang terakhir masuk ke beban kerja terlihat di detail beban kerja, klik **Kotak alat**, pilih **Tampilkan pengguna yang terakhir masuk**, lalu klik **Selesai**. Untuk informasi lebih lanjut tentang pengguna terakhir yang masuk, lihat "Temukan pengguna yang terakhir masuk" (hlm. 393).
10. [Opsional] Untuk menambahkan beban kerja ke rencana:
    a. Klik **Tambahkan beban kerja**.
    b. Pilih beban kerja, lalu klik **Tambahkan**.
    c. Jika ada masalah kompatibilitas yang ingin Anda selesaikan, ikuti prosedur yang dijelaskan di "Menyelesaikan masalah kompatibilitas dengan rencana manajemen jarak jauh" (hlm. 1005).
11. Klik **Buat**.

Dari Semua perangkat

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Klik beban kerja tempat Anda ingin menerapkan rencana manajemen jarak jauh.
3. Klik **Lindungi**, lalu klik **Tambahkan rencana**.
4. Klik **Buat rencana**, lalu pilih **Manajemen jarak jauh**.
5. [Opsional] Untuk mengubah nama default rencana, klik ikon pensil, masukkan nama rencana, lalu klik **Lanjutkan**.
6. Klik **Protokol koneksi**, dan aktifkan protokol yang ingin disediakan dalam rencana manajemen jarak jauh ini untuk koneksi jarak jauh - NEAR, RDP, atau Berbagi Layar Apple.
7. [Opsional] Untuk protokol NEAR, di bagian **Pengaturan keamanan**, pilih atau hapus kotak centang untuk mengaktifkan atau menonaktifkan pengaturan terkait, lalu klik **Selesai**.

Pengaturan	Deskripsi	Tersedia untuk
Kunci beban kerja ketika pengguna terputus dari sesi konsol	Jika memilih pengaturan ini, beban kerja jarak jauh akan dikunci ketika Anda terputus dari sesi konsol.	Windows, macOS
Hanya izinkan satu pengguna pada satu waktu untuk terhubung menggunakan NEAR atau untuk mentransfer file	Jika Anda memilih pengaturan ini, koneksi menggunakan NEAR dan transfer file tidak akan dapat dilakukan ketika ada koneksi jarak jauh yang aktif ke beban kerja.	Windows, macOS, Linux
Izinkan administrator beban kerja terhubung ke semua sesi pengguna non-admin	Jika Anda memilih pengaturan ini, administrator akan diizinkan terhubung ke semua sesi pengguna standar pada	Windows, macOS

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi	Tersedia untuk
	beban kerja. Jika **Izinkan administrator beban kerja terhubung ke semua sesi pengguna non-admin** dan **Izinkan pembuatan sesi sistem** sudah selesai, Anda hanya akan dapat terhubung ke sesi administrator aktif pada beban kerja macOS jarak jauh.	
Izinkan pembuatan sesi sistem	Jika Anda memilih pengaturan ini, ketika membuat koneksi jarak jauh, administrator akan terhubung ke sesi baru, bukan salah satu dari sesi aktif yang sudah ada.	macOS
Izinkan sinkronisasi papan klip	Jika memilih pengaturan ini, Anda akan dapat mentransfer data antara papan klip dan papan klip beban kerja jarak jauh. Misalnya, Anda akan dapat menyalin teks dari file pada beban kerja jarak jauh dan menempelnya di file pada beban kerja, dan sebaliknya.	Windows, macOS, Linux

8. Klik **Pengaturan keamanan**, pilih atau hapus kotak centang untuk mengaktifkan atau menonaktifkan pengaturan terkait, lalu klik **Selesai**.

Pengaturan	Deskripsi
Tampilkan jika beban kerja dikontrol secara jarak jauh	Jika Anda memilih pengaturan ini, pemberitahuan akan ditampilkan di desktop dari beban kerja jarak jauh saat ada koneksi desktop jarak jauh yang aktif ke beban kerja.
Minta izin pengguna untuk mengambil tangkapan layar beban kerja	Jika Anda memilih pengaturan ini, pengguna beban kerja jarak jauh akan diberi tahu ketika administrator meminta transmisi tangkapan layar dari beban kerja.

© Acronis International GmbH, 2003-2024

9. Klik **Manajemen beban kerja**, pilih fitur yang ingin Anda sediakan pada beban kerja jarak jauh, lalu klik **Selesai**.

Pengaturan	Deskripsi	Tersedia di
Transfer file	Memungkinkan transfer file antara beban kerja lokal dan jarak jauh.	Windows, macOS, Linux
Transmisi tangkapan layar	Memungkinkan transmisi tangkapan layar desktop beban kerja jarak jauh ke konsol Cyber Protect.	Windows, macOS, Linux

10. Klik **Pengaturan tampilan**, pilih atau hapus kotak centang untuk mengaktifkan atau menonaktifkan pengaturan terkait, lalu klik **Selesai**.

Catatan
Pengaturan tampilan hanya tersedia untuk koneksi melalui NEAR.

Pengaturan	Deskripsi	Tersedia di
Gunakan Deduplikasi Desktop untuk menangkap desktop	Duplikasi desktop adalah salah satu metode tangkapan layar pada Windows. Di beberapa lingkungan, metode ini mungkin tidak stabil. Jika Anda tidak menggunakan Deduplikasi desktop, Anda akan menggunakan metode dasar (BitBlt) yang jauh lebih lambat, tetapi lebih stabil.	Windows
Gunakan akselerasi OpenCL	Akselerasi OpenCL dapat mempercepat codec Adaptif, yang bertanggung jawab untuk mode kualitas **Seimbang** dengan menjalankan beberapa komputasi di unit pemrosesan grafis (GPU). Hal ini memerlukan instalasi driver OpenCL di Linux jarak jauh. Codec Adaptif menggunakan OpenCL di macOS dan Windows jika tersedia pada	Linux

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi	Tersedia di
	driver grafis.	
Gunakan enkode H.264 perangkat keras	NEAR mendukung tiga mode kualitas: **Halus**, **Seimbang**, dan **Tajam**. Mode **Halus** menggunakan pengodean H.264 perangkat keras untuk mengodekan gambar desktop. Mode **Seimbang** menggunakan codec Adaptif, yang memberikan kualitas gambar penuh dalam 32 bit dibandingkan mode 'video' yang digunakan oleh H.264. Kualitas gambar otomatis disesuaikan menurut kondisi jaringan saat ini dan mempertahankan kecepatan frame saat ini. Mode **Tajam** menggunakan codec Adaptif, yang memberikan kualitas gambar penuh dalam 32 bit dibandingkan mode 'video' yang digunakan oleh H.264. Kualitas gambar selalu penuh, tetapi mungkin dengan frame per detik yang berkurang jika jaringan atau prosesor/kartu video Anda kelebihan beban.	Windows, macOS

11. Jika Anda ingin informasi tentang pengguna yang terakhir masuk ke beban kerja terlihat di detail beban kerja, klik **Kotak alat**, pilih **Tampilkan pengguna yang terakhir masuk**, lalu klik **Selesai**.
    Untuk informasi lebih lanjut tentang pengguna terakhir yang masuk, lihat "Temukan pengguna yang terakhir masuk" (hlm. 393).
12. Klik **Buat**.

Menambahkan beban kerja ke rencana manajemen jarak jauh

Tergantung pada kebutuhan Anda, Anda dapat menambahkan beban kerja ke rencana manajemen jarak jauh setelah rencana dibuat.

© Acronis International GmbH, 2003-2024

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Untuk menambahkan beban kerja ke rencana manajemen jarak jauh

Dari Rencana manajemen jarak jauh

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana manajemen jarak jauh**.
2. Klik rencana manajemen jarak jauh.
3. Bergantung pada apakah rencana sudah diterapkan ke beban kerja atau belum, lakukan hal berikut:
   - Klik **Tambahkan beban kerja**, jika rencana belum diaplikasikan pada beban kerja apa pun.
   - Klik **Kelola beban kerja**, jika rencana sudah diaplikasikan pada beban kerja.
4. Pilih beban kerja dari daftar, lalu klik **Tambahkan**.
5. Klik **Simpan**.
6. Klik **Konfirmasi** untuk menerapkan kuota layanan yang diperlukan ke beban kerja.

Dari Semua perangkat

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Klik beban kerja tempat Anda ingin menerapkan rencana manajemen jarak jauh.
3. Klik **Lindungi**, lalu klik **Tambahkan rencana**.
4. Pada **Pilih rencana dari daftar di bawah ini**, pilih **Pengelolaan jarak jauh** untuk melihat paket pengelolaan jarak jauh saja.
5. Klik **Terapkan**.
6. Klik **Konfirmasi** untuk menerapkan kuota layanan yang diperlukan ke beban kerja.

Menghapus beban kerja dari rencana manajemen jarak jauh

Tergantung pada kebutuhan Anda, Anda dapat menghapus beban kerja dari rencana manajemen jarak jauh.

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Menghapus beban kerja dari rencana manajemen jarak jauh

1. Di konsol Cyber Protect, buka **Manajemen** > **Rencana manajemen jarak jauh**.
2. Klik rencana manajemen jarak jauh.
3. Klik **Kelola beban kerja**.
4. Pilih satu atau beberapa beban kerja yang ingin Anda hapus dari rencana manajemen jarak jauh, lalu klik **Hapus**.

© Acronis International GmbH, 2003-2024

5. Klik **Selesai**.
6. Klik **Simpan**.

Operasi tambahan dengan rencana manajemen jarak jauh yang ada

Dari layar **Rencana manajemen jarak jauh**, Anda dapat melakukan operasi tambahan berikut dengan rencana manajemen jarak jauh: melihat detail, mengedit, melihat aktivitas, melihat peringatan, mengubah nama, mengaktifkan, menonaktifkan, klona, ekspor, dan menghapus.

Lihat detail

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Untuk melihat detail rencana manajemen jarak jauh

1. Di layar **Rencana manajemen jarak jauh**, klik ikon **Tindakan lainnya** dari rencana manajemen jarak jauh.
2. Klik **Lihat detail**.

Edit

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Untuk mengedit rencana

1. Di layar **Rencana manajemen jarak jauh**, klik ikon **Tindakan lainnya** dari rencana manajemen jarak jauh.
2. Klik **Edit**.

Aktivitas

Untuk melihat aktivitas yang terkait dengan rencana manajemen jarak jauh

1. Di layar **Rencana manajemen jarak jauh**, klik ikon **Tindakan lainnya** dari rencana manajemen jarak jauh.
2. Klik **Aktivitas**.
3. Klik aktivitas untuk melihat detail lebih lanjut tentangnya.

Peringatan

Untuk melihat peringatan

1. Di layar **Rencana manajemen jarak jauh**, klik ikon **Tindakan lainnya** dari rencana manajemen jarak jauh.
2. Klik **Peringatan**.

Ganti nama

© Acronis International GmbH, 2003-2024

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Untuk mengubah nama rencana manajemen jarak jauh

1. Di layar **Rencana manajemen jarak jauh**, klik ikon **Tindakan lainnya** dari rencana manajemen jarak jauh.
2. Klik **Ganti nama**.
3. Masukkan nama rencana baru, lalu klik **Lanjutkan**.

Aktifkan

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Untuk mengaktifkan rencana manajemen jarak jauh

1. Di layar **Rencana manajemen jarak jauh**, klik ikon **Tindakan lainnya** dari rencana manajemen jarak jauh.
2. Klik **Aktifkan**.

Nonaktifkan

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Untuk menonaktifkan rencana manajemen jarak jauh

1. Di layar **Rencana manajemen jarak jauh**, klik ikon **Tindakan lainnya** dari rencana manajemen jarak jauh.
2. Klik **Nonaktifkan**.

Klona

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Cara mengklona rencana manajemen jarak jauh

1. Di layar **Rencana manajemen jarak jauh**, klik ikon **Tindakan lainnya** dari rencana manajemen jarak jauh.
2. Klik **Klona**.
3. Klik **Buat**.

Ekspor

© Acronis International GmbH, 2003-2024

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Cara mengekspor rencana manajemen jarak jauh

1. Di layar **Rencana manajemen jarak jauh**, klik ikon **Tindakan lainnya** dari rencana manajemen jarak jauh.
2. Klik **Ekspor**.
   Konfigurasi rencana diekspor dalam format JSON ke mesin lokal.

Hapus

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Untuk menghapus rencana manajemen jarak jauh

1. Di layar **Rencana manajemen jarak jauh**, klik ikon **Tindakan lainnya** dari rencana manajemen jarak jauh.
2. Klik **Hapus**.
3. Pilih **Konfirmasi**, lalu klik **Hapus**.

Masalah kompatibilitas dengan rencana manajemen jarak jauh

Dalam beberapa kasus, menerapkan rencana pemantauan pada beban kerja dapat menyebabkan masalah kompatibilitas. Anda mungkin mengamati masalah kompatibilitas berikut:

- Rencana yang saling bertentangan - masalah ini muncul ketika rencana manajemen jarak jauh lain telah diterapkan pada beban kerja, karena hanya satu rencana manajemen jarak jauh yang dapat diterapkan pada beban kerja.
- Sistem operasi tidak kompatibel - masalah ini muncul ketika sistem operasi beban kerja tidak didukung.
- Agen tidak didukung - masalah ini muncul ketika versi agen perlindungan pada beban kerja kedaluwarsa dan tidak mendukung fungsi desktop jarak jauh.
- Kuota tidak memadai - masalah ini muncul ketika tidak ada kuota layanan yang cukup pada penyewa untuk ditetapkan ke beban kerja yang dipilih.

Jika rencana pemantauan diterapkan hingga 150 beban kerja yang dipilih secara terpisah, Anda akan diminta untuk menyelesaikan konflik yang ada sebelum menyimpan rencana tersebut. Untuk menyelesaikan konflik, hapus akar penyebabnya atau hapus beban kerja yang terdampak dari rencana. Untuk informasi lebih lanjut, lihat "Menyelesaikan masalah kompatibilitas dengan rencana manajemen jarak jauh" (hlm. 1005). Jika Anda menyimpan rencana tanpa menyelesaikan konflik, rencana akan otomatis dinonaktifkan untuk beban kerja yang tidak kompatibel dan peringatan akan ditampilkan.

© Acronis International GmbH, 2003-2024

Jika rencana pemantauan diterapkan ke lebih dari 150 beban kerja atau grup perangkat, rencana akan disimpan terlebih dahulu, lalu diperiksa kompatibilitasnya. Rencana akan otomatis dinonaktifkan untuk beban kerja yang tidak kompatibel dan peringatan akan ditampilkan.

Menyelesaikan masalah kompatibilitas dengan rencana manajemen jarak jauh

Tergantung pada penyebab masalah kompatibilitas, Anda dapat melakukan berbagai tindakan untuk menyelesaikan masalah kompatibilitas sebagai bagian dari proses pembuatan rencana manajemen jarak jauh yang baru.

Catatan
Saat memecahkan masalah kompatibilitas dengan menghapus beban kerja dari suatu rencana, Anda tidak dapat menghapus beban kerja yang menjadi bagian dari grup perangkat.

Cara menyelesaikan masalah kompatibilitas

1. Klik **Tinjau masalah**.
2. [Untuk menyelesaikan masalah kompatibilitas rencana manajemen jarak jauh yang ada dengan menghapus beban kerja dari rencana baru]
   a. Pada tab **Rencana berkonflik**, pilih beban kerja yang ingin Anda hapus.
   b. Klik **Hapus beban kerja dari rencana**.
   c. Klik **Hapus**, lalu klik **Tutup**.
3. [Untuk mengatasi masalah kompatibilitas dengan rencana manajemen jarak jauh dengan menonaktifkan rencana yang sudah diterapkan pada beban kerja]
   a. Klik **Nonaktifkan rencana yang diterapkan**.
   b. Klik **Nonaktifkan**, lalu klik **Tutup**.
4. [Untuk menyelesaikan masalah kompatibilitas dengan sistem operasi yang tidak kompatibel]
   a. Pada tab **Sistem operasi yang tidak kompatibel**, pilih beban kerja yang ingin Anda hapus.
   b. Klik **Hapus beban kerja dari rencana**.
   c. Klik **Hapus**, lalu klik **Tutup**.
5. [Untuk menyelesaikan masalah kompatibilitas agen yang tidak didukung dengan menghapus beban kerja dari rencana]
   a. Pada tab **Agen yang tidak didukung**, pilih beban kerja yang ingin Anda hapus.
   b. Klik **Hapus beban kerja dari rencana**.
   c. Klik **Hapus**, lalu klik **Tutup**.
6. [Untuk menyelesaikan masalah kompatibilitas agen yang tidak didukung dengan memperbarui versi agen] Klik **Buka daftar Agen**.

© Acronis International GmbH, 2003-2024

Catatan
Opsi ini hanya tersedia untuk administrator pelanggan.

7. [Untuk menyelesaikan masalah kompatibilitas kuota tidak memadai dengan menghapus beban kerja dari rencana]
   a. Pada tab **Kuota tidak memadai**, pilih beban kerja yang ingin Anda hapus.
   b. Klik **Hapus beban kerja dari rencana**.
   c. Klik **Hapus**, lalu klik **Tutup**.
8. [Untuk menyelesaikan masalah kompatibilitas kuota tidak memadai dengan meningkatkan kuota penyewa]

   Catatan
   Opsi ini hanya tersedia untuk administrator mitra.

   a. Pada tab **Kuota tidak memadai**, klik **Buka Portal manajemen**.
   b. Tingkatkan layanan kuota untuk pelanggan.

Kredensial beban kerja

Anda dapat menambahkan kredensial administrator atau non-administrator dari beban kerja jarak jauh (nama pengguna dan kata sandi, atau kata sandi VNC), menyimpannya di penyimpanan kredensial awan, lalu menggunakannya untuk autentikasi otomatis saat menghubungkan ke beban kerja yang Anda kelola. Dengan cara itu, alih-alih memasukkan kredensial ini secara manual setiap kali melakukan langkah autentikasi koneksi, Anda dapat menyimpannya di penyimpanan kredensial satu kali, menetapkannya ke beberapa beban kerja, lalu Hubungkan Klien akan menggunakan kredensial ini setiap kali Anda ingin terhubung ke beban kerja dari jarak jauh.

Catatan
Kredensial yang disimpan di penyimpanan kredensial tidak dibagikan antara tingkat penyewa yang berbeda. Kredensial hanya dibagikan kepada tingkat penyewa yang sama untuk penyewa pelanggan atau penyewa mitra yang sama.

Ini berarti bahwa jika penyewa pelanggan memiliki beberapa administrator, penyewa akan melihat dan membagikan kredensial di penyimpanan kredensial, sementara administrator mitra lainnya, atau administrator pelanggan penyewa lain tidak akan dapat melihat atau menggunakan kredensial ini.

Menambahkan kredensial

Anda dapat menambahkan kredensial lalu menggunakannya untuk koneksi jarak jauh ke beberapa beban kerja.

Untuk menambahkan kredensial ke beban kerja dan menyimpannya di penyimpanan Kredensial

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Klik beban kerja tempat Anda ingin menambahkan kredensial.
3. Akses menu **Pengaturan** dengan salah satu cara berikut:
   - Klik **Desktop jarak jauh**, dan kemudian klik **Pengaturan**.
   - Klik **Kelola**, dan kemudian klik **Pengaturan**.
4. Klik **Tambahkan kredensial**.
5. Di **Penyimpanan kredensial**, klik **Tambahkan kredensial**.
6. Masukkan kredensial.

Bidang	Deskripsi
Nama kredensial	Pengidentifikasi kredensial yang akan terlihat di penyimpanan kredensial.
Nama Pengguna	Nama pengguna yang akan digunakan untuk koneksi jarak jauh ke beban kerja target.
Kata sandi	Kata sandi yang akan digunakan untuk koneksi jarak jauh ke beban kerja target.
Kata sandi VNC	Bidang ini hanya tersedia untuk Berbagi layar Apple.

7. Klik **Simpan**.

Menetapkan kredensial ke beban kerja

Setelah menambahkan kredensial, Anda dapat menggunakannya untuk autentikasi otomatis ketika terhubung ke beban kerja yang Anda kelola.

Untuk menetapkan kredensial tersimpan untuk autentikasi otomatis ke beban kerja

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Akses menu **Pengaturan** dengan salah satu cara berikut:
   - Klik **Desktop jarak jauh**, dan kemudian klik **Pengaturan**.
   - Klik **Kelola**, dan kemudian klik **Pengaturan**.
3. Pada tab protokol yang didukung (NEAR, RDP, atau Berbagi Layar Apple), klik **Tambahkan kredensial**.
4. Di **Penyimpanan kredensial**, pilih kredensial dari daftar, lalu klik **Pilih kredensial**.

Menghapus kredensial

Anda dapat menghapus kredensial yang sudah tidak diperlukan lagi.

Untuk menghapus kredensial dari penyimpanan Kredensial

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Akses menu **Pengaturan** dengan salah satu cara berikut:
   - Klik **Desktop jarak jauh**, dan kemudian klik **Pengaturan**.
   - Klik **Kelola**, dan kemudian klik **Pengaturan**.
3. Pada tab protokol yang didukung (NEAR, RDP, atau Berbagi Layar Apple), klik **Hapus**.
4. Di jendela konfirmasi, klik **Hapus**.

Membatalkan penetapan kredensial dari beban kerja

Anda dapat membatalkan penetapan kredensial dari beban kerja, tetapi tetap menyimpannya di penyimpanan Kredensial.

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Akses menu **Pengaturan** dengan salah satu cara berikut:
   - Klik **Desktop jarak jauh**, dan kemudian klik **Pengaturan**.
   - Klik **Kelola**, dan kemudian klik **Pengaturan**.
3. Pada tab protokol yang didukung (NEAR, RDP, atau Berbagi Layar Apple), klik **Batalkan penetapan**.
4. Di jendela konfirmasi, klik **Batalkan penetapan**.

Bekerja dengan beban kerja terkelola

Beban kerja terkelola adalah beban kerja yang terinstal agen Perlindungan.

Anda dapat melakukan tindakan berikut pada beban kerja jarak jauh terkelola:

- terhubung untuk bantuan jarak jauh atau desktop jarak jauh dengan menggunakan NEAR dalam mode kontrol atau hanya lihat
- terhubung untuk desktop jarak jauh dengan menggunakan RDP dalam mode kontrol
- terhubung untuk bantuan jarak jauh atau desktop jarak jauh dengan menggunakan Berbagi Layar Apple dalam mode kontrol, hanya lihat, atau tutup
- terhubung untuk desktop jarak jauh melalui klien web
- memulai ulang, mematikan, tidur, mengosongkan keranjang sampah, dan mengeluarkan pengguna jarak jauh dari beban kerja jarak jauh
- mentransfer file antara beban kerja dan beban kerja jarak jauh
- memantau dengan mengambil tangkapan layar

Catatan
Sambungan desktop jarak jauh ke beban kerja terkelola memerlukan penginstalan agen Perlindungan dan menerapkan rencana manajemen jarak jauh pada beban kerja.

© Acronis International GmbH, 2003-2024

Mengonfigurasi pengaturan RDP

Anda dapat mengonfigurasi pengaturan yang akan diterapkan secara otomatis pada koneksi RDP kontrol jarak jauh ke beban kerja terkelola.

Cara mengonfigurasi pengaturan RDP beban kerja

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Akses menu **Pengaturan** dengan salah satu cara berikut:
   - Klik **Desktop jarak jauh**, dan kemudian klik **Pengaturan**.
   - Klik **Kelola**, dan kemudian klik **Pengaturan**.
3. Pada tab **RDP**, konfigurasikan pengaturannya.

Pengaturan	Deskripsi
Pemutaran audio	Pengaturan ini mengaktifkan atau menonaktifkan pengalihan suara beban kerja jarak jauh pada beban kerja lokal Anda.
Perekaman audio	Pengaturan ini menentukan apakah perekaman audio (berbicara dengan mikrofon) akan ditransfer ke beban kerja jarak jauh.
Alihkan printer	Jika Anda memilih pengaturan ini, printer dari beban kerja Anda akan tersedia pada beban kerja jarak jauh.
Alihkan file	Pengaturan ini menentukan apakah file dari beban kerja lokal akan dibagikan ke beban kerja jarak jauh.
Kedalaman warna	Pengaturan ini menentukan jumlah warna dalam gambar yang akan ditransfer RDP. Nilai yang semakin tinggi memerlukan bandwidth yang semakin tinggi. **Warna tinggi**: 16 bit **Warna sebenarnya**: • 24 bit untuk koneksi RDP melalui klien web • 32 bit untuk koneksi RDP via Hubungkan Klien

4. Klik tombol tutup.

Menghubungkan ke beban kerja terkelola untuk desktop jarak jauh atau bantuan jarak jauh

Catatan
Ketersediaan protokol koneksi yang dapat Anda gunakan untuk koneksi jarak jauh tergantung pada konfigurasi rencana manajemen jarak jauh dan sistem operasi beban kerja jarak jauh.

© Acronis International GmbH, 2003-2024

Prasyarat

- Rencana manajemen jarak jauh dengan protokol koneksi yang sesuai diaktifkan diterapkan pada beban kerja yang dikelola.
- Kuota layanan yang diperlukan ditetapkan ke beban kerja. (Kuota layanan diperoleh secara otomatis saat Anda menerapkan rencana manajemen jarak jauh ke beban kerja.)
- [Untuk koneksi Berbagi layar Apple] Berbagi Layar Apple diaktifkan pada beban kerja macOS.
- 2FA diaktifkan untuk akun pengguna Anda di Acronis Cyber Protect Cloud.

Untuk terhubung dari jarak jauh ke beban kerja terkelola untuk desktop jarak jauh atau bantuan jarak jauh

1. Dalam konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Klik beban kerja yang ingin Anda hubungkan.
3. Klik **Desktop jarak jauh**.
   Secara default, NEAR dipilih sebagai protokol koneksi.
4. [Opsional] Dalam daftar drop-down **Protokol koneksi**, pilih protokol koneksi yang ingin Anda gunakan.
5. Klik mode tampilan yang ingin Anda gunakan.

Protokol	Koneksi jarak jauh ke	Mode tampilan	Tindakan jarak jauh yang didukung
NEAR	Windows Linux macOS	**Kontrol**- Dalam mode ini, Anda akan dapat mengamati dan melakukan operasi pada beban kerja jarak jauh. **Hanya lihat**- Dalam mode ini, Anda hanya akan dapat mengamati beban kerja jarak jauh.	Desktop jarak jauh Bantuan jarak jauh
RDP	Windows	**Kontrol**- Dalam mode ini, Anda akan dapat melihat dan melakukan operasi pada beban kerja jarak jauh.	Desktop jarak jauh

© Acronis International GmbH, 2003-2024

Protokol	Koneksi jarak jauh ke	Mode tampilan	Tindakan jarak jauh yang didukung
		Catatan Jika RDP dinonaktifkan di pengaturan OS beban kerja, jendela pop-up akan muncul. Gunakan jendela ini guna mengaktifkan RDP untuk beban kerja di sesi saat ini atau secara umum: • Jika Anda ingin mengaktifkan RDP untuk beban kerja ini saja di sesi saat ini, pilih **Matikan setelah sesi berakhir**, kemudian klik **Izinkan**. • Jika Anda ingin mengaktifkan RDP untuk beban kerja ini, klik **Izinkan**.	
Berbagi Layar Apple	macOS	**Kontrol**- Dalam mode ini, Anda akan dapat mengamati dan melakukan operasi pada beban kerja jarak jauh. **Hanya lihat**- Dalam mode ini, Anda hanya akan dapat mengamati beban kerja jarak jauh. **Tutup** - hanya tersedia untuk beban kerja macOS. Jika Anda menghubungkan beban kerja jarak jauh dalam mode tutup, tampilan beban kerja jarak jauh akan diredupkan dan pengguna jarak jauh tidak akan dapat melihat tindakan Anda terhadap beban kerja.	Desktop jarak jauh Bantuan jarak jauh

6. Bergantung pada apakah Hubungkan Klien diinstal pada beban kerja atau tidak, lakukan salah satu hal berikut:
   - Jika Hubungkan Klien tidak diinstal, unduh, instal, lalu pilih **Izinkan** pada pop-up konfirmasi yang muncul.
   - Jika Hubungkan Klien sudah diinstal, klik **Buka Connect Client** pada pop-up konfirmasi yang muncul.
7. Di jendela **Autentikasi**, pilih satu opsi autentikasi, lalu berikan kredensial yang diperlukan.

Catatan
Jika Anda telah menetapkan kredensial ke beban kerja, autentikasi akan dilakukan secara otomatis dan langkah ini akan dilewati. Untuk informasi lebih lanjut, lihat "Menetapkan kredensial ke beban kerja" (hlm. 1007).

Opsi autentikasi	Deskripsi
Dengan	Anda akan diizinkan membuat koneksi jarak jauh setelah

© Acronis International GmbH, 2003-2024

Opsi autentikasi	Deskripsi
kredensial beban kerja jarak jauh	memberikan nama pengguna dan kata sandi pengguna administrator pada beban kerja jarak jauh. Opsi ini tersedia untuk NEAR, RDP, dan Berbagi layar Apple. Anda dapat menggunakan opsi ini untuk mengautentikasi desktop jarak jauh dan bantuan jarak jauh.
Minta izin untuk mengamati	Anda akan diizinkan membuat koneksi jarak jauh dalam mode pengamatan setelah pengguna yang masuk pada beban kerja jarak jauh mengizinkannya. Opsi ini tersedia untuk NEAR dan Berbagi layar Apple. Anda dapat menggunakan opsi ini untuk mengautentikasi bantuan jarak jauh.
Minta izin untuk mengontrol	Anda akan diizinkan membuat koneksi jarak jauh dalam mode kontrol setelah pengguna yang masuk pada beban kerja jarak jauh mengizinkannya. Opsi ini tersedia untuk NEAR dan Berbagi layar Apple. Anda dapat menggunakan opsi ini untuk mengautentikasi bantuan jarak jauh.

8. Klik **Hubungkan**, dan kemudian klik sesi yang akan ditampilkan (jika ada lebih dari satu sesi pengguna yang tersedia pada beban kerja).

   Hubungkan Klien akan membuka jendela penampil baru tempat Anda dapat melihat desktop beban kerja jarak jauh. Penampil memiliki toolbar dengan tindakan tambahan yang dapat Anda lakukan pada beban kerja jarak jauh setelah koneksi jarak jauh dibuat. Untuk informasi lebih lanjut, lihat "Menggunakan toolbar di jendela Penampil" (hlm. 1020).

