Acronis

acronis.com

Acronis Cyber Protect 15

Pembaruan 6

Panduan Pengguna

REVISI: 15/06/2023

Daftar isi

Pernyataan hak cipta

Teknologi Acronis yang Dipatenkan

Teknologi yang digunakan dalam produk ini dicakup dan dilindungi oleh satu atau beberapa Nomor Paten AS: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; dan pengajuan paten yang masih menunggu keputusan.

Acronis Cyber Protect 15 edisi

Acronis Cyber Protect 15 tersedia dalam edisi berikut:

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard
- Cyber Backup Lanjutan

Untuk informasi detail mengenai fitur yang disertakan dalam setiap edisi, lihat Perbandingan Edisi Acronis Cyber Protect 15 termasuk Penyebaran awan.

Semua edisi Acronis Cyber Protect 15 dilisensikan berdasarkan jumlah beban kerja yang dilindungi dan jenisnya (stasiun kerja, server, dan host virtual). Edisi Cyber Protect hanya tersedia dengan lisensi berlangganan. Edisi Cyber Backup tersedia dengan lisensi berlangganan dan abadi. Untuk informasi lebih lanjut tentang opsi yang tersedia, lihat "Pelisensian" (hlm. 21).

Kunci lisensi abadi untuk versi 15 tidak dapat digunakan dengan agen cadangan dari Acronis Cyber Backup 12.5. Namun, agen ini akan terus bekerja dengan kunci lisensi lamanya, meskipun server manajemen mereka ditingkatkan ke versi 15.

Lisensi berlangganan cadangan dapat digunakan dengan agen versi 12.5, bahkan ketika agen ditingkatkan ke versi 15. Cyber Protect lisensi berlangganan hanya dapat digunakan oleh agen versi 15.

Agen cadangan versi 12.5 yang terdaftar di server manajemen versi 15 tidak dapat melakukan operasi pemrosesan data di luar host, seperti replikasi cadangan, validasi cadangan, pembersihan, atau konversi ke mesin virtual.

Catatan
Fiturnya bervariasi pada setiap edisi. Beberapa fitur yang dijelaskan di dokumentasi ini mungkin tidak tersedia dengan lisensi Anda. Untuk informasi detail mengenai fitur yang disertakan dalam setiap edisi, lihat Perbandingan Edisi Acronis Cyber Protect 15 termasuk Penyebaran awan.

Fitur Cyber Protect yang didukung sistem operasi

Fitur Cyber Protect didukung pada sistem operasi berikut:

- Windows: Windows 7 dan versi lebih baru, serta Windows Server 2008 R2 dan versi lebih baru.
  Manajemen Windows Defender Antivirus didukung pada Windows 8.1 ke atas.
- Linux: CentOS 7.x, CentOS 8.0, Virtuozzo 7.x, Acronis Cyber Infrastructure 3.x.
  Distribusi dan versi Linux lain mungkin juga mendukung fitur Cyber Protect, tetapi belum pernah diuji.
- macOS: 10.13.x ke atas (hanya mendukung perlindungan Antivirus & Antimalware).

Penting

Fitur Cyber Protect hanya didukung untuk mesin dengan agen perlindungan yang sudah diinstal. Untuk mesin virtual yang dilindungi dalam mode tanpa agen, misalnya oleh Agen untuk Hyper-V, Agen untuk VMware, atau Agen untuk Scale Computing, hanya cadangan yang didukung.

Fitur Cyber Protect	Windows	Linux	macOS
Cadangan forensik	Iya	Tidak	Tidak
Perlindungan data berkelanjutan (CDP)			
CDP untuk file dan folder	Iya	Tidak	Tidak
CDP untuk file yang diubah melalui jalur aplikasi	Iya	Tidak	Tidak
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
Perlindungan Anti-malware Acronis			
Deteksi ransomware berdasarkan perilaku proses (berbasis AI)	Iya	Tidak	Tidak
Deteksi proses cryptomining	Iya	Tidak	Tidak
Proteksi antimalware waktu nyata	Iya	Tidak	Iya
Pemulihan otomatis file yang terpengaruh dari cache lokal	Iya	Tidak	Tidak
Perlindungan diri untuk file cadangan Acronis	Iya	Tidak	Tidak
Perlindungan diri untuk perangkat lunak Acronis	Iya	Tidak	Tidak
Analisis statik untuk file portable yang dapat dieksekusi	Iya	Tidak	Ya*
Proteksi drive eksternal (HDD, flash drive, kartu SD)	Iya	Tidak	Tidak
Perlindungan folder jaringan	Iya	Tidak	Tidak

Perlindungan sisi server	Iya	Tidak	Tidak
Perlindungan Zoom, WebEx, Microsoft Teams, dan perlindungan kerja jarak jauh lainnya	Iya	Tidak	Tidak
Pemindaian antimalware sesuai permintaan	Iya	Tidak	Iya
Pindai file arsip	Iya	Tidak	Iya
Pengecualian file/folder	Iya	Tidak	Ya**
Pengecualian proses	Iya	Tidak	Tidak
Daftar putih seluruh perusahaan	Iya	Tidak	Iya
Deteksi perilaku	Iya	Tidak	Tidak
Karantina	Iya	Tidak	Iya
Pemfilteran URL (http/https)	Iya	Tidak	Tidak
Manajemen Windows Defender Antivirus	Iya	Tidak	Tidak
Manajemen Microsoft Security Essentials	Iya	Tidak	Tidak
Penilaian kerentanan			
Penilaian kerentanan sistem operasi dan aplikasi aslinya	Iya	Ya***	Tidak
Penilaian kerentanan untuk aplikasi pihak ketiga	Iya	Tidak	Tidak
Manajemen patch			
Persetujuan otomatis patch	Iya	Tidak	Tidak
Instalasi patch manual	Iya	Tidak	Tidak
Penjadwalan instalasi patch otomatis	Iya	Tidak	Tidak
Patch aman yang gagal: cadangan mesin sebelum menginstal patch sebagai bagian dari rencana proteksi	Iya	Tidak	Tidak
Pembatalan mulai ulang mesin jika pencadangan sedang berjalan	Iya	Tidak	Tidak
Peta perlindungan data			
Memindai mesin untuk menemukan file yang tidak terlindungi	Iya	Tidak	Tidak

Gambaran umum lokasi yang tidak terlindungi	Iya	Tidak	Tidak
Tindakan protektif dalam peta Perlindungan data	Iya	Tidak	Tidak
Kesehatan disk			
Kontrol kesehatan HDD dan SSD berbasis AI	Iya	Tidak	Tidak
Rencana proteksi pintar berdasarkan peringatan Pusat Operasi Perlindungan Cyber Acronis (CPOC)			
Umpan ancaman	Iya	Tidak	Tidak
Wizard perbaikan	Iya	Tidak	Tidak
Pemindaian cadangan			
Pemindaian cadangan yang dienkripsi	Iya	Tidak	Tidak
Memindai cadangan disk di penyimpanan lokal, bagian jaringan, dan Acronis Cloud Storage	Iya	Tidak	Tidak
Pemulihan aman			
Pemindaian antimalware dengan perlindungan Acronis Antivirus & Antimalware selama proses pemulihan	Iya	Tidak	Tidak
Desktop jarak jauh			
Koneksi melalui klien berbasis HTML5	Iya	Tidak	Tidak
Koneksi melalui klien Windows RDP asli	Iya	Tidak	Tidak
Penghapusan jarak jauh	Ya****	Tidak	Tidak
Monitor Cyber Protect	Iya	Tidak	Iya

* Pada macOS, analisis statis untuk file portabel yang dapat dieksekusi hanya didukung untuk pemindaian terjadwal.

** Pada macOS, Anda dapat menggunakan pengecualian untuk menentukan file dan folder yang tidak akan dipindai oleh perlindungan waktu nyata atau pemindaian terjadwal.

*** Penilaian kerentanan tergantung pada ketersediaan laporan keamanan resmi untuk distribusi tertentu, contohnya https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce, dan lain-lain.

**** Penghapusan jarak jauh hanya tersedia untuk mesin yang menjalankan Windows 10 atau versi yang lebih baru.

Pelisensian

Untuk melindungi beban kerja menggunakan Acronis Cyber Protect, Anda membutuhkan lisensi. Lisensi tidak diperlukan untuk menginstal Acronis Cyber Protect.

Tipe lisensi

Acronis Cyber Protect tersedia dengan lisensi berlangganan. Dalam periode validitas, yang dimulai sejak tanggal pembelian, tersedia pembaruan tak terbatas dan dukungan teknis gratis. Setelah masa berlaku berakhir, paket perlindungan yang ada berhenti bekerja dan paket perlindungan baru tidak dapat dibuat.

Tersedia pembaruan untuk lisensi abadi legasi. Beberapa fitur, seperti penyebaran awan atau cadangan awan-ke-awan tidak tersedia dengan lisensi abadi.

Lisensi percobaan juga tersedia. Lisensi ini memberi Anda akses ke semua fitur produk selama 30 hari sejak aktivasi lisensi.

Untuk detail lebih lanjut tentang opsi lisensi yang berbeda, lihat Acronis Cyber Protect 15: TJU lisensi dan peningkatan/penurunan versi di basis pengetahuan kami. Acronis Kebijakan pemberian lisensi tersedia di https://www.acronis.com/company/licensing.html.

Penting
Acronis Cyber Protect 15 Update 3 memperkenalkan model lisensi baru. Langkah ini memerlukan pendaftaran lisensi dan aktivasi server manajemen lokal.

Lisensi di Acronis Cyber Protect 15 Update 3 dan versi yang lebih baru

Di Acronis Cyber Protect 15 Update 3 dan versi yang lebih baru, tidak ada kunci lisensi yang ditambahkan di konsol lokal server manajemen (`https://<alamat IP server manajemen Anda>:<port>`).

Sebagai gantinya, Anda menambahkan lisensi ke akun Anda di Portal Pelanggan Acronis (`https://account.acronis.com`), lalu Anda mengelola lisensi Anda di konsol cloud Acronis Cyber Protect (`https://cloud.acronis.com`).

Manajemen lisensi server manajemen offline memerlukan operasi baik di konsol lokal maupun cloud.

Untuk mempelajari lebih lanjut tentang konsol lokal dan awan, lihat "Acronis konsol akun, lokal dan awan" (hlm. 23).

Untuk mulai menggunakan server manajemen dengan Acronis Cyber Protect 15 Update 3 dan versi yang lebih baru

1. Tambahkan satu atau beberapa lisensi ke akun Anda di Acronis Portal Pelanggan (https://account.acronis.com).
   Lisensi yang Anda beli secara online secara otomatis ditambahkan ke akun ini.
2. [Untuk mode penerapan lokal] Aktifkan server manajemen Anda.
3. Alokasikan lisensi ke server manajemen.

Jenis server manajemen

Bergantung pada mode penyebaran, Anda dapat menggunakan jenis server manajemen berikut:

- Server manajemen awan
- Server manajemen di lokasi
  - Server manajemen online
  - Server manajemen offline

Anda dapat memiliki lebih dari satu server manajemen di akun Acronis Anda. Anda juga dapat menggunakan mode penerapan campuran dengan server manajemen awan dan server manajemen lokal.

Jika Anda menggunakan beberapa server manajemen, Anda dapat membagi kuota lisensi di antara mereka. Untuk informasi lebih lanjut tentang cara melakukannya, lihat "Mentransfer kuota lisensi ke server manajemen lainnya" (hlm. 33).

Server manajemen awan

Dengan penerapan awan, Anda tidak menginstal dan memelihara server manajemen di jaringan Anda. Anda menggunakan server manajemen yang sudah disebarkan di pusat data Acronis dan Anda hanya perlu menginstal agen perlindungan untuk beban kerja Anda.

Server manajemen awan tidak memerlukan aktivasi. Itu selalu online dan informasi lisensi secara otomatis disinkronkan antara server dan akun Acronis Anda.

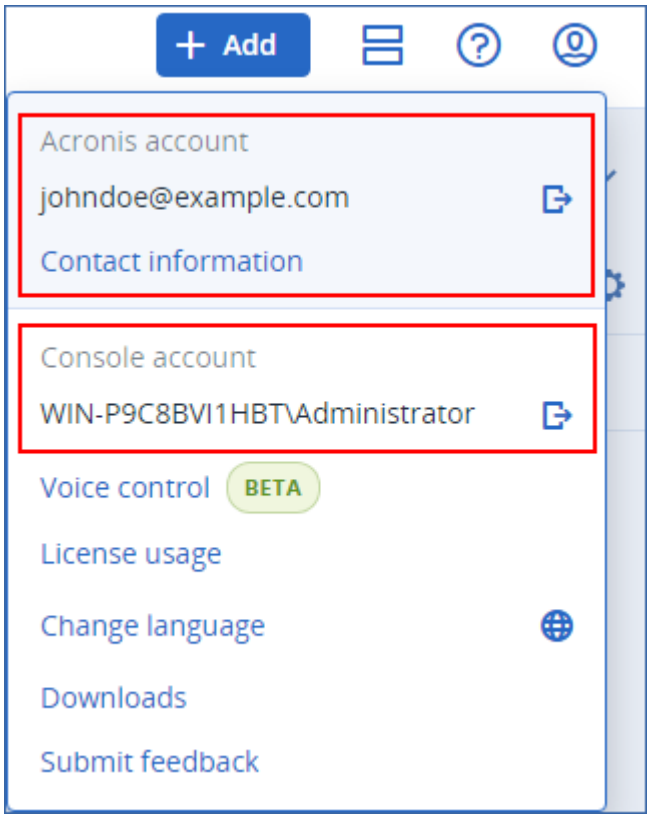
Server manajemen di lokasi

Dengan penyebaran lokal, Anda menginstal server manajemen dan agen perlindungan di jaringan Anda. Anda dapat memiliki server manajemen offline yang tidak tersambung ke Internet atau server manajemen online yang memiliki akses ke Internet.