Menghubungkan ke beban kerja terkelola melalui klien web

Anda dapat membuat koneksi desktop jarak jauh ke beban kerja terkelola melalui klien web.

Prasyarat

- Kuota layanan standar ditetapkan ke beban kerja.
- Rencana manajemen jarak jauh yang mengaktifkan RDP diterapkan pada beban kerja yang dikelola.
- RDP diaktifkan pada beban kerja terkelola.
- Browser Anda mendukung HTML5.
- 2FA diaktifkan untuk akun pengguna Anda di Acronis Cyber Protect Cloud.

Untuk terhubung dari jarak jauh ke beban kerja melalui klien web

© Acronis International GmbH, 2003-2024

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Klik beban kerja yang ingin Anda hubungkan dari jarak jauh, lalu klik **Desktop jarak jauh**>**Hubungkan melalui klien web**.
3. Masukkan login dan kata sandi untuk mengakses beban kerja, kemudian klik **Hubungkan**.

> **Catatan**
> Jika Anda telah menetapkan kredensial ke beban kerja, autentikasi akan dilakukan secara otomatis dan langkah ini akan dilewati. Untuk informasi lebih lanjut, lihat "Menetapkan kredensial ke beban kerja" (hlm. 1007).

Mentransfer file

Anda dapat mentransfer file dengan mudah antara beban kerja lokal dan beban kerja terkelola.

Prasyarat

- Rencana manajemen jarak jauh yang memiliki protokol NEAR dan transfer file yang diaktifkan diterapkan pada beban kerja.
- Kuota Manajemen Tingkat Lanjut diterapkan pada beban kerja.
- 2FA diaktifkan untuk akun pengguna Anda di Acronis Cyber Protect Cloud.

Cara mentransfer file dari jarak jauh antara beban kerja dan beban kerja terkelola

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Klik beban kerja yang ingin Anda transfer filenya.
3. Klik **Kelola**, dan kemudian **Transfer file**.
4. Bergantung pada apakah Hubungkan Klien diinstal pada beban kerja atau tidak, lakukan salah satu hal berikut:
   - Jika Hubungkan Klien tidak diinstal, unduh, instal, lalu klik **Izinkan** pada pop-up konfirmasi yang muncul.
   - Jika Hubungkan Klien sudah diinstal, klik **Buka Connect Client** pada pop-up konfirmasi yang muncul.
5. Di jendela **Autentikasi**, pilih satu opsi autentikasi, lalu berikan kredensial yang diperlukan.

Opsi autentikasi	Deskripsi
Dengan kredensial beban kerja jarak jauh	Anda akan diizinkan membuat koneksi jarak jauh setelah memberikan nama pengguna dan kata sandi pengguna administrator pada beban kerja jarak jauh.
Minta izin untuk transfer file	Anda akan diizinkan untuk mentransfer file setelah pengguna yang masuk pada beban kerja jarak jauh mengizinkannya.

6. Di jendela **Transfer file**, telusuri file lalu tarik dan lepas file ke tujuan yang diinginkan.

© Acronis International GmbH, 2003-2024

Catatan
File beban kerja lokal dicantumkan di panel sebelah kiri, sementara file beban kerja jarak jauh dicantumkan di panel sebelah kanan.
Ketika transfer file dimulai, file dicantumkan di panel **Tugas**.

7. [Opsional] Jika Anda ingin menghapus tugas yang sudah selesai dari panel **Tugas**, klik **Hapus yang sudah selesai**.
8. Ketika semua transfer selesai, tutup jendela.

Melakukan tindakan kontrol pada beban kerja terkelola

Anda dapat mengelola beban kerja jarak jauh dengan melakukan tindakan kontrol dasar pada beban kerja tersebut: keranjang sampah kosong, tidur, mulai kembali, matikan, dan keluarkan pengguna jarak jauh.

Prasyarat

- Kuota layanan standar diterapkan ke beban kerja.
- 2FA diaktifkan untuk akun pengguna Anda di Acronis Cyber Protect Cloud.

Kosongkan keranjang sampah

Untuk mengosongkan keranjang sampah pada beban kerja jarak jauh

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Klik beban kerja tempat Anda ingin melakukan tindakan ini.
3. Klik **Kelola**, lalu klik **Kosongkan keranjang sampah**.
4. Pilih sesi pengguna tempat Anda ingin melakukan tindakan ini, lalu klik **Kosongkan keranjang sampah**.

Tidur

Untuk mengaktifkan mode tidur pada beban kerja jarak jauh

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Klik beban kerja tempat Anda ingin melakukan tindakan ini.
3. Klik **Kelola**, lalu klik **Tidur**.

Mulai Kembali

Untuk memulai ulang beban kerja jarak jauh

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Klik beban kerja tempat Anda ingin melakukan tindakan ini.
3. Klik **Kelola**, lalu klik **Mulai Kembali**.

© Acronis International GmbH, 2003-2024

- Untuk beban kerja Windows, pilih apakah Anda ingin mengizinkan pengguna yang secara lokal masih masuk dalam beban kerja untuk menyimpan perubahan sebelum beban kerja dimulai ulang, pilih penggunanya, lalu klik **Mulai Kembali** lagi.
- Untuk beban kerja macOS, pilih apakah Anda ingin mengizinkan pengguna yang secara lokal masih masuk dalam beban kerja untuk menyimpan perubahan sebelum beban kerja dimulai ulang, pilih penggunanya, lalu klik **Mulai Kembali** lagi.
- Untuk beban kerja Linux, Klik **Mulai Kembali**.

Matikan

Untuk mematikan beban kerja jarak jauh

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Klik beban kerja tempat Anda ingin melakukan tindakan ini.
3. Klik **Kelola**, lalu klik **Matikan**.
   - Untuk beban kerja Windows, pilih apakah Anda ingin mengizinkan pengguna yang secara lokal masih masuk dalam beban kerja untuk menyimpan perubahan sebelum beban kerja dimatikan, pilih penggunanya, lalu klik **Matikan** lagi.
   - Untuk beban kerja macOS, pilih apakah Anda ingin mengizinkan pengguna yang secara lokal masih masuk dalam beban kerja untuk menyimpan perubahan sebelum beban kerja dimatikan, lalu klik **Matikan** lagi.
   - Untuk beban kerja Linux, Klik **Matikan** lagi.

Keluarkan pengguna jarak jauh

Untuk mengeluarkan pengguna dari beban kerja jarak jauh

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Klik beban kerja tempat Anda ingin melakukan tindakan ini.
3. Klik **Kelola**, lalu klik **Keluarkan pengguna jarak jauh**.
4. Pilih akun pengguna yang ingin Anda keluarkan, lalu klik **Keluar**.

Pemantauan beban kerja melalui transmisi tangkapan layar

Anda dapat memantau status beban kerja menggunakan fitur Transmisi tangkapan layar.

Prasyarat

- Rencana manajemen jarak jauh dengan fitur transmisi Tangkapan Layar yang diaktifkan diterapkan pada beban kerja.
- Versi agen Perlindungan telah diperbarui dan mendukung fitur Transmisi tangkapan layar.
- Kuota layanan Manajemen Tingkat Lanjut diterapkan pada beban kerja.
- Beban kerja ini online.
- 2FA diaktifkan untuk akun pengguna Anda di Acronis Cyber Protect Cloud.

© Acronis International GmbH, 2003-2024

Memantau beban kerja melalui Transmisi tangkapan layar

Untuk memantau beban kerja melalui transmisi Tangkapan layar

1. Di konsol Cyber Protect, buka **Perangkat**>**Transmisi tangkapan layar**.
2. Klik beban kerja yang ingin Anda pantau.
3. Pilih sesi pengguna.
4. Pilih tampilan.
5. Pilih kecepatan refresh untuk mengambil tangkapan layar baru desktop.
6. Pilih kualitas gambar.
7. Untuk mengunduh tangkapan layar, klik ikon unduh.

Mengambil tangkapan layar beban kerja

Cara mengambil tangkapan layar beban kerja terkelola

1. Di konsol Cyber Protect, buka **Perangkat** > **Mesin dengan agen**.
2. Klik beban kerja yang ingin Anda ambil tangkapan layarnya.
3. Klik **Kelola**, lalu klik **Ambil tangkapan layar desktop**.
   Layar **Transmisi tangkapan layar** akan terbuka, dengan beban kerja yang sudah dipilih sebelumnya. Bergantung pada pengaturan rencana manajemen jarak jauh yang diterapkan pada beban kerja, Anda akan melihat tangkapan layar atau Anda akan melihat tangkapan layar setelah pengguna beban kerja jarak jauh menyetujui permintaan tersebut.

Mengamati beberapa beban kerja terkelola secara bersamaan

Anda dapat mengamati desktop dari beberapa beban kerja jarak jauh secara bersamaan dalam satu jendela.

Catatan
Jumlah desktop yang dapat Anda lihat secara bersamaan di jendela bergantung pada ukuran monitor Anda.

Prasyarat

- NEAR / Apple Screen Sharing diaktifkan dalam rencana manajemen jarak jauh yang diterapkan pada beban kerja.
- Kuota layanan Manajemen Tingkat Lanjut diterapkan pada beban kerja.
- 2FA diaktifkan untuk akun pengguna Anda di Acronis Cyber Protect Cloud.

Cara mengamati beberapa beban kerja secara bersamaan

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih beban kerja yang ingin Anda amati.

© Acronis International GmbH, 2003-2024

3. Klik **Multi-tampilan**.
4. Bergantung pada apakah Hubungkan Klien diinstal pada beban kerja atau tidak, lakukan salah satu hal berikut:
   - Jika Hubungkan Klien tidak diinstal, unduh, instal, lalu pilih **Izinkan** pada pop-up konfirmasi yang muncul.
   - Jika Hubungkan Klien sudah diinstal, klik **Buka Connect Client** pada pop-up konfirmasi yang muncul.
5. Di jendela **Autentikasi**, pilih satu opsi autentikasi, lalu berikan kredensial yang diperlukan.

Opsi autentikasi	Deskripsi
Dengan kredensial beban kerja jarak jauh	Anda akan diizinkan membuat koneksi jarak jauh setelah memberikan nama pengguna dan kata sandi pengguna administrator pada beban kerja jarak jauh.
Minta izin untuk mengamati	Anda akan diizinkan membuat koneksi jarak jauh dalam mode pengamatan setelah pengguna yang masuk pada beban kerja jarak jauh mengizinkannya.

6. Jika Anda ingin menggunakan metode dan kredensial autentikasi yang sama ketika terhubung ke semua beban kerja jarak jauh yang dipilih di langkah 2, pilih **Gunakan di komputer lainnya**.
7. Klik **Hubungkan**.

   Pada toolbar jendela multi-tampilan, Anda dapat memilih mode tampilan untuk menghubungkan beban kerja. Tindakan ini akan membuka jendela Penampil terpisah untuk beban kerja tersebut.

Catatan

Jika semua beban kerja yang dipilih offline atau versi agen yang diinstal sudah kedaluwarsa, beban kerja tidak akan ditampilkan di jendela multi-tampilan.

Semua koneksi multi-tampilan ke beban kerja jarak jauh berada dalam mode tampilan **Hanya lihat**.

Bekerja dengan beban kerja tidak terkelola

Beban kerja tidak terkelola adalah beban kerja yang tidak terinstal agen Perlindungan.

Anda dapat melakukan tindakan berikut pada beban kerja jarak jauh tidak terkelola:

- terhubung untuk bantuan jarak jauh dengan menggunakan Acronis Bantuan Cepat
- terhubung untuk desktop jarak jauh atau bantuan jarak jauh dengan menggunakan alamat IP
- transfer file antara beban kerja dan beban kerja jarak jauh menggunakan Bantuan Cepat

© Acronis International GmbH, 2003-2024

Catatan
Terhubung dari jarak jauh ke beban kerja yang tidak terkelola dengan menggunakan Bantuan Cepat, pastikan bahwa:

- Paket Manajemen Tingkat Lanjut diaktifkan untuk penyewa pelanggan Anda.
- Aplikasi Bantuan Cepat berjalan pada beban kerja jarak jauh yang ingin Anda hubungkan.

Menghubungkan ke beban kerja tidak terkelola melalui Acronis Bantuan Cepat

Anda dapat menggunakan fitur Bantuan cepat untuk terhubung dari jarak jauh sesuai permintaan ke beban kerja yang tidak terkelola dan memberikan bantuan satu kali.

Prasyarat

- Paket Manajemen Tingkat Lanjut ditetapkan ke penyewa pelanggan Anda.
- 2FA diaktifkan untuk akun pengguna Anda di Acronis Cyber Protect Cloud.
- Pengguna jarak jauh telah memberikan ID beban kerja dan kode akses dari Bantuan Cepat.
- Pengguna jarak jauh telah mengunduh dan menjalankan Acronis Bantuan Cepat.

Untuk terhubung ke beban kerja pada bantuan jarak jauh dengan menggunakan Bantuan Cepat

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Klik **Bantuan Cepat**.
3. Dalam jendela **Bantuan Cepat**, masukkan ID beban kerja yang diberikan pengguna akhir kepada Anda, lalu pilih **Hubungkan**.
4. Klik **Hubungkan**.
5. Bergantung pada apakah Hubungkan Klien diinstal pada beban kerja atau tidak, lakukan salah satu hal berikut:
   - Jika Hubungkan Klien tidak diinstal, unduh, instal, lalu pilih **Izinkan** pada pop-up konfirmasi yang muncul.
   - Jika Hubungkan Klien sudah diinstal, klik **Buka Connect Client** pada pop-up konfirmasi yang muncul.
6. Di jendela **Autentikasi**, masukkan kode akses.
7. Hubungkan Klien akan membuka jendela penampil baru tempat Anda dapat melihat desktop beban kerja jarak jauh. Penampil memiliki toolbar dengan tindakan tambahan yang dapat Anda lakukan pada beban kerja jarak jauh setelah koneksi jarak jauh dibuat. Untuk informasi lebih lanjut, lihat "Menggunakan toolbar di jendela Penampil" (hlm. 1020).

© Acronis International GmbH, 2003-2024

Menghubungkan ke beban kerja yang tidak terkelola melalui alamat IP

Jika beban kerja tidak terkelola ada di LAN, Anda dapat terhubung pada kontrol jarak jauh atau bantuan jarak jauh menggunakan alamat IP-nya. Koneksi ini tidak memerlukan akses Internet.

Prasyarat

- Paket Manajemen Tingkat Lanjut ditetapkan ke penyewa pelanggan Anda.
- 2FA diaktifkan untuk akun pengguna Anda di Acronis Cyber Protect Cloud.

Untuk terhubung ke beban kerja pada desktop atau bantuan jarak jauh dengan menggunakan alamat IP-nya

1. Di konsol Cyber Protect, buka **Semua perangkat**.
2. Klik **Bantuan Cepat**.
3. Klik tab **Melalui alamat IP**.
4. Masukkan alamat IP dan port beban kerja.
5. Pilih protokol koneksi - RDP (Beban kerja Windows) atau Berbagi layar Apple (untuk beban kerja macOS), bergantung pada sistem operasi beban kerja jarak jauh.

   Catatan
   Koneksi melalui RDP mendukung tindakan desktop jarak jauh, dan koneksi melalui Berbagi layar Apple mendukung tindakan desktop jarak jauh dan bantuan jarak jauh.

6. Klik **Hubungkan**.
7. Di jendela **Autentikasi**, berikan kredensial yang diperlukan.

Untuk koneksi Berbagi Layar Apple, Hubungkan Klien akan membuka jendela penampil baru tempat Anda dapat melihat desktop beban kerja jarak jauh. Penampil memiliki toolbar dengan tindakan tambahan yang dapat Anda lakukan pada beban kerja jarak jauh setelah koneksi jarak jauh dibuat. Untuk informasi lebih lanjut, lihat "Menggunakan toolbar di jendela Penampil" (hlm. 1020).

Mentransfer file melalui Acronis Bantuan Cepat

Anda dapat menggunakan fitur Bantuan cepat untuk mentransfer file antara beban kerja dan beban kerja tidak terkelola.

Prasyarat

- Paket Manajemen Tingkat Lanjut ditetapkan ke penyewa pelanggan Anda.
- 2FA diaktifkan untuk akun pengguna Anda di Acronis Cyber Protect Cloud.

© Acronis International GmbH, 2003-2024

- Pengguna jarak jauh telah mengunduh dan menjalankan Acronis Bantuan Cepat.
- Pengguna jarak jauh telah memberikan ID komputer dan kode akses dari Bantuan Cepat.

Untuk mentransfer file ke beban kerja dengan menggunakan Bantuan Cepat

1. Di konsol Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Klik **Bantuan cepat**.
3. Di jendela **Bantuan cepat**, masukkan ID beban kerja yang diberikan pengguna akhir kepada Anda, lalu pilih **Transfer File**.
4. Klik **Hubungkan**.
5. Bergantung pada apakah Hubungkan Klien diinstal pada beban kerja atau tidak, lakukan salah satu hal berikut:
   - Jika Hubungkan Klien tidak diinstal, unduh, instal, lalu pilih **Izinkan** pada pop-up konfirmasi yang muncul.
   - Jika Hubungkan Klien sudah diinstal, klik **Buka Connect Client** pada pop-up konfirmasi yang muncul.
6. Di jendela **Autentikasi**, masukkan kode akses.
7. Di jendela **Transfer file**, telusuri file lalu tarik dan lepas file ke tujuan yang diinginkan.

   Catatan
   File beban kerja lokal dicantumkan di panel sebelah kiri, sementara file beban kerja jarak jauh dicantumkan di panel sebelah kanan.
   Ketika transfer file dimulai, file dicantumkan di panel **Tugas**.

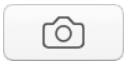
8. [Opsional] Jika Anda ingin menghapus tugas yang sudah selesai dari panel **Tugas**, klik **Hapus yang sudah selesai**.
9. Ketika semua transfer selesai, tutup jendela.

Menggunakan toolbar di jendela Penampil

Setelah terhubung ke beban kerja jarak jauh, Anda dapat menggunakan toolbar jendela penampil untuk melakukan berbagai tindakan.

Ikon	Deskripsi
	Ukuran aktual Menskalakan desktop beban kerja jarak jauh sehingga satu piksel desktop jarak jauh sesuai dengan satu piksel pada jendela penampil.
	Zoom agar pas Menskalakan desktop beban kerja agar pas dengan jendela penampil.

© Acronis International GmbH, 2003-2024

Ikon	Deskripsi
	Kunci dan **Buka kunci layar** Menampilkan placeholder pada layar beban kerja jarak jauh sehingga pengguna jarak jauh tidak akan melihat tindakan Anda.
	**Ambil tangkapan layar** Menyimpan gambar desktop server jarak jauh ke file lokal.
	Pilih tampilan Memilih tampilan beban kerja jarak jauh yang ingin Anda lihat dan resolusi yang diinginkan. Tersedia untuk koneksi Berbagi Layar Apple ke macOS, dan koneksi NEAR ke semua sistem operasi.
	Kualitas gambar Menyesuaikan kualitas gambar layar jarak jauh dari hitam putih hingga setinggi mungkin pada koneksi Berbagi Layar Apple.
	Kualitas gambar NEAR Menyesuaikan rasio kualitas/performa pada koneksi NEAR. Sisi kiri penggeser (Halus) lebih memprioritaskan performa dibandingkan kualitas gambar, sisi kanan (Tajam) berarti kualitas layar desktop jarak jauh terbaik, tetapi mungkin dengan performa yang lebih buruk.
	Kirim Ctrl+Alt+Del Mengirimkan urutan Ctrl + Alt + Delete ke beban kerja jarak jauh. Tersedia untuk beban kerja Windows dan Linux.
	Transfer File Membuka jendela Manajer File untuk bertukar file antara beban kerja jarak jauh dan lokal. Tersedia untuk koneksi NEAR.
	Sematkan toolbar Menonaktifkan penyembunyian otomatis toolbar penampil. Tersedia untuk beban kerja Windows.
	Layar penuh Beralih ke mode layar penuh dan menskalakan beban kerja jarak jauh untuk memenuhi layar lokal sepenuhnya. Tersedia untuk beban kerja Windows.

© Acronis International GmbH, 2003-2024

Ikon	Deskripsi
	Tutup Menutup jendela Penampil dan mengakhiri sesi kontrol jarak jauh. Tersedia untuk beban kerja Windows.

Bergantung pada jenis koneksi, opsi tambahan mungkin tersedia ketika Anda mengeklik ikon **Lainnya**.

Opsi	Deskripsi
Mulai perekaman / Hentikan perekaman	Rekam sesi desktop jarak jauh saat ini. Rekaman sesi disimpan sebagai file .crec pada beban kerja lokal. Anda dapat membuka file .crec dengan Acronis Hubungkan Klien. Tersedia untuk koneksi NEAR
Sinkronisasi otomatis papan klip	Ketika opsi ini aktif, klien akan otomatis menyinkronkan papan klip lokal dan papan klip komputer jarak jauh. Tersedia untuk koneksi NEAR dan Berbagi Layar Apple
Kirim papan klip **Dapatkan papan klip**	**Kirim Papan Klip** menggantikan isi papan klip komputer jarak jauh dengan isi papan klip lokal. **Dapatkan Papan Klip** mentransfer isi papan klip komputer jarak jauh ke papan klip lokal.
Keyboard pintar / Tombol raw / Tombol raw dengan semua pintasan	Mengubah mode input keyboard untuk koneksi saat ini. **Keyboard pintar**- klien mentransmisikan kode Unicode simbol yang diketik secara lokal ke komputer jarak jauh **Tombol raw**- klien menggunakan kode raw tombol keyboard yang Anda tekan. **Tombol raw dengan semua pintasan**- klien menonaktifkan pintasan sistem lokal sehingga akan ditransmisikan juga ke sistem operasi jarak jauh.
Keyboard fokus pada mengarahkan pointer mouse	Ketika diaktifkan, klien hanya menangkap input keyboard ketika kursor mouse lokal diletakkan di atas jendela Penampil. Ketika dinonaktifkan, klien menangkap keyboard setiap kali jendelanya aktif.
Tampilkan info koneksi / Sembunyikan info koneksi	Ketika **Tampilkan info koneksi** dipilih, panel informasi kecil akan muncul di layar desktop jarak jauh dan menunjukkan informasi paling penting mengenai koneksi saat ini.
Suara jarak jauh	Memungkinkan klien mengalihkan suara dari komputer jarak jauh ke komputer lokal.

© Acronis International GmbH, 2003-2024

Opsi	Deskripsi
	Tersedia untuk koneksi NEAR
Preferensi	Konfigurasi pengaturan Hubungkan Klien. Untuk informasi lebih lanjut, lihat "Mengonfigurasi pengaturan Hubungkan Klien" (hlm. 1023).

Merekam dan memutar sesi jarak jauh

Anda dapat merekam sesi jarak jauh melalui NEAR di Acronis Hubungkan Klien.

Untuk merekam sesi jarak jauh

1. Pada toolbar Viewer di Hubungkan Klien, klik **Lainnya**, dan pilih **Mulai Merekam**.
2. Pilih nama dan lokasi untuk rekaman.

   Secara default, file akan diberi nama dengan tanggal dan waktu saat ini serta berlokasi di folder **Dokumen** dalam direktori home pengguna saat ini. Selama perekaman aktif, di toolbar **Viewer** Anda akan melihat lingkaran merah berkedip di sudut kanan atas layar remote dan timer perekaman.
3. Untuk menghentikan perekaman, klik **Lainnya**, lalu klik **Hentikan Perekaman**. Di Mac, Anda juga bisa klik **Berhenti** di toolbar.

   Semua file .crec yang dibuat oleh Acronis Hubungkan Klien secara default akan dibuka dengan Acronis Hubungkan Klien.

Untuk memutar rekaman

1. Temukan lokasi file rekaman.
2. Buka file.

   Pemutar rekaman Acronis Hubungkan Klien terbuka. Perhatikan bahwa Anda tidak dapat melakukan penelusuran di sepanjang rekaman. Untuk menemukan momen tertentu dalam rekaman, tunggulah sampai pemutar mencapai momen tersebut.
3. [Opsional] Untuk mengatur kecepatan pemutar, gunakan ikon **<<** dan **>>** di bagian kontrol pemutaran.

   Rekaman disimpan sebagai urutan peristiwa yang telah ditransmisikan ke dan dari server jarak jauh selama koneksi berlangsung. Ini memastikan kualitas terbaik dari rekaman dengan ukuran file minimum tercapai. Namun, ini juga bisa berarti bahwa melakukan penelusuran di sepanjang rekaman tidak mungkin dilakukan. Mengubah rekaman menjadi format video juga tidak mungkin dilakukan untuk saat ini.

Mengonfigurasi pengaturan Hubungkan Klien

Setelah menginstal Hubungkan Klien pada beban kerja Anda, Anda dapat mengonfigurasi pengaturannya sesuai dengan preferensi.

Untuk mengonfigurasi pengaturan Hubungkan Klien

© Acronis International GmbH, 2003-2024

1. Di menu start, cari **Hubungkan Klien**, lalu mulai.
2. Konfigurasikan pengaturan di tab **Umum**.

Opsi	Deskripsi
Tulis log verbose	Pilih opsi ini untuk mengizinkan Hubungkan Klien menulis log verbose. Jika dinonaktifkan, klien hanya akan menulis informasi umum ke file log.
Pengaturan proxy	Pilih untuk menggunakan Proxy sistem default atau mengonfigurasi Proxy SOCKSS kustom.

3. Konfigurasikan pengaturan pada tab **Penampil**.

Opsi	Deskripsi
Minta konfirmasi ketika menutup penampil	Pilih opsi ini jika ingin Hubungkan Klien menampilkan pesan konfirmasi saat Anda mencoba menutup jendela Penampil untuk mencegah penutupan yang tidak disengaja.
Ketika diminimalkan	Pilih apakah akan menangguhkan aktivitas Penampil saat diminimalkan untuk mengurangi beban CPU.
Ketika dimaksimalkan	Pilih apakah akan mengaktifkan mode layar penuh saat dimaksimalkan.
Transfer papan klip	Aktifkan opsi untuk menampilkan indikator transfer Papan klip di jendela Penampil setiap kali Anda menyalin atau menempelkan teks dan gambar.
Mode Keyboard	Aktifkan opsi untuk menampilkan indikator mode Input di judul jendela Penampil setiap kali peristiwa mouse dan keyboard dikirim ke mesin jarak jauh.
Papan klip	Pilih **Sinkronkan papan klip secara otomatis** untuk mengaktifkan sinkronisasi papan klip, jika tersedia.
Kirim peristiwa keyboard	Pilih apakah akan mengambil input keyboard lokal kapan pun jendela Hubungkan Klien aktif atau hanya ketika pointer mouse lokal Anda berada di atasnya.
Warna latar belakang Penampil	Ubah warna latar belakang jendela Penampil.
Hubungkan kembali secara otomatis	Pilih **Aktifkan untuk terhubung kembali secara otomatis**, jika Anda ingin Hubungkan Klien secara otomatis membuat kembali koneksi jika terputus.
H.264	Anda dapat menonaktifkan dekoder perangkat keras.
Tutup saat idle	Pilih interval waktu idle untuk menutup jendela Penampil.

4. Konfigurasikan pengaturan pada tab **Keyboard**.

© Acronis International GmbH, 2003-2024

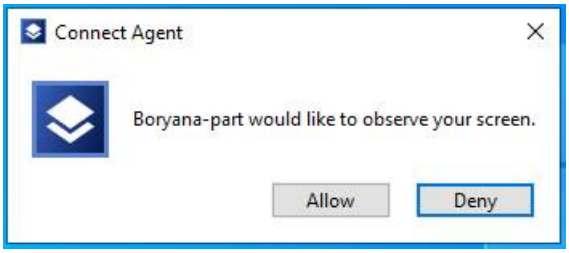
Opsi	Deskripsi
Pemetaan pengubah	Ubah perilaku tombol pengubah dengan menu pop-up. Pengaturan ini disimpan secara terpisah untuk koneksi NEAR, Berbagi layar Apple, dan RDP.
Mode input	Untuk setiap jenis koneksi (dipilih di header panel), pilih mode input keyboard default.

5. Klik **OK**.

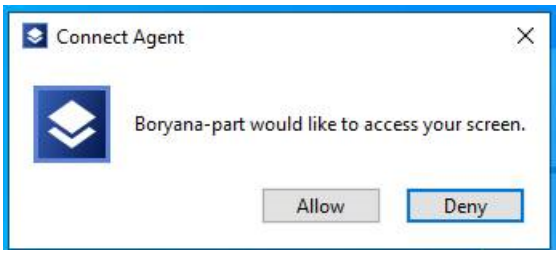
Pemberitahu desktop jarak jauh

Connect Agent menampilkan dialog tindakan (pemberi tahu) pada desktop beban kerja jarak jauh dalam kasus berikut:

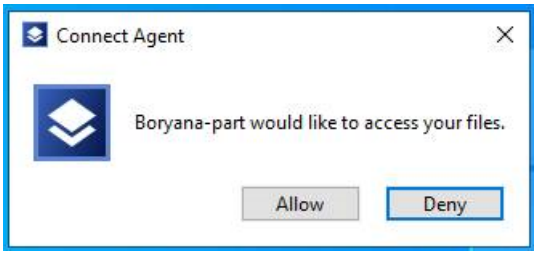
- ketika Anda mencoba terhubung ke beban kerja secara jarak jauh dengan meminta izin untuk mengamati. Pengguna yang masuk ke beban kerja jarak jauh secara lokal dapat mengizinkan atau menolak permintaan.



- ketika Anda mencoba terhubung ke beban kerja secara jarak jauh dengan meminta izin untuk mengontrol. Pengguna yang masuk ke beban kerja jarak jauh secara lokal dapat mengizinkan atau menolak permintaan.



- ketika Anda mencoba melakukan pertukaran file antara beban kerja dan beban kerja jarak jauh dengan meminta izin untuk mentransfer file. Pengguna yang masuk ke beban kerja jarak jauh secara lokal dapat mengizinkan atau menolak permintaan.

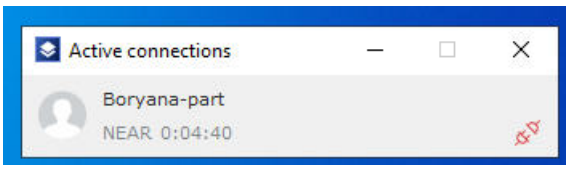


© Acronis International GmbH, 2003-2024

Ketika Anda membuat koneksi desktop jarak jauh ke beban kerja, pengguna yang masuk ke beban kerja akan melihat pemberitahu koneksi yang berbeda yang berisi informasi berikut:

- nama pengguna yang terhubung dari jarak jauh
- protokol koneksi yang digunakan untuk membuat koneksi jarak jauh
- durasi koneksi jarak jauh

Pengguna yang masuk ke beban kerja jarak jauh secara lokal dapat mengakhiri koneksi kapan saja dengan mengeklik ikon **Putuskan hubungan** atau ikon **Tutup**.



© Acronis International GmbH, 2003-2024

Pemantauan kesehatan dan kinerja beban kerja

Anda dapat memantau parameter sistem dan kesehatan beban kerja di organisasi Anda. Jika parameter melebihi batas normal, Anda akan segera diberi tahu dan dapat menyelesaikan masalah dengan cepat. Anda juga dapat mengonfigurasi peringatan kustom dan tindakan respons otomatis. Ini adalah tindakan yang akan dilakukan secara otomatis untuk menyelesaikan anomali dalam perilaku beban kerja.

Catatan
Fungsi pemantauan memerlukan instalasi agen Perlindungan versi 15.0.35324 atau lebih baru pada beban kerja.

Rencana pemantauan

Untuk mulai memantau kinerja, perangkat keras, perangkat lunak, sistem, dan parameter keamanan dari beban kerja terkelola Anda, terapkan rencana pemantauan untuk mereka. Rencana pemantauan terdiri dari berbagai monitor yang dapat Anda aktifkan dan konfigurasikan. Beberapa monitor mendukung jenis pemantauan berbasis anomali. Untuk informasi lebih lanjut tentang rencana pemantauan, lihat "Rencana pemantauan" (hlm. 1061). Untuk informasi selengkapnya tentang monitor yang tersedia yang dapat Anda konfigurasikan dalam rencana pemantauan, lihat "Monitor yang dapat dikonfigurasi" (hlm. 1028).

Jika agen tidak dapat mengumpulkan data dari beban kerja karena alasan tertentu, sistem akan mengeluarkan peringatan.

Jenis pemantauan

Anda harus mengonfigurasi jenis pemantauan untuk setiap monitor yang Anda aktifkan dalam rencana. Jenis pemantauan menentukan algoritme yang akan digunakan monitor untuk memperkirakan perilaku normal dan deviasi beban kerja. Ada dua jenis pemantauan: berbasis ambang batas dan berbasis anomali. Beberapa monitor hanya mendukung jenis pemantauan berbasis ambang batas.

Pemantauan berbasis ambang batas melacak apakah nilai parameter di atas atau di bawah nilai ambang yang Anda konfigurasikan. Dengan jenis pemantauan ini, Anda bertanggung jawab untuk menentukan nilai ambang batas yang tepat untuk beban kerja. Sistem menentukan perilaku normal berdasarkan nilai ambang batas statis ini dan tanpa mempertimbangkan kondisi khusus lain yang mungkin menyebabkan perilaku tersebut. Untuk alasan ini, pemantauan berbasis ambang mungkin kurang akurat dibandingkan dengan pemantauan berbasis anomali.

Pemantauan berbasis anomali menggunakan pembelajaran mesin untuk membuat pola perilaku normal untuk beban kerja dan untuk mendeteksi perilaku abnormal. Untuk informasi lebih lanjut, lihat "Pemantauan berbasis anomali" (hlm. 1028).

© Acronis International GmbH, 2003-2024

Pemantauan berbasis anomali

Pemantauan berbasis anomali menggunakan model pembelajaran mesin untuk membuat pola perilaku normal untuk beban kerja dan untuk mendeteksi anomali (lonjakan yang tak terduga dalam data rangkaian waktu) dalam perilaku beban kerja. Ketika Anda mengaktifkan jenis pemantauan ini, sistem membuat model dan memulai pelatihan sendiri serta menyesuaikan model untuk beban kerja tertentu berdasarkan data yang dikumpulkan dari beban kerja. Artinya, di awal periode pelatihan, datanya mungkin tidak akan sepenuhnya akurat. Membuat model yang andal memerlukan pelatihan model setidaknya selama tiga minggu. Saat sistem mengumpulkan lebih banyak data dan menganalisis set data historis, sistem perlahan akan menyempurnakan model dan membuat ambang batas atas dan bawah yang dinamis untuk setiap metrik beban kerja. Tipe pemantauan ini lebih fleksibel dibandingkan dengan pemantauan berbasis ambang batas, karena sistem memantau nilai parameter dan konteksnya. Misalnya, beban kerja tertentu mungkin akan memiliki muatan yang lebih besar pada jam-jam tertentu. Tipe pemantauan berbasis ambang batas akan salah mengartikannya sebagai perilaku tidak normal dan akan memicu peringatan.

Anda dapat mengatur ulang model pembelajaran mesin beban kerja. Dalam hal ini, sistem akan menghapus semua data dan model untuk monitor yang diterapkan ke beban kerja. Untuk informasi lebih lanjut, lihat "Memulai ulang model pembelajaran mesin" (hlm. 1071).

Platform yang didukung untuk pemantauan

Fungsi pemantauan didukung oleh sistem operasi berikut.

Versi Windows yang didukung	Versi macOS yang didukung
• 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 yang dapat dikonfigurasi

Fungsi pemantauan mendukung monitor berikut, dibagi menjadi enam kategori: Perangkat Keras, Performa, Perangkat Lunak, Sistem, Keamanan, dan Kustom.

© Acronis International GmbH, 2003-2024

Monitor	Deskripsi	Sistem Operasi yang Didukung	Frekuensi pengumpulan data	Dukungan pemantauan berbasis anomali	Ketersediaan dalam Perlindungan standar atau Manajemen Tingkat Lanjut
Perangkat keras					
Ruang disk	Memantau ruang bebas pada drive tertentu dari beban kerja.	Windows macOS	1 menit	Iya	Perlindungan standar
Suhu CPU	Memantau suhu CPU.	Windows macOS	30 detik	Iya	Manajemen Tingkat Lanjut
Suhu GPU	Memantau suhu GPU.	Windows macOS	30 detik	Iya	Manajemen Tingkat Lanjut
Perubahan perangkat keras	Memantau perubahan perangkat keras, seperti menambah, melepas, atau mengganti perangkat keras pada beban kerja	Windows macOS	24 jam	Tidak	Perlindungan standar
Performa					
Penggunaan CPU	Memantau penggunaan CPU secara keseluruhan (berdasarkan semua CPU pada beban kerja).	Windows macOS	30 detik	Iya	Manajemen Tingkat Lanjut
Penggunaan memori	Memantau penggunaan memori secara keseluruhan	Windows macOS	30 detik	Iya	Manajemen Tingkat Lanjut

© Acronis International GmbH, 2003-2024

Monitor	Deskripsi	Sistem Operasi yang Didukung	Frekuensi pengumpulan data	Dukungan pemantauan berbasis anomali	Ketersediaan dalam Perlindungan standar atau Manajemen Tingkat Lanjut
	(oleh semua slot memori pada beban kerja).				
Kecepatan transfer disk	Memantau kecepatan baca dan tulis setiap disk fisik pada beban kerja.	Windows macOS	30 detik	Iya	Manajemen Tingkat Lanjut
Penggunaan jaringan	Memantau lalu lintas masuk dan keluar untuk setiap adaptor jaringan beban kerja.	Windows macOS	30 detik	Iya	Manajemen Tingkat Lanjut
Penggunaan CPU berdasarkan proses	Memantau penggunaan CPU berdasarkan proses tertentu.	Windows macOS	30 detik	Tidak	Manajemen Tingkat Lanjut
Penggunaan memori berdasarkan proses	Memantau penggunaan memori berdasarkan proses yang dipilih.	Windows macOS	30 detik	Tidak	Manajemen Tingkat Lanjut
Kecepatan transfer disk berdasarkan proses	Memantau kecepatan baca dan tulis dari proses yang dipilih.	Windows macOS	30 detik	Tidak	Manajemen Tingkat Lanjut

© Acronis International GmbH, 2003-2024

Monitor	Deskripsi	Sistem Operasi yang Didukung	Frekuensi pengumpulan data	Dukungan pemantauan berbasis anomali	Ketersediaan dalam Perlindungan standar atau Manajemen Tingkat Lanjut
Penggunaan jaringan berdasarkan proses	Memantau lalu lintas masuk dan keluar dari proses yang dipilih.	Windows macOS	30 detik	Tidak	Manajemen Tingkat Lanjut
Perangkat Lunak					
Status layanan Windows	Memantau status layanan Windows yang dipilih (Berjalan atau Berhenti).	Windows	30 detik	Tidak	Manajemen Tingkat Lanjut
Status proses	Memantau status proses yang dipilih (Berjalan atau Berhenti).	Windows macOS	30 detik	Tidak	Manajemen Tingkat Lanjut
Perangkat lunak yang diinstal	Memantau penginstalan, pembaruan, atau penghapusan aplikasi perangkat lunak.	Windows macOS	24 jam	Tidak	Manajemen Tingkat Lanjut
Sistem					
Mulai ulang sistem terakhir	Memantau saat beban kerja dimulai ulang.	Windows macOS	1 jam	Tidak	Perlindungan standar
Log event Windows	Memantau peristiwa penting bisnis	Windows	10 menit	Tidak	Manajemen Tingkat Lanjut

© Acronis International GmbH, 2003-2024

Monitor	Deskripsi	Sistem Operasi yang Didukung	Frekuensi pengumpulan data	Dukungan pemantauan berbasis anomali	Ketersediaan dalam Perlindungan standar atau Manajemen Tingkat Lanjut
	tertentu di log peristiwa Windows.				
Ukuran file dan folder	Memantau ukuran total file atau folder yang dipilih.	Windows macOS	10 menit	Tidak	Perlindungan standar
Keamanan					
Status Pembaruan Windows	Memantau status Pembaruan Windows dari beban kerja dan apakah peningkatan terbaru diinstal.	Windows	15 menit	Tidak	Manajemen Tingkat Lanjut
Status firewall	Memantau status firewall internal atau pihak ketiga yang diinstal pada beban kerja.	Windows macOS	5 menit	Tidak	Manajemen Tingkat Lanjut
Status perangkat lunak antimalware	Memantau status perangkat lunak antimalware internal atau pihak ketiga yang diinstal pada beban kerja.	Windows macOS	5 menit	Tidak	Manajemen Tingkat Lanjut

© Acronis International GmbH, 2003-2024

Monitor	Deskripsi	Sistem Operasi yang Didukung	Frekuensi pengumpulan data	Dukungan pemantauan berbasis anomali	Ketersediaan dalam Perlindungan standar atau Manajemen Tingkat Lanjut
Upaya masuk gagal	Memantau upaya login yang gagal pada beban kerja.	Windows	1 jam	Tidak	Manajemen Tingkat Lanjut
Status AutoRun	Memantau apakah fitur AutoRun untuk media penyimpanan yang dapat dilepas diaktifkan.	Windows	1 jam	Tidak	Manajemen Tingkat Lanjut
Kustom					
Kustom	Memantau objek khusus melalui menjalankan skrip.	Windows macOS	kustom	Tidak	Manajemen Tingkat Lanjut

Pengaturan monitor ruang Disk

Ruang disk memantau ruang bebas pada drive tertentu dari beban kerja.

Catatan
Ketika menghitung ruang, monitor menggunakan bit biner (1024 bit per KB, 1024 KB per MB, dan 1024 MB per GB) untuk beban kerja Windows dan macOS.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Pemantauan berbasis ambang batas	
Drive	Drive yang ingin Anda monitor. Nilai berikut tersedia. • **Drive sistem** —Ini adalah nilai default.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	• **Drive apa pun**
Operator	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Kurang dari** —Ini adalah nilai default. • **Kurang dari atau sama dengan**
Ambang batas ruang kosong disk	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat dalam rentang 1-100 (%). Nilai default adalah 20.
Sertakan drive yang dapat dilepas	Pengaturan ini tersedia jika nilai **Drive** adalah **Drive apa pun**. Pilih pengaturan ini jika Anda ingin menambahkan drive yang dapat dilepas, seperti drive flash USB, untuk pemantauan. Secara default, pengaturan dinonaktifkan.
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 30.
Pemantauan berbasis anomali	
Drive	Drive yang ingin Anda monitor. Nilai berikut tersedia. • **Drive sistem** —Ini adalah nilai default. • **Drive apa pun**
Periode pelatihan model	Periode ketika sistem akan melatih model pembelajaran mesin berdasarkan data yang dikumpulkan dari agen, dan kemudian akan membuat pola perilaku normal beban kerja. Semakin lama periode pelatihan model, semakin tepat pola perilaku jangka panjang yang dapat diciptakan sistem. Kami merekomendasikan periode pelatihan model minimum adalah dua puluh satu hari. Masukkan nilai bilangan bulat (hari). Nilai default adalah 21.
Terima peringatan anomali selama periode	Jika memilih pengaturan ini, Anda akan menerima peringatan tentang anomali selama periode pelatihan model. Peringatan ini mungkin palsu, karena model masih dilatih dan mungkin tidak cukup akurat. Secara default, pengaturan dipilih.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
pelatihan	
Tingkat sensitivitas	Tingkat sensitivitas bertindak sebagai filter awal untuk anomali jika nilainya berada dalam rentang tertentu. Filter beroperasi secara terpisah dari algoritme deteksi anomali. Tujuannya adalah untuk menghentikan anomali yang berada di rentang tertentu agar tidak diproses oleh algoritme deteksi anomali. Selama periode pelatihan model: 1. Algoritme dilatih menggunakan data yang dikumpulkan selama pelatihan. 2. Algoritme melakukan deteksi anomali pada data pelatihan. 3. Proses pemfilteran yang didasarkan pada rata-rata dan deviasi standar berlaku. 4. Semua anomali yang ada di interval yang ditentukan difilter. 5. Dari titik data anomali yang tersisa, anomali dengan level terendah dipilih. Level ini (angka float antara 0 dan 1) dicatat dalam model. Selama prediksi: 1. Algoritme memprediksi anomali pada data inferensi. 2. Anomali yang diprediksi difilter berdasarkan rata-rata dan deviasi standar, sesuai level sensitivitas. 3. Anomali yang tersisa difilter lebih lanjut berdasarkan prinsip berikut: nilai di atas level ambang batas dianggap anomali, sementara nilai di bawah level ambang batas dianggap perilaku normal. Nilai berikut tersedia. • **Rendah** — Level rendah sama dengan nilai rata-rata dan nilai deviasi standar. • **Normal** — Ini adalah nilai default. Level normal sama dengan nilai rata-rata dan dua kali nilai deviasi standar. • **Tinggi** — Level tinggi sama dengan nilai rata-rata dan tiga kali nilai deviasi standar.
Durasi anomali	Sistem akan mengeluarkan peringatan untuk anomali yang terdeteksi hanya jika perilaku abnormal terus terjadi untuk periode tertentu. Nilai default adalah 30 menit.

Pengaturan monitor suhu CPU

Suhu CPU memantau suhu CPU beban kerja.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
Pemantauan berbasis ambang batas	
Suhu CPU telah terlampaui (C°)	Nilai maksimum metrik yang dipantau. Jika nilai terlampaui, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (C°). Nilai default adalah 80.
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.
Pemantauan berbasis anomali	
Periode pelatihan model	Periode ketika sistem akan melatih model pembelajaran mesin berdasarkan data yang dikumpulkan dari agen, dan kemudian akan membuat pola perilaku normal beban kerja. Semakin lama periode pelatihan model, semakin tepat pola perilaku jangka panjang yang dapat diciptakan sistem. Kami merekomendasikan periode pelatihan model minimum adalah dua puluh satu hari. Masukkan nilai bilangan bulat (hari). Nilai default adalah 21.
Tingkat sensitivitas	Tingkat sensitivitas bertindak sebagai filter awal untuk anomali jika nilainya berada dalam rentang tertentu. Filter beroperasi secara terpisah dari algoritme deteksi anomali. Tujuannya adalah untuk menghentikan anomali yang berada di rentang tertentu agar tidak diproses oleh algoritme deteksi anomali. Selama periode pelatihan model: 1. Algoritme dilatih menggunakan data yang dikumpulkan selama pelatihan. 2. Algoritme melakukan deteksi anomali pada data pelatihan. 3. Proses pemfilteran yang didasarkan pada rata-rata dan deviasi standar berlaku. 4. Semua anomali yang ada di interval yang ditentukan difilter. 5. Dari titik data anomali yang tersisa, anomali dengan level terendah dipilih. Level ini (angka float antara 0 dan 1) dicatat dalam model. Selama prediksi: 1. Algoritme memprediksi anomali pada data inferensi. 2. Anomali yang diprediksi difilter berdasarkan rata-rata dan deviasi standar, sesuai level sensitivitas. 3. Anomali yang tersisa difilter lebih lanjut berdasarkan prinsip berikut: nilai di atas level ambang batas dianggap anomali,

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	sementara nilai di bawah level ambang batas dianggap perilaku normal. Nilai berikut tersedia. • **Rendah** — Level rendah sama dengan nilai rata-rata dan nilai deviasi standar. • **Normal** — Ini adalah nilai default. Level normal sama dengan nilai rata-rata dan dua kali nilai deviasi standar. • **Tinggi** — Level tinggi sama dengan nilai rata-rata dan tiga kali nilai deviasi standar.
Durasi anomali	Sistem akan mengeluarkan peringatan untuk anomali yang terdeteksi hanya jika perilaku abnormal terus terjadi untuk periode tertentu. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 15.

Pengaturan monitor suhu GPU

Suhu GPU memantau suhu GPU beban kerja.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Pemantauan berbasis ambang batas	
Suhu GPU telah terlampaui	Nilai maksimum metrik yang dipantau. Jika nilainya terlampaui, sistem mendeteksi anomali. Masukkan nilai bilangan bulat (C°). Nilai default adalah 80.
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.
Pemantauan berbasis anomali	
Periode pelatihan model	Periode ketika sistem akan melatih model pembelajaran mesin berdasarkan data yang dikumpulkan dari agen, dan kemudian akan membuat pola perilaku normal beban kerja. Semakin lama periode pelatihan model, semakin tepat pola perilaku jangka panjang yang dapat diciptakan sistem. Kami merekomendasikan periode pelatihan model minimum adalah dua puluh satu hari. Masukkan nilai bilangan bulat (hari). Nilai default adalah 21.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
Tingkat sensitivitas	Tingkat sensitivitas bertindak sebagai filter awal untuk anomali jika nilainya berada dalam rentang tertentu. Filter beroperasi secara terpisah dari algoritme deteksi anomali. Tujuannya adalah untuk menghentikan anomali yang berada di rentang tertentu agar tidak diproses oleh algoritme deteksi anomali. Selama periode pelatihan model: 1. Algoritme dilatih menggunakan data yang dikumpulkan selama pelatihan. 2. Algoritme melakukan deteksi anomali pada data pelatihan. 3. Proses pemfilteran yang didasarkan pada rata-rata dan deviasi standar berlaku. 4. Semua anomali yang ada di interval yang ditentukan difilter. 5. Dari titik data anomali yang tersisa, anomali dengan level terendah dipilih. Level ini (angka float antara 0 dan 1) dicatat dalam model. Selama prediksi: 1. Algoritme memprediksi anomali pada data inferensi. 2. Anomali yang diprediksi difilter berdasarkan rata-rata dan deviasi standar, sesuai level sensitivitas. 3. Anomali yang tersisa difilter lebih lanjut berdasarkan prinsip berikut: nilai di atas level ambang batas dianggap anomali, sementara nilai di bawah level ambang batas dianggap perilaku normal. Nilai berikut tersedia. • **Rendah** — Level rendah sama dengan nilai rata-rata dan nilai deviasi standar. • **Normal** — Ini adalah nilai default. Level normal sama dengan nilai rata-rata dan dua kali nilai deviasi standar. • **Tinggi** — Level tinggi sama dengan nilai rata-rata dan tiga kali nilai deviasi standar.
Durasi anomali	Sistem akan mengeluarkan peringatan untuk anomali yang terdeteksi hanya jika perilaku abnormal terus terjadi untuk periode tertentu. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 15.

Pengaturan monitor Perubahan perangkat keras

Perubahan perangkat keras memantau perubahan perangkat keras, seperti menambah, melepas, atau mengganti perangkat keras pada beban kerja.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
Komponen perangkat keras	Pilih satu atau beberapa komponen perangkat keras yang ingin Anda pantau perubahannya. Nilai berikut tersedia. • **Semua** — Ini adalah nilai default. • **Motherboard** • **CPU** • **RAM** • **Disk** • **GPU** • **Adaptor jaringan**
Apa yang akan dipantau	Tentukan perubahan komponen perangkat keras yang dipilih yang ingin Anda pantau. Anda dapat memilih beberapa item dari daftar. Nilai berikut tersedia. • **Semua perubahan** —Ini adalah nilai default. • **Komponen yang baru ditambahkan** • **Komponen yang diganti** • **Komponen yang dihapus**

Pengaturan monitor penggunaan CPU

Penggunaan CPU memantau total penggunaan CPU (pemanfaatan prosesor) beban kerja. Jika beban kerja memiliki beberapa CPU, total penggunaan CPU adalah jumlah penggunaan CPU dari masing-masing CPU.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Pemantauan berbasis ambang batas	
Operator	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Batas penggunaan CPU	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	Masukkan nilai bilangan bulat dalam rentang 1-100 (%). Nilai default adalah 90.
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.
Pemantauan berbasis anomali	
Periode pelatihan model	Periode ketika sistem akan melatih model pembelajaran mesin berdasarkan data yang dikumpulkan dari agen, dan kemudian akan membuat pola perilaku normal beban kerja. Semakin lama periode pelatihan model, semakin tepat pola perilaku jangka panjang yang dapat diciptakan sistem. Kami merekomendasikan periode pelatihan model minimum adalah dua puluh satu hari. Masukkan nilai bilangan bulat (hari). Nilai default adalah 21.
Terima peringatan anomali selama periode pelatihan	Jika memilih pengaturan ini, Anda akan menerima peringatan tentang anomali selama periode pelatihan model. Peringatan ini mungkin palsu, karena model masih dilatih dan mungkin tidak cukup akurat. Secara default, pengaturan dipilih.
Tingkat sensitivitas	Tingkat sensitivitas bertindak sebagai filter awal untuk anomali jika nilainya berada dalam rentang tertentu. Filter beroperasi secara terpisah dari algoritme deteksi anomali. Tujuannya adalah untuk menghentikan anomali yang berada di rentang tertentu agar tidak diproses oleh algoritme deteksi anomali. Selama periode pelatihan model: 1. Algoritme dilatih menggunakan data yang dikumpulkan selama pelatihan. 2. Algoritme melakukan deteksi anomali pada data pelatihan. 3. Proses pemfilteran yang didasarkan pada rata-rata dan deviasi standar berlaku. 4. Semua anomali yang ada di interval yang ditentukan difilter. 5. Dari titik data anomali yang tersisa, anomali dengan level terendah dipilih. Level ini (angka float antara 0 dan 1) dicatat dalam model. Selama prediksi: 1. Algoritme memprediksi anomali pada data inferensi. 2. Anomali yang diprediksi difilter berdasarkan rata-rata dan deviasi standar, sesuai level sensitivitas. 3. Anomali yang tersisa difilter lebih lanjut berdasarkan prinsip berikut: nilai di atas level ambang batas dianggap anomali, sementara nilai di bawah

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	level ambang batas dianggap perilaku normal. Nilai berikut tersedia. • **Rendah** — Level rendah sama dengan nilai rata-rata dan nilai deviasi standar. • **Normal** — Ini adalah nilai default. Level normal sama dengan nilai rata-rata dan dua kali nilai deviasi standar. • **Tinggi** — Level tinggi sama dengan nilai rata-rata dan tiga kali nilai deviasi standar.
Durasi anomali	Sistem akan mengeluarkan peringatan untuk anomali yang terdeteksi hanya jika perilaku abnormal terus terjadi untuk periode tertentu. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 15.

Pengaturan monitor Penggunaan memori

Penggunaan memori memantau total penggunaan memori oleh semua modul memori pada beban kerja.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Pemantauan berbasis ambang batas	
Operator	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Ambang batas penggunaan memori	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat dalam rentang 1-100 (%). Nilai default adalah 90.
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
Pemantauan berbasis anomali	
Periode pelatihan model	Periode ketika sistem akan melatih model pembelajaran mesin berdasarkan data yang dikumpulkan dari agen, dan kemudian akan membuat pola perilaku normal beban kerja. Semakin lama periode pelatihan model, semakin tepat pola perilaku jangka panjang yang dapat diciptakan sistem. Kami merekomendasikan periode pelatihan model minimum adalah dua puluh satu hari. Masukkan nilai bilangan bulat (hari). Nilai default adalah 21.
Terima peringatan anomali selama periode pelatihan	Jika memilih pengaturan ini, Anda akan menerima peringatan tentang anomali selama periode pelatihan model. Peringatan ini mungkin palsu, karena model masih dilatih dan mungkin tidak cukup akurat. Secara default, pengaturan dipilih.
Tingkat sensitivitas	Tingkat sensitivitas bertindak sebagai filter awal untuk anomali jika nilainya berada dalam rentang tertentu. Filter beroperasi secara terpisah dari algoritme deteksi anomali. Tujuannya adalah untuk menghentikan anomali yang berada di rentang tertentu agar tidak diproses oleh algoritme deteksi anomali. Selama periode pelatihan model: 1. Algoritme dilatih menggunakan data yang dikumpulkan selama pelatihan. 2. Algoritme melakukan deteksi anomali pada data pelatihan. 3. Proses pemfilteran yang didasarkan pada rata-rata dan deviasi standar berlaku. 4. Semua anomali yang ada di interval yang ditentukan difilter. 5. Dari titik data anomali yang tersisa, anomali dengan level terendah dipilih. Level ini (angka float antara 0 dan 1) dicatat dalam model. Selama prediksi: 1. Algoritme memprediksi anomali pada data inferensi. 2. Anomali yang diprediksi difilter berdasarkan rata-rata dan deviasi standar, sesuai level sensitivitas. 3. Anomali yang tersisa difilter lebih lanjut berdasarkan prinsip berikut: nilai di atas level ambang batas dianggap anomali, sementara nilai di bawah level ambang batas dianggap perilaku normal. Nilai berikut tersedia. • **Rendah** — Level rendah sama dengan nilai rata-rata dan nilai deviasi standar. • **Normal** — Ini adalah nilai default. Level normal sama dengan nilai rata-rata dan dua kali nilai deviasi standar.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	• **Tinggi** — Level tinggi sama dengan nilai rata-rata dan tiga kali nilai deviasi standar.
Durasi anomali	Sistem akan mengeluarkan peringatan untuk anomali yang terdeteksi hanya jika perilaku abnormal terus terjadi untuk periode tertentu. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 30 menit.

Pengaturan monitor kecepatan transfer Disk

Kecepatan transfer disk memantau kecepatan baca dan tulis setiap disk fisik pada beban kerja.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Pemantauan berbasis ambang batas	
Apa yang akan dipantau	Pilih kecepatan yang ingin Anda monitor. Nilai berikut tersedia. • **Kecepatan baca dan Kecepatan tulis**. Ini adalah nilai default. • **Kecepatan baca** • **Kecepatan tulis**
Operator kecepatan baca	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari**. Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Ambang batas kecepatan baca	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (kb/detik). Nilai defaultnya adalah 0 kb/detik.
Periode waktu kecepatan baca	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.
Operator kecepatan	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
tulis	Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Ambang batas kecepatan tulis	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (kb/detik). Nilai defaultnya adalah 0 kb/detik.
Periode waktu kecepatan tulis	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.
Pemantauan berbasis anomali	
Periode pelatihan model	Periode ketika sistem akan melatih model pembelajaran mesin berdasarkan data yang dikumpulkan dari agen, dan kemudian akan membuat pola perilaku normal beban kerja. Semakin lama periode pelatihan model, semakin tepat pola perilaku jangka panjang yang dapat diciptakan sistem. Kami merekomendasikan periode pelatihan model minimum adalah dua puluh satu hari. Masukkan nilai bilangan bulat (hari). Nilai default adalah 21.
Terima peringatan anomali selama periode pelatihan	Jika memilih pengaturan ini, Anda akan menerima peringatan tentang anomali selama periode pelatihan model. Peringatan ini mungkin palsu, karena model masih dilatih dan mungkin tidak cukup akurat. Secara default, pengaturan dipilih.
Apa yang akan dipantau	Pilih kecepatan yang ingin Anda monitor. Nilai berikut tersedia. • **Kecepatan baca dan Kecepatan tulis**. Ini adalah nilai default. • **Kecepatan baca** • **Kecepatan tulis**
Tingkat sensitivitas	Tingkat sensitivitas bertindak sebagai filter awal untuk anomali jika nilainya berada dalam rentang tertentu. Filter beroperasi secara terpisah dari algoritme deteksi anomali. Tujuannya adalah untuk menghentikan anomali yang berada di rentang tertentu agar tidak diproses oleh algoritme deteksi anomali.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	Selama periode pelatihan model: 1. Algoritme dilatih menggunakan data yang dikumpulkan selama pelatihan. 2. Algoritme melakukan deteksi anomali pada data pelatihan. 3. Proses pemfilteran yang didasarkan pada rata-rata dan deviasi standar berlaku. 4. Semua anomali yang ada di interval yang ditentukan difilter. 5. Dari titik data anomali yang tersisa, anomali dengan level terendah dipilih. Level ini (angka float antara 0 dan 1) dicatat dalam model. Selama prediksi: 1. Algoritme memprediksi anomali pada data inferensi. 2. Anomali yang diprediksi difilter berdasarkan rata-rata dan deviasi standar, sesuai level sensitivitas. 3. Anomali yang tersisa difilter lebih lanjut berdasarkan prinsip berikut: nilai di atas level ambang batas dianggap anomali, sementara nilai di bawah level ambang batas dianggap perilaku normal. Nilai berikut tersedia. • **Rendah** — Level rendah sama dengan nilai rata-rata dan nilai deviasi standar. • **Normal** — Ini adalah nilai default. Level normal sama dengan nilai rata-rata dan dua kali nilai deviasi standar. • **Tinggi** — Level tinggi sama dengan nilai rata-rata dan tiga kali nilai deviasi standar.
Durasi anomali (Kecepatan baca)	Sistem akan mengeluarkan peringatan untuk anomali yang terdeteksi hanya jika perilaku abnormal terus terjadi untuk periode tertentu. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 25.
Durasi anomali (Kecepatan tulis)	Sistem akan mengeluarkan peringatan untuk anomali yang terdeteksi hanya jika perilaku abnormal terus terjadi untuk periode tertentu. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 25.