Server manajemen di lokasi memerlukan aktivasi. Untuk informasi lebih lanjut tentang aktivasi, lihat "Mengaktifkan server manajemen" (hlm. 27).

Catatan

Dua akun berbeda ditampilkan di konsol lokal dari server manajemen lokal yang diaktifkan: akun Acronis, yang digunakan untuk menyinkronkan informasi lisensi; dan akun konsol, yang digunakan untuk mengakses konsol lokal itu sendiri.



Server manajemen lokal online

Anda mengaktifkan server manajemen online melalui Internet, dengan masuk ke akun Acronis Anda saat mengakses konsol lokal untuk pertama kalinya.

Server manajemen lokal offline

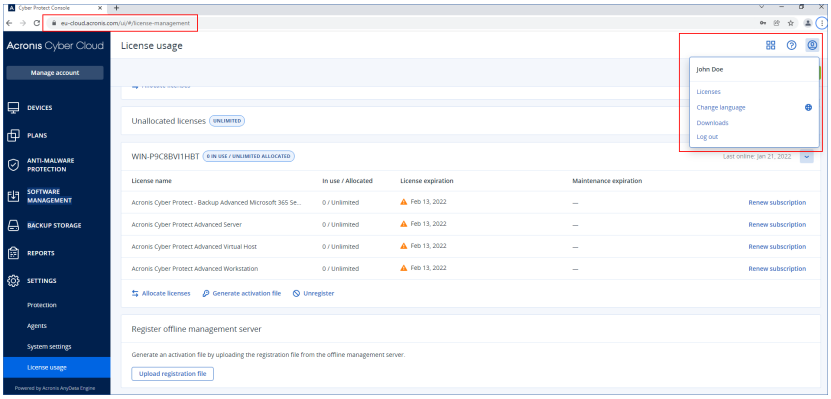
Anda mengaktifkan server manajemen offline dan menyinkronkan informasi lisensinya ke akun Acronis Anda secara manual, melalui file.

Acronis konsol akun, lokal dan awan

Untuk menggunakan Acronis Cyber Protect serta mengelola lisensi Anda dan penggunaannya, Anda membutuhkan akun Acronis. Semua lisensi dan server manajemen Anda terdaftar ke akun tersebut.

Dengan akun ini, Anda mengakses konsol berikut:

- Konsol cloud (`https://cloud.acronis.com`)

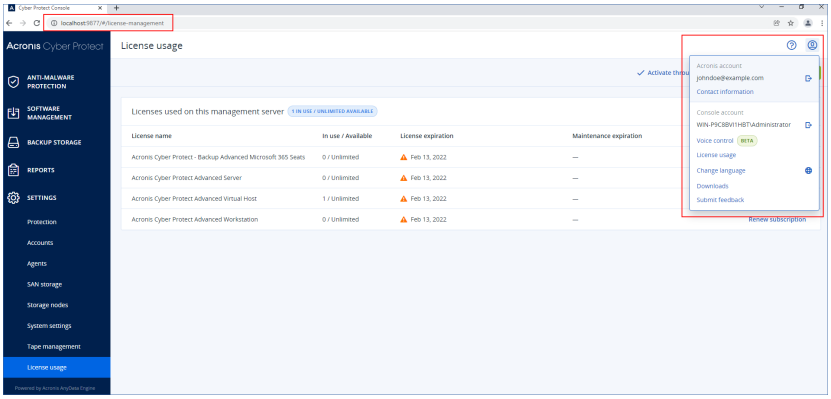


Catatan

Setelah Anda masuk ke konsol cloud, URL-nya berubah dan menunjukkan pusat data yang tepat yang menjadi milik akun Anda. Misalnya, `https://eu-cloud.acronis.com` or `https://jp-cloud.acronis.com`.

Konsol awan adalah lokasi utama tempat Anda mengelola lisensi. Di sini, pada tab **Pengaturan** > **Penggunaan lisensi**, Anda dapat mengalokasikan lisensi dan kuota lisensi yang tersedia ke server manajemen tertentu, mengalokasikan ulang kuota lisensi ke server manajemen lain, atau menyelesaikan pendaftaran server manajemen offline.

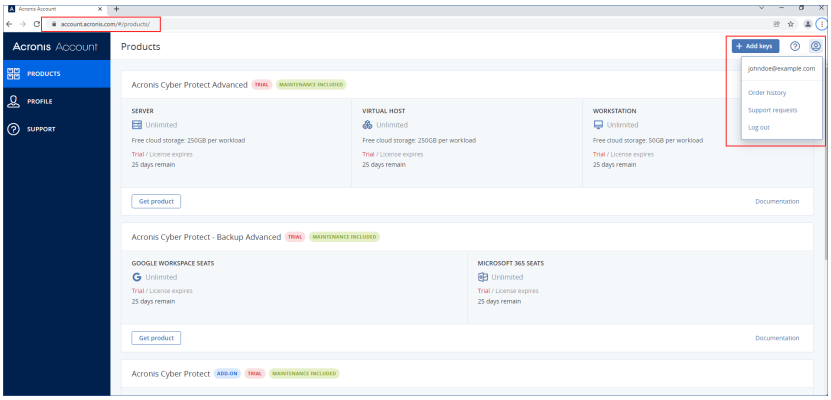
- Konsol lokal dari server manajemen lokal (`https://<alamat IP server manajemen Anda>:<port>`)



Di sini, Anda dapat memeriksa lisensi yang dialokasikan, kuota dan penggunaannya, serta tanggal kedaluwarsanya.

Anda menggunakan konsol lokal, bersama dengan konsol cloud, saat Anda mengaktifkan server manajemen offline atau mengalokasikan lisensi untuk itu.

- Acronis Portal Pelanggan (`https://account.acronis.com`)



Di Portal Pelanggan Acronis, Anda dapat mengelola produk yang dibeli, misalnya, dengan memeriksa tanggal kedaluwarsa langganan Anda, menambahkan kunci lisensi baru, mendaftarkan pembaruan lisensi, atau meminta peningkatan. Anda juga dapat menghubungi tim Dukungan, mengunduh file instalasi produk, dan mengakses dokumentasi produk.

Mengelola lisensi

Tabel di bawah ini merangkum operasi yang tersedia dan menunjukkan tempat untuk melakukannya.

Operasi	Lokasi
Menambahkan lisensi ke akun Anda	Anda menambahkan lisensi di Portal Pelanggan Acronis (`https://account.acronis.com`). Lisensi yang Anda beli secara online secara otomatis ditambahkan di sana.
Mengaktifkan server manajemen	Anda mengaktifkan server manajemen dengan mendaftarkannya di akun Anda. Anda mengaktifkan server manajemen online di konsol lokal mereka (`https://<alamat IP server manajemen Anda>:<port>`), dengan masuk ke akun Acronis Anda. Aktivasi server manajemen offline memerlukan operasi baik di konsol lokal maupun awan.
Mengalokasikan lisensi ke server manajemen Memodifikasi alokasi lisensi yang ada	Di server manajemen online, Anda mengalokasikan lisensi menggunakan konsol awan (`https://cloud.acronis.com`). Lisensi yang dialokasikan secara otomatis disinkronkan ke server manajemen. Di server manajemen offline, Anda perlu mengalokasikan lisensi melalui file aktivasi. Prosedur ini mengharuskan Anda menggunakan konsol lokal server manajemen (`https://<alamat IP server manajemen Anda>:<port>`) dan konsol awan (`https://cloud.acronis.com`).
Menetapkan lisensi untuk beban kerja	Operasi ini otomatis.
Membatalkan	Anda membatalkan pendaftaran server manajemen online dengan menggunakan konsol awan (`https://cloud.acronis.com`).

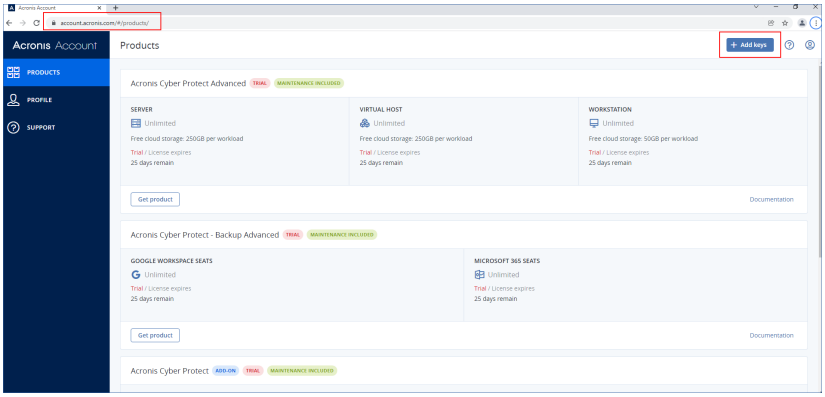
Operasi	Lokasi
pendaftaran server manajemen dari akun Anda	Anda membatalkan pendaftaran server manajemen offline melalui file penonaktifan. Prosedur ini mengharuskan Anda menggunakan konsol lokal server manajemen offline (`https://<alamat IP server manajemen Anda>:<port>`) dan konsol awan (`https://cloud.acronis.com`). Untuk membatalkan pendaftaran server manajemen offline yang aksesnya tidak Anda miliki, Anda hanya menggunakan konsol awan.

Menambahkan lisensi ke akun Acronis Anda

Untuk menggunakan lisensi, Anda harus menambahkannya ke akun Acronis Anda. Lisensi yang Anda beli secara online ditambahkan secara otomatis ke akun Anda. Anda harus menambahkan secara manual lisensi yang Anda beli secara offline.

Untuk menambahkan lisensi di akun Acronis Anda

1. Masuk ke Acronis Portal Pelanggan (`https://account.acronis.com`) dengan menggunakan kredensial akun Acronis Anda.
2. Di menu navigasi, klik **Produk**.
3. Klik **Tambah kunci**.



4. Masukkan satu atau beberapa kunci lisensi, satu per baris, lalu klik **Tambah**.

> **Catatan**
> Anda dapat memasukkan hingga 100 kunci lisensi sekaligus.

Lisensi sekarang ditambahkan ke akun Anda dan Anda dapat mengelola penggunaannya di konsol cloud (`https://cloud.acronis.com`).

Penting
Sebelum memutakhirkan ke Acronis Cyber Protect 15 Update 3, ekspor lisensi abadi yang disimpan secara lokal ke file, lalu tambahkan ke akun Acronis Anda.

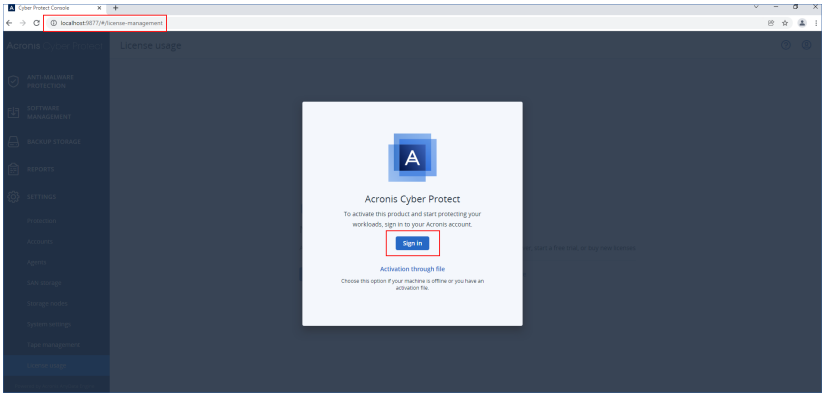
Untuk memeriksa kunci lisensi yang Anda masukkan secara lokal di server manajemen, buka `https://<alamat IP server manajemen Anda>:<port>/api/account_server/v2/licensing/legacy/license_keys`.

Mengaktifkan server manajemen

Anda mengaktifkan server manajemen dengan mendaftarkannya dalam akun Acronis Anda.

Untuk mengaktifkan server manajemen online

1. Setelah menginstal Acronis Cyber Protect server manajemen, buka konsol lokalnya (`https://<alamat IP server manajemen Anda>:<port>`).
2. Dalam kotak dialog yang terbuka, klik **Masuk**.



3. Masuk ke akun Acronis Anda.

Akibatnya, server manajemen secara otomatis terdaftar dan diaktifkan.

Untuk mulai melindungi beban kerja Anda, alokasikan setidaknya satu lisensi ke server ini. Untuk informasi lebih lanjut tentang cara mengalokasikan lisensi, lihat "Mengalokasikan lisensi ke server manajemen" (hlm. 30).

Catatan
Server manajemen online memerlukan akses Internet untuk menyinkronkan informasi lisensi ke akun Acronis Anda. Jika server tersebut tetap offline selama lebih dari 30 hari, rencana proteksinya akan berhenti berfungsi dan beban kerja Anda akan menjadi tidak terlindungi.

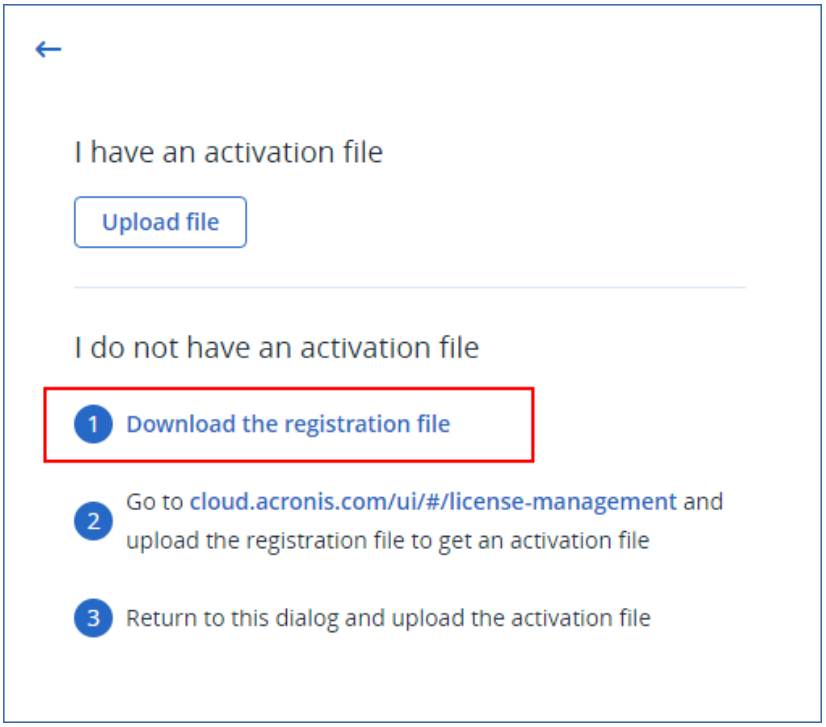
Jika Anda keluar dari akun Acronis di konsol lokal, informasi lisensi tidak dapat disinkronkan. Jika Anda tidak mendaftar lagi dalam waktu 30 hari, paket perlindungan akan berhenti berfungsi dan beban kerja Anda tidak akan terlindungi.