Pengaturan monitor Penggunaan jaringan

Penggunaan jaringan memantau lalu lintas masuk dan keluar untuk setiap adaptor jaringan beban kerja.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
Pemantauan berbasis ambang batas	
Arah lalu lintas	Arah lalu lintas yang ingin Anda monitor. Nilai berikut tersedia. • **Lalu lintas Masuk dan Keluar**. Ini adalah nilai default. • **Lalu lintas masuk** • **Lalu lintas keluar**
Operator lalu lintas masuk	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Ambang batas lalu lintas masuk	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (kb/detik). Nilai defaultnya adalah 0 kb/detik.
Periode waktu lalu lintas masuk	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.
Operator lalu lintas keluar	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Ambang batas lalu lintas keluar	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (kb/detik). Nilai defaultnya adalah 0 kb/detik.
Periode waktu lalu lintas keluar	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.
Pemantauan berbasis anomali	
Periode pelatihan model	Periode ketika sistem akan melatih model pembelajaran mesin berdasarkan data yang dikumpulkan dari agen, dan kemudian akan membuat pola perilaku normal beban kerja. Semakin lama periode pelatihan model, semakin tepat pola perilaku jangka panjang yang dapat diciptakan sistem. Kami merekomendasikan periode pelatihan model minimum adalah dua puluh satu hari. Masukkan nilai bilangan bulat (hari). Nilai default adalah 21.
Terima peringatan anomali selama periode pelatihan	Jika memilih pengaturan ini, Anda akan menerima peringatan tentang anomali selama periode pelatihan model. Peringatan ini mungkin palsu, karena model masih dilatih dan mungkin tidak cukup akurat. Secara default, pengaturan dipilih.
Arah lalu lintas	• **Lalu lintas Masuk dan Keluar**. Ini adalah nilai default. • **Lalu lintas masuk** • **Lalu lintas keluar**
Tingkat sensitivitas	Tingkat sensitivitas bertindak sebagai filter awal untuk anomali jika nilainya berada dalam rentang tertentu. Filter beroperasi secara terpisah dari algoritme deteksi anomali. Tujuannya adalah untuk menghentikan anomali yang berada di rentang tertentu agar tidak diproses oleh algoritme deteksi anomali. Selama periode pelatihan model: 1. Algoritme dilatih menggunakan data yang dikumpulkan selama pelatihan. 2. Algoritme melakukan deteksi anomali pada data pelatihan. 3. Proses pemfilteran yang didasarkan pada rata-rata dan deviasi standar berlaku. 4. Semua anomali yang ada di interval yang ditentukan difilter. 5. Dari titik data anomali yang tersisa, anomali dengan level terendah dipilih. Level ini (angka float antara 0 dan 1) dicatat dalam model. Selama prediksi: 1. Algoritme memprediksi anomali pada data inferensi. 2. Anomali yang diprediksi difilter berdasarkan rata-rata dan deviasi standar, sesuai level sensitivitas. 3. Anomali yang tersisa difilter lebih lanjut berdasarkan prinsip berikut: nilai di atas level ambang batas dianggap anomali, sementara nilai di bawah level ambang batas dianggap perilaku normal.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	Nilai berikut tersedia. • **Rendah** — Level rendah sama dengan nilai rata-rata dan nilai deviasi standar. • **Normal** — Ini adalah nilai default. Level normal sama dengan nilai rata-rata dan dua kali nilai deviasi standar. • **Tinggi** — Level tinggi sama dengan nilai rata-rata dan tiga kali nilai deviasi standar.
Durasi anomali (Masuk)	Sistem akan mengeluarkan peringatan untuk anomali yang terdeteksi hanya jika perilaku abnormal terus terjadi untuk periode tertentu. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 25.
Durasi anomali (Keluar)	Sistem akan mengeluarkan peringatan untuk anomali yang terdeteksi hanya jika perilaku abnormal terus terjadi untuk periode tertentu. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 25.

Pengaturan penggunaan CPU berdasarkan monitor proses

Penggunaan CPU berdasarkan proses memantau penggunaan CPU dari proses yang dipilih. Jika ada beberapa instans proses yang sama, sistem akan memantau total penggunaan semua instans proses dan mengeluarkan peringatan ketika syarat terpenuhi.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Nama proses	Nama proses yang ingin Anda monitor. Masukkan nama proses tanpa ekstensi.
Operator	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Ambang batas	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat dalam rentang 1-100 (%). Nilai default adalah

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	90.
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.

Pengaturan penggunaan Memori berdasarkan monitor proses

Penggunaan Memori berdasarkan proses memantau penggunaan memori dari proses yang dipilih. Jika ada beberapa instans proses yang sama, sistem akan memantau total penggunaan semua instans proses dan mengeluarkan peringatan ketika syarat terpenuhi.

Catatan
Agen menggunakan set kerja proses total (privat dan bersama) untuk memperkirakan ukuran penggunaan memori berdasarkan proses. Hal tersebut menyebabkan ukuran yang ditunjukkan widget dapat berbeda dari ukuran penggunaan memori yang ditampilkan di Windows Task Manager (set kerja privat).

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Nama proses	Nama proses yang ingin Anda monitor. Masukkan nama proses tanpa ekstensi.
Operator	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Ambang batas	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (kb). Nilai default adalah 1.
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.

© Acronis International GmbH, 2003-2024

Pengaturan kecepatan transfer Disk berdasarkan monitor proses

Kecepatan transfer disk berdasarkan proses memantau kecepatan baca dan tulis dari proses yang dipilih. Jika ada beberapa instans proses yang sama, sistem akan memantau total penggunaan semua instans proses dan mengeluarkan peringatan ketika syarat terpenuhi.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Nama proses	Nama proses yang ingin Anda monitor. Masukkan nama proses tanpa ekstensi.
Apa yang akan dipantau	Kecepatan yang ingin Anda monitor. Nilai berikut tersedia. • **Kecepatan baca dan Kecepatan tulis**. Ini adalah nilai default. • **Kecepatan baca** • **Kecepatan tulis**
Operator kecepatan baca	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Ambang batas kecepatan baca	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (kb/detik). Nilai defaultnya adalah 0 kb/detik.
Periode waktu kecepatan baca	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.
Operator kecepatan tulis	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
Ambang batas kecepatan tulis	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (kb/detik). Nilai defaultnya adalah 0 kb/detik.
Periode waktu kecepatan tulis	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.

Pengaturan penggunaan Jaringan berdasarkan monitor proses

Penggunaan jaringan berdasarkan proses memantau lalu lintas masuk dan keluar dari proses yang dipilih. Jika ada beberapa instans proses yang sama, sistem akan memantau total penggunaan semua instans proses dan mengeluarkan peringatan ketika syarat terpenuhi untuk semua instans.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Nama proses	Nama proses yang ingin Anda monitor. Masukkan nama proses tanpa ekstensi.
Arah lalu lintas	Arah lalu lintas yang ingin Anda monitor. Nilai berikut tersedia. • **Lalu lintas masuk dan Lalu lintas keluar**. Ini adalah nilai default. • **Lalu lintas masuk** • **Lalu lintas keluar**
Operator lalu lintas masuk	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Ambang batas lalu lintas masuk	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (kb/detik). Nilai defaultnya adalah 0 kb/detik.
Periode waktu lalu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
lintas masuk	Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.
Operator lalu lintas keluar	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Lebih dari atau sama dengan** • **Kurang dari** • **Kurang dari atau sama dengan**
Ambang batas lalu lintas keluar	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (kb/detik). Nilai defaultnya adalah 0 kb/detik.
Periode waktu lalu lintas keluar	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 5.

Pengaturan monitor status layanan Windows

Status layanan Windows memantau apakah layanan Windows yang dipilih sedang berjalan atau berhenti.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Nama layanan	Nama layanan Windows yang ingin Anda monitor. Anda dapat memilih nama layanan dari daftar layanan Windows. Daftar diisi oleh semua agen penyewa setelah pemindaian inventaris perangkat lunak berhasil diselesaikan pada beban kerja. Anda juga dapat menambahkan nama layanan yang tidak ada dalam daftar. Ini adalah satu-satunya pilihan yang tersedia jika pemindaian inventaris perangkat lunak tidak dilakukan pada beban kerja.
Status layanan	Jika layanan dalam status yang dipilih, sistem akan menghasilkan peristiwa. Nilai berikut tersedia. • **Berjalan** • **Berhenti**—Ini adalah nilai default.
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 1.

Pengaturan monitor Status proses

Status proses memantau apakah proses yang dipilih sedang berjalan atau berhenti. Jika ada beberapa instans dari proses yang sama, sistem akan memantau setiap instans dari proses tersebut dan akan mengeluarkan peringatan saat syarat terpenuhi untuk semua instans dari proses tersebut.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Nama proses	Nama proses yang ingin Anda monitor. Masukkan nama file yang dapat dieksekusi tanpa ekstensi.
Status proses	Jika proses dalam status yang dipilih, sistem akan menghasilkan peristiwa. Nilai berikut tersedia. • **Berjalan** • **Berhenti**—Ini adalah nilai default.
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-60 (menit). Nilai default adalah 1.

Pengaturan monitor Perangkat lunak yang diinstal

Perangkat lunak yang diinstal memantau instalasi, pembaruan, atau penghapusan aplikasi perangkat lunak pada beban kerja.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Perangkat lunak yang akan dipantau	Tentukan perangkat lunak yang ingin Anda monitor. Nilai berikut tersedia. • **Semua perangkat lunak**—Ini adalah nilai default. • **Perangkat lunak tertentu**
Nama perangkat	Pengaturan ini tersedia jika Anda memilih nilai **Perangkat lunak tertentu** untuk **Perangkat lunak yang akan dipantau**.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
lunak	Masukkan nama satu atau beberapa aplikasi perangkat lunak. Anda dapat memilih nama aplikasi perangkat lunak dari daftar layanan Windows. Daftar diisi oleh semua agen penyewa setelah pemindaian inventaris perangkat lunak berhasil diselesaikan pada beban kerja. Anda juga dapat menambahkan nama aplikasi perangkat lunak yang tidak ada dalam daftar. Ini adalah satu-satunya pilihan yang tersedia jika pemindaian inventaris perangkat lunak tidak dilakukan pada beban kerja.
Status instalasi	Tentukan jika Anda ingin memonitor perangkat lunak yang diinstal, tidak diinstal, atau diperbarui. Nilai berikut tersedia. • **Diinstal** - Ini adalah nilai default. Jika Anda memilih nilai ini, monitor akan menyalakan peringatan saat aplikasi perangkat lunak baru diinstal pada beban kerja. • **Diperbarui** - Jika Anda memilih nilai ini, monitor akan menyalakan peringatan ketika aplikasi perangkat lunak diperbarui. • **Tidak terpasang** - Jika Anda memilih nilai ini, monitor akan menghasilkan peringatan ketika aplikasi perangkat lunak dihapus instalasinya atau tidak tersedia pada beban kerja.

Pengaturan monitor Mulai ulang sistem terakhir

Mulai ulang sistem terakhir saat beban kerja terakhir dimulai ulang.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Beban kerja belum dimulai ulang untuk	Periode (jumlah hari) sejak mulai ulang beban kerja terakhir. Jika beban kerja belum dimulai ulang untuk jangka waktu yang lebih lama dari jangka waktu yang Anda tentukan, sistem akan mengeluarkan peringatan. Masukkan nilai bilangan bulat dalam rentang 1-180 (hari). Nilai default adalah 30.

Pengaturan monitor log peristiwa Windows

Log peristiwa Windows memantau peristiwa tertentu yang penting untuk bisnis di log peristiwa Windows.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Nama log peristiwa	Pilih log peristiwa tertentu dari daftar log peristiwa Windows yang tersedia di Windows Event Viewer.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
	Nilai berikut tersedia. • **Salah satu** —Ini adalah nilai default. • **Aplikasi** • **Keamanan** • **Sistem**
Sumber peristiwa	Nama sumber peristiwa Anda dapat memilih nilai dari daftar sumber peristiwa yang dikumpulkan dari semua agen penyewa atau memasukkan nama sumber baru secara manual. Jika pemindaian inventaris perangkat lunak dinonaktifkan untuk penyewa, daftar sumber peristiwa akan kosong.
Mode pencocokan	Di bidang ini, Anda dapat menentukan apakah menghubungkan pengaturan **ID Peristiwa**, **Jenis peristiwa**, dan **Deskripsi peristiwa** menggunakan **Salah satu** atau **Semua** operator. Nilai berikut tersedia. • **Salah satu** —Ini adalah nilai default. Peringatan akan dikeluarkan jika salah satu kriteria yang dipilih cocok. • **Semua** — Peringatan akan dikeluarkan jika semua kriteria yang dipilih cocok.
ID Peristiwa	Masukkan satu atau beberapa ID peristiwa, dipisahkan oleh koma. Jika sistem menemukan salah satu kode peristiwa yang Anda masukkan di bidang ini di log peristiwa, peringatan akan dikeluarkan.
Jenis event	Pilih satu atau beberapa jenis peristiwa yang ingin Anda pantau. Nilai berikut tersedia. • **Salah satu** —Ini adalah nilai default. • **Eror** • **Peringatan** • **Informasi** • **Audit sukses** • **Audit gagal**
Deskripsi peristiwa	Kata kunci atau frasa tertentu dalam deskripsi acara yang ingin Anda cari. Setiap kata kunci atau frasa yang Anda masukkan harus diapit tanda kutip dan harus dipisahkan dengan koma. Jika sistem menemukan salah satu kata kunci atau frasa yang Anda masukkan, peringatan akan dikeluarkan.
Jumlah kejadian	Jumlah minimum kejadian dalam log yang harus dimiliki suatu peristiwa selama periode waktu agar sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat dalam rentang 1-1000.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat, lalu pilih satuannya: menit atau jam. Nilai default adalah 60 menit.

Pengaturan monitor ukuran File dan folder

Ukuran file dan folder memantau ukuran total file dan folder yang dipilih.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
File dan folder untuk dipantau	Jalur file atau folder yang ingin Anda pantau. Anda juga dapat menentukan file atau folder yang ingin Anda kecualikan dari pemantauan. Anda dapat menggunakan karakter wildcard berikut. • * — untuk nol atau karakter lainnya dalam nama file atau folder • ? — untuk satu karakter dalam nama file atau folder Untuk beban kerja Windows: • Jalur lengkap harus dimulai dari huruf drive diikuti oleh pemisah :\. • Anda dapat menggunakan garis miring atau garis miring terbalik sebagai karakter pemisah jalur. • Nama file atau folder tidak boleh diakhiri dengan spasi atau titik. Untuk beban kerja macOS: • Jalur lengkap harus dimulai dari direktori root. • Anda dapat menggunakan garis miring sebagai karakter pemisah jalur. • Nama file atau folder tidak boleh diakhiri dengan spasi atau titik. Menentukan lokasi tertentu tidak wajib untuk filter pengecualian. File yang dimasukkan tanpa lokasi tertentu akan dikecualikan dalam folder yang dipantau.
Operator	Operator adalah fungsi bersyarat yang menentukan cara mengukur kinerja pada metrik. Nilai berikut tersedia. • **Lebih dari** —Ini adalah nilai default. • **Kurang dari**
Nilai ambang batas	Nilai ambang batas dan nilai **Operator** menentukan kinerja normal metrik yang dipantau. Ketika nilai metrik yang dipantau melebihi batas normal, sistem mengeluarkan peringatan. Masukkan nilai bilangan bulat (MB).

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 10-60 (menit). Nilai default adalah 10.

Pengaturan monitor status Pembaruan Windows

Status Pembaruan Windows memantau status Pembaruan Windows dari beban kerja dan apakah pembaruan terbaru diinstal.

Jika Anda mengaktifkan monitor ini, sistem akan mengeluarkan peringatan dalam kasus berikut.

- Pembaruan Windows dinonaktifkan pada beban kerja.
- Pembaruan Windows diaktifkan pada beban kerja, tetapi pembaruan terbaru tidak diinstal.

Pengaturan monitor status Firewall

Status firewall memantau status firewall internal atau pihak ketiga yang diinstal pada beban kerja.

Jika Anda mengaktifkan monitor ini, sistem akan mengeluarkan peringatan dalam kasus berikut.

- Firewall OS bawaan (Firewall Windows Defender atau firewall macOS) dinonaktifkan dan tidak ada firewall pihak ketiga yang berjalan.
- Firewall Windows Defender dinonaktifkan untuk jaringan publik.
- Firewall Windows Defender dinonaktifkan untuk jaringan privat.
- Firewall Windows Defender dinonaktifkan untuk jaringan domain.

Pengaturan monitor upaya masuk gagal

Upaya masuk gagal memantau upaya masuk yang gagal pada beban kerja.

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Ambang batas upaya masuk yang gagal	Nilai ambang batas menentukan batas kinerja normal metrik yang dipantau. Ketika nilai ambang batas terlampaui, nilainya melebihi batas normal. Masukkan nilai bilangan bulat. Nilai default adalah 60.
Jangka waktu	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan. Masukkan nilai bilangan bulat dalam rentang 1-24 dan pilih unit: jam atau hari. Nilai default adalah 12.

© Acronis International GmbH, 2003-2024

Pengaturan status monitor perangkat lunak antimalware

Status perangkat lunak antimalware memantau perangkat lunak antimalware bawaan atau pihak ketiga yang diinstal pada beban kerja.

Jika Anda mengaktifkan monitor ini, sistem akan mengeluarkan peringatan ketika mengidentifkasi salah satu syarat berikut.

- Perangkat lunak antimalware tidak diinstal pada beban kerja.
- Perangkat lunak antimalware diinstal, tetapi tidak berjalan.
- Perangkat lunak antimalware diinstal dan berjalan, tetapi definisi malware bukan yang terbaru.

Catatan
Syarat ini diperiksa oleh sistem operasi Windows dan Windows Server.

Sistem operasi	Perangkat lunak antimalware yang didukung
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton antivirus • SentinelOne • Trend Micro Endpoint Security with 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

© Acronis International GmbH, 2003-2024

Sistem operasi	Perangkat lunak antimalware yang didukung
	• 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 **Catatan** Pengawasan ini dapat berfungsi dengan aplikasi antimalware lainnya, meskipun tidak dijamin.
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Anti-virus for Mac • Sophos Home • Sophos Endpoint Protection • Avast Security for Mac • AVG AntiVirus for Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus for Mac • Comodo Antivirus for Mac • K7 Antivirus for Mac • Vipre Advanced Security • Total AV for Mac **Catatan** Pengawasan ini dapat berfungsi dengan aplikasi antimalware lainnya, meskipun tidak dijamin.

Pengaturan monitor status fitur AutoRun

Status fitur AutoRun memantau apakah fitur AutoRun untuk media yang dapat dilepas diaktifkan.

Untuk alasan keamanan, kami menyarankan Anda menonaktifkan fitur AutoRun untuk media yang dapat dilepas pada beban kerja. Jika fitur diaktifkan, sistem akan mengeluarkan peringatan.

Pengaturan monitor Kustom

Kustom memantau objek kustom dengan menjalankan skrip.

© Acronis International GmbH, 2003-2024

Anda dapat mengonfigurasi pengaturan berikut untuk monitor.

Pengaturan	Deskripsi
Skrip yang dijalankan	Daftar skrip yang ditentukan dari repositori skrip.
Jadwal	Waktu saat skrip dijalankan dan, secara opsional, syarat tambahan yang harus dipenuhi untuk menjalankan skrip. Nilai berikut tersedia. • **Jadwalkan berdasarkan waktu** — Skrip akan berjalan tepat pada waktu, hari, minggu, atau bulan yang Anda tentukan. Ini adalah nilai default. **Jenis jadwal** — **Per jam**, **Harian**, atau **Bulanan** **Berjalan dalam rentang waktu** — Rentang waktu untuk menjalankan skrip. • **Ketika pengguna masuk ke sistem** — Skrip akan berjalan ketika pengguna masuk ke beban kerja. • **Ketika pengguna keluar dari sistem** — Skrip akan berjalan ketika pengguna keluar dari beban kerja. • **Pada startup sistem** — Tugas akan berjalan saat sistem operasi beban kerja dimulai. • **Saat sistem dimatikan** — Skrip akan berjalan ketika beban kerja dimatikan. • **Saat sistem online** — Skrip akan berjalan ketika beban kerja tersedia secara online. **Syarat memulai** — Tugas akan dilakukan pada waktu atau peristiwa yang ditentukan hanya jika memenuhi syarat. Dengan beberapa syarat yang semuanya harus dipenuhi secara bersamaan untuk memulai tugas. Secara default, syarat **Cegah mode tidur atau hibernasi untuk memulai tugas terjadwal** dipilih. **Jika syarat memulai tidak terpenuhi, tetap jalankan tugas setelahnya** — Secara default, syarat ini diaktifkan. Nilai default adalah 1 jam.
Akun untuk mengeksekusi skrip	Akun tempat skrip akan dijalankan. Nilai berikut tersedia. • **Akun sistem** — Ini adalah nilai default. • **Akun yang sedang masuk**
Durasi maksimum	Periode maksimum skrip dapat berjalan pada beban kerja. Jika skrip tidak diselesaikan selama periode ini, operasi akan gagal. Masukkan nilai bilangan bulat dalam rentang 1-1440 (menit). Nilai default adalah 3 menit.

© Acronis International GmbH, 2003-2024

Pengaturan	Deskripsi
Kebijakan eksekusi PowerShell	Kebijakan eksekusi PowerShell. Nilai berikut tersedia. • **Undefined** • **AllSigned** • **Bypass** — Ini adalah nilai default. • **RemoteSigned** • **Restricted** • **Unrestricted** Untuk informasi lebih lanjut tentang nilai ini, lihat dokumentasi Microsoft.

Rencana pemantauan

Rencana pemantauan adalah rencana yang Anda terapkan pada beban kerja terkelola untuk mengaktifkan dan mengonfigurasi fungsionalitas pemantauan.

Jika tidak ada rencana pemantauan yang diterapkan pada beban kerja, fitur pemantauan tidak akan tersedia untuk beban kerja tersebut.

Catatan
Ketersediaan pengaturan yang dapat Anda konfigurasikan di rencana pemantauan bergantung pada paket layanan yang diterapkan pada penyewa. Untuk mengakses semua pengaturan, aktifkan paket Manajemen Tingkat Lanjut.

Membuat rencana pemantauan

Anda dapat membuat rencana pemantauan lalu menambahkan beban kerja ke rencana tersebut untuk mengonfigurasi fungsi pemantauan pada beban kerja terkelola.

Prasyarat

Versi agen yang diinstal pada beban kerja yang didukung oleh fungsionalitas pemantauan.

Cara membuat rencana pemantauan

Dari Rencana pemantauan

1. Di konsol Perlindungan, buka **Manajemen** > **Rencana pemantauan**.
2. Buat rencana pemantauan menggunakan salah satu dari kedua opsi.
   - Jika tidak ada rencana pemantauan dalam daftar, klik **Buat**.
   - Jika ada rencana pemantauan dalam daftar, klik **Buat rencana**.
3. Di jendela **Buat rencana pemantauan**, bergantung pada apakah paket Manajemen Tingkat Lanjut diaktifkan untuk penyewa Anda, lakukan hal berikut:

© Acronis International GmbH, 2003-2024

- Jika penyewa Anda menggunakan perlindungan Standar, keempat monitor berikut ditambahkan secara otomatis ke rencana pemantauan: Ruang disk, Perubahan perangkat keras, Mulai ulang sistem terakhir, serta Ukuran file dan folder.
- Jika paket Manajemen Tingkat Lanjut diaktifkan untuk penyewa Anda, pilih salah satu opsi templat, lalu klik **Berikutnya**.

Opsi	Deskripsi
Disarankan	Pilih opsi ini untuk membuat rencana pemantauan dengan konfigurasi pemantauan.
Kustom	Gunakan opsi ini untuk membuat rencana pemantauan dari awal.

4. [Opsional] Untuk mengubah nama default rencana, klik ikon pensil, masukkan nama rencana, lalu klik **Oke**.
5. [Opsional] Untuk menambahkan monitor ke rencana, klik **Tambahkan monitor**, klik monitor dalam daftar, dan klik **Tambahkan**.

   Catatan
   Pengaturan monitor akan diisikan secara otomatis dengan nilai default.
   Anda dapat menambahkan maksimum tiga monitor dengan jenis yang sama dan maksimum 30 monitor total ke rencana pemantauan.

6. [Opsional] Di layar parameter monitor, ubah pengaturan default monitor dan peringatan, lalu klik **Selesai**.

   Catatan
   Anda dapat mengonfigurasi pengaturan yang berbeda untuk setiap monitor. Untuk informasi lebih lanjut, lihat "Monitor yang dapat dikonfigurasi" (hlm. 1028) dan "Mengonfigurasi peringatan pemantauan" (hlm. 1072).

7. [Opsional] Untuk menghapus monitor, klik ikon tempat sampah, lalu klik **Hapus**.
8. [Opsional] Untuk menambahkan beban kerja ke rencana:
   a. Klik **Tambahkan beban kerja**.
   b. Pilih beban kerja, lalu klik **Tambahkan**.
   c. Jika ada masalah kompatibilitas yang ingin Anda selesaikan, ikuti prosedur yang dijelaskan di "Menyelesaikan masalah kompatibilitas dengan rencana pemantauan" (hlm. 1070).
9. Klik **Buat**.

Dari Semua perangkat

1. Di konsol Perlindungan, buka **Perangkat** > **Semua perangkat**.
2. Klik beban kerja tempat Anda ingin menerapkan rencana pemantauan.
3. Klik **Lindungi**.
4. Bergantung pada apakah rencana pemantauan diterapkan ke beban kerja, lakukan hal berikut:

© Acronis International GmbH, 2003-2024

- Jika rencana pemantauan sudah diterapkan ke beban kerja, klik **Buat rencana**, lalu pilih **Pemantauan**.
- Jika tidak ada rencana pemantauan yang diterapkan pada beban kerja, klik **Tambahkan rencana**, lalu **Buat rencana**, lalu pilih **Pemantauan**.

5. Di jendela **Buat rencana pemantauan**, pilih salah satu opsi templat, lalu klik **Berikutnya**.

Opsi	Deskripsi
Disarankan	Pilih opsi ini untuk membuat rencana pemantauan dengan konfigurasi pemantauan.
Kustom	Gunakan opsi ini untuk membuat rencana pemantauan dari awal.

6. [Opsional] Untuk mengubah nama default rencana, klik ikon pensil, masukkan nama rencana, lalu klik **Oke**.
7. [Opsional] Jika Anda ingin mengubah pengaturan monitor dan peringatan, konfigurasikan nilai baru, lalu klik **Selesai**.

   Catatan
   Anda dapat menambahkan maksimum tiga monitor dengan jenis yang sama dan maksimum 30 monitor total ke rencana pemantauan.

8. [Opsional] Di layar parameter monitor, ubah pengaturan default monitor dan peringatan, lalu klik **Selesai**.

   Catatan
   Anda dapat mengonfigurasi pengaturan yang berbeda untuk setiap monitor. Untuk informasi lebih lanjut, lihat "Monitor yang dapat dikonfigurasi" (hlm. 1028) dan "Mengonfigurasi peringatan pemantauan" (hlm. 1072).

9. [Opsional] Untuk menghapus monitor, klik ikon tempat sampah, lalu klik **Hapus**.
10. Klik **Buat**.

Menambahkan beban kerja ke rencana pemantauan

Bergantung pada kebutuhan, Anda dapat menambahkan beban kerja ke rencana pemantauan setelah rencana dibuat.

Prasyarat

- 2FA diaktifkan untuk akun pengguna Anda.
- Versi agen yang diinstal pada beban kerja yang didukung oleh fungsionalitas pemantauan.
- Setidaknya satu rencana pemantauan tersedia.

Cara menambahkan beban kerja ke rencana pemantauan

© Acronis International GmbH, 2003-2024

Dari Rencana pemantauan

1. Di konsol Perlindungan, buka **Manajemen** > **Rencana pemantauan**.
2. Klik rencana pemantauan.
3. Bergantung pada apakah rencana sudah diterapkan ke beban kerja atau belum, lakukan hal berikut:
   - Klik **Tambahkan beban kerja**, jika rencana belum diaplikasikan pada beban kerja apa pun.
   - Klik **Kelola beban kerja**, jika rencana sudah diaplikasikan pada beban kerja apa pun.
4. Pilih beban kerja dari daftar, lalu klik **Tambahkan**.
5. Klik **Simpan**.
6. Jika perlu, klik **Konfirmasi** untuk menerapkan kuota layanan yang diperlukan ke beban kerja.

Dari Semua perangkat

1. Di konsol Perlindungan, buka **Perangkat** > **Semua perangkat**.
2. Klik beban kerja tempat Anda ingin menerapkan rencana pemantauan.
3. Klik **Lindungi.**
4. Temukan rencana pemantauan tempat Anda ingin menambahkan beban kerja, dan klik **Terapkan**.
5. Jika perlu, klik **Konfirmasi** untuk menerapkan kuota layanan yang diperlukan ke beban kerja.

Membatalkan rencana pemantauan

Anda dapat membatalkan rencana pemantauan dari beban kerja tempat rencana tersebut diterapkan.

Prasyarat

Setidaknya satu rencana pemantauan diterapkan ke beban kerja.

Cara membatalkan rencana pemantauan

1. Di konsol Perlindungan, buka **Perangkat** > **Semua perangkat**.
2. Klik beban kerja, lalu klik **Lindungi**.
3. Klik ikon **Tindakan lainnya** dari rencana pemantauan yang ingin Anda batalkan, lalu klik **Batalkan**.

Mengonfigurasi tindakan respons otomatis

Tindakan respons otomatis pada peristiwa yang disiagakan adalah tindakan atau tindakan yang telah ditetapkan sebelumnya yang dipicu secara otomatis sebagai respons terhadap peristiwa atau insiden yang terdeteksi. Tindakan-tindakan ini dirancang untuk mengurangi potensi ancaman dan meminimalkan kerusakan.

© Acronis International GmbH, 2003-2024

Anda dapat mengonfigurasi satu atau beberapa tindakan respons otomatis pada peristiwa yang disiagakan. Jumlah maksimum tindakan respons otomatis per monitor adalah 20.

Untuk mengonfigurasi tindakan respons otomatis

1. Di konsol Perlindungan, buka **Manajemen** > **Rencana pemantauan**.
2. Pilih rencana pemantauan yang ingin Anda konfigurasikan tindakan respons otomatisnya.
3. Pilih monitor yang ingin dikonfigurasikan tindakan respons otomatisnya, atau, jika Anda belum menambahkan monitor, klik **Tambah monitor**, klik monitor dalam daftar, klik **Tambah**, lalu pilih monitor.
4. Klik tautan di samping **Tindakan respons otomatis**.
5. Pada jendela **Tindakan respons otomatis**, tambahkan satu atau beberapa tindakan respons yang akan dilakukan secara otomatis saat peringatan dipicu.
6. Konfigurasikan setiap tindakan respons. Misalnya, jika Anda telah menambahkan tindakan respons **Mulai layanan Windows**, lakukan hal berikut:
   a. Di samping **Layanan Windows**, klik **Tentukan**.
   b. Di bidang **Layanan**, pilih layanan yang akan dimulai sebagai tindakan respons.
   c. Klik **Selesai**.
7. Pada daftar semua tindakan respons yang ditambahkan, gunakan panah atas dan bawah atau seret dan lepas untuk mengatur urutan tindakan respons.
8. Konfigurasikan cara menangani tindakan respons berurutan jika tindakan respons sebelumnya gagal. Pilih salah satu dari opsi berikut:
   a. **Lanjutkan dengan tindakan respons berikutnya**.
   b. **Jangan lanjutkan dengan tindakan respons berikutnya**.
9. Klik **Selesai**.

   Anda akan melihat jumlah tindakan yang dikonfigurasi di samping pengaturan **Tindakan respons otomatis** pada rencana pemantauan Anda. Anda dapat mengedit atau menghapus tindakan ini, serta menambahkan tindakan baru kapan saja.

Tabel berikut ini mencantumkan dan menjelaskan semua tindakan respons otomatis yang tersedia dalam pengaturan monitor.

Tindakan respons otomatis	Deskripsi	OS yang didukung
Jalankan skrip	Jika Anda menambahkan tindakan ini, Anda bisa: 1. Memilih skrip tertentu untuk dijalankan pada beban kerja. 2. Menentukan akun tempat Anda ingin menjalankan skrip. 3. Menentukan durasi maksimum operasi.	Windows, macOS

© Acronis International GmbH, 2003-2024

Tindakan respons otomatis	Deskripsi	OS yang didukung
	4. Menentukan kebijakan eksekusi PowerShell. 5. Jalankan skrip. Untuk melakukan tindakan ini, Anda memerlukan lisensi Paket Manajemen Tingkat Lanjut untuk beban kerja (jika belum ditetapkan). Sistem akan menjalankan skrip jarak jauh yang dipilih dengan parameter yang ditentukan ketika kondisi terpenuhi.	
Mulai ulang beban kerja	Jika Anda menambahkan tindakan ini, sistem akan memulai ulang beban kerja dari jarak jauh ketika kondisi terpenuhi.	Windows, macOS
Hentikan proses	Jika Anda menambahkan tindakan ini, Anda dapat menentukan proses yang akan dihentikan melalui input nama proses secara manual. Sistem akan menghentikan proses ketika kondisi terpenuhi.	Windows, macOS
Mulai layanan Windows	Jika Anda menambahkan tindakan ini, Anda dapat memilih layanan Windows mana yang akan dimulai dari daftar dinamis layanan yang diisi dari agen. Sistem akan memulai layanan ketika kondisi terpenuhi.	Windows
Hentikan layanan Windows	Jika Anda menambahkan tindakan ini, Anda dapat memilih layanan Windows mana yang akan dihentikan dari daftar dinamis layanan yang diisi dari agen. Sistem akan menghentikan layanan ketika kondisi terpenuhi.	Windows
Aktifkan Pembaruan Windows	Jika Anda menambahkan tindakan ini, sistem akan mengaktifkan Pembaruan Windows saat kondisi terpenuhi. Tindakan ini hanya tersedia untuk monitor status Pembaruan Windows.	Windows
Nonaktifkan AutoRun pada drive yang dapat dilepas	Jika Anda menambahkan tindakan ini, sistem akan menonaktifkan fitur AutoRun pada	Windows

© Acronis International GmbH, 2003-2024

Tindakan respons otomatis	Deskripsi	OS yang didukung
	media penyimpanan yang dapat dilepas untuk beban kerja saat kondisi terpenuhi. Tindakan ini hanya tersedia untuk monitor status fitur Autorun.	

Operasi tambahan dengan rencana pemantauan

Dari layar **Rencana monitoring**, Anda dapat melakukan operasi tambahan berikut dengan rencana monitoring: melihat detail, mengedit, melihat aktivitas, melihat peringatan, mengubah nama, mengaktifkan, menonaktifkan, klona, ekspor, dan menghapus.

Lihat detail

Cara melihat detail rencana pemantauan

1. Di layar **Rencana pemantauan**, klik ikon **Tindakan lainnya** dari rencana pemantauan.
2. Klik **Lihat detail**.
3. [Opsional] Jika Anda ingin melihat detail monitor yang diaktifkan di rencana, klik nama monitor.

Edit

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Untuk mengedit rencana

1. Di layar **Rencana pemantauan**, klik ikon **Tindakan lainnya** dari rencana pemantauan.
2. Klik **Edit**.
3. [Opsional] Untuk menghapus monitor dari rencana, klik ikon tempat sampah yang terletak di sebelah kanan nama monitor.
4. [Opsional] Untuk mengaktifkan atau menonaktifkan monitor dalam rencana, gunakan tombol di sebelah nama monitor.
5. [Opsional] Untuk mengedit parameter monitor, lakukan hal berikut.
   a. Klik nama monitor.
   b. Klik gambaran umum parameter monitor.
   c. Di layar **Parameter monitor**, konfigurasikan peringatan, lalu klik **Selesai**.

> **Catatan**
> Anda dapat mengonfigurasi pengaturan yang berbeda untuk setiap monitor. Untuk informasi lebih lanjut, lihat "Monitor yang dapat dikonfigurasi" (hlm. 1028) dan "Mengonfigurasi peringatan pemantauan" (hlm. 1072).

© Acronis International GmbH, 2003-2024

d. Tutup layar dan konfirmasikan perubahan.

6. [Opsional] Untuk menambahkan monitor, klik **Tambahkan monitor**, lalu, jika perlu, edit parameter seperti yang dijelaskan di langkah sebelumnya.
7. Klik **Simpan**.

Aktivitas

Cara melihat aktivitas terkait rencana pemantauan

1. Di layar **Rencana pemantauan**, klik ikon **Tindakan lainnya** dari rencana pemantauan.
2. Klik **Aktivitas**.
3. Klik aktivitas untuk melihat detail lebih lanjut tentangnya.

Peringatan

Untuk melihat peringatan

1. Di layar **Rencana pemantauan**, klik ikon **Tindakan lainnya** dari rencana pemantauan.
2. Klik **Peringatan**.

Ganti nama

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Cara mengganti nama rencana pemantauan

1. Di layar **Rencana pemantauan**, klik ikon **Tindakan lainnya** dari rencana pemantauan.
2. Klik **Ganti nama**.
3. Masukkan nama rencana baru, lalu klik **OK**.

Aktifkan

Prasyarat

- 2FA diaktifkan untuk akun pengguna Anda.
- Rencana pemantauan diterapkan pada setidaknya satu beban kerja.

Cara mengaktifkan rencana pemantauan

1. Di layar **Rencana pemantauan**, klik ikon **Tindakan lainnya** dari rencana pemantauan.
2. Klik **Aktifkan**.

Nonaktifkan

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

© Acronis International GmbH, 2003-2024

Cara menonaktifkan rencana pemantauan

1. Di layar **Rencana pemantauan**, klik ikon **Tindakan lainnya** dari rencana pemantauan.
2. Klik **Nonaktifkan**.

Klona

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Cara mengklona rencana monitoring

1. Di layar **Rencana pemantauan**, klik ikon **Tindakan lainnya** dari rencana pemantauan.
2. Klik **Klona**.
3. Klik **Buat**.

Ekspor

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Cara mengekspor rencana monitoring

1. Di layar **Rencana pemantauan**, klik ikon **Tindakan lainnya** dari rencana pemantauan.
2. Klik **Ekspor**.
   Konfigurasi rencana diekspor dalam format JSON ke mesin lokal.

Hapus

Prasyarat

2FA diaktifkan untuk akun pengguna Anda.

Cara menghapus rencana pemantauan

1. Di layar **Rencana pemantauan**, klik ikon **Tindakan lainnya** dari rencana pemantauan.
2. Klik **Hapus**.
3. Pilih **Konfirmasi**, lalu klik **Hapus**.

Masalah kompatibilitas dengan rencana pemantauan

Dalam beberapa kasus, menerapkan rencana pemantauan pada beban kerja dapat menyebabkan masalah kompatibilitas. Anda mungkin mengamati masalah kompatibilitas berikut:

- Sistem operasi tidak kompatibel - masalah ini muncul ketika sistem operasi beban kerja tidak didukung.

© Acronis International GmbH, 2003-2024

- Agen tidak didukung – masalah ini muncul ketika versi agen perlindungan pada beban kerja kedaluwarsa dan tidak mendukung fungsi pemantauan.
- Kuota tidak memadai - masalah ini muncul ketika tidak ada kuota layanan yang cukup pada penyewa untuk ditetapkan ke beban kerja yang dipilih.

Jika rencana pemantauan diterapkan hingga 150 beban kerja yang dipilih secara terpisah, Anda akan diminta untuk menyelesaikan konflik yang ada sebelum menyimpan rencana tersebut. Untuk menyelesaikan konflik, hapus akar penyebabnya atau hapus beban kerja yang terdampak dari rencana. Untuk informasi lebih lanjut, lihat "Menyelesaikan masalah kompatibilitas dengan rencana pemantauan" (hlm. 1070). Jika Anda menyimpan rencana tanpa menyelesaikan konflik, rencana akan otomatis dinonaktifkan untuk beban kerja yang tidak kompatibel dan peringatan akan ditampilkan.

Jika rencana pemantauan diterapkan ke lebih dari 150 beban kerja atau grup perangkat, rencana akan disimpan terlebih dahulu, lalu diperiksa kompatibilitasnya. Rencana akan otomatis dinonaktifkan untuk beban kerja yang tidak kompatibel dan peringatan akan ditampilkan.

Menyelesaikan masalah kompatibilitas dengan rencana pemantauan

Bergantung pada penyebab masalah kompatibilitas, Anda dapat melakukan berbagai tindakan untuk menyelesaikan masalah sebagai bagian dari proses membuat rencana pemantauan baru.

Cara menyelesaikan masalah kompatibilitas

1. Klik **Tinjau masalah**.
2. [Opsional] Untuk menyelesaikan masalah kompatibilitas dengan sistem operasi yang tidak kompatibel dengan menghapus beban kerja dari rencana:
   a. Pada tab **Sistem operasi yang tidak kompatibel**, pilih beban kerja yang ingin Anda hapus.
   b. Klik **Hapus beban kerja dari rencana**.
   c. Klik **Hapus**, lalu klik **Tutup**.
3. [Opsional] Untuk menyelesaikan masalah kompatibilitas dengan sistem operasi yang tidak kompatibel dengan menonaktifkan monitor dalam rencana:
   a. Pada tab **Sistem operasi yang tidak kompatibel**, pilih monitor yang ingin Anda hapus.
   b. Klik **Nonaktifkan monitor**.
   c. Klik **Nonaktifkan**, lalu klik **Tutup**.
4. [Opsional] Untuk menyelesaikan masalah kompatibilitas agen yang tidak didukung dengan menghapus beban kerja dari rencana:
   a. Pada tab **Agen yang tidak didukung**, pilih beban kerja yang ingin Anda hapus.
   b. Klik **Hapus beban kerja dari rencana**.
   c. Klik **Hapus**, lalu klik **Tutup**.

© Acronis International GmbH, 2003-2024

5. [Opsional] Untuk menyelesaikan masalah kompatibilitas agen yang tidak didukung dengan memperbarui versi agen, klik **Buka daftar Agen**.

   Catatan
   Opsi ini hanya tersedia untuk administrator pelanggan.

6. [Opsional] Untuk menyelesaikan masalah kompatibilitas kuota tidak memadai dengan menghapus beban kerja dari rencana:
   a. Pada tab **Kuota tidak memadai**, pilih beban kerja yang ingin Anda hapus.
   b. Klik **Hapus beban kerja dari rencana**.
   c. Klik **Hapus**, lalu klik **Tutup**.
7. [Opsional] Untuk menyelesaikan masalah kompatibilitas kuota tidak memadai dengan meningkatkan kuota penyewa:
   a. Pada tab **Kuota tidak memadai**, klik **Buka portal manajemen**.
   b. Tingkatkan layanan kuota untuk pelanggan.

      Catatan
      Opsi ini hanya tersedia untuk administrator mitra.

Memulai ulang model pembelajaran mesin

Anda dapat memulai ulang model beban kerja saat beban kerjanya menjadi usang atau tidak valid. Tindakan ini akan menghapus model yang dibuat dan data yang dikumpulkan untuk beban kerja oleh monitor dengan jenis pemantauan berbasis anomali, dan kemudian akan mulai melatih model pembelajaran mesin untuk beban kerja dari awal.

Untuk memulai ulang model pembelajaran mesin untuk beban kerja

1. Di konsol Perlindungan, buka **Perangkat** > **Semua perangkat**.
2. Klik beban kerja dari daftar, lalu klik tab **Detail**.
3. Di bagian **Mulai ulang model pembelajaran mesin**, klik **Mulai ulang**.
4. Di jendela konfirmasi, klik **Mulai ulang** lagi.

Peringatan pemantauan

Peringatan monitoring ditampilkan di konsol Perlindungandan dikirim melalui email ketika perilaku beban kerja yang dimonitor berada di luar norma. Peringatan tersebut memastikan bahwa para pemangku kepentingan diberi tahu secepat mungkin ketika ada masalah di lingkungan IT organisasi.

© Acronis International GmbH, 2003-2024

Catatan
Untuk mengaktifkan peringatan monitoring melalui email, Anda harus mengkonfigurasi setidaknya satu kebijakan notifikasi email untuk jenis peringatan yang sesuai. Untuk informasi lebih lanjut, lihat "Mengonfigurasi kebijakan notifikasi email" (hlm. 1079).

Mengonfigurasi peringatan pemantauan

Anda dapat mengonfigurasi pengaturan peringatan monitor ketika menambahkan monitor ke rencana pemantauan, atau ketika mengedit monitor yang sudah tersedia di rencana pemantauan.

Cara mengonfigurasi peringatan pemantauan

1. Di jendela **Parameter monitor**, buka bagian **Keluarkan peringatan**.
2. Di **Tingkat keparahan peringatan**, pilih tingkat keparahan yang terkait dengan prioritas peringatan.

Opsi	Deskripsi
Kritis	Peringatan ini memiliki prioritas tertinggi dan terkait dengan masalah penting untuk operasi beban kerja. Segera selesaikan masalah ini.
Eror	Peringatan kesalahan tidak terlalu parah dan menunjukkan bahwa ada yang salah atau perilaku tidak normal. Selesaikan masalah secara tepat waktu untuk mencegah masalah yang lebih parah.
Peringatan	Peringatan menunjukkan bahwa ada beberapa kondisi yang harus Anda ketahui, tetapi mungkin belum menyebabkan masalah. Selesaikan masalah setelah Anda memperbaiki masalah yang menyebabkan peringatan kritis dan kesalahan. Ini adalah nilai default.
Informasi	Peringatan ini memiliki prioritas paling rendah. Tingkat keparahan Informasi tidak menunjukkan masalah. Peringatan tersebut memberikan informasi tentang tindakan terkait objek yang dipantau.

3. Di **Frekuensi peringatan**, pilih frekuensi peringatan yang harus dikeluarkan sistem ketika syarat terpenuhi.

Opsi	Deskripsi
Satu kali hingga pemeriksaan lolos	Sistem akan mengeluarkan peringatan satu kali hingga pemeriksaan berhasil diselesaikan. Ini adalah nilai default.
Setelah gagal beruntun X kali	Sistem akan mengeluarkan peringatan setelah pemeriksaan gagal X kali berturut-turut, dan X adalah bilangan bulat.

4. Di **Pesan peringatan**, klik ikon pensil untuk mengedit pesan peringatan default yang akan digunakan ketika sistem mengeluarkan peringatan. Anda dapat menentukan pesan peringatan

© Acronis International GmbH, 2003-2024

kustom yang berisi variabel. Untuk informasi lebih lanjut tentang variabel yang dapat Anda gunakan, lihat "Variabel peringatan pemantauan" (hlm. 1073).

Catatan
Anda dapat mengonfigurasi lebih dari satu pesan peringatan untuk beberapa monitor.

5. Aktifkan **Resolusi otomatis peringatan** jika Anda ingin sistem otomatis menyelesaikan peringatan saat metrik pemantauan kembali ke keadaan normal dan perilaku kembali normal. Secara default, pengaturan diaktifkan.

Variabel peringatan pemantauan

Anda dapat mengonfigurasi variabel peringatan yang berbeda untuk monitor yang berbeda. Untuk menggunakan variabel, itu harus diapit {{}}.

Tabel berikut memberikan informasi lebih lanjut tentang variabel yang tersedia.

Variabel	Deskripsi	Tersedia untuk monitor
plan_name	Nama kebijakan	Semua monitor
monitor_name	Nama sub kebijakan dalam rencana pemantauan	Semua monitor
workload_ name	Nama beban kerja	Semua monitor
threshold_ value	Syarat pemantauan khusus atau ambang batas untuk mengeluarkan peringatan	Semua monitor yang mendukung pemantauan berbasis ambang batas.
threshold_unit	Unit yang terkait dengan nilai ambang batas. Misalnya, %, MB, atau mb/detik.	Semua monitor yang mendukung pemantauan berbasis ambang batas.
time_period	Sistem akan mengeluarkan peringatan untuk masalah yang terdeteksi hanya jika nilai metrik melebihi batas normal selama periode yang ditentukan.	Semua monitor yang mendukung pemantauan berbasis ambang batas.
time_unit	Unit yang terkait dengan periode waktu (detik/menit/jam/hari).	Semua monitor yang mendukung pemantauan berbasis ambang batas.
anomaly_value	Nilai anomali	Semua monitor yang mendukung pemantauan berbasis

© Acronis International GmbH, 2003-2024

Variabel	Deskripsi	Tersedia untuk monitor
		anomali.
anomaly_unit	Unit yang akan dikaitkan dengan nilai anomali	Semua monitor yang mendukung pemantauan berbasis anomali.
deviation_value	Nilai deviasi	Semua monitor yang mendukung pemantauan berbasis anomali.
deviation_unit	Unit yang akan dikaitkan dengan nilai deviasi	Semua monitor yang mendukung pemantauan berbasis anomali.
drive_name	Drive untuk Windows, atau partisi untuk macOS	Ruang disk,
CPU_model	Model CPU yang dipantau	Suhu CPU
GPU_model	Model GPU yang dipantau	Suhu GPU
hardware_model	Model komponen yang dipantau	Perubahan perangkat keras
hardware_component	Jenis perangkat keras yang dipantau	Perubahan perangkat keras
hardware_model_old	Model komponen yang dipantau yang diganti	Perubahan perangkat keras
hardware_model_new	Model komponen baru yang dipantau yang ditambahkan	Perubahan perangkat keras
disk_model	Model disk	Kecepatan transfer disk
network_adapter_model	Model adaptor jaringan	Penggunaan jaringan
process_name	Nama proses	Penggunaan CPU berdasarkan proses Penggunaan memori berdasarkan proses Kecepatan transfer disk berdasarkan proses Penggunaan jaringan berdasarkan proses

© Acronis International GmbH, 2003-2024

Variabel	Deskripsi	Tersedia untuk monitor
		Status proses
service_name	Nama layanan	Status layanan Windows
software_name	Nama aplikasi perangkat lunak	Perangkat lunak yang diinstal
software_ version	Versi aplikasi perangkat lunak	Perangkat lunak yang diinstal
software_ version_old	Versi aplikasi perangkat lunak sebelum pembaruan	Perangkat lunak yang diinstal
software_ version_new	Versi aplikasi perangkat lunak baru atau yang diperbarui	Perangkat lunak yang diinstal
number_of_ occurrences	Frekuensi peristiwa muncul di log	Log event Windows
event_types	Jenis peristiwa	Log event Windows
event_source	Sumber peristiwa	Log event Windows
event_log_ name	Nama peristiwa	Log event Windows
firewall_ software_name	Nama perangkat lunak firewall	Status firewall
antimalware_ software_name	Nama perangkat lunak antimalware	Status perangkat lunak antimalware
user_name	Nama pengguna	Status fitur AutoRun
script_name	Nama skrip	Kustom

Tindakan respons manual

Saat melihat peringatan, Anda dapat memilih tindakan respons yang ingin dilakukan pada peristiwa yang diperingatkan.

Cara melakukan tindakan respons manual

1. Di konsol Perlindungan, buka **Peringatan**.
2. Buka peringatan yang ingin Anda lihat.
3. Klik **Tindakan respons**, lalu pilih tindakan respons dari daftar drop-down.

© Acronis International GmbH, 2003-2024

Daftar tindakan respons yang tersedia untuk peringatan tertentu bergantung pada jenis peringatan, ketersediaan fitur untuk penyewa tertentu, dan sistem operasi beban kerja.

Tabel berikut mencantumkan dan menjelaskan semua tindakan respons manual sebagai referensi Anda.

Tindakan respons manual	Deskripsi	OS yang didukung
Jelajahi tren penggunaan ruang disk	Membuka jendela dengan grafik **Penggunaan ruang disk**, tempat Anda dapat: • Telusuri perubahan penggunaan ruang disk dari waktu ke waktu (selama 1 hari/7 hari/1 bulan terakhir). • Telusuri delta untuk penggunaan ruang disk dalam nilai relatif (%) untuk periode yang dipilih.	Windows, macOS
Telusuri tren pertumbuhan ukuran file	Membuka jendela dengan grafik **Pertumbuhan ukuran file**, tempat Anda dapat: • Telusuri perubahan ukuran total file dan folder yang dipantau dari waktu ke waktu (selama 1 hari/7 hari/1 bulan terakhir). • Telusuri delta untuk ukuran total file dalam nilai relatif (%) untuk periode yang dipilih.	Windows, macOS
Jalankan skrip	Membuka jendela, tempat Anda dapat: 1. Memilih skrip tertentu untuk dijalankan pada beban kerja. 2. Menentukan akun tempat Anda ingin menjalankan skrip. 3. Menentukan durasi maksimum operasi. 4. Menentukan kebijakan eksekusi PowerShell. 5. Jalankan skrip. Untuk melakukan tindakan ini, Anda memerlukan lisensi Paket Manajemen Tingkat Lanjut untuk beban kerja (jika belum ditetapkan).	Windows, macOS
Sambungkan melalui NEAR	Acronis Hubungkan Klien membuat koneksi jarak jauh.	Windows, macOS
Sambungkan melalui RDP	Acronis Hubungkan Klien membuat koneksi jarak jauh.	Windows

© Acronis International GmbH, 2003-2024

Tindakan respons manual	Deskripsi	OS yang didukung
Buka inventaris perangkat keras	Anda diarahkan ke tab **Inventaris perangkat keras** untuk beban kerja saat ini.	Windows, macOS
Jelajahi 10 proses teratas yang memuat CPU	Membuka jendela dengan 10 proses teratas yang telah memuat CPU dan mungkin menyebabkan panas berlebih (Snapshot sistem pada saat pembuatan peringatan).	Windows, macOS
Jelajahi 10 proses teratas yang memuat GPU	Membuka jendela dengan 10 proses teratas yang telah memuat GPU dan mungkin menyebabkan panas berlebih (Snapshot sistem pada saat pembuatan peringatan).	Windows, macOS
Jelajahi 10 proses teratas yang memuat memori	Membuka jendela dengan 10 proses teratas yang telah memuat memori (Snapshot sistem pada saat pembuatan peringatan).	Windows, macOS
Jelajahi 10 proses teratas yang memuat disk	Membuka jendela dengan 10 proses teratas yang telah memuat disk (Snapshot sistem pada saat pembuatan peringatan).	Windows, macOS
Jelajahi 10 proses teratas yang memuat jaringan	Membuka jendela dengan 10 proses teratas yang telah memuat adaptor antarmuka jaringan (Snapshot sistem pada saat pembuatan peringatan).	Windows, macOS
Jelajahi penggunaan sumber daya berdasarkan proses	Membuka jendela dengan informasi mendetail tentang penggunaan sumber daya perangkat keras oleh proses terkait: penggunaan CPU, penggunaan memori, disk I/O, penggunaan jaringan.	Windows, macOS
Mulai ulang beban kerja	Membuka jendela konfirmasi. Memulai ulang beban kerja setelah konfirmasi.	Windows, macOS
Mulai layanan Windows	Membuka jendela konfirmasi. Memulai layanan Windows setelah konfirmasi.	Windows
Hentikan layanan Windows	Membuka jendela konfirmasi. Menghentikan layanan Windows setelah konfirmasi.	Windows
Hentikan proses	Membuka jendela konfirmasi. Menghentikan proses yang dimaksud peringatan setelah konfirmasi.	Windows, macOS
Aktifkan Pembaruan Windows	Membuka jendela konfirmasi. Mengaktifkan Pembaruan Windows setelah konfirmasi.	Windows
Nonaktifkan fitur AutoRun	Membuka jendela konfirmasi. Menonaktifkan	Windows

© Acronis International GmbH, 2003-2024

Tindakan respons manual	Deskripsi	OS yang didukung
pada drive yang dapat dilepas	fitur AutoRun pada level sistem beban kerja setelah konfirmasi.	

Penting
Untuk alasan keamanan, autentikasi dua faktor diperlukan untuk melakukan tindakan respons manual berikut:

- Jalankan skrip
- Sambungkan melalui NEAR
- Sambungkan melalui RDP
- Mulai ulang beban kerja
- Mulai layanan Windows
- Hentikan layanan Windows
- Hentikan proses
- Aktifkan Pembaruan Windows
- Nonaktifkan fitur AutoRun pada drive yang dapat dilepas

Melihat peringatan monitoring untuk beban kerja

Di tab **Peringatan**, Anda dapat melihat peringatan monitoring dari beban kerja spesifik dan melakukan berbagai tindakan peringatan.

Untuk melihat peringatan monitoring untuk beban kerja

1. Di konsol Perlindungan, buka **Semua perangkat**.
2. Klik beban kerja, dan kemudian pilih tab **Peringatan**.
3. [Opsional] Di panel peringatan monitoring, lakukan salah satu dari tindakan berikut:
   - Untuk menghapus peringatan, klik **Hapus**.
   - Untuk melakukan tindakan respons, klik **Tindakan respons**, dan kemudian klik tindakannya.
   - Untuk menghubungi tim Dukungan, klik **Dapatkan dukungan**.
4. [Opsional] Untuk menghapus semua peringatan monitoring untuk beban kerja, klik **Hapus semua**.

Melihat log peringatan dari peringatan pemantauan

Anda dapat melihat semua peristiwa yang terkait dengan peringatan pemantauan dalam urutan kronologis: tindakan respons (baik otomatis maupun manual) yang dilakukan, dan notifikasi email

© Acronis International GmbH, 2003-2024

yang dikirim.

Cara melihat log audit peringatan pemantauan

1. Di konsol Perlindungan, buka **Peringatan**.
2. Buka **Tampilan tabel**.
3. Di daftar peringatan, klik peringatan pemantauan yang ingin Anda lihat.
4. Klik **Detail**, lalu klik **Log peringatan**.

Mengonfigurasi kebijakan notifikasi email

Kebijakan notifikasi email menentukan pengguna mana yang akan menerima notifikasi email dari berbagai monitor.

Dari layar **Notifikasi email**, Anda dapat melakukan tindakan berikut dengan kebijakan notifikasi email: menambahkan, mengedit, mengaktifkan, menonaktifkan, dan menghapus.

Menambahkan

Cara menambahkan kebijakan notifikasi email baru

1. Di konsol Perlindungan, buka **Pengaturan** > **Notifikasi email**.
2. Klik **Tambah Kebijakan**.
3. Klik **Pilih penerima**.
4. Di layar **Pilih penerima**, pilih pengguna yang Anda inginkan untuk menerima peringatan email, dan kemudian klik **Pilih**.
5. Di **Jenis Peringatan**, pilih monitor yang Anda inginkan agar sistem mengirim peringatan via email.
6. Klik **Tambah**.

Edit

Untuk mengedit kebijakan notifikasi email

1. Di konsol Perlindungan, buka **Pengaturan** > **Notifikasi email**.
2. Klik ikon elipsis pada Kebijakan notifikasi, lalu klik **Edit**.
3. [Opsional] Untuk mengubah penerima, klik **Edit penerima**, tambahkan atau hapus pengguna dari daftar, lalu klik **Pilih**.
4. [Opsional] Dalam **Jenis Peringatan**, pilih jenis peringatan monitoring yang ingin Anda kirimkan ke penerima yang dipilih.
5. Klik **Simpan**.

Aktifkan

Untuk mengaktifkan kebijakan notifikasi email

© Acronis International GmbH, 2003-2024

1. Di konsol Perlindungan, buka **Pengaturan** > **Notifikasi email**.
2. Di layar **Notifikasi email**, klik ikon **...** pada Kebijakan notifikasi email.
3. Klik **Aktifkan**.

Nonaktifkan

Untuk menonaktifkan kebijakan notifikasi email

1. Di konsol Perlindungan, buka **Pengaturan** > **Notifikasi email**.
2. Di layar **Notifikasi email**, klik ikon **...** pada Kebijakan notifikasi email.
3. Klik **Nonaktifkan**.

Hapus

Untuk menghapus kebijakan notifikasi email

1. Di konsol Perlindungan, buka **Pengaturan** > **Notifikasi email**.
2. Di layar **Notifikasi email**, klik ikon **...** pada Kebijakan notifikasi email.
3. Klik **Hapus**, lalu klik **Konfirmasi**.

Melihat data monitor

Untuk setiap beban kerja, Anda dapat melihat daftar monitor yang diterapkan, status monitor saat ini, dan detail riwayat kinerja dalam tampilan grafis. Anda dapat menggunakan informasi ini untuk menganalisis keadaan beban kerja dan bagaimana keadaan tersebut berubah seiring waktu.

Prasyarat

- Rencana pemantauan diterapkan pada beban kerja.
- Beban kerja ini online dan memiliki data untuk monitor yang terkait.
- Versi agen yang diinstal pada beban kerja mendukung rencana pemantauan.