Untuk mengaktifkan server manajemen offline

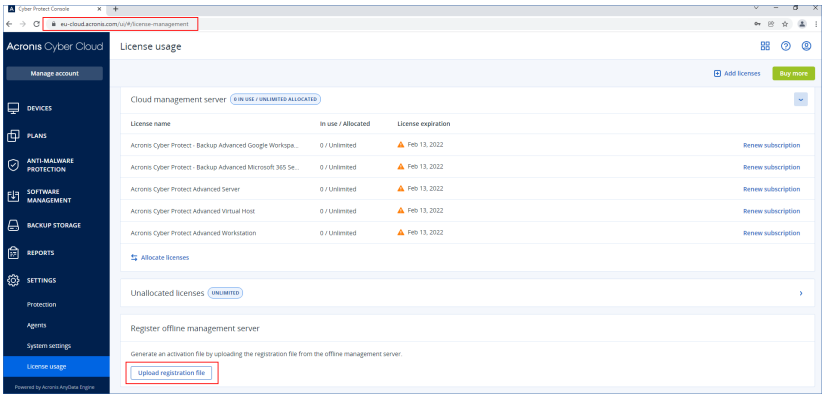
Aktivasi server manajemen offline memerlukan operasi baik di konsol lokal maupun awan.

Untuk mengakses konsol cloud, Anda memerlukan mesin kedua yang terhubung ke Internet.

1. Setelah menginstal Acronis Cyber Protect server manajemen, buka konsol lokalnya (`https://<alamat IP server manajemen Anda>:<port>`).
2. Dalam kotak dialog yang terbuka, klik **Aktivasi melalui file**.
3. Di bawah **Saya tidak memiliki file aktivasi**, klik **Unduh file pendaftaran**.



   File registrasi diunduh ke mesin Anda.
4. Pada mesin dengan akses ke Internet, masuk ke konsol cloud (`https://cloud.acronis.com`), lalu buka **Pengaturan** > **Penggunaan lisensi**.
5. Di bagian **Mendaftarkan server manajemen offline**, klik **Unggah file registrasi**.



6. Di kotak dialog yang terbuka, klik **Jelajahi**, lalu pilih file pendaftaran yang Anda unduh dari server manajemen offline.
7. Dalam kotak dialog yang terbuka, klik **Unduh file**.

   File aktivasi diunduh ke mesin Anda.

Penting

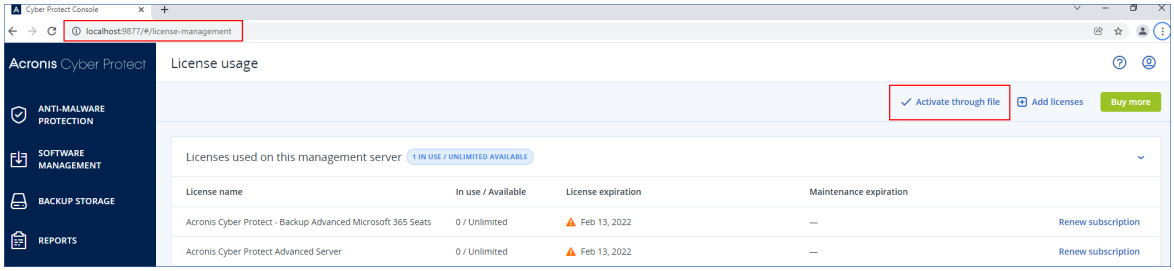
Jika server manajemen offline ini adalah satu-satunya server manajemen di lingkungan Anda, lisensi di akun Acronis Anda akan dialokasikan secara otomatis ke server tersebut. File aktivasi akan berisi informasi ini, sehingga tidak diperlukan alokasi tambahan.

Jika ini bukan satu-satunya server manajemen di lingkungan Anda, setelah aktivasi, Anda harus mengalokasikan lisensi dengan mengikuti prosedur di "Mengalokasikan lisensi ke server manajemen" (hlm. 30).

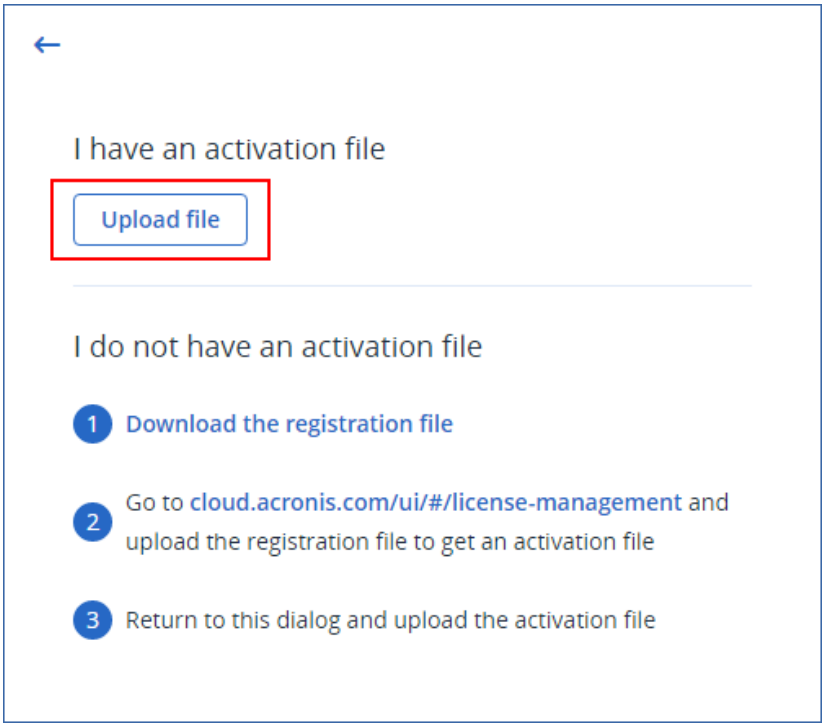
8. Di konsol lokal server manajemen offline (`https://<alamat IP server manajemen Anda>:<port>`), buka kotak dialog **Aktivasi melalui file**.

Catatan

Jika kotak dialog **Aktivasi melalui file** tidak terbuka, navigasikan ke **Pengaturan** > **Penggunaan lisensi**, lalu klik **Aktifkan melalui file**.



9. Di bawah **Saya memiliki file aktivasi**, klik **Unggah file**, lalu pilih file aktivasi yang Anda unduh dari konsol cloud.



Akibatnya, server manajemen offline terdaftar di akun Acronis Anda dan diaktifkan.

Catatan
Anda mungkin tidak dapat mengaktifkan server manajemen yang berjalan pada mesin virtual yang tidak unik secara UUID. UUID mesin virtual mungkin diduplikasi saat Anda mengkloningnya atau mengonversinya dengan VMware vCenter Converter, misalnya. Jika Anda menghadapi masalah serupa, hubungi tim Dukungan kami.

Untuk informasi selengkapnya tentang cara mencegah duplikasi UUID pada mesin virtual VMware, lihat Mengedit mesin virtual dengan UUID.bios duplikat (1002403).

Mengalokasikan lisensi ke server manajemen

Untuk menggunakan lisensi, Anda harus mengalokasikan kuotanya atau bagian dari kuotanya ke server manajemen. Anda dapat mengalokasikan lebih dari satu lisensi ke server manajemen. Selain itu, Anda dapat membagi kuota lisensi dan mengalokasikan pembagian kuota yang berbeda ke server manajemen yang berbeda.

Catatan
Jika hanya ada satu server manajemen di akun Acronis Anda, semua lisensi Anda secara otomatis dialokasikan ke server ini. Untuk mempelajari cara mengalokasikan ulang lisensi ke server manajemen lain, lihat "Mentransfer kuota lisensi ke server manajemen lainnya" (hlm. 33).

Jika Anda memiliki lebih dari satu server manajemen di akun Anda Acronis, lisensi baru akan ditampilkan di bawah **Lisensi yang tidak terisi** di konsol awan (`https://cloud.acronis.com`). Anda perlu mengalokasikan lisensi ini secara manual.

Semua operasi dengan lisensi secara otomatis disinkronkan ke server manajemen online. Untuk menyinkronkan perubahan alokasi ke server manajemen offline, buat file aktivasi baru, lalu ulangi prosedur alokasi. Untuk mempelajari lebih lanjut tentang server manajemen yang berbeda, lihat "Jenis server manajemen" (hlm. 22).

Untuk mengalokasikan lisensi ke server manajemen online

1. Di konsol cloud (`https://cloud.acronis.com`), klik **Pengaturan** > **Penggunaan lisensi**.
2. Navigasi ke server manajemen yang ingin Anda alokasikan lisensi.
3. Klik **Alokasikan lisensi**.
4. Di kotak dialog yang terbuka, tentukan lisensi dan kuota lisensi yang ingin Anda alokasikan ke server ini.
5. Klik **Simpan**.

Akibatnya, informasi lisensi secara otomatis disinkronkan ke server manajemen dan Anda dapat menggunakan lisensi yang dialokasikan untuk melindungi beban kerja Anda.

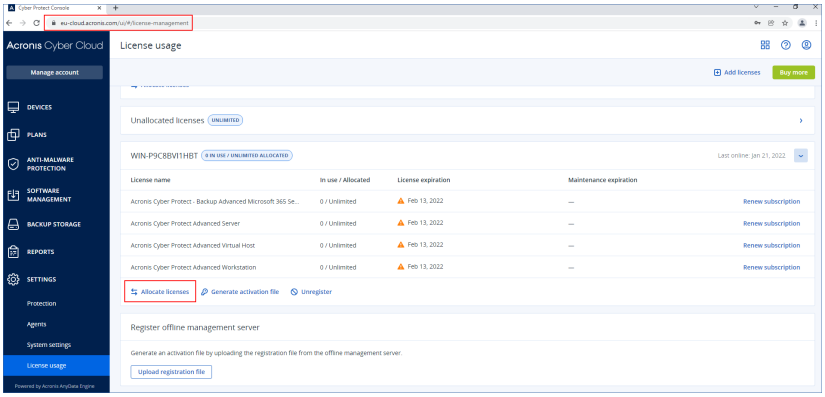
Untuk memodifikasi alokasi, ulangi prosedur di atas.

Penting
Jika kuota lisensi yang dimodifikasi lebih kecil dari jumlah agen perlindungan, agen yang paling sedikit dimuat akan berhenti bekerja. Pilihan ini otomatis. Jika tidak sesuai dengan kebutuhan Anda, tetapkan ulang lisensi yang tersedia secara manual.

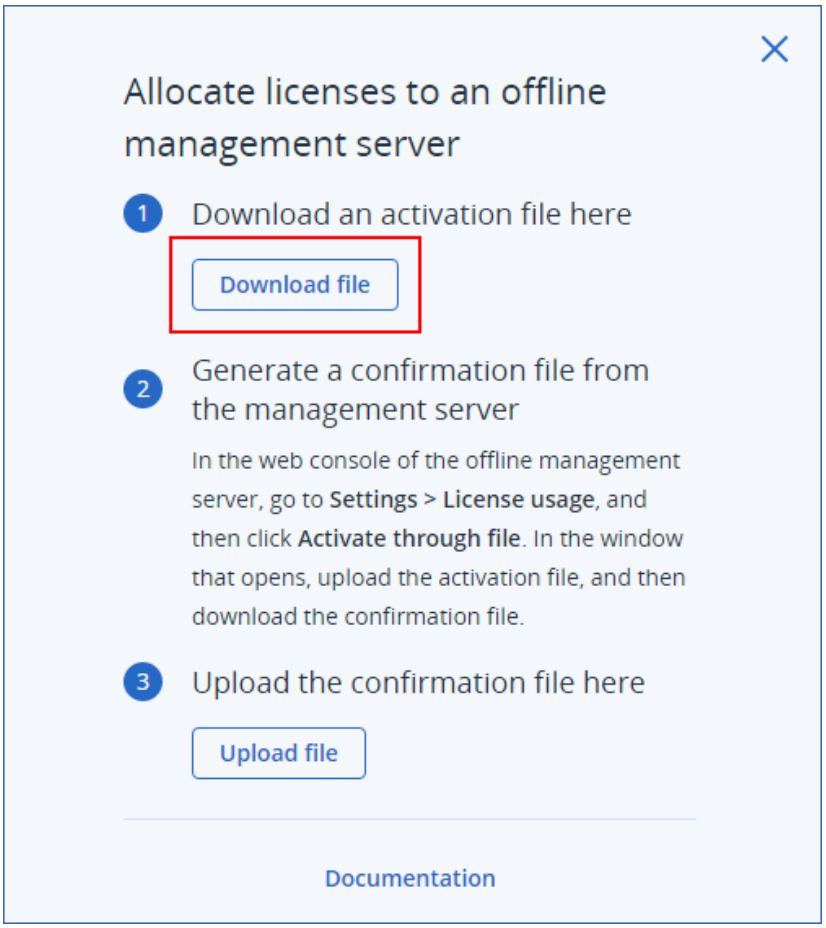
Untuk mengalokasikan lisensi ke server manajemen offline

Untuk mengalokasikan lisensi ke server manajemen offline, Anda harus menggunakan cloud dan konsol lokal. Untuk mengakses konsol cloud, Anda memerlukan mesin kedua yang terhubung ke Internet.