Cara melihat monitor yang diterapkan ke beban kerja dan data monitor

1. Di konsol Perlindungan, buka **Perangkat** > **Semua perangkat**.
2. Klik beban kerja, lalu klik tab **Pemantauan**.

   Tab **Pemantauan** menampilkan widget untuk setiap monitor yang diaktifkan untuk beban kerja. Setiap widget menampilkan informasi berikut.

Informasi yang ditampilkan	Deskripsi
Nama monitor	Nama monitor
Hasil terakhir	Nilai terbaru metrik yang dipantau atau status peristiwa terbaru

© Acronis International GmbH, 2003-2024

Informasi yang ditampilkan	Deskripsi
Pemeriksaan terakhir	Tanggal dan waktu saat monitor mengumpulkan data terakhir
Peringatan	Jumlah peringatan yang dihasilkan oleh monitor dan masih belum terselesaikan. Jika ada setidaknya satu peringatan yang belum diselesaikan yang dihasilkan oleh monitor ini, klik nomor untuk membuka tab **Peringatan**. Peringatan akan disaring dan hanya peringatan untuk monitor ini yang akan ditampilkan.

Catatan
Widget terlihat di tab 15 menit (atau frekuensi monitor minimum yang diatur untuk monitor) setelah Anda menerapkan rencana pemantauan ke beban kerja.

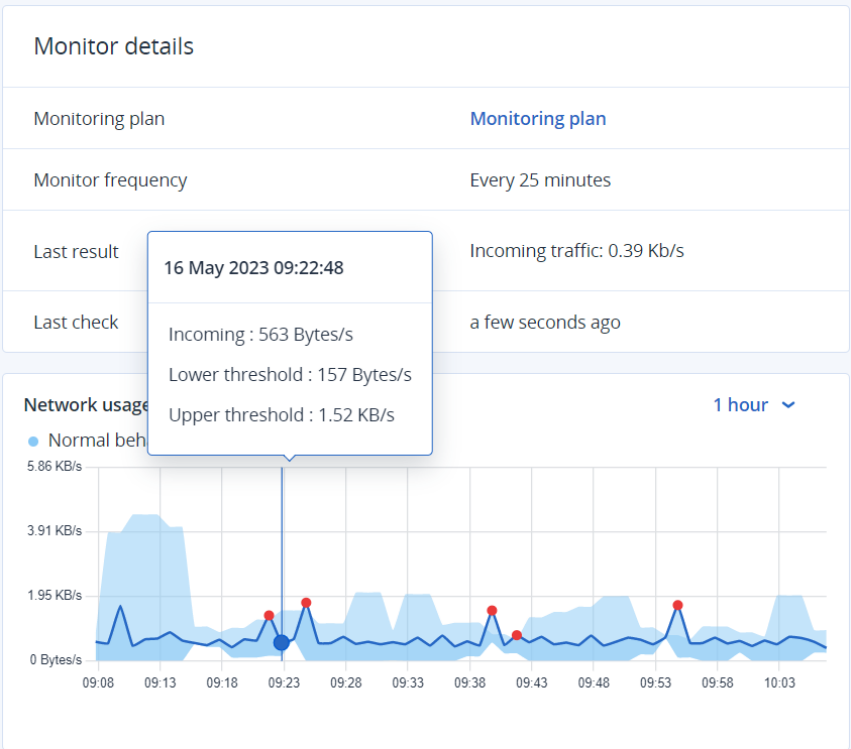
3. [Opsional] Untuk melihat detail selengkapnya tentang monitor, dan jika berlaku, data historis yang dikumpulkan untuk metrik yang dipantau, klik ikon elipsis, lalu klik **Detail** di widget monitor.
   Untuk mengetahui informasi lebih lanjut tentang detail monitor yang dapat Anda lihat di widget, lihat "Widget monitor" (hlm. 1081).

Widget monitor

Di widget monitor, Anda dapat melihat detail monitor berikut.

Detail	Deskripsi
Rencana pemantauan	Nama rencana pemantauan yang berisi monitor. Nama rencana pemantauan adalah tautan yang membuka rencana pemantauan dalam mode tampilan.
Frekuensi monitor	Interval waktu saat monitor mengumpulkan data dari beban kerja
Hasil terakhir	Nilai terbaru metrik yang dipantau atau status peristiwa terbaru
Pemeriksaan terakhir	Tanggal dan waktu saat monitor mengumpulkan data terakhir
Peringatan terakhir	Tanggal dan waktu saat peringatan terakhir dikeluarkan. Bidang hanya ditampilkan jika setidaknya satu peringatan telah dibuat untuk monitor.
Grafik historis	Untuk monitor yang mengumpulkan data rangkaian waktu, widget menampilkan data historis untuk periode yang dipilih (1 jam, 6 jam, 12 jam, 1 hari, 1 minggu, atau 1 bulan) dalam tampilan grafik. Grafik menampilkan nilai aktual dari metrik selama periode yang Anda pilih.

© Acronis International GmbH, 2003-2024

Detail	Deskripsi
	Jika karena alasan tertentu agen tidak mengirimkan data yang dikumpulkan ke cloud, nilai yang hilang ditampilkan dalam bentuk garis putus-putus yang menghubungkan titik data dengan nilai aktual yang mendahului dan mengikuti nilai yang hilang. Untuk monitor yang menggunakan monitoring berbasis **Anomali**, grafik menampilkan area garis acuan, sebuah garis yang menunjukkan nilai aktual dari metrik beserta anomalinya. Anomali adalah lonjakan atau nilai yang berada di luar garis acuan dan ditampilkan sebagai titik merah pada grafik. Jika Anda mengarahkan pointer mouse ke grafik, Anda dapat melihat nilai aktual dan nilai ambang batas untuk waktu tertentu.  **Catatan** Data pada grafik ditampilkan dalam zona waktu sistem lokal. Itu adalah zona waktu browser dari beban kerja tempat Anda mengakses konsol Perlindungan.

© Acronis International GmbH, 2003-2024

Alat bantu Cyber Protection tambahan

Mode kepatuhan

Mode Kepatuhan dirancang untuk klien dengan tuntutan keamanan yang lebih tinggi. Mode ini membutuhkan enkripsi wajib untuk semua cadangan dan hanya mengizinkan kata sandi enkripsi yang diatur langsung di lokasi.

Dengan mode Kepatuhan, semua cadangan yang dibuat dalam penyewa pelanggan dan unit-unitnya secara otomatis dienkripsi dengan algoritma AES dan kunci 256-bit. Pengguna hanya dapat mengatur kata sandi enkripsi pada perangkat yang dilindungi, dan tidak dapat mengaturnya dalam rencana proteksi.

Penting
Mode Kepatuhan tidak dapat dinonaktifkan.

Pembatasan

- Mode Kepatuhan hanya kompatibel dengan versi agen 15.0.26390 atau lebih tinggi.
- Mode kepatuhan tidak tersedia untuk perangkat yang menjalankan Red Hat Enterprise Linux 4.x atau 5.x, dan turunannya.
- Layanan cloud tidak dapat mengakses kata sandi enkripsi. Karena keterbatasan ini, beberapa fitur tidak tersedia untuk penyewa dalam mode Kepatuhan.

Fitur yang tidak didukung

Fitur-fitur berikut tidak tersedia untuk penyewa dalam mode Kepatuhan:

- Pemulihan melalui konsol Cyber Protect
- Penjelajahan tingkat file cadangan melalui konsol Cyber Protect
- Pencadangan awan ke awan
- Pencadangan situs web
- Cadangan aplikasi
- Pencadangan perangkat seluler
- Pemindaian antimalware pada cadangan
- Pemulihan aman
- Pembuatan daftar putih korporat otomatis
- Peta perlindungan data
- Pemulihan bencana
- Laporan dan dasbor yang terkait ke fitur yang tidak tersedia

© Acronis International GmbH, 2003-2024

Mengatur kata sandi enkripsi

Anda harus mengatur kata sandi enkripsi secara lokal pada perangkat yang dilindungi. Anda tidak dapat menetapkan kata sandi enkripsi di rencana proteksi Tanpa kata sandi, pencadangan selanjutnya akan gagal.

Peringatan!
Tidak ada cara untuk memulihkan cadangan terenkripsi jika Anda menghilangkan atau lupa kata sandi.

Anda dapat mengubah kata sandi enkripsi dengan cara berikut:

1. Selama penginstalan agen proteksi (untuk Windows, macOS, dan Linux).
2. Dengan menggunakan baris perintah (untuk Windows dan Linux).
   Ini adalah satu-satunya cara untuk mengatur kata sandi enkripsi pada alat virtual.
   Untuk informasi lebih lanjut tentang cara mengatur kata sandi enkripsi dengan alat **Acropsh**, lihat "Enkripsi" (hlm. 441).
3. Di Cyber Protect Monitor (untuk Windows dan macOS).

Untuk mengatur kata sandi enkripsi di Cyber Protect Monitor

1. Di perangkat terlindungi, masuk sebagai administrator.
2. Klik ikon Cyber Protect Monitor di area notifikasi (di Windows) atau bar menu (di macOS).
3. Klik ikon roda gigi.
4. Klik **Enkripsi**.
5. Atur kata sandi enkripsi.
6. Klik **OK**.

Mengubah kata sandi enkripsi

Anda dapat mengubah kata sandi enkripsi sebelum rencana proteksi membuat cadangan apa pun.

Kami menyarankan Anda untuk tidak mengubah kata sandi enkripsi setelah pencadangan dibuat, karena pencadangan berikutnya akan gagal. Untuk melanjutkan proteksi mesin yang sama, Anda perlu membuat rencana proteksi baru. Mengubah kedua kata sandi enkripsi dan rencana proteksi akan membuat cadangan baru yang dienkripsi dengan kata sandi terbaru. Cadangan yang dibuat sebelum perubahan ini tidak akan terpengaruh.

Atau, Anda dapat membiarkan rencana proteksi yang telah diterapkan, dan hanya mengubah nama file cadangan di dalamnya. Ini juga akan membuat cadangan baru yang dienkripsi dengan kata sandi terbaru. Untuk mempelajari lebih lanjut tentang nama file cadangan, lihat "Nama file cadangan" (hlm. 450).

Anda dapat mengubah kata sandi enkripsi dengan cara berikut:

© Acronis International GmbH, 2003-2024

1. Di Cyber Protect Monitor (untuk Windows dan macOS).
2. Dengan menggunakan baris perintah (untuk Windows dan Linux).
   Untuk informasi lebih lanjut tentang cara mengatur kata sandi enkripsi dengan alat **Acropsh**, lihat "Enkripsi" (hlm. 441).

Memulihkan cadangan untuk penyewa dalam mode Kepatuhan

Dengan mode Kepatuhan, Anda tidak dapat memulihkan cadangan di konsol Cyber Protect.

Opsi berikut tersedia:

- Memulihkan seluruh mesin, disk, atau file menggunakan media yang dapat di-boot.
- Mengekstrak file dari cadangan lokal mesin Windows dengan agen terinstal, menggunakan Windows File Explorer.

Penyimpanan yang tidak dapat diubah

Dengan penyimpanan yang tidak dapat diubah, Anda dapat mengakses cadangan yang dihapus selama periode retensi tertentu. Anda dapat memulihkan konten dari cadangan ini, tetapi Anda tidak dapat mengubah, memindahkan, atau menghapusnya. Ketika periode retensi berakhir, cadangan yang dihapus akan dihapus secara permanen.

Penyimpanan yang tidak dapat diubah berisi cadangan berikut:

- Cadangan yang dihapus secara manual.
- Cadangan yang dihapus secara otomatis, sesuai dengan pengaturan di bagian **Berapa lama akan disimpan** dalam rencana proteksi atau bagian **Aturan retensi** dalam rencana pembersihan.

Cadangan yang dihapus dalam penyimpanan yang tidak dapat diubah masih menggunakan ruang penyimpanan dan dikenakan biaya yang sesuai.

Penyewa yang dihapus tidak dikenakan biaya untuk penyimpanan apa pun, termasuk penyimpanan yang tidak dapat diubah.

Mode penyimpanan yang tidak dapat diubah

Untuk penyewa pelanggan, penyimpanan yang tidak dapat diubah tersedia dalam mode berikut:

Penyimpanan yang tidak dapat diubah tersedia dalam mode berikut:

- **Mode tata kelola**
  Anda dapat menonaktifkan dan mengaktifkan kembali penyimpanan yang tidak dapat diubah. Anda dapat mengubah periode retensi atau beralih ke mode Kepatuhan.
- **Mode kepatuhan**

  Peringatan!
  Memilih mode Kepatuhan tidak dapat dibatalkan.

© Acronis International GmbH, 2003-2024

Anda tidak dapat menonaktifkan penyimpanan yang tidak dapat diubah. Anda tidak dapat mengubah periode retensi dan tidak dapat kembali ke mode Tata Kelola.

Penyimpanan dan agen yang didukung

- Penyimpanan yang tidak dapat diubah hanya didukung pada penyimpanan cloud.

  Penyimpanan yang tidak dapat diubah tersedia untuk penyimpanan cloud yang dihosting Acronis dan yang dihosting mitra yang menggunakan Acronis Cyber Infrastructure versi 4.7.1 atau lebih baru.

  Semua penyimpanan yang dapat digunakan dengan Acronis Cyber Infrastructure Gateway Cadangan didukung. Misalnya, penyimpanan Acronis Cyber Infrastructure, penyimpanan Amazon S3 dan EC2, dan penyimpanan Microsoft Azure.

  Penyimpanan yang tidak dapat diubah memerlukan Port TCP 40440 dibuka untuk layanan Gateway cadangan di Acronis Cyber Infrastructure. Dalam versi 4.7.1 dan seterusnya, Port TCP 40440 secara otomatis dibuka dengan jenis lalu lintas **Cadangan (ABGW) publik**. Untuk informasi lebih lanjut tentang jenis lalu lintas, lihat dokumen Acronis Cyber Infrastructure.
- Penyimpanan yang tidak dapat diubah memerlukan agen proteksi versi 21.12 (build 15.0.28532) atau versi lebih baru.
- Hanya cadangan TIBX (Versi 12) yang didukung.

Mengaktifkan penyimpanan yang tidak dapat diubah

Anda dapat mengonfigurasi pengaturan penyimpanan yang tidak dapat diubah di konsol Cyber Protect atau di portal manajemen. Keduanya memberikan akses ke pengaturan yang sama. Prosedur di bawah ini menggunakan konsol Cyber Protect. Untuk mempelajari cara mengkonfigurasi pengaturan penyimpanan yang tidak dapat diubah di portal manajemen, lihat Mengkonfigurasi penyimpanan yang tidak dapat diubah di panduan administrator.

Mengonfigurasi pengaturan penyimpanan yang tidak dapat diubah memerlukan autentikasi dua faktor dalam penyewa yang memiliki akun administrator.

Cara mengaktifkan penyimpanan yang tidak dapat diubah

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Buka **Pengaturan** > **Pengaturan Sistem**.
3. Gulir daftar opsi cadangan default, lalu klik **Penyimpanan yang tidak dapat diubah**.
4. Aktifkan switch **Penyimpanan yang tidak dapat diubah**.
5. Tentukan periode retensi antara 14 dan 3650 hari.

   Periode retensi default adalah 14 hari. Periode retensi yang lebih lama akan menyebabkan peningkatan penggunaan penyimpanan.
6. Pilih mode penyimpanan yang tidak dapat diubah, lalu konfirmasi pilihan Anda, jika diminta.

© Acronis International GmbH, 2003-2024

Dalam mode Tata Kelola, Anda dapat mengaktifkan atau menonaktifkan penyimpanan yang tidak dapat diubah, dan mengubah periode penyimpanan. Anda dapat beralih dari mode Tata Kelola ke mode Kepatuhan.

Peringatan!
Beralih ke mode Kepatuhan tidak dapat dibalikkan. Setelah Anda memilih mode Kepatuhan, Anda tidak dapat menonaktifkan penyimpanan yang tidak dapat diubah, atau mengubah mode atau periode retensinya.

7. Klik **Simpan**.
8. Untuk membuat arsip yang ada mendukung penyimpanan yang tidak dapat diubah, buat cadangan baru di arsip tersebut.
   Untuk membuat cadangan baru, jalankan rencana proteksi secara manual atau sesuai jadwal.

Peringatan!
Jika Anda menghapus cadangan sebelum membuat arsip mendukung penyimpanan yang tidak dapat diubah, cadangan tersebut akan dihapus secara permanen.

Menonaktifkan penyimpanan yang tidak dapat diubah

Catatan
Anda hanya dapat menonaktifkan penyimpanan yang tidak dapat diubah hanya dalam mode Tata Kelola.

Cara menonaktifkan penyimpanan yang tidak dapat diubah

1. Masuk ke konsol Cyber Protect sebagai administrator.
2. Di menu navigasi, klik **Pengaturan** > **Pengaturan sistem**.
3. Gulir daftar opsi cadangan default, lalu klik **Penyimpanan yang tidak dapat diubah**.
4. Nonaktifkan switch **Penyimpanan yang tidak dapat diubah**.
5. Konfirmasi pilihan Anda dengan mengeklik **Nonaktifkan**.

Peringatan!
Penonaktifan penyimpanan yang tidak dapat diubah tidak segera berlaku. Selama masa tenggang 14 hari, penyimpanan yang tidak dapat diubah masih aktif dan Anda dapat mengakses cadangan yang dihapus sesuai dengan periode penyimpanan aslinya. Ketika masa tenggang berakhir, semua cadangan di penyimpanan yang tidak dapat diubah akan dihapus secara permanen.

Mengakses cadangan yang dihapus dalam penyimpanan yang tidak dapat diubah

Selama periode retensi yang ditentukan, Anda dapat mengakses cadangan yang dihapus dan memulihkan data dari cadangan tersebut.

© Acronis International GmbH, 2003-2024

Catatan
Untuk memberi akses ke cadangan yang telah dihapus, port 40440 pada penyimpanan cadangan harus diaktifkan untuk koneksi masuk.

Untuk mengakses cadangan yang dihapus

1. Pada tab **Penyimpanan cadangan**, pilih penyimpanan awan yang berisi penyimpanan yang dihapus.
2. [Hanya untuk arsip yang dihapus] Untuk melihat arsip yang dihapus, klik **Tampilkan yang dihapus**.
3. Pilih arsip yang berisi cadangan yang ingin Anda pulihkan.
4. Klik **Tampilkan cadangan**, lalu klik **Tampilkan yang dihapus**.
5. Pilih cadangan yang ingin Anda pulihkan.
6. Lanjutkan dengan operasi pemulihan, seperti dijelaskan dalam "Pemulihan" (hlm. 495).

Penyimpanan geo-redundan

Penyimpanan geo-redundan memastikan ketahanan data dengan menyalinnya secara asinkron ke lokasi sekunder yang secara geografis jauh dari lokasi utama. Dengan redundansi geografis, data Anda dapat diakses meskipun lokasi utama tidak tersedia.

Penting
Data yang direplikasi membutuhkan ruang penyimpanan yang sama dengan data asli.

Mengaktifkan dan menonaktifkan penyimpanan geo-redundan

Prasyarat

- Penyimpanan geo-redundan tersedia di konsol Cyber Protect hanya setelah administrator mitra mengaktifkannya di portal Manajemen atau melalui API.
- Hanya administrator yang dapat mengaktifkan atau menonaktifkan penyimpanan geo-redundan di konsol Cyber Protect. Pastikan Anda memiliki hak administrator.

Untuk mengaktifkan penyimpanan geo-redundan

1. [Hanya jika penyimpanan geo-redundansi diaktifkan melalui API] Pada peringatan di atas "Geo-redundansi tersedia untuk semua data Anda di awan", klik **Aktifkan Penyimpanan Cloud Geo-redundan**.
2. Di konsol Cyber Protect, buka **Pengaturan** > **Pengaturan sistem**.
3. Gulir daftar opsi pencadangan default, lalu klik **Penyimpanan Cloud Geo-redundan**.
4. Aktifkan tombol **Penyimpanan Cloud Geo-redundan**.
5. Klik **Simpan**.

© Acronis International GmbH, 2003-2024

Kini, data Anda akan direplikasi ke lokasi sekunder dan akan tetap tersedia meskipun lokasi utama gagal.

Untuk menonaktifkan penyimpanan geo-redundan

Peringatan!
Data yang direplikasi akan dihapus dalam waktu satu hari setelah Anda menonaktifkan redundansi geografis.

1. Di konsol Cyber Protect, buka **Pengaturan** > **Pengaturan sistem**.
2. Gulir daftar opsi pencadangan, lalu klik **Penyimpanan Cloud Geo-redundan**.
3. Nonaktifkan tombol **Penyimpanan Cloud Geo-redundan**.
4. Konfirmasikan pilihan Anda dengan mengetik **Nonaktifkan**, lalu klik **Nonaktifkan**.

Status Geo-replikasi

Redundansi geografis menyiratkan bahwa data direplikasi ke lokasi sekunder. Status geo-replikasi menunjukkan tahap proses ini. Status berikut mungkin terjadi:

- **Telah Disinkronisasi**—Data telah direplikasi ke lokasi sekunder.
- **Sinkronisasi**—Data sedang direplikasi ke lokasi sekunder. Durasi operasi ini bergantung pada ukuran data.
- **Ditunda**—Replikasi data ditangguhkan untuk sementara.
- **Dinonaktifkan**—Replikasi data dinonaktifkan.

Untuk memeriksa status replikasi di konsol Cyber Protect

1. Di konsol Cyber Protect, buka **Penyimpanan cadangan**.
2. Pilih lokasi dan set cadangan.
3. Klik **Detail**, lalu periksa status di **Status replikasi geografis**.

Pembatasan

- Saat ini, lokasi sekunder untuk data yang direplikasi hanya tersedia di Amerika Serikat dan Kanada.
- Untuk informasi tentang batasan layanan Pemulihan Bencana saat menggunakan redundansi geografis, lihat dokumentasi Pemulihan Bencana.

© Acronis International GmbH, 2003-2024

Glosarium

A

Agen pencegah hilangnya data

Komponen klien dari sistem pencegah hilangnya data yang melindungi komputer host dari penggunaan tanpa izin, transmisi, dan penyimpanan data rahasia, terlindungi, atau sensitif dengan menerapkan kombinasi teknik analisis konteks dan konten, serta menegakkan kebijakan pencegah hilangnya data yang dikelola secara terpusat. Perlindungan cyber menyediakan agen pencegah hilangnya data berfitur lengkap. Akan tetapi, fungsionalitas agen pada komputer terlindungi terbatas pada set fitur pencegah hilangnya data yang tersedia untuk pelisensian dalam Perlindungan cyber, dan bergantung pada rencana proteksi yang berlaku pada komputer tersebut.

Agen perlindungan

Agen perlindungan adalah agen yang akan diinstal pada mesin untuk perlindungan data.

Alamat IP publik

[Pemulihan Bencana] Alamat IP yang diperlukan untuk menyediakan server awan dari Internet.

Alat VPN

[Pemulihan Bencana] Mesin virtual khusus yang memungkinkan koneksi antara jaringan lokal dan situs awan melalui terowongan VPN yang aman. Alat VPN disebarkan di situs lokal.

C

Cadangan bertambah bertahap

Cadangan yang menyimpan perubahan data terhadap cadangan terbaru. Anda membutuhkan akses ke cadangan lain untuk memulihkan data dari cadangan inkremental.

Cadangan diferensial

Cadangan diferensial menyimpan perubahan data terhadap cadangan penuh terbaru. Anda membutuhkan akses ke cadangan penuh yang dimaksud untuk memulihkan data dari cadangan diferensial.

Cadangan penuh

Cadangan diri berisi semua data yang dipilih untuk dicadangkan. Anda tidak membutuhkan akses ke cadangan lain untuk memulihkan data dari cadangan penuh.

Cadangan tanpa induk

Cadangan tanpa induk adalah cadangan yang tidak terkait dengan rencana proteksi lagi.

D

Database perangkat USB

[Kontrol perangkat] Modul kontrol perangkat menyimpan database perangkat USB yang menjadi sumber penambahan ke daftar pengecualian dari kontrol akses perangkat. Basis data mendaftarkan perangkat USB berdasarkan ID perangkat, yang dapat dimasukkan dengan tangan atau dipilih dari perangkat yang dikenal di konsol Cyber Protect.

© Acronis International GmbH, 2003-2024

F

Failback

Mengalihkan beban kerja dari server cadangan (seperti replika mesin virtual atau server pemulihan yang berjalan di awan) kembali ke server produksi.

Failover

Mengalihkan beban kerja dari server produksi ke server cadangan (seperti replika mesin virtual atau server pemulihan yang berjalan di awan).

Finalisasi

Operasi yang mengubah mesin virtual sementara yang berjalan dari cadangan menjadi mesin virtual permanen. Secara fisik, ini berarti memulihkan semua disk mesin virtual, beserta semua perubahan yang terjadi saat mesin sedang berjalan, ke penyimpanan data yang menyimpan perubahan tersebut.

Format cadangan file tunggal

Format cadangan, di mana cadangan penuh awal dan bertahap selanjutnya akan disimpan ke file .tibx tunggal. Format ini memanfaatkan kecepatan metode pencadangan inkremental, sekaligus menghindari kekurangan utamanya, yaitu kesulitan menghapus cadangan yang lama. Perangkat lunak menandai blok yang digunakan oleh cadangan lama sebagai "kosong" dan menulis cadangan baru ke blok ini. Format ini menghasilkan pembersihan yang sangat cepat, dengan sedikit pemakaian sumber daya. Format cadangan file tunggal tidak tersedia saat mencadangkan ke lokasi yang tidak mendukung akses-acak baca dan tulis.

G

Gateway VPN (sebelumnya, server VPN atau gateway konektivitas)

[Pemulihan Bencana] Mesin virtual khusus yang menyediakan koneksi antara jaringan situs lokal dan situs awan melalui terowongan VPN yang aman. Gateway VPN disebarkan di situs awan.

J

Jaringan produksi

[Pemulihan Bencana] Jaringan internal yang diperluas menggunakan terowongan VPN dan mencakup situs lokal dan awan. Server lokal dan server awan dapat berkomunikasi dalam jaringan produksi.

Jaringan uji

[Pemulihan Bencana] Jaringan virtual terisolasi yang digunakan untuk menguji proses failover.

K

Koneksi situs-ke-situs (S2S)

[Pemulihan Bencana] Koneksi yang memperluas jaringan lokal ke awan, melalui terowongan VPN yang aman.

Koneksi titik-ke-situs (P2S)

[Pemulihan Bencana] Suatu koneksi VPN aman dari luar ke situs awan dan lokal menggunakan perangkat titik akhir Anda (seperti komputer atau laptop).

© Acronis International GmbH, 2003-2024

M

Mesin fisik

Mesin yang dicadangkan oleh agen yang diinstal di sistem operasi.

Mesin virtual

Mesin virtual yang dicadangkan di level hypervisor oleh agen eksternal seperti Agen untuk VMware atau Agen untuk Hyper-V. Mesin virtual dengan agen di dalamnya diperlakukan sebagai fisik dari sudut pencadangan.

Modul

Modul adalah bagian dari rencana proteksi yang menyediakan fungsi perlindungan data tertentu, misalnya modul pencadangan, modul perlindungan Antivirus & Antimalware, dan sebagainya.

Modul kontrol perangkat

Sebagai bagian dari rencana proteksi, modul kontrol perangkat memanfaatkan subset fungsional dari agen pencegah hilangnya data pada tiap komputer terlindungi demi mendeteksi, dan mencegah akses dan transmisi data tanpa izin melalui saluran komputer lokal. Hal ini mencakup akses pengguna ke perangkat periferal dan port, pencetakan dokumen, operasi salin/tempel papan klip, operasi format dan keluarkan media, maupun sinkronisasi dengan perangkat bergerak yang terhubung di lokasi terkait. Modul kontrol perangkat menyediakan kendali granural dan kontekstual pada tipe perangkat dan port yang dapat diakses pengguna di komputer terlindungi dan tindakan yang dapat dilakukan pengguna ke perangkat tersebut.

P

Pencegah hilangnya data (sebelumnya, pencegah kebocoran data)

Sistem teknologi terintegrasi dan prosedur organisasi yang bertujuan untuk mendeteksi dan mencegah penyingkapan/akses secara sengaja atau tidak ke data rahasia, terlindungi, atau sensitif yang dilakukan oleh entitas tanpa izin di luar atau dalam organisasi, atau pengiriman data tersebut ke lingkungan yang tidak tepercaya.

R

Rencana proteksi

Rencana proteksi adalah rencana yang menggabungkan modul Perlindungan Data, termasuk Cadangan, proteksi Antivirus & Antimalware, pemfilteran URL, Antivirus Windows Defender, Microsoft Security Essentials, penilaian Kerentanan, manajemen Patch, peta Perlindungan Data, kontrol Perangkat.

Runbook

[Pemulihan Bencana] Rencana skenario berisi langkah-langkah yang dapat dikonfigurasi yang mengotomatisasi tindakan pemulihan bencana.

S

Server awan

[Pemulihan Bencana] Referensi umum ke server pemulihan atau utama.

Server pemulihan

[Pemulihan Bencana] Replika VM dari mesin asli, berdasarkan cadangan server terlindungi

© Acronis International GmbH, 2003-2024

yang disimpan di awan. Server pemulihan digunakan untuk mengalihkan beban kerja dari server asli, jika terjadi bencana.

Server utama

[Pemulihan Bencana] Mesin virtual yang tidak memiliki mesin yang tertaut di situs lokal (seperti server pemulihan). Server utama digunakan untuk melindungi aplikasi atau menjalankan berbagai layanan tambahan (seperti server web).

Set cadangan

Sekelompok cadangan yang untuknya aturan retensi individual dapat diterapkan. Untuk skema pencadangan Kustom, set cadangan sesuai dengan metode pencadangan (Penuh, Diferensial, dan Inkremental). Pada kasus lain, set cadangan adalah Bulanan, Harian, Mingguan, dan Per jam. Cadangan bulanan adalah cadangan yang pertama dibuat pada awal suatu bulan. Pencadangan mingguan adalah cadangan yang pertama dibuat pada hari yang dipilih pada opsi Pencadangan mingguanguan (klik ikon roda gigi, lalu Opsi cadangan > Pencadangan mingguan). Jika cadangan mingguan adalah cadangan pertama yang dibuat pada awal suatu bulan, cadangan ini dianggap sebagai cadangan bulanan. Dalam hal ini, cadangan mingguan akan dibuat pada hari yang dipilih minggu berikutnya. Cadangan harian adalah cadangan yang dibuat pada awal suatu hari, kecuali jika pencadangan gagal dalam pencadangan bulanan atau mingguan. Cadangan per jam adalah cadangan yang pertama dibuat pada awal suatu jam, kecuali jika pencadangan gagal dalam pencadangan bulanan, mingguan, atau harian.

Situs awan (atau situs DR)

[Pemulihan Bencana] Situs jarak jauh yang di-host di awan dan digunakan untuk menjalankan infrastruktur pemulihan, jika terjadi bencana.

Situs lokal

[Pemulihan Bencana] Infrastruktur lokal yang disebarkan di lokasi perusahaan Anda.

T

Tujuan titik pemulihan (RPO)

[Pemulihan Bencana] Jumlah data yang hilang akibat penonaktifan, dihitung sebagai jumlah waktu dari rencana penonaktifan atau peristiwa bencana. Ambang batas RPO menjelaskan interval waktu maksimum yang diperbolehkan antara titik pemulihan terakhir yang tepat untuk failover dan waktu terkini.

U

Uji alamat IP

[Pemulihan Bencana] Alamat IP yang diperlukan jika terjadi failover uji, untuk mencegah duplikasi alamat IP produksi.

V

Validasi

Operasi yang memeriksa kemungkinan pemulihan data dari cadangan. Validasi cadangan file akan meniru pemulihan semua file dari carangan ke tujuan dummy. Validasi cadangan disk akan menghitung checksum untuk tiap blok data yang tersimpan di cadangan. Kedua prosedur bersifat intensif sumber daya. Meskipun keberhasilan validasi menandakan tingginya kemungkinan

© Acronis International GmbH, 2003-2024

keberhasilan pemulihan, proses validasi tidak memeriksa semua faktor yang memengaruhi proses pemulihan.

© Acronis International GmbH, 2003-2024

Indeks

3

32-bit atau 64-bit? 708

A

Abaikan penulis VSS yang gagal 491

Abaikan sektor buruk 459

Active Protection 820

Active Protection di Cyber Backup edisi Standard 835

Advanced Data Loss Prevention 864

Agen cloud dan agen lokal 596

Agen mana yang saya perlukan? 61

Agen untuk Advanced Data Loss Prevention 25

Agen untuk Exchange (untuk pencadangan kotak surat) 26

Agen untuk File Sync & Share 25

Agen untuk Hyper-V 29

Agen untuk Linux 27

Agen untuk Mac 28

Agen untuk Microsoft 365 26

Agen untuk MySQL/MariaDB 27

Agen untuk Oracle 27

Agen untuk oVirt 30

Agen untuk oVirt - peran dan port yang diperlukan 157

Agen untuk Pencegahan Kebocoran Data 25

Agen untuk Scale Computing HC3 29

Agen untuk Scale Computing HC3 – peran yang diperlukan 143

Agen untuk SQL, Agen untuk Active Directory, Agen untuk Exchange (untuk cadangan database dan cadangan keberadaan aplikasi) 25

Agen untuk Synology 30

Agen untuk Virtuozzo 29

Agen untuk Virtuozzo Hybrid Infrastructure 29

Agen untuk VMware - pencadangan tanpa LAN 686

Agen untuk VMware – hak istimewa yang diperlukan 696

Agen untuk VMware (Virtual Appliance) 29

Agen untuk VMware (Windows) 29

Agen untuk Windows 23

Akses situs web berbahaya 845

Akses VPN jarak jauh titik-ke-situs 749

Akses VPN ke situs lokal 770

Aktifkan atau nonaktifkan kontrol perangkat 365

Aktifkan atau nonaktifkan notifikasi OS dan peringatan layanan. 369

Aktifkan cadangan penuh VSS 492

Alamat IP publik dan uji 745

Alasan Anda memerlukan Deteksi dan Tanggapan Titik Akhir (EDR) 892

Alat bantu "tibxread" untuk mendapatkan data yang dicadangkan 466

Alat bantu Cyber Protection tambahan 1083

Alat VPN 744

Algoritme distribusi 690

Alur kerja konfigurasi pemfilteran URL 845

Alur kerja manajemen patch 959

© Acronis International GmbH, 2003-2024

Amazon 41

Analisis detail insiden 903

Antimalware Tingkat Lanjut 820

Apa definisi perlindungan Google Workspace? 638

Apa itu file cadangan? 450

Apa itu insiden? 898

Apa itu kemacetan? 534

Apa manfaat penyimpanan cadangan disk atau volume? 402

Apa saja item yang dapat dicadangkan? 592, 603, 609, 619, 623, 627, 646, 650, 654, 672

Apa saja item yang dapat dipulihkan? 592, 603, 609, 619, 624, 628, 647, 650, 655

Apa saja item yang tidak dapat dipulihkan? 625

Apa yang akan direplikasi 199

Apa yang dapat Anda cadangkan 589

Apa yang dipindai 953

Apa yang memicu aturan kebijakan? 868

Apa yang perlu Anda ketahui 589

Apa yang perlu Anda ketahui tentang konversi 210

Apa yang saya perlukan untuk mencadangkan situs web? 672

Apa yang saya perlukan untuk menggunakan pencadangan keberadaan aplikasi? 567

Apakah paket yang diperlukan sudah diinstal? 68

Aplikasi awan 298

Aturan firewall untuk server awan 802

Aturan instalasi umum 42

Aturan kebijakan untuk disk dan volume 403

Aturan kebijakan untuk file dan folder 406

Aturan pencadangan umum 42

Aturan pengecualian dan ekstensi 308

Aturan retensi 434

Aturan retensi sesuai dengan skema pencadangan 435

Autentikasi dua faktor 19

B

Bagaimana cara kerjanya? 889

Bagaimana cara mendapatkan data forensik dari cadangan? 464

Bagaimana cara mengurangi kemacetan 535

Bagaimana file masuk ke folder karantina? 856

Bagaimana pembuatan Secure Zone mengubah disk 415

Bahasa yang didukung 878-879, 882-883

Baru-baru ini terdampak 297

Batalkan rencana dari grup 362

Batasan untuk memulihkan file di konsol Cyber Protect 516

Batasan untuk nama file cadangan 451

Beban kerja 328

Beban kerja CyberApp 390

Beban kerja terakumulasi 391

Bekerja dengan beban kerja CyberApp 391

Bekerja dengan beban kerja terkelola 1008

Bekerja dengan beban kerja tidak terkelola 1017

Bekerja dengan beban kerja yang terkumpul 392

Bekerja dengan cadangan yang dienkripsi 797

© Acronis International GmbH, 2003-2024

Bekerja dengan fitur proteksi Tingkat Lanjut 862

Bekerja dengan log 771

Bekerja dengan modul kontrol Perangkat 362

Bekerja di VMware vSphere 680

Berapa banyak agen yang diperlukan untuk pencadangan dan pemulihan data klaster? 564

Berapa banyak agen yang diperlukan untuk pencadangan dan pemulihan keberadaan-klaster? 566

Berapa jumlah agen yang saya perlukan? 135, 139, 145, 153

Berbagi Layar Apple 990

Berbasis Linux 706

Berbasis WinPE/WinRE 706

Browser web yang didukung 23

Buat kembali konfigurasi 770

Burndown insiden keamanan 287

C

Cadangan 56, 395

Cadangan database 561

Cadangan inkremental/diferensial cepat 459

Cadangan keberadaan aplikasi 567

Cara kerja autodiscovery 124

Cara kerja failback 787

Cara kerja failover 779

Cara kerja instalasi jarak jauh agen 126

Cara kerja konversi reguler ke mesin virtual 212

Cara kerja perutean 741, 744, 749

Cara kerjanya 228, 290, 302, 305, 408, 444, 465, 658, 835, 843

Cara membuat Secure Zone 415

Cara memulai pencadangan data Anda 590

Cara memulihkan data ke perangkat seluler 590

Cara menavigasi tahapan serangan 911

Cara menetapkan hak pengguna 85

Cara menganalisis insiden keamanan yang membutuhkan perhatian segera 899

Cara menggunakan Deteksi dan Tanggapan Titik Akhir (EDR) 897

Cara menggunakan notarisasi 444, 658

Cara menggunakan Secure Zone 42

Cara menghapus Secure Zone 416

Cara menginvestigasi insiden di rantai cyber kill 906

Cara menguji apakah Deteksi dan Tanggapan Titik Akhir (EDR) bekerja dengan baik 948

Cara meninjau data melalui konsol Cyber Protect 591

Cara menjalankan failover server DHCP 786

Cara menjalankan failover server menggunakan DNS lokal 786

Cari atribut untuk beban kerja awan-ke-awan 345

Cari atribut untuk beban kerja non-awan-ke-awan 346

Catatan untuk pengguna Mac 497

Cek akses ke driver pada lingkungan yang dapat di-boot 508

Cek alamat IP perangkat 431

Citra WinPE 717

Citra WinRE 717

© Acronis International GmbH, 2003-2024

Citrix 37

Coba lagi, jika eror terjadi 458, 521

Coba lagi, jika kesalahan terjadi selama pembuatan snapshot VM 459

Codec Adaptif 989

Contoh 87-89, 97-98, 109, 111, 146-148, 427-432, 437

Cadangan darurat jika terjadi blok buruk pada hard disk 425

Menginstal paket secara manual di Fedora 14 71

Contoh penggunaan 439, 676, 680, 692

D

Daftar izin jenis perangkat 378

Daftar izin perangkat USB 379

Daftar perangkat USB di komputer 383

Daftar putih perusahaan 858

daftarkan cadangan 467

daftarkan konten 468

Dalam 599

Dalam Cyber Protection 639

dapatkan konten 469

Dasbor Aktivitas 260

Dasbor Ikhtisar 259

Dasbor Peringatan 261

Data forensik 462

Data yang dianggap Informasi Identitas Pribadi (PII) 880

Data yang dianggap Informasi Kesehatan yang Dilindungi 878

Data yang dianggap PCI DSS 882

Data yang dilaporkan berdasarkan tipe widget 315

Database perangkat USB 381

Deduplikasi dalam arsip 455

Deduplikasi Data 56

Definisi data sensitif 878

Deskripsi 852

Deskripsi opsi 470

Detail pemindaian cadangan 297

Deteksi dan Tanggapan Titik Akhir (EDR) 892

Deteksi dengan taktik 287

Deteksi proses cryptomining 823

Deteksi tujuan mandiri 877

Di Google Workspace 639

Di mana saya dapat melihat nama file cadangan? 451

Di Microsoft 365 599

Diperlukan hak istimewa untuk akun masuk 84

Distribusi Insiden Teratas per beban kerja 285

Ditandai sebagai Rahasia 882

Driver penyimpanan massal akan tetap diinstal 509

Dukungan beberapa penyewaan 327

Dukungan untuk migrasi mesin virtual 693

E

Ekspresi logika untuk Bahasa Jepang 881

Ekspresi logika untuk semua bahasa yang didukung kecuali Bahasa Jepang 881

Ekspresi logika yang digunakan untuk deteksi konten 879, 881-882

Enkripsi 441

© Acronis International GmbH, 2003-2024

F

Failback 684

Failback ke mesin fisik target 792

Failback ke target mesin virtual 788

Failover pada replika 683

Failover Pemulihan Bencana 937

Failover produksi 779

Failover uji otomatis 780, 782

File log VPN IPSec Multi-situs 776

File skrip 712

Filter file (Penyertaan/Pengecualian) 460

Filter penyertaan dan pengecualian 460

Finalisasi mesin 678

Finalisasi mesin berjalan dari cadangan awan 679

Finalisasi vs. pemulihan reguler 679

Fitur 893

Fitur antimalware 818

Fitur desktop dan bantuan jarak jauh yang didukung 986

Fitur perlindungan yang didukung oleh sistem operasi 44

Fitur yang didukung per platform 815

Fitur yang tidak didukung 1083

Flashback 522

Folder kustom layanan mandiri sesuai permintaan 858

Format cadangan 454

Format cadangan dan file cadangan 454

Fungsi utama 730

G

Gateway VPN 744, 749

Grup awan-ke-awan dan grup non-awan-ke-awan 340

Grup bawaan 338

Grup bawaan dan grup khusus 338

Grup dinamis 339

Grup kata kunci 883

Grup kustom 339

Grup perangkat 338

Grup statis 339

Grup statis dan grup dinamis 339

H

H.264 989

Hak pengguna yang diperlukan 571, 599, 639

Hak pengguna yang diperlukan untuk pencadangan keberadaan aplikasi 568

Halaman manajemen database perangkat USB 381

Hemat daya baterai 429

hitung hash 469

Host lokasi cadangan tersedia 428

I

Ikhtisar klaster Exchange Server 565

Ikhtisar solusi ketersediaan tinggi SQL Server 563

Ikhtisar tentang proses pengiriman data fisik 482

Indeks pencarian 660

© Acronis International GmbH, 2003-2024

Informasi apa yang termasuk dalam tahap serangan? 911

Informasi Identitas Pribadi (PII) 879

Informasi Kesehatan yang Dilindungi (PHI) 878

Informasi untuk administrator mitra 334

Infrastruktur jaringan awan 739

Instalasi 78

Instalasi atau penghapusan instalasi tanpa pengawasan 86

Instalasi atau penghapusan instalasi tanpa pengawasan di Windows 86

Instalasi atau penghapusan tanpa pengawasan di Linux 104

Instalasi dan penghapusan instalasi tanpa pengawasan dengan file EXE 86

Instalasi dan penghapusan instalasi tanpa pengawasan dengan file MSI 94

Instalasi dan penghapusan instalasi tanpa pengawasan di macOS 110

Instalasi dinamis dan penghapusan instalasi komponen 85

Integrasi untuk DirectAdmin, cPanel, dan Plesk 675

Interaksi dengan opsi pencadangan lainnya 486

Inventaris perangkat keras 978

Inventaris perangkat lunak 974

Investigasi simpul individu di rantai cyber kill 913

Investigasi tahapan serangan insiden 909

Izin 870

Izin kebijakan 547-548

Izin yang diperlukan untuk instalasi tanpa pengawasan di macOS 112

J

Jadwal 250, 306, 954, 962

Jadwal dan syarat mulai 250

Jadwal pencadangan 417

Jadwalkan berdasarkan event 423

Jadwalkan berdasarkan waktu 420

Jadwalkan pemindaian 828, 853

Jalankan cepat skrip 256

Jalankan pencadangan forensik pada beban kerja sesuai permintaan 934

Jalankan sebagai mesin virtual 205

Jangan dimulai ketika memakai koneksi bermeter 430

Jangan dimulai ketika terkoneksi ke jaringan Wi-Fi berikut 431

Jangan menampilkan pesan dan dialog saat memproses (mode diam) 459, 522

Jendela pencadangan 479

Jenis cadangan 419

Jenis cadangan apa yang saya perlukan? 65

Jenis kontrol 715

Jenis mesin virtual yang didukung 210

Jenis pemantauan 1027

Jenis pemindaian 818

Jenis peringatan 262

Jika Anda memilih untuk membuat mesin virtual di server virtualisasi 212

Jika Anda memilih untuk menyimpan mesin virtual sebagai set file 212

K

Karantina 824, 856

© Acronis International GmbH, 2003-2024

Kasus penggunaan untuk persetujuan dan pengujian patch otomatis 968

Kasus penggunaan untuk persetujuan patch otomatis tanpa pengujian 971

Kata sandi dengan karakter spesial atau spasi kosong 122

Kategori sensitivitas kustom 886

Kategori yang akan difilter 845

Keamanan 990

Keamanan tingkat file 522

Kecepatan output selama pencadangan 482

Kecualikan maisng-masing perangkat USB dari kontrol akses 369

Kecualikan subklas perangkat dari kontrol akses 369

Kegagalan manual 796

Kelas penyimpanan yang didukung 547

Kelola insiden Anda di halaman Insiden 894

Kerentanan yang ada 295

Kesesuaian Pemulihan Bencana dengan perangkat lunak enkripsi 734

Keterbatasan saat menggunakan Penyimpanan Cloud Geo-redundan 734

Ketersediaan opsi pemulihan 518

Ketersediaan opsi pencadangan 445

Ketersediaan Tinggi mesin yang dipulihkan 699

Kiat penting 435

Kompatibilitas dengan penyimpanan Dell EMC Data Domain 43

Kompatibilitas dengan perangkat lunak enkripsi 42

Kompatibilitas format cadangan lintas berbagai versi produk 455

Komponen untuk instalasi tanpa pengawasan (EXE) 94

Komponen untuk instalasi tanpa pengawasan (MSI) 102

Koneksi jarak jauh ke beban kerja 936

Koneksi ke beban kerja jarak jauh untuk desktop jarak jauh atau bantuan jarak jauh 991

Koneksi lokal 722

Koneksi SSH ke alat virtual 172

Koneksi titik-ke-situs aktif 770

Koneksi VPN IPsec Multi-situs 748

Koneksi VPN Terbuka Situs-ke-situs 742, 760

Konfigurasi jaringan gateway VPN 744

Konfigurasi klaster yang didukung 563, 565

Konfigurasi konektivitas awal 751

Konfigurasi ulang alamat IP 762

Konflik antara rencana baru dan yang ada 220

Konflik antara rencana individu dan grup 220

Konsep pengaturan jaringan 740

Konsol Cyber Protect 318

Konsolidasi cadangan 449

Konversi ke mesin virtual 209

Konversi reguler ke mesin virtual vs. menjalankan mesin virtual dari cadangan 211

Kredensial beban kerja 1006

Kriteria filter 461

Kunci akses 548-549

Kuota 675

L

Langkah 1 58

© Acronis International GmbH, 2003-2024

Langkah 2 58

Langkah 3 58

Langkah 4 58

Langkah 5 59

Langkah 6 60

Laporan 311

Laporan pelisensian kursi Microsoft 365 600

Layanan Cyber Protection yang diinstal di lingkungan Anda 185

Layanan Menyalin Bayangan Volume (VSS) 491

Layanan Menyalin Bayangan Volume (VSS) untuk mesin virtual 493

Layanan Menyalin Bayangan Volume VSS untuk mesin virtual 685

Layanan yang diinstal di macOS 186

Layanan yang diinstal di Windows 185

Level (Semua pelanggan) penyewa mitra 320

Level penyewa pelanggan 320

Lewati eksekusi tugas 491

Lihat atau ubah pengaturan akses 368

Lihat peringatan kontrol perangkat 372

Linux 403

Log event Windows 495, 526

Lokasi karantina di mesin 857

Lokasi yang didukung 200-201, 208, 440

M

Mac 403

Manajemen daya VM 526, 685

Manajemen firewall 855

Manajemen jaringan 760

Manajemen lisensi untuk server manajemen di lokasi 194

Manajemen patch 959

Masalah dan batasan yang diketahui 891

Masalah kompatibilitas dengan rencana manajemen jarak jauh 1004

Masalah kompatibilitas dengan rencana pemantauan 1069

Masalah kompatibilitas dengan rencana skrip 255

Masalah lisensi 220

Masalah yang diketahui 666

Matikan daya mesin virtual ketika memulai pemulihan 526

McAfee Endpoint Encryption dan PGP Whole Disk Encryption 43

Media yang dapat di-boot berbasis Linux 708

Media yang dapat di-boot berbasis Linux atau WinPE/WinRE? 706

Media yang dapat di-boot berbasis WinPE dan WinRE 717

Media yang dapat di-boot kustom atau siap pakai? 705

Mekanisme penilaian #CyberFit 228

Melakukan autodiscovery dan manual discovery 127

Melakukan autodiscovery mesin pada level penyewa mitra 324

Melakukan failback ke mesin fisik 794

Melakukan failback ke mesin virtual 789

Melakukan failback manual 796

Melakukan failover 784

Melakukan failover permanen 683

Melakukan instalasi ulang gateway VPN 764

© Acronis International GmbH, 2003-2024

Melakukan konfigurasi pada mode hanya-Awan 751

Melakukan konfigurasi pada server DNS kustom 767

Melakukan tindakan kontrol pada beban kerja terkelola 1014

Melihat beban kerja pelanggan tertentu 322

Melihat daftar patch yang tersedia 965

Melihat dan memperbarui lokasi cadangan cloud publik 545

Melihat data monitor 1080

Melihat detail kemacetan 536

Melihat detail tentang item dalam daftar putih 860

Melihat insiden mana yang saat ini tidak dimitigasi 901

Melihat log peringatan dari peringatan pemantauan 1078

Melihat peringatan monitoring untuk beban kerja 1078

Melihat riwayat distribusi 691

Melihat riwayat eksekusi 812

Melihat status failover uji otomatis 783

Melindungi akun apl kolaborasi Microsoft 365 638

Melindungi Always On Availability Group (AAG) 563

Melindungi aplikasi Microsoft 557

Melindungi buku catatan OneNote 637

Melindungi data Exchange Online 609

Melindungi data Exchange yang Dihosting 592

Melindungi data Gmail 646

Melindungi data Google Workspace 638

Melindungi data Microsoft 365 596

Melindungi data MySQL dan MariaDB 665

Melindungi Database Availability Group (DAG) 565

Melindungi Database Oracle 664

Melindungi file drive Shared 654

Melindungi file Google Drive 650

Melindungi file OneDrive 619

Melindungi kotak surat Exchange Online 603

Melindungi Microsoft SharePoint 557

Melindungi Microsoft SQL Server dan Microsoft Exchange Server 557

Melindungi pengontrol domain 558

Melindungi perangkat seluler 588

Melindungi server hosting web 675

Melindungi situs SharePoint Online 623

Melindungi situs web 671

Melindungi situs web dan server hosting 671

Melindungi Tim Microsoft 365 627

Memahami dan menyesuaikan tampilan rantai cyber kill 908

Memahami deteksi kemacetan 534

Memahami ruang lingkup dan dampak insiden 902

Memahami tindakan yang diambil untuk memitigasi insiden 914

Memahami tingkat proteksi Anda saat ini 259

Memasang database Server Exchange 581

Membandingkan versi skrip 246

Membatalkan penetapan kredensial dari beban kerja 1008

Membatalkan rencana pemantauan 1064

Membatasi jumlah total mesin virtual yang dicadangkan secara simultan 699

© Acronis International GmbH, 2003-2024

Memberikan izin sistem yang diperlukan kepada Connect Agent 82

Membuat cadangan dalam arsip cadangan yang sudah ada 453

Membuat file transformasi dan mengekstrak paket instalasi 170

Membuat grup dinamis 342

Membuat grup perangkat dinamis pada level mitra 323

Membuat grup perangkat statis pada level mitra 323

Membuat grup statis 340

Membuat kebijakan alur data dan aturan kebijakan 864

Membuat kloning skrip 243

Membuat media fisik yang dapat di-boot 706

Membuat media WinPE atau WinRE yang dapat di-boot 718

Membuat media yang dapat di-boot untuk memulihkan sistem operasi 705

Membuat proyek Google Cloud pribadi. 641

Membuat rencana manajemen jarak jauh 993

Membuat rencana pemantauan 1061

Membuat rencana proteksi 214

Membuat rencana proteksi pemulihan bencana 736

Membuat rencana replikasi 681

Membuat rencana replikasi cadangan 198

Membuat rencana skrip 248

Membuat rencana validasi 202

Membuat runbook 807

Membuat server pemulihan 776

Membuat server utama 799

Membuat skrip 238

Membuat skrip dengan menggunakan AI (ScriptPilot) 240

Membuat snapshot LVM 471

Membuat token pendaftaran 167

Memecahkan masalah kompatibilitas dengan rencana skrip 255

Memecahkan masalah konfigurasi VPN IPsec 773

Memeriksa aktivitas firewall awan 806

Memeriksa status validasi cadangan 207

Memeriksa ukuran indeks pencarian 661

Memilih data Exchange Server 562

Memilih data SharePoint Online 625

Memilih data yang akan dicadangkan 400

Memilih database SQL 561

Memilih disk atau volume 401

Memilih file atau folder 404

Memilih file drive Shared 655

Memilih file Google Drive 651

Memilih file OneDrive 620

Memilih folder umum 611

Memilih keseluruhan mesin 400

Memilih komponen untuk instalasi 131

Memilih konfigurasi ESXi 407

Memilih kotak surat 610

Memilih kotak surat Exchange Online 593

Memilih kotak surat Exchange Server 570

Memilih kotak surat Gmail 647

Memilih kotak surat Microsoft 365 604

Memilih status sistem 407

Memilih tim 628

© Acronis International GmbH, 2003-2024

Memilih tingkat penyewa 320

Memilih tujuan 412

Memperbarui agen 173

Memperbarui agen di beban kerja yang dilindungi BitLocker 178

Memperbarui agen secara manual 174

Memperbarui agen secara otomatis 176

Memperbarui Agen untuk Synology 164

Memperbarui akses ke koneksi cloud publik 555

Memperbarui akses ke langganan Microsoft Azure 551

Memperbarui definisi Cyber Protection sesuai jadwal 183

Memperbarui definisi Cyber Protection sesuai permintaan 183

Memperbarui kebijakan untuk perusahaan atau unit 872

Memperbarui kebijakan untuk salah satu atau lebih pengguna di dalam perusahaan atau unit 872

Memperbarui, membangun ulang, atau menghapus indeks 661

Mempersiapkan mesin untuk instalasi jarak jauh 130

Memprioritaskan insiden yang membutuhkan perhatian segera 899

Memulai dengan Cyber Protection 19

Memulai Secure Shell daemon 172

Memulai ulang model pembelajaran mesin 1071

Memulihkan aplikasi 558

Memulihkan beberapa file 510

Memulihkan buku catatan OneNote yang dicadangkan 637

Memulihkan cadangan untuk penyewa dalam mode Kepatuhan 1085

Memulihkan dari cadangan 936

Memulihkan data dari cadangan keberadaan aplikasi 667

Memulihkan data klaster Exchange 566

Memulihkan data SharePoint Online 626

Memulihkan database 669

Memulihkan database Exchange 579

Memulihkan database master 578

Memulihkan database sistem 578

Memulihkan database SQL 571

Memulihkan database SQL ke mesin non-orisinal 574

Memulihkan database SQL ke mesin orisinal 572

Memulihkan database SQL sebagai file 575

Memulihkan disk menggunakan media yang dapat di-boot 506

Memulihkan drive Shared dan file drive Shared 656

Memulihkan file di konsol Cyber Protect 510

Memulihkan file drive Shared 657

Memulihkan file Google Drive 653

Memulihkan file menggunakan media yang dapat di-boot 515

Memulihkan file OneDrive 622

Memulihkan folder umum dan item folder 618

Memulihkan Google Drive dan file Google Drive 652

Memulihkan instans 668

Memulihkan item kotak surat 585, 594, 604, 612, 649

© Acronis International GmbH, 2003-2024

Memulihkan item kotak surat ke file PST 616

Memulihkan item kotak surat tim ke file PST 633

Memulihkan keseluruhan drive Shared 656

Memulihkan keseluruhan Google Drive 652

Memulihkan keseluruhan OneDrive 621

Memulihkan keseluruhan tim 629

Memulihkan konfigurasi ESXi 517

Memulihkan kotak surat 583, 593, 604, 611, 648

Memulihkan kotak surat dan item kotak surat 593, 604, 611, 648

Memulihkan kotak surat Exchange dan item kotak surat 581

Memulihkan kotak surat tim 633

Memulihkan mesin 498

Memulihkan mesin dengan pemulihan Satu-klik 477

Memulihkan mesin fisik 498

Memulihkan mesin virtual 504

Memulihkan OneDrive dan file OneDrive 621

Memulihkan pesan email dan pertemuan 635

Memulihkan rutinitas yang disimpan 671

Memulihkan saluran atau file tim dalam saluran tim 630

Memulihkan seluruh kotak surat ke file data PST 614

Memulihkan seluruh server 668

Memulihkan situs tim atau item spesifik dalam suatu situs 636

Memulihkan situs web 674

Memulihkan status sistem 517

Memulihkan tabel 670

Memvalidasi cadangan 530

Memverifikasi keaslian file dengan Layanan Notaris 513, 659

Menambahkan akses ke koneksi cloud publik 553

Menambahkan akses ke langganan Microsoft Azure 550

Menambahkan beban kerja ke grup statis 342

Menambahkan beban kerja ke konsol Cyber Protect 329

Menambahkan beban kerja ke rencana manajemen jarak jauh 1000

Menambahkan beban kerja ke rencana pemantauan 1063

Menambahkan file yang dikarantina ke daftar putih 859

Menambahkan kredensial 1006

Menambahkan organisasi Google Workspace 640

Menambahkan organisasi Microsoft 365 601, 605

Menambahkan persyaratan untuk mesin virtual 569

Menambahkan VLAN 722

Menampilkan inventaris perangkat lunak dari satu perangkat 977

Menampilkan perangkat keras dari satu perangkat 982

Menampilkan status pencadangan di vSphere Client 695

Menandatangani file dengan ASign 513

Mencabut rencana proteksi 218

Mencadangkan beban kerja ke cloud publik 538

Mencadangkan data klaster Exchange 566

© Acronis International GmbH, 2003-2024

Mencadangkan database yang termasuk dalam AAG 564

Mencadangkan ke Amazon S3 546

Mencadangkan ke Microsoft Azure 546

Mencadangkan ke Wasabi 548

Mencadangkan mesin Hyper-V klaster 699

Mencadangkan server awan 806

Mencadangkan situs web 672

Mencegah penghapusan instalasi atau modifikasi agen yang tidak sah 178

Mendaftarkan dan membatalkan pendaftaran beban kerja secara manual 119

Mendaftarkan media yang dapat di-boot 720

Mendapatkan ID aplikasi dan rahasia aplikasi 601

Mendapatkan sertifikat untuk cadangan dengan data forensik 466

Mendefinisikan lokasi cadangan di Amazon S3 541

Mendefinisikan lokasi cadangan di Wasabi 543

Menentukan apa yang perlu dilindungi dan cara melindunginya 195

Menentukan lokasi cadangan di Microsoft Azure 538

Menentukan pengaturan umpan ancaman 918

Menentukan tindakan respons untuk proses yang mencurigakan 938

Menerapkan pemulihan bencana 730

Menerapkan rencana ke grup 361

Menerapkan rencana proteksi default 226

Menerapkan rencana proteksi pada beban kerja 216

Menetapkan aturan firewall untuk server awan 803

Menetapkan kembali alamat IP 766

Menetapkan kredensial ke beban kerja 1007

Menetapkan tindakan respons untuk entri registri yang mencurigakan 943

Mengakses alat virtual melalui klien SSH 173

Mengakses cadangan yang dihapus dalam penyimpanan yang tidak dapat diubah 1087

Mengakses layanan Cyber Protection 22

Mengaktifkan Advanced Data Loss Prevention di rencana proteksi 874

Mengaktifkan akun 19

Mengaktifkan atau menonaktifkan pencarian yang ditingkatkan dalam rencana yang ada 663