1. Pada mesin dengan akses Internet, masuk ke konsol cloud (`https://cloud.acronis.com`), lalu klik **Pengaturan** > **Penggunaan lisensi**.
2. Navigasi ke server manajemen yang ingin Anda alokasikan lisensi.
3. Klik **Alokasikan lisensi**.

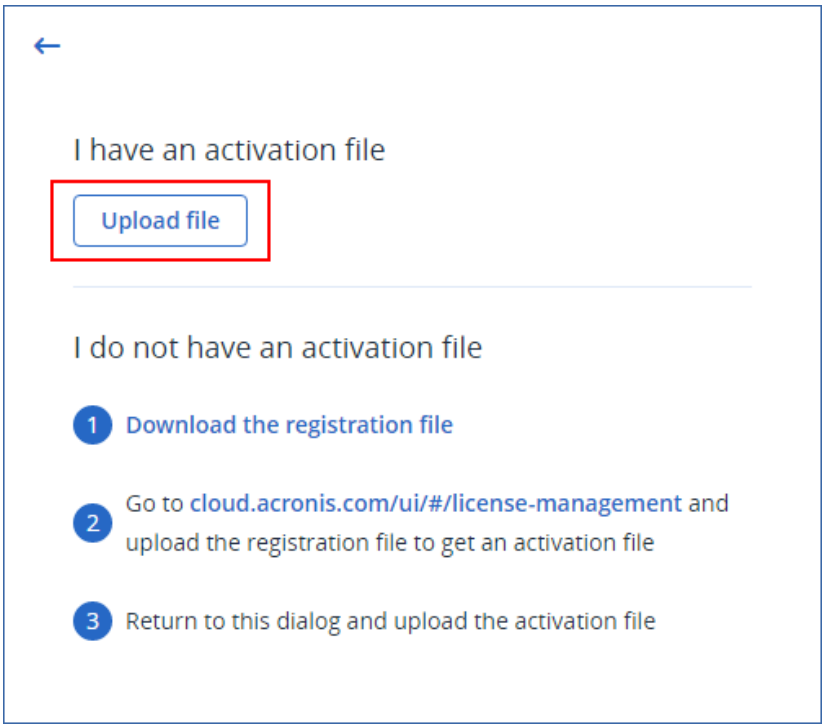


4. Di kotak dialog yang terbuka, tentukan lisensi dan kuota lisensi yang ingin Anda alokasikan ke server ini.
5. Klik **Simpan**.
6. Di kotak dialog **Alokasikan lisensi ke server manajemen offline**, klik **Unduh file**.



File aktivasi diunduh ke mesin Anda.

7. Di konsol lokal server manajemen offline (`https://<alamat IP server manajemen Anda>:<port>`), navigasikan ke **Pengaturan** > **Penggunaan lisensi**, lalu klik **Aktifkan melalui file**.
8. Di kotak dialog yang terbuka, di bawah **Saya memiliki file aktivasi**, klik **Unggah file**, lalu pilih file aktivasi yang Anda unduh dari konsol cloud.



Akibatnya, informasi lisensi disinkronkan antara akun Acronis Anda dan server manajemen offline.

Untuk menambah kuota lisensi yang dialokasikan, ulangi prosedur di atas.

Untuk mengurangi kuota lisensi yang dialokasikan, lihat "Mengurangi kuota lisensi yang dialokasikan ke server manajemen offline" (hlm. 34).

Mentransfer kuota lisensi ke server manajemen lainnya

Anda dapat mentransfer kuota lisensi dari satu server manajemen ke yang lainnya. Opsi ini mungkin berguna ketika lisensi yang dialokasikan ke server manajemen tidak digunakan oleh beban kerja apa pun dan Anda memerlukan lebih banyak lisensi untuk server manajemen lain.

Catatan
Jika hanya ada satu server manajemen di akun Acronis Anda, semua lisensi Anda secara otomatis dialokasikan ke server ini.

Jika Anda memiliki lebih dari satu server manajemen di akun Acronis Anda, lisensi baru akan ditampilkan di bawah **Lisensi yang tidak terisi** di konsol awan (`https://cloud.acronis.com`). Anda perlu mengalokasikan lisensi ini secara manual.

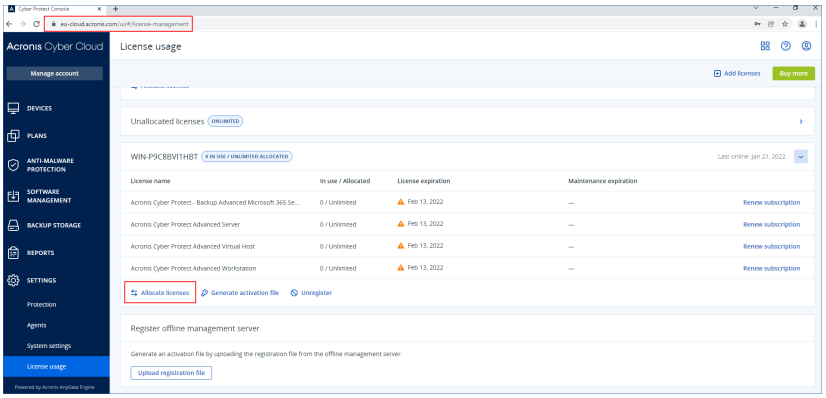
Untuk mentransfer kuota lisensi ke server manajemen lainnya

1. Kurangi kuota lisensi yang dialokasikan ke server manajemen asli dengan mengikuti prosedur di "Mengalokasikan lisensi ke server manajemen" (hlm. 30).
   Kuota lisensi yang dirilis muncul di bagian **Lisensi yang tidak terisi** di konsol awan.
2. Alokasikan kuota lisensi ke server manajemen kedua dengan mengikuti prosedur di "Mengalokasikan lisensi ke server manajemen" (hlm. 30).

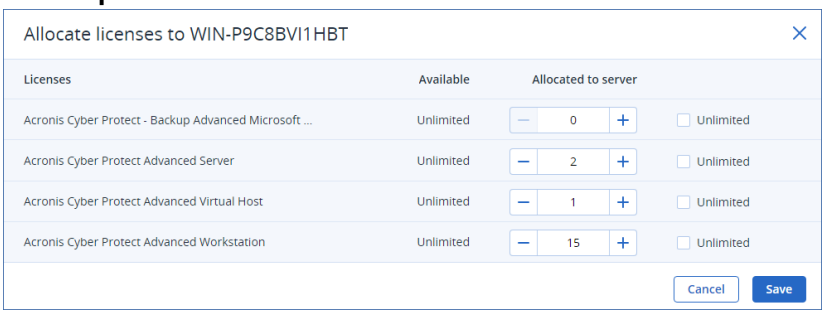
Mengurangi kuota lisensi yang dialokasikan ke server manajemen offline

Untuk mengurangi kuota lisensi yang dialokasikan ke server manajemen offline, Anda harus menggunakan cloud dan konsol lokal. Untuk mengakses konsol cloud, Anda memerlukan mesin kedua yang terhubung ke Internet.

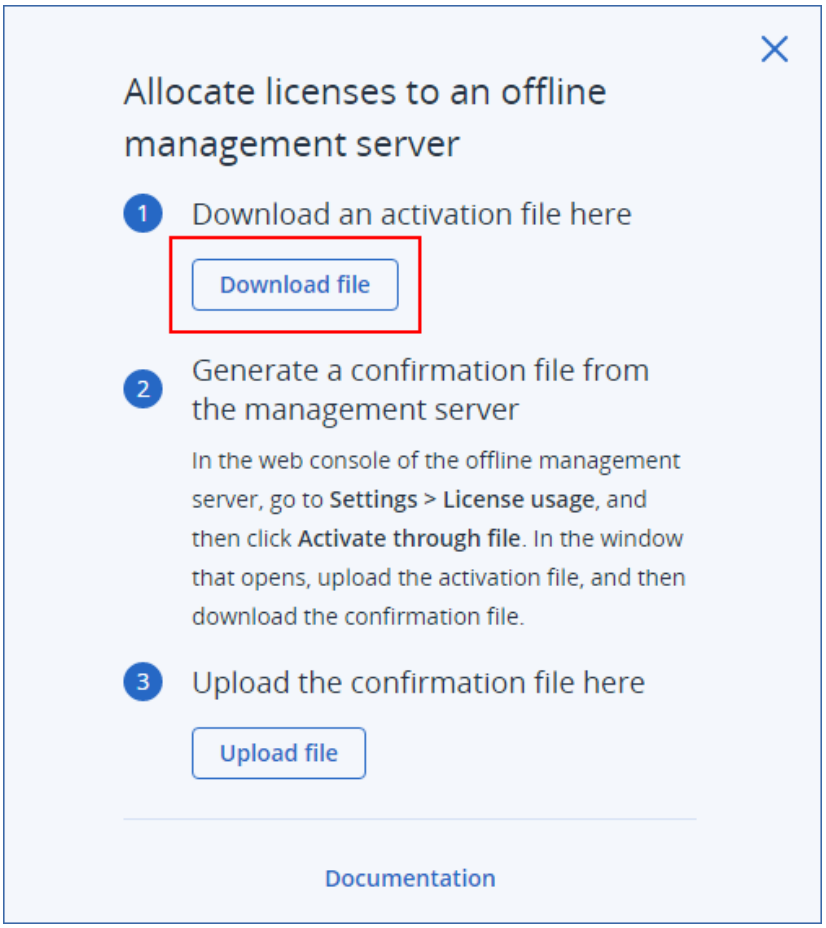
1. Pada mesin dengan akses ke Internet, masuk ke konsol cloud (`https://cloud.acronis.com`), lalu klik **Pengaturan** > **Penggunaan lisensi**.
2. Navigasikan ke server manajemen yang ingin Anda alokasikan lisensinya, lalu klik **Alokasikan lisensi**.



3. Di kotak dialog yang terbuka, ubah lisensi dan kuota lisensi yang dialokasikan ke server ini, lalu klik **Simpan**.

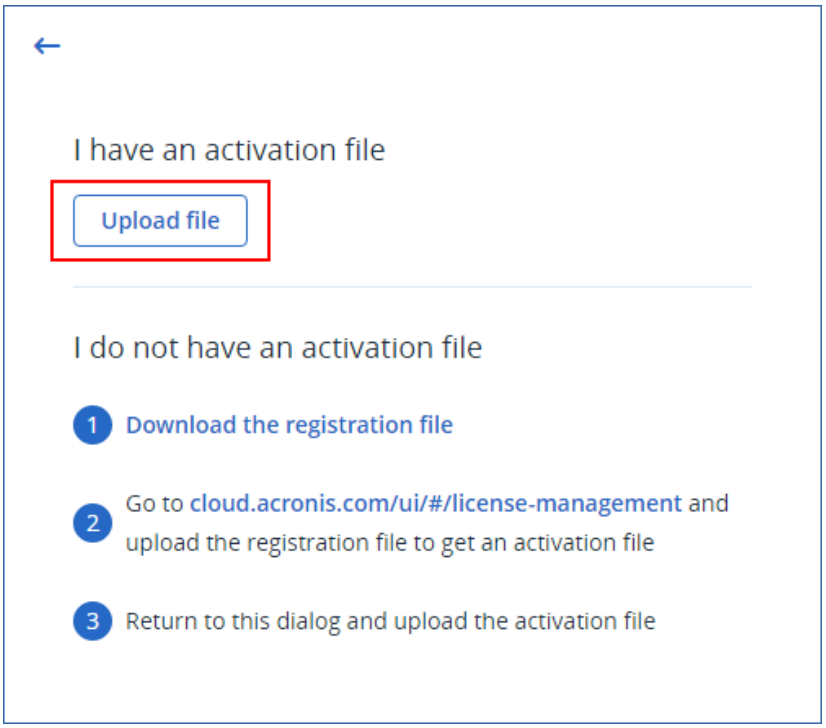


   Alokasi baru sekarang tertunda. Untuk membatalkannya, klik **Hapus alokasi ini**.
4. Di kotak dialog **Alokasikan lisensi ke server manajemen offline**, klik **Unduh file**.

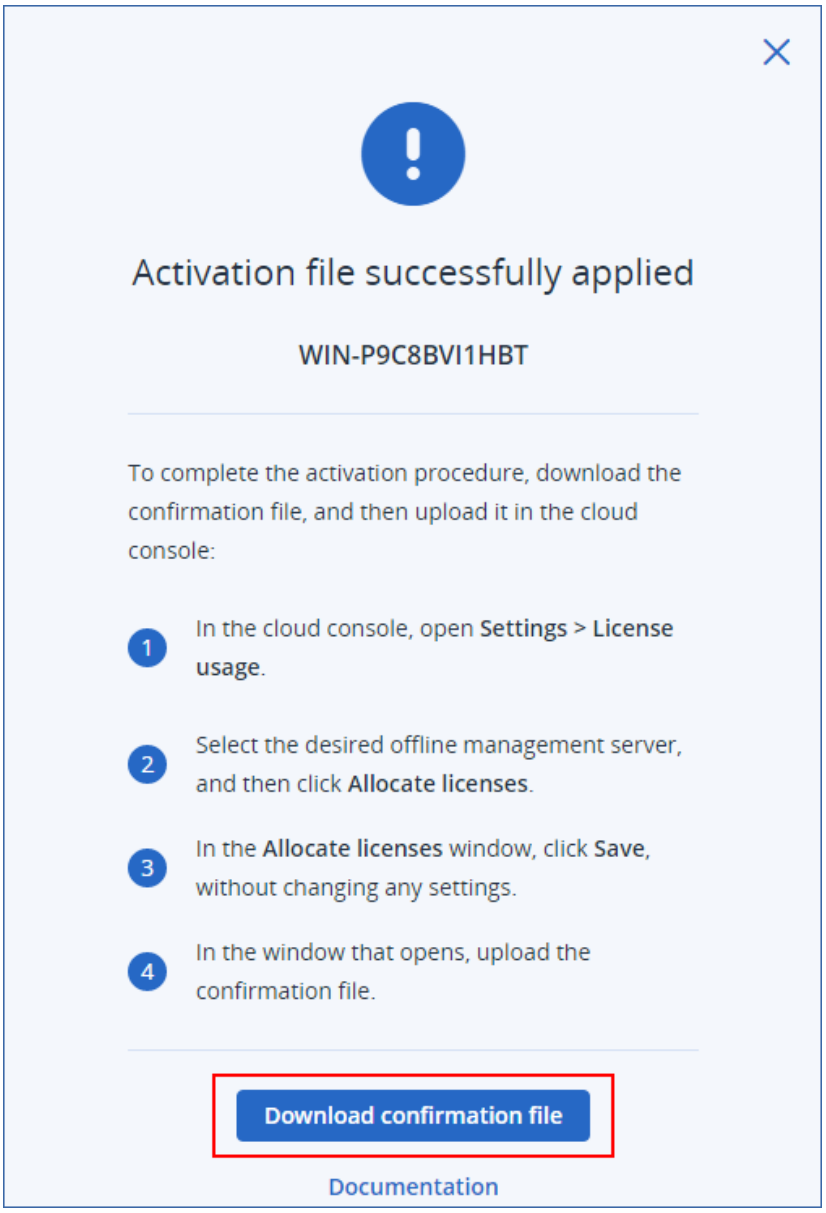


File aktivasi diunduh ke mesin Anda.