Mengaktifkan atau menonaktifkan rencana proteksi 219

Mengaktifkan dan menonaktifkan koneksi Situs-ke-situs 765

Mengaktifkan dan menonaktifkan manajemen firewall 856

Mengaktifkan dan menonaktifkan penyimpanan geo-redundan 1088

Mengaktifkan fungsionalitas Deteksi dan Tanggapan Titik Akhir (EDR) 895

Mengaktifkan mode monitoring untuk Endpoint Detection and Response (EDR) 946

Mengaktifkan pemindaian inventaris perangkat keras 979

Mengaktifkan pemindaian inventaris perangkat lunak 974

Mengaktifkan pemulihan Sekali klik 474

Mengaktifkan pencarian yang ditingkatkan dalam cadangan yang dienkripsi 662

© Acronis International GmbH, 2003-2024

Mengaktifkan penggunaan modul kontrol perangkat pada macOS 366

Mengaktifkan penyimpanan yang tidak dapat diubah 1086

Mengaktifkan Startup Recovery Manager 727

Mengalihkan jenis koneksi Situs-ke-situs 765

Mengalihkan suara dari beban kerja Linux jarak jauh 991

Mengalihkan suara dari beban kerja macOS jarak jauh 991

Mengalihkan suara dari beban kerja Windows jarak jauh 990

Mengamati beberapa beban kerja terkelola secara bersamaan 1016

Mengapa ada cadangan bulanan dengan skema per jam? 436

Mengapa menggunakan Pembangun Media yang Dapat Di-Boot? 707

Mengapa menggunakan pencadangan keberadaan aplikasi? 567

Mengapa menggunakan runbook? 807

Mengapa perlu mencadangkan data Microsoft 365? 596

Mengapa perlu menggunakan Secure Zone? 414

Mengatur frekuensi pencadangan Microsoft 365 608

Mengatur fungsi pemulihan bencana 736

Mengatur kata sandi enkripsi 1084

Mengatur kata sandi root pada alat virtual 172

Mengatur konektivitas 740

Mengatur mode tampilan 723

Mengatur server pemulihan 776

Mengatur server utama 798

Mengecualikan proses dari kontrol akses 384

Mengedit atau menghapus skrip 244

Mengedit grup dinamis 360

Mengedit Parameter default server pemulihan 738

Mengedit rencana proteksi 217

Mengedit rencana proteksi default 227

Mengeksekusi runbook 812

Mengekspor cadangan 531

Mengekstrak file dari pencadangan lokal 516

Mengekstrak file MSI, MST, dan CAB 95

Mengelola akses akun cloud publik 546

Mengelola akses ke langganan Microsoft Azure 549

Mengelola akses ke layanan penyimpanan cloud publik lainnya 553

Mengelola beban kerja di konsol Cyber Protect 318

Mengelola beban kerja target untuk rencana 252

Mengelola file yang dikarantina 857

Mengelola file yang tidak terlindungi yang terdeteksi 306

Mengelola inventaris perangkat keras dan perangkat lunak Anda 974

Mengelola isolasi jaringan dari beban kerja 928

Mengelola jaringan 760

Mengelola kerentanan yang ditemukan 957

Mengelola lingkungan virtualisasi 694

Mengelola mesin yang ditemukan 132

Mengelola pencadangan serta pemulihan beban kerja dan file 395

Mengelola pengaturan alat VPN 764

© Acronis International GmbH, 2003-2024

Mengelola pengaturan koneksi titik-ke-situs 769

Mengelola server awan 801

Mengembalikan ke disk RAM awal asli 510

Menggabungkan aturan kebijakan alur data 870

Mengganti port yang digunakan oleh agen proteksi 60

Menggunakan Agen untuk Office 365 yang diinstal secara lokal 601

Menggunakan konsol Cyber Protect sebagai administrator mitra 320

Menggunakan kontrol perangkat 365

Menggunakan mode Observasi untuk memperbarui kebijakan pengguna 872

Menggunakan Mode penerapan adaptif untuk memperbarui kebijakan pengguna 873

Menggunakan penyimpanan yang terpasang secara lokal 689

Menggunakan toolbar di jendela Penampil 1020

Menggunakan Universal Restore 507

Menggunakan variabel 453

Menggunakan versi awan Agen untuk Microsoft 365 605

Menghapus akses ke koneksi cloud publik 556

Menghapus akses ke langganan Microsoft Azure 552

Menghapus beban kerja dari konsol Cyber Protect 334

Menghapus beban kerja dari rencana manajemen jarak jauh 1001

Menghapus beberapa cadangan 532

Menghapus cadangan di luar Cyber Protect konsol 533

Menghapus grup 360

Menghapus instalasi agen 180

Menghapus kredensial 1007

Menghapus mesin 678

Menghapus organisasi Microsoft 365 607

Menghapus rencana proteksi 219

Menghapus semua peringatan 305

Menghapus Server DNS kustom 768

Menghentikan eksekusi runbook 812

Menghentikan failover 683

Menghubungkan ke beban kerja terkelola melalui klien web 1012

Menghubungkan ke beban kerja terkelola untuk desktop jarak jauh atau bantuan jarak jauh 1009

Menghubungkan ke beban kerja tidak terkelola melalui Acronis Bantuan Cepat 1018

Menghubungkan ke beban kerja untuk desktop jarak jauh atau bantuan jarak jauh 984

Menghubungkan ke beban kerja yang tidak terkelola melalui alamat IP 1019

Menghubungkan ke mesin yang di-boot dari media yang dapat di-boot 722

Menginstal agen and komponen (kombinasi MSI dan MST) 96

Menginstal agen proteksi 75

Menginstal agen proteksi di Linux 78

Menginstal agen proteksi di macOS 81

Menginstal agen proteksi di Windows 76

Menginstal Agen untuk Synology 160

Menginstal dan mencopot agen and komponen (EXE) 87

Menginstal dan mencopot agen and komponen (MSI dan pemilihan langsung) 96

© Acronis International GmbH, 2003-2024

Menginstal dan menyebarkan agen Cyber Protection 58

Menginstal paket dari repositori 69

Menginstal paket secara manual 70

Menginstal patch sesuai permintaan 972

Mengizinkan lalu lintas DHCP melalui L2 VPN 769

Mengonfigurasi akses VPN jarak jauh Titik-ke-situs 759

Mengonfigurasi akun pengguna di Virtuozzo Hybrid Infrastructure 146

Mengonfigurasi alat virtual 136, 141, 149, 155

Mengonfigurasi aturan retensi 438

Mengonfigurasi cadangan CDP 411

Mengonfigurasi cadangan keberadaan aplikasi 666

Mengonfigurasi enkripsi dalam rencana proteksi 441

Mengonfigurasi enkripsi sebagai properti mesin 442

Mengonfigurasi failover uji otomatis 783

Mengonfigurasi jaringan di Virtuozzo Hybrid Infrastructure 145

Mengonfigurasi jumlah percobaan ulang jika terjadi kesalahan 207

Mengonfigurasi kebijakan notifikasi email 1079

Mengonfigurasi koneksi VPN Terbuka Situs-ke-situs 751

Mengonfigurasi masa pakai patch dalam daftar 967

Mengonfigurasi pengaturan Hubungkan Klien 1023

Mengonfigurasi pengaturan jaringan 722

Mengonfigurasi pengaturan RDP 1009

Mengonfigurasi pengaturan server proxy 71

Mengonfigurasi pengaturan server proxy di Cyber Protect Monitor 311

Mengonfigurasi pengaturan VPN IPsec Multi-situs 753

Mengonfigurasi peringatan pemantauan 1072

Mengonfigurasi persetujuan patch otomatis 968

Mengonfigurasi perutean lokal 769

Mengonfigurasi proteksi antivirus dan antimalware Anda 814

Mengonfigurasi rencana proteksi pada proses patch Uji 969

Mengonfigurasi rencana proteksi patch Produksi 970

Mengonfigurasi tindakan respons otomatis 1064

Mengonfigurasi VPN IPsec Multi-situs 753

Mengonfigurasi VPN Terbuka Situs-ke-situs 751

Mengubah akun masuk pada mesin Windows 84

Mengubah batas waktu untuk heartbeat VM dan validasi tangkapan layar 206

Mengubah format cadangan ke versi 12 (TIBX) 455

Mengubah kata sandi enkripsi 1084

Mengubah kredensial akses Microsoft 365 603

Mengubah kredensial akses SQL Server atau Exchange Server 588

Mengubah kuota layanan mesin 184

Mengubah registrasi beban kerja 123

Mengubah SID 525

Mengubah status skrip 245

© Acronis International GmbH, 2003-2024

Menguji replika 682

Mengumpulkan paket jaringan 772

Mengunduh agen proteksi 75

Mengunduh data untuk beban kerja yang terpengaruh baru-baru ini 298

Mengunduh file dari penyimpanan awan 512

Mengunduh file log VPN IPsec 775

Mengunduh keluaran dari operasi skrip 246

Mengunduh log alat VPN 772

Mengunduh log gateway VPN 772

Mengunduh program penyiapan 159

Menilai kerentanan dan mengelola patch 950

Meninjau dan memitigasi IOC pada beban kerja yang terdampak 919

Meninjau dan menganalisis IOC yang ditemukan 920

Meninjau insiden 897

Menjalankan cadangan awan-ke-awan secara manual 196

Menjalankan failover uji 780

Menjalankan mesin 677

Menjalankan mesin virtual dari cadangan (Pemulihan Instan) 676

Menjalankan pemindaian inventaris perangkat keras secara manual 979

Menjalankan pemindaian inventaris perangkat lunak secara manual 975

Menjalankan pemindaian Skor #CyberFit 232

Menjalankan pencadangan secara manual 433

Menjalankan pencadangan sesuai jadwal 420

Menjalankan Rencana proteksi patch uji dan menolak patch yang tidak aman 971

Menjalankan skrip pra-beku dan pasca-leleh secara otomatis 692

Menjelajahi inventaris perangkat keras 980

Menjelajahi inventaris perangkat lunak 975

Menonaktifkan failover uji otomatis 784

Menonaktifkan Pemulihan Sekali klik 476

Menonaktifkan pencarian teks lengkap untuk cadangan Gmail 664

Menonaktifkan penetapan otomatis untuk agen 692

Menonaktifkan penyimpanan yang tidak dapat diubah 1087

Menonaktifkan Startup Recovery Manager 728

Mentransfer file 1013

Mentransfer file melalui Acronis Bantuan Cepat 1019

Menyalin pustaka Microsoft Exchange Server 587

Menyebarkan agen melalui Kebijakan Grup 167

Menyebarkan Agen untuk oVirt (Alat Virtual) 152

Menyebarkan Agen untuk Scale Computing HC3 (Alat Virtual) 139

Menyebarkan Agen untuk Synology 158

Menyebarkan Agen untuk Virtuozzo Hybrid Infrastructure (Alat Virtual) 144

Menyebarkan Agen untuk VMware (Virtual Appliance) 135

Menyebarkan templat OVA 153

Menyebarkan templat OVF 136

Menyebarkan templat QCOW2 140, 148

Menyelesaikan masalah kompatibilitas dengan rencana manajemen jarak jauh 1005

Menyelesaikan masalah kompatibilitas dengan

© Acronis International GmbH, 2003-2024

rencana pemantauan 1070
Menyelesaikan pertentangan rencana 220
Menyelidiki insiden 905
Menyertakan database SQL Server 578
Menyesuaikan izin dalam aturan kebijakan alur data 869
Menyetujui patch secara manual 972
Menyiapkan objek Kebijakan Grup 171
Menyimpan file log agen 186
Merekam dan memutar sesi jarak jauh 1023
Mesin fisik ke virtual 501
Mesin perilaku 824
Mesin virtual Microsoft Azure and Amazon EC2 705
Mesin yang ditemukan 284
Mesin yang rentan 294
Metode validasi 204
Microsoft 34
Microsoft Azure 41
Microsoft BitLocker Drive Encryption 42
Microsoft Defender Antivirus 852
Microsoft Defender Antivirus dan Microsoft Security Essentials 852
Microsoft Security Essentials 852
Microsoft SQL Server 457
Migrasi melalui media yang dapat di-boot 704
Migrasi mesin 701
Mode boot 520
Mode cadangan klaster 456
Mode hanya-awan 741, 762
Mode kepatuhan 1083
Mode penyimpanan yang tidak dapat diubah 1085
Modul dan rencana proteksi 213
Monitor Cyber Protect 30, 310
Monitor yang dapat dikonfigurasi 1028
Mounting volume dari cadangan 528
MTTR insiden keamanan 286
Mulai kembali beban kerja 933

N

Nama file cadangan 450
Nama file cadangan default 451
Nama tanpa variabel 452
NEAR 989
Nilai bidang tindakan 387
Nonaktifkan DRS otomatis untuk agen 135
Notarisasi 444, 658
Notarisasi cadangan dengan data forensik 465
Notifikasi OS dan peringatan layanan 377
Nutanix 40
Nyalakan mesin virtual target ketika pemulihan selesai 526

O

Objek level atas 713
Objek variabel 713
Operasi dengan mesin virtual Microsoft Azure 798
Operasi dengan pencadangan 526
Operasi dengan runbook 811
Operasi dengan server utama 801
Operasi jarak jauh dengan media yang dapat di-boot 724

© Acronis International GmbH, 2003-2024

Operasi khusus dengan mesin virtual 676

Operasi lokal dengan media yang dapat di-boot 723

Operasi tambahan dengan rencana manajemen jarak jauh yang ada 1002

Operasi tambahan dengan rencana pemantauan 1067

Operasi yang didukung dengan volume logis 56

Operator pencarian 357

Opsi cadangan 445

Opsi cadangan default 445

Opsi failback 685

Opsi masuk yang berbeda 990

Opsi pemulihan 518

Opsi penjadwalan tambahan 432

Opsi penyimpanan lanjutan 413

Opsi replikasi 684

Opsi tambahan 421

Oracle 39

Orkestrasi (runbook) 807

oVirt/Red Hat Virtualization 4.2 dan 4.3/Oracle Virtualization Manager 4.3 157

oVirt/Red Hat Virtualization 4.4, 4.5 158

P

Pada beban kerja, agen, dan lokasi pencadangan apa yang mengalami hambatan? 537

Pada event Windows Event Log 424

Paket Linux 68

Parallels 38

Parameter 709

Parameter dasar 106

Parameter informasi 108

Parameter instalasi 106

Parameter Kernel 709

Parameter pemasangan atau penghapusan instalasi tanpa pengawasan 105

Parameter pendaftaran 107

Parameter penghapusan instalasi 109

Parameter peristiwa 425

Parameter runbook 810

Parameter tambahan 108

Parameter untuk fitur lama 109

Parameter untuk instalasi tanpa pengawasan (EXE) 89

Parameter untuk instalasi tanpa pengawasan (MSI) 98

Patch beban kerja 932

Pelacakan perubahan blok (CBT) 456

Pelacakan Perubahan Blok (CBT) 684

Pemantauan 259

Pemantauan beban kerja melalui transmisi tangkapan layar 1015

Pemantauan berbasis anomali 1028

Pemantauan kesehatan dan kinerja beban kerja 1027

Pemantauan kesehatan disk 289

Pembagian 489

Pembangun Media Yang Dapat Di-Boot 707

Pembaruan kebijakan alur data 871

Pembaruan otomatis komponen 181

Pembaruan yang tidak ada berdasarkan kategori 296

© Acronis International GmbH, 2003-2024

Pembatasan 33, 36-41, 145, 153, 159, 211, 234, 289, 400-401, 405, 408, 414, 498, 512, 521, 600, 619, 624, 628, 640, 647, 650-651, 654-655, 665, 672, 681, 687, 727, 732, 861, 1083

Pembatasan dan masalah yang diketahui 637

Pemberitahu desktop jarak jauh 1025

Pembersihan 208

Pembuatan Skrip Cyber 234

Pemfilteran URL 842

Pemindaian antimalware pada cadangan 860

Pemindaian terjadwal 819

Pemotongan log 471

Pemrosesan data off-host 197

Pemulihan 57, 495

Pemulihan aman 497

Pemulihan dari berbagi jaringan 712

Pemulihan dari penyimpanan awan 711

Pemulihan database yang termasuk dalam AAG 564

Pemulihan dengan media yang dapat di-boot secara lokal 723

Pemulihan dengan mulai kembali 499

Pemulihan jalur lengkap 523

Pemulihan ke kontainer Virtuozzo atau mesin virtual Virtuozzo 516

Pemulihan lintas platform 496

Pemulihan sekali klik 473

Penambahan manual ke daftar putih 859

Penambahan otomatis ke daftar putih 859

Penanganan eror 458, 521, 684-685

Penanganan kegagalan tugas 490

Pencadangan berbasis agen dan tanpa agen 65

Pencadangan keberadaan klaster 565

Pencadangan kotak surat 569

Pencadangan mingguan 494

Pencadangan prapembaruan 965

Pencadangan sektor demi sektor 489

Pencarian dalam cadangan cloud ke cloud 659

Pencarian driver otomatis 508

Pencarian teks lengkap 660

Pencegahan eksploit 825

Penemuan manual mesin 124

Pengalihan suara jarak jauh 990

Pengaturan Active Protection di Cyber Backup Standard 835

Pengaturan akses 372

Pengaturan daftar putih 859

Pengaturan frekuensi pencadangan Google Workspace 645

Pengaturan jaringan 721

Pengaturan keamanan IPsec/IKE 756

Pengaturan kecepatan transfer Disk berdasarkan monitor proses 1050

Pengaturan keranjang 548-549

Pengaturan kinerja dan cadangan jendela 478

Pengaturan lanjutan 876

Pengaturan manajemen patch dalam rencana proteksi 960

Pengaturan monitor kecepatan transfer Disk 1043

Pengaturan monitor Kustom 1059

Pengaturan monitor log peristiwa Windows 1054

© Acronis International GmbH, 2003-2024

Pengaturan monitor Mulai ulang sistem terakhir 1054

Pengaturan monitor penggunaan CPU 1039

Pengaturan monitor Penggunaan jaringan 1045

Pengaturan monitor Penggunaan memori 1041

Pengaturan monitor Perangkat lunak yang diinstal 1053

Pengaturan monitor Perubahan perangkat keras 1038

Pengaturan monitor ruang Disk 1033

Pengaturan monitor status Firewall 1057

Pengaturan monitor status fitur AutoRun 1059

Pengaturan monitor status layanan Windows 1052

Pengaturan monitor status Pembaruan Windows 1057

Pengaturan monitor Status proses 1053

Pengaturan monitor suhu CPU 1035

Pengaturan monitor suhu GPU 1037

Pengaturan monitor ukuran File dan folder 1056

Pengaturan monitor upaya masuk gagal 1057

Pengaturan pemfilteran URL 845

Pengaturan penggunaan CPU berdasarkan monitor proses 1048

Pengaturan penggunaan Jaringan berdasarkan monitor proses 1051

Pengaturan penggunaan Memori berdasarkan monitor proses 1049

Pengaturan penilaian kerentanan 953

Pengaturan perlindungan 181

Pengaturan perlindungan Antivirus dan antimalware 819

Pengaturan peta perlindungan data 306

Pengaturan privasi 21

Pengaturan status monitor perangkat lunak antimalware 1058

Pengaturan Universal Restore 508

Pengecualian 855

Pengecualian file 522

Pengecualian proteksi 831

Pengecualian URL 851

Pengelolaan organisasi Microsoft 365 yang ditambahkan pada tingkat berbeda 606

Pengguna idle 427

Pengguna telah keluar 428

Penghapusan aman data dari beban kerja yang terkelola 389

Penghapusan otomatis untuk lingkungan pelanggan yang tidak digunakan di situs awan 750

Pengikatan manual 691

Pengikatan mesin virtual 690

Pengiriman Data Fisik 482

Pengontrol Domain Active Directory untuk konektivitas VPN L2 Terbuka 758

Pengontrol Domain Active Directory untuk konektivitas VPN L3 IPsec 758

Penilaian kerentanan 950

Penilaian kerentanan untuk mesin Linux 956

Penilaian kerentanan untuk mesin Windows 956

Penilaian kerentanan untuk perangkat macOS 957

Penjadwalan 488

© Acronis International GmbH, 2003-2024

Penyelesaian masalah 133

Penyewa dalam mode Kepatuhan 516

Penyimpanan cache 183

Penyimpanan geo-redundan 1088

Penyimpanan yang tidak dapat diubah 1085

Peran pengguna dan hak Pembuatan Skrip Cyber 235

Peran yang diperlukan 157

Perangkat seluler yang didukung 589

Perbandingan rencana proteksi default 221

Performa 523, 685

Periksa indikator penyusupan (IOC) dari serangan terhadap beban kerja Anda yang diketahui secara publik 917

Periksa serangan yang diungkapkan secara publik pada beban kerja Anda menggunakan umpan ancaman 894

Peringatan 448

Peringatan cadangan 262

Peringatan EDR 279

Peringatan kontrol perangkat 386

Peringatan Kontrol Perangkat 280

Peringatan pelisensian 276

Peringatan pemantauan 1071

Peringatan pemfilteran URL 278

Peringatan pemulihan bencana 266

Peringatan proteksi Antimalware 272

Peringatan sistem 281

Peringatan status kesehatan disk 293

Perintah pasca-pemulihan 525

Perintah pasca-pencadangan 485

Perintah pengambilan data pra/pasca 485

Perintah pengambilan pasca-data 487

Perintah pengambilan pra-data 486

Perintah pra-pencadangan 484

Perintah pra/pasca 483, 524, 685

Perintah sebelum pemulihan 524

Peristiwa Pencegahan Kehilangan Data 884

Perlindungan antivirus and antimalware 817

Perlindungan aplikasi kolaborasi dan komunikasi 258

Perlindungan cyber 282

Perlindungan data berkelanjutan (CDP) 408

Perlindungan diri 822

Perlindungan folder jaringan 821

Perlindungan SAP HANA 664

Perlindungan sisi server 821

Perlindungan waktu nyata 818, 827, 854

Persetujuan patch otomatis 967

Persiapan 58, 78, 508

- WinPE 2.x dan 3.x 719
- WinPE 4.0 ke atas 720

Persyaratan 516, 529

Persyaratan akses yang diperlukan untuk cadangan ke penyimpanan cloud publik 546

Persyaratan jaringan untuk Agen Virtuozzo Hybrid Infrastructure (Alat Virtual) 145

Persyaratan kata sandi 19

Persyaratan pada akun pengguna 582

Persyaratan perangkat lunak 23, 731, 895

Persyaratan sistem 751

Persyaratan sistem untuk agen 65, 135, 139, 144, 152

© Acronis International GmbH, 2003-2024

Persyaratan tambahan untuk mesin yang menjalankan Windows 569

Persyaratan tambahan untuk pencadangan keberadaan aplikasi 560

Persyaratan tentang Kontrol Akun Pengguna (UAC) 131

Persyaratan umum 559

Persyaratan untuk alat VPN 751

Persyaratan untuk memulai 251, 426

Persyaratan untuk mesin virtual ESXi 560

Persyaratan untuk mesin virtual Hyper-V 560

Peta organisasi 888

Peta perlindungan data 293, 305

Pilih penyedia snapshot 492

Platform virtualisasi yang didukung 32, 731

Platform yang didukung 234, 814, 988

Platform yang didukung untuk pemantauan 1028

Port 751

Port TCP yang diperlukan untuk pencadangan dan replikasi mesin virtual VMware 59

Port yang dibutuhkan oleh komponen Downloader 60

Port yang diperlukan 158

Prakonfigurasi beberapa koneksi jaringan 721

Prasyarat 124, 160, 163, 165-167, 173-174, 234, 245, 320, 324, 391-392, 408, 477, 516, 559, 666, 676, 693, 754, 759, 764, 767-768, 775-776, 789, 794, 799, 972, 975, 977, 980, 982, 993, 1001-1004, 1010, 1012-1016, 1018-1019, 1061, 1063-1064, 1067-1069, 1069, 1080

Prioritas CPU 480

Produk Apple dan pihak ketiga yang didukung 952

Produk Apple yang didukung 952

Produk Linux yang didukung 953

Produk Microsoft 960

Produk Microsoft dan produk pihak ketiga yang didukung 951

Produk Microsoft yang didukung 951

Produk pihak ketiga Windows 961

Produk pihak ketiga yang didukung untuk macOS 953

Produk pihak ketiga yang didukung untuk Windows OS 952

Prosedur pemulihan spesifik perangkat lunak 42

Proses cadangan forensik 463

Proses Universal Restore 509

Proteksi cerdas 301

Protokol koneksi jarak jauh 989

Provisi disk 684

R

RDP 990

Red Hat dan Linux 37

Redistribusi 691

Referensi cepat pemulihan 495

Referensi cepat rencana proteksi 397

Rekomendasi 521

Rekomendasi dan langkah remediasi 894

Rekomendasi umum untuk situs lokal 755

Rekomendasi untuk ketersediaan Layanan Domain Active Directory 758

Remediasi insiden 920

Remediasi insiden positif palsu 925

© Acronis International GmbH, 2003-2024

Remediasi seluruh insiden 921

Rencana manajemen jarak jauh 992

Rencana pada level administrasi yang berbeda 253

Rencana pemantauan 1027, 1061

Rencana pemindaian cadangan 196

Rencana pencadangan untuk aplikasi awan 196

Rencana proteksi 196

Rencana proteksi default 221

Rencana proteksi individu untuk integrasi panel kontrol hosting 227

Rencana skrip 247

Rencana yang didukung untuk grup perangkat 340

Replikasi 439

Replikasi cadangan 198

Replikasi mesin virtual 680

Replikasi vs. mencadangkan 680

Repositori skrip 247

Ringkasan instalasi patch 296

Riwayat instalasi patch 296

Riwayat keparahan insiden 286

S

Scale Computing 37

Sebelum Anda memulai 135, 139, 144, 152, 158

Seeding replika awal 685

Sekilas pembahasan tentang dasbor 895

Selanjutnya 737

Server Microsoft Exchange 457

Server pemulihan 745

Server utama 747

Sesuai interval waktu 429

Siapkan driver 508

Simpan informasi sistem jika pemulihan dengan reboot gagal 522

Simpan peristiwa keamanan selama 180 hari 895

Sistem file yang didukung 53

Sistem operasi dan lingkungan yang Didukung 23

Sistem operasi dan versi yang didukung 44

Sistem operasi Windows yang didukung 855

Sistem Operasi yang Didukung 731

Skema cadangan 417

Skenario Penggunaan 529

Skor #CyberFit berdasarkan mesin 288

Skor #CyberFit untuk mesin 227

Skrip 237

Skrip dalam media yang dapat di-boot 711

Skrip kustom 712

Skrip yang sudah ditentukan 711

Snapshot intermediet 213

Snapshot multivolume 473

Snapshot pencadangan tingkat file 462

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) 882

Startup Recovery Manager 727

Status ancaman 285

Status Geo-replikasi 1089

Status instalasi patch 295

Status jaringan beban kerja 288

© Acronis International GmbH, 2003-2024

Status proteksi 283

Status rencana 195

Status validasi 202

Struktur aturan 867

Struktur autostart.json 713

Struktur kebijakan alur data 866

Sumber data yang didukung 410

Syarat mulai tugas 490

T

Tab aktivitas 322

Tab Aktivitas 309

Tab manajemen 195

Tab manajemen perangkat lunak 322

Tab Penyimpanan cadangan 526

Tab Perangkat 322

Tab peringatan 321

Tambah atau hapus perangkat USB dari database 370

Tambahkan atau hapus proses, file, atau jaringan dalam daftar blokir atau daftar izin rencana proteksi 944

Tanggal dan waktu untuk file 521

Tempat untuk mendapatkan aplikasi Cyber Protect 590

Temukan pengguna yang terakhir masuk 393

Tentang Cyber Disaster Recovery Cloud 730

Tentang jadwal pencadangan 639

Tentang layanan Pengiriman Data Fisik 482

Tentang Secure Zone 414

Terima pemberitahuan peringatan saat terjadi pelanggaran 893

Tes failover 780

Tetapkan tindakan respons untuk beban kerja yang terpengaruh 927

Tetapkan tindakan respons untuk file yang mencurigakan 942

Tidak ada pencadangan yang berhasil untuk jumlah hari berurutan yang ditentukan 448

Tindakan 871

Tindakan default 853

Tindakan dengan rencana proteksi 215

Tindakan respons manual 1075

Tindakan saat deteksi 836

Tindakan untuk merespons simpul rantai cyber kill individu 926

Tingkat kompresi 458

Tingkat lanjut 854

Tingkat penyewa mitra di Cyber Protect konsol 321

Tinjauan dan manajemen kebijakan 871

Tips berguna 606, 641

Titik komputasi 734

Titik mount 472, 523

Transfer suara 990

Tujuan yang didukung 411

Tunggu sampai persyaratan jadwal dipenuhi 490

U

Umpan ancaman 301

Unduh konfigurasi untuk OpenVPN 770

Universal Restore di Linux 509

Universal Restore di Windows 508

© Acronis International GmbH, 2003-2024

V

Validasi 201

Validasi cadangan 456, 520

Validasi tangkapan layar 205

Variabel peringatan pemantauan 1073

Verifikasi checksum 204

Versi Database Oracle yang didukung 31

Versi MariaDB yang didukung 32

Versi Microsoft Exchange Server yang didukung 30

Versi Microsoft SharePoint yang didukung 31

Versi Microsoft SQL Server yang didukung 30

Versi MySQL yang didukung 31

Versi percobaan Cyber Disaster Recovery Cloud 733

Versi SAP HANA yang didukung 31

Versi skrip 244

Versi yang didukung 637

Virtuozzo 40

Visualisasi alur cerita penyerangan yang mudah dipahami 894

Vituozzo Hybrid Infrastructure 41

VM heartbeat 205

VMware 32

VPN Terbuka Situs-ke-situs - Informasi tambahan 186

W

Widget Advanced Data Loss Prevention dalam dasbor Ikhtisar 885

Widget Deteksi dan Tanggapan Titik Akhir (EDR) 284

Widget instalasi patch 295

Widget inventaris perangkat keras 300

Widget inventaris perangkat lunak 299

Widget kesehatan disk 290

Widget monitor 1081

Widget penilaian kerentanan 294

Widget peringatan 282

Widget sesi jarak jauh 301

Windows 402

Y

Yang baru di konsol Cyber Protect 319

Yang dapat Anda lakukan dengan sebuah replika 681

Yang perlu Anda ketahui tentang finalisasi 679

© Acronis International GmbH, 2003-2024