5. Di konsol lokal server manajemen offline (`https://<alamat IP server manajemen Anda>:<port>`), navigasikan ke **Pengaturan** > **Penggunaan lisensi**, lalu klik **Aktifkan melalui file**.
6. Di kotak dialog yang terbuka, di bawah **Saya memiliki file aktivasi**, klik **Unggah file**, lalu pilih file aktivasi yang Anda unduh dari konsol cloud.

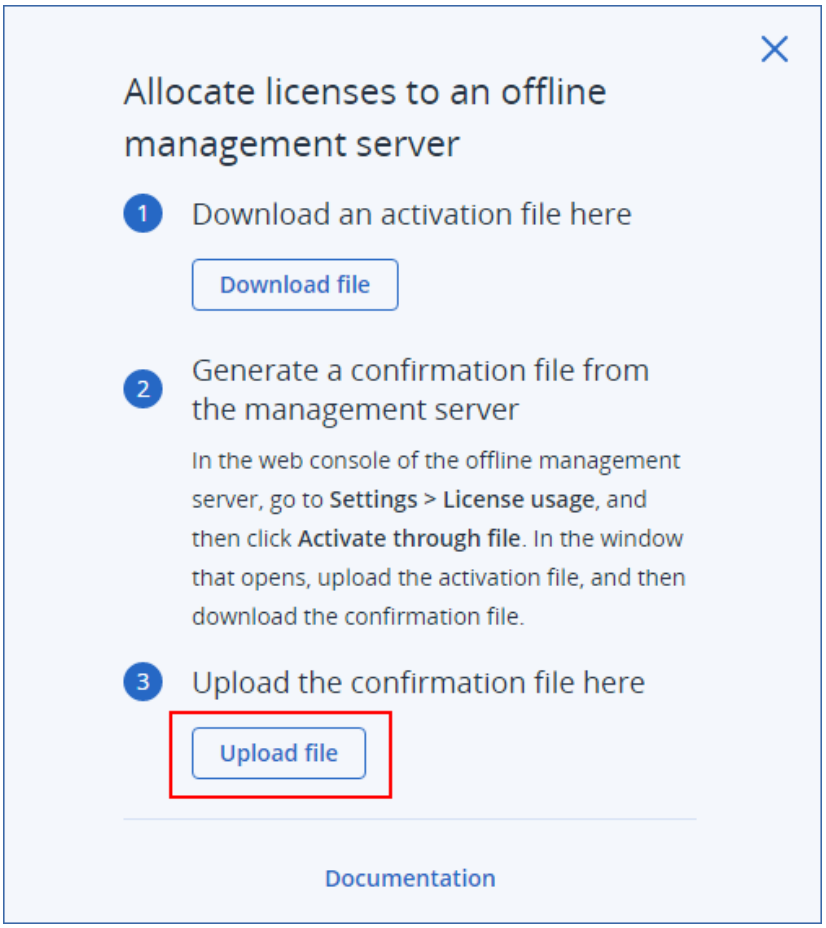


7. Dalam kotak dialog yang terbuka, klik **Unduh file konfirmasi**.



File konfirmasi diunduh ke mesin Anda.

8. Di konsol cloud (`https://cloud.acronis.com`), klik **Pengaturan** > **Penggunaan lisensi**.
9. Navigasikan ke server manajemen yang ingin Anda alokasikan lisensinya, lalu klik **Alokasikan lisensi**.
10. Dalam kotak dialog yang terbuka, klik **Simpan**, tanpa mengubah pengaturan apa pun.
11. Di kotak dialog **Alokasikan lisensi ke server manajemen offline**, klik **Unggah file**, lalu pilih file konfirmasi yang Anda unduh dari server manajemen offline.



Akibatnya, informasi lisensi disinkronkan antara akun Acronis Anda dan server manajemen offline.

Penting
Jika kuota lisensi yang dimodifikasi lebih kecil dari jumlah agen perlindungan, agen yang paling sedikit dimuat akan berhenti bekerja. Pilihan ini otomatis. Jika tidak sesuai dengan kebutuhan Anda, tetapkan ulang lisensi yang tersedia secara manual.

Penetapan lisensi ke beban kerja

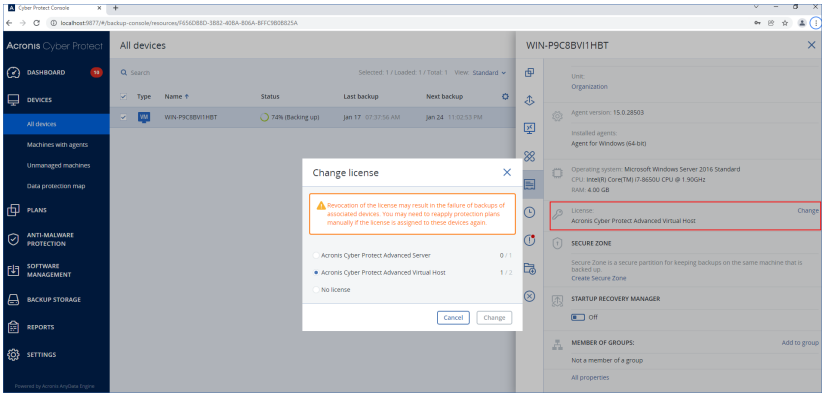
Server manajemen mendistribusikan lisensi yang dialokasikan antara beban kerja yang terdaftar di server ini.

Server manajemen menetapkan lisensi untuk beban kerja pada saat Anda pertama kali menerapkan rencana proteksi untuk beban kerja ini. Jika lebih dari satu lisensi dialokasikan ke server manajemen, lisensi yang paling sesuai akan diberikan kepada beban kerja, tergantung pada jenis beban kerja, sistem operasi, dan tingkat perlindungan yang diperlukan.

Untuk memeriksa lisensi yang ditetapkan, di konsol web server manajemen, pilih beban kerja yang diinginkan, lalu klik **Rincian**.

Untuk menetapkan kembali lisensi ke beban kerja secara manual

1. Di konsol web server manajemen, klik **Perangkat**, lalu pilih beban kerja yang diinginkan.
2. Klik **Detail**.
3. [Untuk server manajemen lokal] Navigasikan ke bagian **Lisensi**, lalu klik **Ubah**.
4. [Untuk server manajemen awn] Navigasikan ke bagian **Kuota layanan**, lalu klik **Ubah**.
5. Pilih lisensi (kuota layanan) yang diinginkan, lalu klik **Ubah**.



Pembatasan

Untuk server manajemen offline, penggunaan kuota lisensi saat ini hanya ditampilkan di konsol lokal. Server manajemen offline tidak menyinkronkan data ini ke akun Acronis Anda dan tidak tersedia di konsol cloud.

Masalah yang diketahui

Di konsol cloud, penggunaan lisensi atau penetapan lisensi **Virtual Host** mungkin tidak ditampilkan dengan benar. Untuk informasi lebih lanjut, lihat artikel basis pengetahuan ini.

Membatalkan pendaftaran server manajemen

Untuk membatalkan pendaftaran server manajemen online

1. Di konsol awan (`https://cloud.acronis.com`), klik **Pengaturan** > **Penggunaan lisensi**.
2. Navigasi ke server manajemen yang diinginkan, lalu klik **Batalkan pendaftaran**.
3. Jendela **Batalkan pendaftaran server manajemen** ditampilkan.
4. Masukkan alamat email yang terkait dengan akun untuk mengonfirmasi pembatalan pendaftaran.
5. Klik **Batalkan pendaftaran**.

Hasilnya, semua lisensi yang dialokasikan ke server yang tidak terdaftar dilepaskan dan dapat dialokasikan ke server manajemen lain di akun Anda. Di konsol lokal server manajemen yang tidak terdaftar, lisensi direset ke nol.

Untuk membatalkan pendaftaran server manajemen offline

Ada dua titik masuk yang berbeda untuk membatalkan pendaftaran server manajemen offline:

Di konsol lokal:

1. Di konsol lokal, klik **Batalkan pendaftaran** di baris tempat akun ditampilkan.. Jendela **Batalkan pendaftaran server manajemen** ditampilkan.
2. Di kolom **Masuk**, ketikkan alamat email yang terkait dengan administrator lokal.
3. Klik **Batalkan pendaftaran**.
4. Layar pop-up **Batalkan pendaftaran berhasil** ditampilkan.
5. Klik **Unduh file pembatalan pendaftaran**.
6. Di konsol awan, klik **Batalkan pendaftaran**. Jendela **Batalkan pendaftaran server manajemen** ditampilkan.
7. Klik **Batalkan pendaftaran server manajemen offline**. Jendela **Batalkan pendaftaran server manajemen offline** ditampilkan.
8. Klik **Jelajahi**, lalu pilih file batalkan pendaftaran yang Anda unduh dari konsol lokal.
9. Klik **Batalkan pendaftaran**.

Di konsol awan:

1. Pada mesin dengan akses Internet, masuk ke konsol awan (`https://cloud.acronis.com`), lalu klik **Pengaturan** > **Penggunaan lisensi**.
2. Navigasi ke server manajemen yang diinginkan, lalu klik **Batalkan pendaftaran**. Jendela **Batalkan pendaftaran server manajemen** ditampilkan.
3. Klik **Batalkan pendaftaran server manajemen offline**. Jendela **Batalkan pendaftaran server manajemen offline** ditampilkan.
4. Di konsol lokal server manajemen yang ingin Anda batalkan pendaftarannya (`https://<alamat IP server manajemen Anda>:<port>`), buka **Pengaturan** > **Penggunaan lisensi**, lalu klik **Batalkan pendaftaran**. File pembatalan registrasi diunduh ke mesin Anda.
5. Di konsol awan, kembali ke jendela **Batalkan pendaftaran server manajemen offline**.
6. Klik **Jelajahi**, lalu pilih file batalkan pendaftaran yang Anda unduh dari konsol lokal.
7. Klik **Batalkan pendaftaran**.
8. Atau, jika Anda tidak memiliki akses ke mesin tempat server manajemen diinstal, klik **Saya tidak memiliki akses ke mesin dengan server manajemen**.

   Peringatan!
   Mesin ini akan diblokir dan dihapus secara permanen dari akun Anda. Anda tidak akan dapat mendaftarkan server manajemen di mesin ini lagi.

Hasilnya, semua lisensi yang dialokasikan ke server yang tidak terdaftar dilepaskan dan dapat dialokasikan ke server manajemen lain di akun Anda. Di konsol lokal server manajemen yang tidak terdaftar, lisensi direset ke nol.

Lisensi di Acronis Cyber Protect 15 Update 2 dan versi sebelumnya

Untuk mulai menggunakan versi Acronis Cyber Protect 15 Update 2 dan versi sebelumnya, Anda perlu menambahkan setidaknya satu kunci lisensi ke server manajemen. Lisensi ditetapkan secara otomatis ke mesin ketika rencana proteksi diterapkan.

Lisensi juga dapat ditetapkan dan dicabut secara manual. Operasi manual dengan lisensi hanya tersedia untuk administrator organisasi. Untuk informasi lebih lanjut tentang administrator, lihat "Unit dan akun administratif" (hlm. 635).

Menambahkan kunci lisensi ke server manajemen

Di Acronis Cyber Protect15 Update 2 dan versi sebelumnya, Anda menambahkan kunci lisensi ke server manajemen.

Untuk menambahkan kunci lisensi ke server manajemen

1. Di Cyber Protect konsol web, buka **Pengaturan** > **Lisensi**.
2. Klik **Tambah kunci**.
3. Masukkan satu kunci lisensi atau lebih, dengan satu kunci per baris.
4. Klik **Tambah**.
5. [Saat menambahkan kunci lisensi berlangganan] Untuk mengaktifkan lisensi berlangganan, masuk ke akun Acronis Anda.
   a. Di formulir masuk, masukkan kredensial yang Anda gunakan untuk Portal Pelanggan Acronis (`https://account.acronis.com`), lalu klik **Masuk**.
   b. Konfirmasikan akun Anda, lalu klik **Sinkronkan**.
   c. Setelah operasi selesai, klik **Selesai**.
6. Di panel **Tambahkan kunci lisensi**, klik **Selesai**.

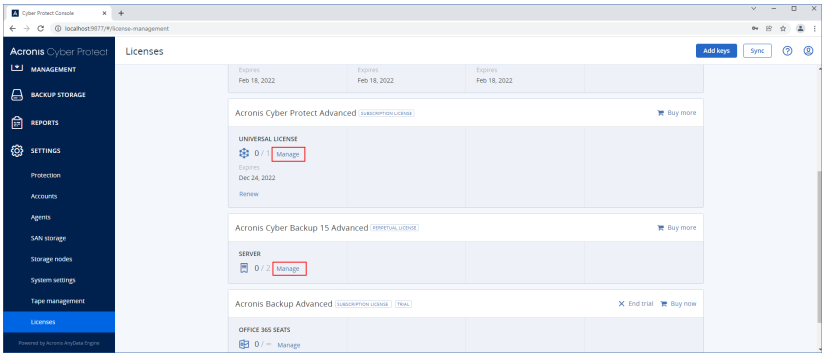
Catatan
Anda dapat secara otomatis mengimpor kunci lisensi berlangganan yang terdaftar di akun Acronis Anda, alih-alih menambahkannya ke server manajemen lagi. Untuk mengimpor kunci lisensi, di panel **Tambahkan kunci lisensi**, klik **Sinkronkan dengan akun Acronis**, lalu masuk ke akun Acronis Anda.

Mengelola lisensi berlangganan

Sebelum menetapkan lisensi ke beban kerja, Anda harus menambahkan kunci lisensi ke server manajemen. Untuk informasi lebih lanjut tentang cara melakukannya, lihat "Menambahkan kunci lisensi ke server manajemen" (hlm. 41).

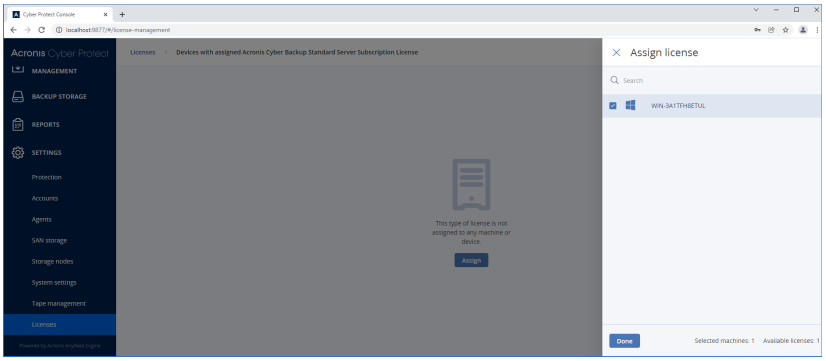
Untuk menetapkan lisensi berlangganan ke beban kerja

1. Di Cyber Protect konsol web, buka **Pengaturan** > **Lisensi**.
2. Arahkan ke lisensi yang diinginkan, lalu klik **Kelola**.



3. Klik **Tetapkan**.

   Beban kerja yang dapat Anda tetapkan lisensi ini akan ditampilkan.



4. Pilih beban kerja, lalu klik **Selesai**.

Untuk mencabut lisensi berlangganan dari beban kerja

1. Di Cyber Protect konsol web, buka **Pengaturan** > **Lisensi**.
2. Arahkan ke lisensi yang diinginkan, lalu klik **Kelola**.

   Semua beban kerja yang diberikan lisensi ini akan ditampilkan.
3. Pilih beban kerja dari mana Anda ingin mencabut lisensi.
4. Klik **Cabut**.
5. Konfirmasi keputusan Anda.

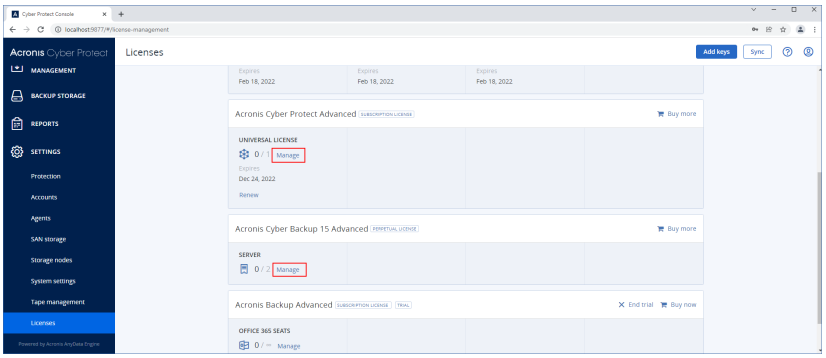
   Lisensi yang dicabut dilepaskan dan Anda dapat menetapkannya ke beban kerja lain.

Mengelola lisensi seumur hidup

Sebelum menetapkan lisensi ke beban kerja, Anda harus menambahkan kunci lisensi ke server manajemen. Untuk informasi lebih lanjut tentang cara melakukannya, lihat "Menambahkan kunci lisensi ke server manajemen" (hlm. 41).

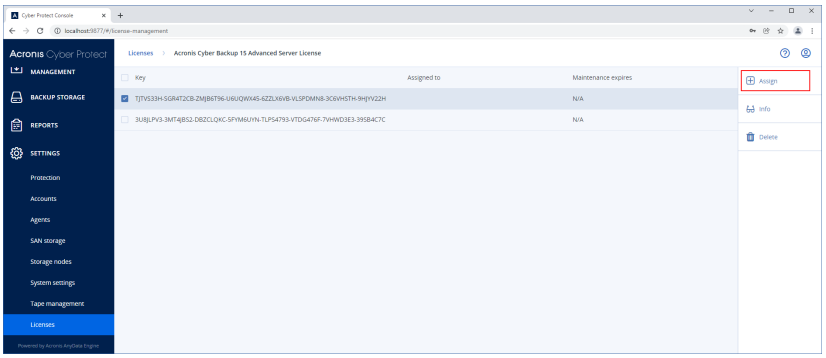
Untuk menetapkan lisensi abadi ke beban kerja

1. Di Cyber Protect konsol web, buka **Pengaturan** > **Lisensi**.
2. Arahkan ke lisensi yang diinginkan, lalu klik **Kelola**.



Kunci lisensi yang sesuai dengan lisensi yang dipilih akan ditampilkan.

3. Pilih kunci lisensi yang ingin Anda tetapkan ke beban kerja.
4. Klik **Tetapkan**.



Beban kerja yang dapat Anda tetapkan kunci lisensi ini akan ditampilkan.

5. Pilih beban kerja, lalu klik **Selesai**.

Untuk mencabut lisensi abadi dari beban kerja

1. Di Cyber Protect konsol web, buka **Pengaturan** > **Lisensi**.
2. Pilih lisensi yang diinginkan, lalu klik **Kelola**.

   Kunci lisensi yang sesuai dengan lisensi yang dipilih akan ditampilkan. Periksa beban kerja yang diberikan kunci lisensi ini di kolom **Ditugaskan ke**.
3. Pilih kunci lisensi yang ingin Anda cabut.
4. Klik **Cabut**.
5. Konfirmasi keputusan Anda.

   Kunci lisensi yang dicabut tetap ada dalam daftar lisensi dan Anda dapat menetapkannya ke beban kerja lain.

Instalasi

Instalasi

Acronis Cyber Protect mendukung dua metode penyebaran: lokal dan awan. Perbedaan utama di antara keduanya adalah lokasi server manajemen Acronis Cyber Protect.

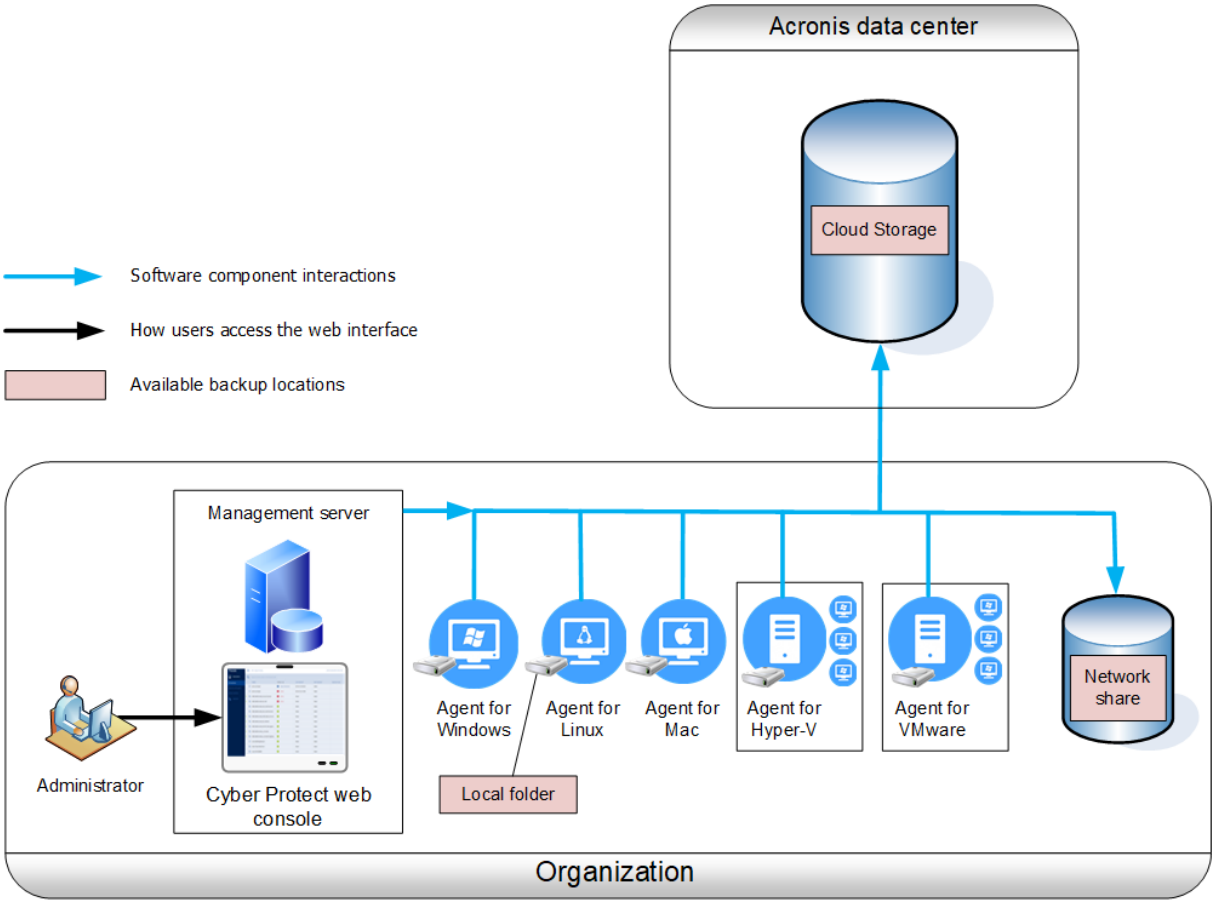
Server manajemen adalah titik pusat untuk mengelola semua cadangan Anda. Dengan penyebaran lokal, peralatan tersebut diinstal di jaringan lokal Anda; dengan penyebaran awan, peralatan berada di salah satu pusat data Acronis. Antarmuka web ke server ini disebut dengan konsol web Cyber Protect.

Server manajemen bertanggung jawab untuk komunikasi dengan agen perlindungan dan menjalankan fungsi manajemen rencana umum. Sebelum melakukan setiap aktivitas perlindungan, agen merujuk ke server manajemen untuk memverifikasi prasyarat. Terkadang, koneksi ke server manajemen bisa terputus, sehingga dapat menghalangi penyebaran rencana proteksi baru. Meski demikian, jika rencana proteksi telah disebarkan ke mesin, agen akan melanjutkan operasi perlindungan selama 30 hari setelah komunikasi dengan server manajemen terputus.

Kedua jenis penyebaran mengharuskan agen perlindungan untuk diinstal pada setiap mesin yang ingin Anda cadangkan. Jenis penyimpanan yang didukung juga sama. Ruang penyimpanan awan dijual terpisah dari lisensi Acronis Cyber Protect.

Penyebaran di lokasi

Penyebaran di lokasi artinya semua komponen produk diinstal di jaringan lokal Anda. Ini adalah satu-satunya metode penyebaran yang tersedia dengan lisensi seumur hidup. Anda juga harus menggunakan metode ini jika mesin Anda tidak terhubung ke Internet.



Lokasi server manajemen

Anda dapat menginstal server manajemen pada mesin yang menjalankan Windows atau Linux.

Instalasi di Windows disarankan karena Anda akan dapat menyebarkan agen ke mesin lain dari server manajemen. Dengan lisensi Lanjutan, dimungkinkan untuk membuat unit organisasi dan menambahkan administrator ke dalamnya. Dengan cara ini, Anda dapat mendelegasikan manajemen perlindungan ke orang lain yang izin aksesnya akan dibatasi secara ketat untuk unit terkait.

Instalasi di Linux direkomendasikan hanya di lingkungan Linux. Anda akan perlu menginstal agen secara lokal di mesin yang ingin Anda buat cadangannya.

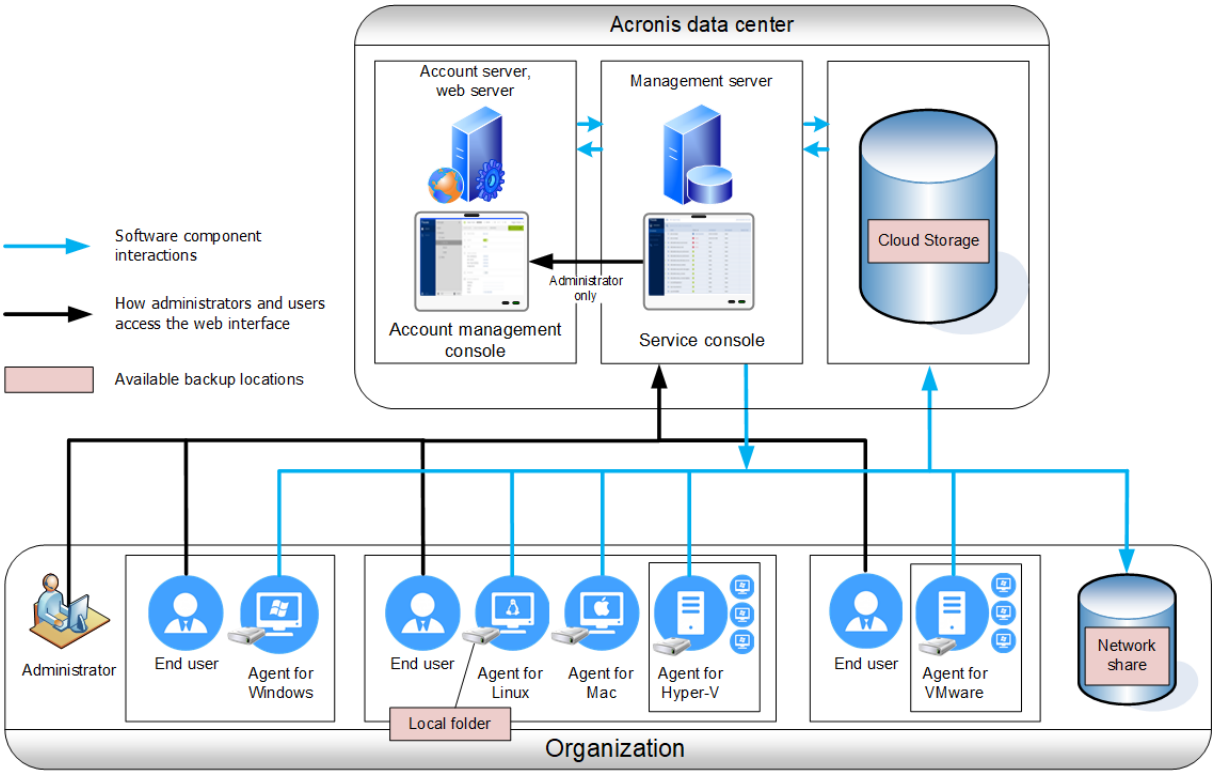
Penyebaran awan

Penyebaran awan berarti bahwa server manajemen terletak di salah satu pusat data Acronis. Pendekatan ini bermanfaat agar Anda tidak perlu memelihara server manajemen di jaringan lokal Anda. Anda dapat menganggap Acronis Cyber Protect sebagai layanan perlindungan cyber yang diberikan kepada Anda oleh Acronis.

Akses ke server akun memungkinkan Anda untuk membuat akun pengguna, menetapkan kuota penggunaan layanan untuknya, dan membuat grup pengguna (unit) untuk mencerminkan struktur

organisasi Anda. Setiap pengguna dapat mengakses konsol web Cyber Protect, mengunduh agen yang diperlukan, dan menginstalnya di mesin mereka dalam hitungan menit.

Akun administrator dapat dibuat di level unit atau organisasi. Setiap akun memiliki pandangan yang dicakupkan pada bidang kendali mereka. Pengguna hanya memiliki akses ke cadangan mereka sendiri.



Tabel berikut merangkum perbedaan antara penyebaran di lokasi dan awan. Setiap kolom mencantumkan fitur yang tersedia hanya di jenis penyebaran terkait.

Penyebaran di lokasi	Penyebaran awan
• Lisensi abadi dapat digunakan • Server manajemen lokal yang dapat digunakan di lingkungan air-gap* • Server SFTP sebagai lokasi pencadangan • Acronis Infrastruktur Cyber sebagai lokasi pencadangan • Alat rekaman dan Simpul Penyimpanan Acronis sebagai lokasi pencadangan** • Tingkatkan versi Acronis Cyber Protect sebelumnya, termasuk Acronis Backup untuk VMware	• Pencadangan awan ke awan untuk data Microsoft 365, termasuk perlindungan grup, folder umum, OneDrive***, dan data SharePoint Online • Pencadangan awan ke awan untuk data Google Workspace • Agen untuk Mac mendukung prosesor berbasis x64 maupun ARM, seperti Apple silicon M1 dan M2 • Agen untuk Virtuozzo (pencadangan mesin virtual Virtuozzo di tingkat hypervisor) • Agen untuk oVirt (pencadangan mesin virtual KVM di tingkat hypervisor) • Agen untuk Virtuozzo Hybrid Infrastructure

	(pencadangan mesin virtual Virtuozzo Hybrid Infrastructure di tingkat hypervisor) • Pemulihan bencana sebagai layanan awan****

* Untuk informasi lebih lanjut tentang mengaktifkan server manajemen di lingkungan air-gap, lihat "Untuk mengaktifkan server manajemen offline" (hlm. 27).

** Fitur ini tidak tersedia pada edisi Standar.

***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 di arsip.

**** Fitur ini hanya tersedia dengan add-on Pemulihan Bencana layanan.

Komponen

Agen

Agen adalah aplikasi yang melakukan pencadangan data, pemulihan data, dan operasi lain pada mesin yang dikelola oleh Acronis Cyber Protect.

Agen untuk Windows diinstal bersama dengan Agen untuk Exchange, Agen untuk SQL, Agen untuk Active Directory, dan Agen untuk Oracle. Jika Anda menginstal, misalnya, Agen untuk SQL, Anda juga akan dapat mencadangkan seluruh mesin tempat agen diinstal.

Beberapa agen hanya dapat diinstal pada mesin dengan peran atau aplikasi tertentu, misalnya, Agen untuk Hyper-V diinstal pada mesin yang menjalankan peran Hyper-V, Agen untuk SQL – pada mesin yang menjalankan database SQL, Agen untuk Exchange – pada mesin yang menjalankan peran Kotak Surat Server Microsoft Exchange, dan Active Directory – pada pengontrol domain.

Pilih agen, tergantung pada apa yang akan Anda cadangkan. Tabel berikut meringkas informasi, untuk membantu Anda membuat keputusan.

Apa yang akan Anda cadangkan?	**Agen mana yang akan diinstal?**	**Di mana akan menginstalnya?**	**Ketersediaan agen**	
			Lokal	**Awan**
Mesin fisik				
Disk, volume, dan file di mesin fisik yang menjalankan Windows	Agen untuk Windows	Di mesin yang akan dicadangkan.	+	+
Disk, volume, dan file di mesin fisik yang menjalankan Linux	Agen untuk Linux		+	+

Disk, volume, dan file di mesin fisik menjalankan macOS	Agen untuk Mac		+	+
Aplikasi				
Database SQL	Agen untuk SQL	Di mesin yang menjalankan Microsoft SQL Server.	+	+
Database dan kotak surat Exchange	Agen untuk Exchange	Pada mesin yang menjalankan peran Kotak surat Microsoft Exchange Server.* Jika hanya diperlukan pencadangan kotak surat, agen dapat diinstal pada mesin Windows apa pun yang memiliki akses jaringan ke mesin yang menjalankan peran Akses Klien pada Microsoft Exchange Server.	+ Tidak ada cadangan kotak surat	+
Kotak surat Microsoft 365	Agen untuk Office 365	Di mesin Windows yang terhubung ke Internet.	+	+
Mesin yang menjalankan Active Directory Domain Services	Agen untuk Active Directory	Pada pengontrol domain.	+	+
Mesin yang menjalankan Database Oracle	Agen untuk Oracle	Pada mesin yang menjalankan Database Oracle.	+	-
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	Pada host ESXi.	+	+

	VMware (Virtual Appliance)			
Mesin virtual Hyper-V	Agen untuk Hyper-V	Pada host Hyper-V.	+	+
Mesin virtual Scale Computing HC3	Agen untuk Scale Computing HC3	Di host Scale Computing HC3.	+	+
Mesin virtual yang dihosting di Windows Azure	Sama halnya untuk mesin fisik***	Di mesin yang akan dicadangkan.	+	+
Mesin virtual yang dihosting di Amazon EC2			+	+
Mesin virtual Citrix XenServer			+****	+
Mesin virtual Red Hat Virtualization (RHV/RHEV)				
Mesin Virtual berbasis Kernel (KVM)				
Mesin virtual Oracle				
Mesin virtual Nutanix AHV				
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 instruksi mendetail, lihat "Pencadangan bebas LAN".

***Mesin virtual dianggap virtual jika dicadangkan oleh agen eksternal. Jika agen diinstal di sistem tamu, operasi pencadangan dan pemulihan akan sama dengan mesin fisik. Meskipun demikian, mesin dianggap sebagai virtual ketika Anda menetapkan kuota untuk jumlah mesin dalam penyebaran awan.

****Dengan lisensi Host Virtual Lanjutan Acronis Cyber Protect, mesin virtual ini dianggap sebagai virtual (lisensi per host digunakan). Dengan lisensi Host Virtual Acronis Cyber Protect, mesin ini dianggap sebagai fisik (lisensi per mesin digunakan).

Komponen-komponen lainnya

Komponen	Fungsi	Di mana akan menginstalnya?	Ketersediaan	
			Lokal	Awan
Server Manajemen	Server Manajemen adalah titik pusat untuk mengelola semua cadangan Anda. Dengan penyebaran di lokasi, server diinstal di jaringan lokal Anda. Server ini mengelola agen dan menyediakan antarmuka web untuk pengguna.	Di mesin yang menjalankan Windows atau Linux.	+	-
Komponen untuk Instalasi Jarak Jauh	Simpan paket instalasi agen ke folder lokal.	Di mesin Windows yang menjalankan server manajemen.	+	-
Layanan Pemindaian	Komponen opsional yang memungkinkan pemindaian antimalware pada pencadangan di penyimpanan awan, atau di folder lokal atau jaringan. Layanan Pemindaian memerlukan database Microsoft SQL Server atau PostgreSQL. Ini tidak kompatibel dengan the database SQLite default yang digunakan server manajemen.	Di mesin Windows atau Linux yang menjalankan server manajemen.	+	-

Pembangun Media Yang Dapat Di-Boot	Membuat media yang dapat di-boot.	Di mesin yang menjalankan Windows atau Linux.	+	-
Command-Line Tool	Mendukung antarmuka baris perintah dengan utilitas **acrocmd**. **acrocmd** tidak berisi alat bantu apa pun yang mengeksekusi perintah secara fisik. Alat ini hanya menyediakan antarmuka baris perintah untuk komponen - agen Cyber Protect dan server manajemen.	Di mesin yang menjalankan Windows, Linux, atau macOS.	+	+
Monitor Acronis Cyber Protect 15	Menyediakan antarmuka pengguna grafis untuk Agen untuk Windows dan Agen untuk Mac. Ini menampilkan informasi tentang status proteksi mesin tempat agen diinstal, dan memungkinkan penggunanya untuk mengonfigurasikan pengaturan cadangan enkripsi dan server proxy. Di Windows, Acronis Cyber Protect 15 Monitor meminta agar Agen untuk Windows diinstal di mesin yang sama.	Di mesin yang menjalankan Windows atau macOS.	+	+
Simpul Penyimpanan	Menyimpan cadangan. Diperlukan untuk katalogisasi dan deduplikasi. Simpul Penyimpanan meminta agar Agen untuk Windows diinstal di mesin yang sama.	Di mesin yang menjalankan Windows.	+	-

Layanan Katalog	Melakukan katalogisasi cadangan di simpul penyimpanan.	Di mesin yang menjalankan Windows.	+	-
Server PXE	Memungkinkan mesin boot ke media yang dapat di-boot melalui jaringan.	Di mesin yang menjalankan Windows.	+	-

Menggunakan Acronis Cyber Protect dengan solusi keamanan lainnya di lingkungan Anda

Anda dapat menggunakan Acronis Cyber Protect dengan atau tanpa solusi keamanan lainnya, seperti perangkat lunak antivirus yang berdiri sendiri, di lingkungan Anda.

Tanpa solusi keamanan lainnya, Anda dapat menggunakan Acronis Cyber Protect untuk perlindungan cyber lengkap atau untuk pencadangan dan pemulihan konvensional, tergantung pada lisensi serta kebutuhan Anda. Untuk informasi lebih lanjut mengenai fitur yang tersedia dalam setiap lisensi, lihat "Perbandingan Edisi Acronis Cyber Protect 15 termasuk penyebaran Awan." Anda dapat menyesuaikan cakupan rencana proteksi dengan hanya mengaktifkan modul yang Anda butuhkan.

Anda dapat memilih Acronis Cyber Protect untuk perlindungan cyber yang lengkap, termasuk perlindungan dari virus dan malware lainnya, meskipun memiliki solusi keamanan lain di lingkungan Anda. Dalam hal ini, Anda perlu menonaktifkan atau menghapus solusi keamanan lainnya untuk menghindari konflik.

Atau, Anda mungkin ingin meningkatkan perlindungan cyber tanpa menonaktifkan atau menghapus solusi keamanan saat ini. Hal ini juga dapat dilakukan – cukup pastikan bahwa Anda tidak menggunakan modul Antivirus dan antimalware di rencana proteksi Anda. Semua modul lainnya dapat digunakan secara bebas.

Pembatasan

- Pemindaian antimalware pada cadangan mengharuskan Anda menginstal Layanan Pemindaian saat menginstal Server Manajemen Cyber Protect.
- Akses jarak jauh melalui klien HTML5 hanya tersedia jika Server Manajemen Cyber Protect diinstal pada mesin yang menjalankan Linux.

Persyaratan perangkat lunak

Browser web yang didukung

Antarmuka web mendukung browser web berikut:

- Google Chrome 29 ke atas
- Mozilla Firefox 23 ke atas
- Opera 16 ke atas
- Windows Internet Explorer 10 ke atas

Catatan
Dalam penerapan awan, Internet Explorer tidak didukung.

- 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

Agen untuk Windows

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows XP Professional SP2 (x86) – didukung dengan versi khusus Agen untuk Windows. Untuk detail dan batasan dukungan ini, lihat "Agen untuk Windows XP SP2".
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2 ke atas – Standard dan Enterprise edition (x86, x64)

Catatan
Acronis Cyber Protect memerlukan pembaruan KB940349 dari Microsoft, yang tidak dapat lagi diunduh secara terpisah. Untuk memastikan bahwa fungsi yang awalnya disediakan oleh KB940349 tersedia di mesin Anda, instal semua pembaruan yang tersedia saat ini untuk Windows Server 2003.
Untuk informasi lebih lanjut tentang KB940349, lihat artikel basis pengetahuan ini.

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

Catatan

Untuk menggunakan Acronis Cyber Protect dengan Windows 7, Anda harus menginstal pembaruan berikut dari Microsoft:

- 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 – Standard, Enterprise, Datacenter, Foundation, dan Web edition
- 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

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

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

- Agen untuk SQL tidak didukung untuk penyebaran di lokasi (on-premises) pada edisi Windows 7 Starter dan Home (x86, x64)

Agen untuk Exchange (untuk pencadangan kotak surat

Agen ini dapat diinstal pada mesin dengan atau tanpa Microsoft Exchange Server.

- 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 – Standard, Enterprise, Datacenter, Foundation, dan Web edition

- 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 Office 365

- Windows Server 2008 – edisi Standard, Enterprise, Datacenter, Foundation, dan Web (hanya x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation, dan Web edition
- 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

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 Linux

Catatan
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 Acronis Cyber Protect 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, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- 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, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise Kernel dan Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

Sebelum menginstal produk pada sistem yang tidak menggunakan RPM Package Manager, seperti sistem Ubuntu, Anda harus menginstal pengelola ini secara manual; misalnya, dengan menjalankan perintah berikut (sebagai pengguna root): `apt-get install rpm`

Jika Distribusi Linux Anda tidak mendukung mekanisme D-Bus (misalnya, Red Hat Enterprise Linux 6.x atau CentOS 6.x) Acronis Cyber Protect akan menggunakan lokasi default untuk menyimpan kunci aman karena sistem operasi tidak menyediakan lokasi D-Bus yang kompatibel.

* Hanya didukung dengan kernel dari 4.18 hingga 5.19

Agen untuk Mac

Catatan
Prosesor berbasis ARM, seperti Apple silicon M1 dan M2, tidak didukung.

- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13

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 dengan Hyper-V – semua opsi instalasi, kecuali untuk Nano Server

Agen untuk Scale Computing HC3 (Alat Virtual)

Agen ini dikirimkan sebagai alat virtual yang disebarkan di klaster Scale Computing HC3 melalui konsol web Cyber Protect. Tidak ada penginstal yang berdiri sendiri untuk agen ini.

Scale Computing Hypercore 8.8, 8.9, 9.0

Server Manajemen (hanya untuk penyebaran di lokasi)

Di Windows

- Windows 7 – semua edisi (x86, x64)

> **Catatan**
> Untuk menggunakan Acronis Cyber Protect dengan Windows 7, Anda harus menginstal pembaruan berikut dari Microsoft:
> - 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, dan Foundation
- 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 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

Di Linux

Catatan
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 Acronis Cyber Protect 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 versi yang lebih baru, termasuk distribusi x86_64 berikut.

Distribusi x86 tidak didukung.

- Red Hat Enterprise Linux 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- 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, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise Kernel dan Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

Sebelum menginstal produk pada sistem yang tidak menggunakan RPM Package Manager, seperti sistem Ubuntu, Anda harus menginstal pengelola ini secara manual; misalnya, dengan menjalankan perintah berikut (sebagai pengguna root): `apt-get install rpm`

Jika Distribusi Linux Anda tidak mendukung mekanisme D-Bus (misalnya, Red Hat Enterprise Linux 6.x atau CentOS 6.x) Acronis Cyber Protect akan menggunakan lokasi default untuk menyimpan kunci aman karena sistem operasi tidak menyediakan lokasi D-Bus yang kompatibel.

* Hanya didukung dengan kernel dari 4.18 hingga 5.19

Simpul Penyimpanan (hanya untuk penyebaran di lokasi)

- Windows Server 2008 – edisi Standard, Enterprise, Datacenter, dan Foundation (hanya x64)
- Windows Small Business Server 2008
- Windows 7 – semua edisi (hanya x64)
- Windows Server 2008 R2 – edisi Standard, Enterprise, Datacenter, dan Foundation
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- 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
- Windows 10 – Home, Pro, Education, Enterprise, dan IoT Enterprise edition
- 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

Agen untuk Windows XP SP2

Agen untuk Windows XP SP2 hanya mendukung versi Windows XP SP2 32-bit.

Untuk melindungi mesin yang menjalankan Windows XP SP1 (x64), Windows XP SP2 (x64), atau Windows XP SP3 (x86), gunakan Agen untuk Windows reguler.

Agen untuk Windows XP SP2 memerlukan lisensi Acronis Cyber Backup 12.5. Kunci lisensi Acronis Cyber Protect tidak didukung.

Instalasi

Agen untuk Windows XP SP2 membutuhkan setidaknya 550 MB ruang disk dan 150 MB RAM. Saat mencadangkan, agen biasanya mengonsumsi sekitar 350 MB memori. Konsumsi puncak dapat mencapai 2 GB, tergantung pada jumlah data yang sedang diproses.

Agen untuk Windows XP SP2 hanya dapat diinstal secara lokal di mesin yang ingin Anda buat cadangannya. Untuk mengunduh program pengaturan agen, klik ikon akun di sudut kanan atas, lalu klik **Unduhan** > **Agen untuk Windows XP SP2**.

Monitor Cyber Protect dan Pembangun Media Yang Dapat Di-Boot tidak dapat diinstal. Untuk mengunduh file ISO media yang dapat di-boot, klik ikon akun di sudut kanan atas > **Unduhan** > **Media yang dapat di-boot**.

Pembaruan

Agen untuk Windows XP SP2 tidak mendukung fungsi pembaruan jarak jauh. Untuk memperbarui agen, unduh versi baru program pengaturan, lalu ulangi instalasi.

Jika Anda memperbarui Windows XP dari SP2 ke SP3, hapus instalasi Agen untuk Windows XP SP2, lalu instal Agen untuk Windows reguler.

Pembatasan

- Hanya pencadangan level disk yang tersedia. File individual dapat dipulihkan dari disk atau cadangan volume.
- Jadwalkan berdasarkan peristiwa tidak didukung.
- Syarat untuk eksekusi rencana proteksi tidak didukung.
- Hanya tujuan pencadangan berikut yang didukung:
  - Penyimpanan awan
  - Folder lokal
  - Folder jaringan
  - Secure Zone
- Format cadangan **Versi 12** dan fitur yang memerlukan format cadangan **Versi 12** tidak didukung. Secara khusus, pengiriman data fisik tidak tersedia. Opsi **Jendela performa dan pencadangan**, jika diaktifkan, hanya menerapkan pengaturan level hijau.
- Pemilihan disk/volume individual untuk pemulihan dan pemetaan disk manual selama pemulihan tidak didukung di antarmuka web. Fungsi ini tersedia di bawah media yang dapat di-boot.
- Pemrosesan data off-host tidak didukung.
- Agen untuk Windows XP SP2 tidak dapat melakukan operasi berikut dengan cadangan:
  - Mengonversi cadangan ke mesin virtual
  - Mounting volume dari cadangan
  - Mengekstrak file dari cadangan
  - Ekspor dan validasi manual cadangan.

  Anda dapat melakukan operasi ini menggunakan agen lain.
- Cadangan yang dibuat oleh Agen untuk Windows XP SP2 tidak dapat dijalankan sebagai mesin virtual.

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

SQL Server Express editions dari versi SQL Server di atas juga 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).
- 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

Acronis Cyber Protect 15 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

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.

Platform virtualisasi yang didukung

Tabel berikut merangkum bagaimana berbagai platform virtualisasi didukung.

Catatan
Vendor dan versi hypervisor berikut yang didukung melalui metode **Cadangkan dari dalam OS tamu** telah diuji secara khusus. Akan tetapi, bahkan jika Anda menjalankan hypervisor dari vendor atau hypervisor dengan versi yang tidak tercantum di bawah ini, metode **Pencadangan dari dalam OS tamu** masih dapat berfungsi dengan baik dalam semua skenario wajib.

Jika Anda mengalami masalah saat menggunakan Acronis Cyber Protect dengan kombinasi vendor hypervisor dan versi Anda, hubungi tim Dukungan untuk investigasi lebih lanjut.

Platform	Cadangkan di tingkat hypervisor (pencadangan tanpa agen)	Pencadangan dari dalam OS tamu
VMware		
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	+	+
VMware vSphere Hypervisor (ESXi Gratis)**		+
VMware Server (Server VMware Virtual) VMware Workstation		+

VMware ACE VMware Player		
Microsoft* **		
Windows Server 2008 (x64) dengan Hyper-V Windows Server 2008 R2 dengan Hyper-V 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 with 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 dan 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8, 8.9, 9.0	+	+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6		Hanya tamu virtual sepenuhnya (disebut juga HVM). Tamu paravirtualized (disebut juga PV) tidak didukung.
Red Hat dan Linux		

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		+
Virtualisasi Red Hat (dikelola oleh oVirt) 4.2, 4.3, 4.4 (hanya tersedia dengan penyebaran awan)	+	+
Mesin Virtual berbasis Kernel (KVM)		+
Mesin Virtual (KVM) berbasis kernel yang dikelola oleh oVirt 4.3 yang berjalan di Red Hat Enterprise Linux 7.6, 7.7 atau CentOS 7.6, 7.7 (hanya tersedia dengan penyebaran awan dan dengan lisensi Tingkat Lanjut)	+	+
Mesin Virtual (KVM) berbasis kernel yang dikelola oleh oVirt 4.4 yang berjalan di Red Hat Enterprise Linux 8.x atau CentOS Stream 8.x (hanya tersedia dengan penyebaran awan dan dengan lisensi Tingkat Lanjut)	+	+
Mesin Virtual (KVM) berbasis kernel yang dikelola oleh oVirt 4.5 yang berjalan di Red Hat Enterprise Linux 8.x atau CentOS Stream 8.x (hanya tersedia dengan penyebaran awan dan dengan lisensi Tingkat Lanjut)	+	+
Parallels		
Workstation Parallels		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Hanya tamu virtual sepenuhnya (disebut juga HVM). Tamu paravirtualized (disebut juga PV) tidak didukung.
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x hingga		+

20180425.x		
Virtuozzo (hanya tersedia dengan penyebaran awan)		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	Hanya mesin virtual. Kontainer tidak didukung.
Virtuozzo 7.0.13, 7.0.14	Hanya kontainer ploop. Mesin virtual tidak didukung.	Hanya mesin virtual. Kontainer tidak didukung.
Virtuozzo Hybrid Server 7.5	+	Hanya mesin virtual. Kontainer tidak didukung.
Virtuozzo Hybrid Infrastructure (hanya tersedia dengan penyebaran awan)		
Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5	+	+
Amazon		
Instans Amazon EC2		+
Microsoft Azure		
Mesin virtual Azure		+

* 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.

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

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 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.

- **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 VMware dan Agen untuk Hyper-V tidak mencadangkan volume LUN yang terhubung oleh inisiator iSCSI yang bekerja dalam sistem operasi tamu. Karena hypervisor ESXi dan Hyper-V tidak mengenali volume seperti itu, volume tersebut tidak akan tercakup dalam snapshot level 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 Linux yang berisi volume logis (LVM)**

  Agen untuk VMware dan Agen untuk Hyper-V tidak mendukung operasi berikut untuk mesin Linux dengan LVM:
  - Migrasi P2V dan V2P. Gunakan Agen untuk Linux atau media yang dapat di-boot untuk mencadangkan dan media yang dapat di-boot untuk memulihkan.
  - Menjalankan mesin virtual dari cadangan yang dibuat oleh Agen untuk Linux atau media yang dapat di-boot.
  - Mengonversi cadangan yang dibuat oleh Agen untuk Linux atau media yang dapat di-boot ke mesin virtual.
- **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** (diperkenalkan di VMware vSphere 6.5)

  Boot Aman dinonaktifkan setelah mesin virtual dipulihkan sebagai mesin virtual baru. Anda dapat mengaktifkan secara manual opsi ini setelah pemulihan selesai.
- **Pencadangan konfigurasi ESXi** tidak didukung untuk VMware vSphere 7.0.

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

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

   Untuk **gcc**, pastikan versi yang dikembalikan dengan perintah sama seperti di `gcc version` 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:

  ```
  yum list installed | 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:

   ```
   yum list installed | 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: `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	**linux-headers**	Jalankan perintah berikut:

Debian	**linux-image** **gcc** **make** **perl**	`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:

- 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.

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
- CheckPoint Harmony Endpoint
- 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 merekomendasikan Anda menginstal perangkat lunak enkripsi sebelum 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.
2. Instalasi agen perlindungan.
3. Buat Secure Zone.
4. Jangan sertakan Secure Zone saat mengenkripsi disk atau volumenya.

Aturan pencadangan umum

Anda dapat melakukan pencadangan tingkat disk pada sistem operasi. Jangan mencoba mencadangkan menggunakan media yang dapat di-boot.

Prosedur pemulihan spesifik perangkat lunak

Microsoft BitLocker Drive Encryption dan CheckPoint Harmony Endpoint

Anda dapat memulihkan sistem menggunakan pemulihan dengan mulai ulang atau media yang dapat di-boot.

Pemulihan dengan mulai kembali

Untuk memulihkan sistem yang terenkripsi, ikuti langkah-langkah di "Memulihkan mesin fisik" (hlm. 307).

Pastikan persyaratan di "Pemulihan dengan mulai kembali" (hlm. 314) terpenuhi.

Catatan
Untuk volume terenkripsi Bitlocker, pemulihan dengan mulai ulang hanya tersedia di mesin berbasis UEFI yang menjalankan Windows 7 dan lebih baru atau Windows Server 2008 R2 dan lebih baru. Untuk volume terenkripsi CheckPoint, pemulihan dengan mulai ulang hanya tersedia di mesin berbasis UEFI yang menjalankan Windows 10 dan Windows 11.

Pemulihan dengan mulai ulang tidak tersedia di mesin berbasis BIOS atau mesin yang menjalankan Linux atau macOS.

Pemulihan dengan media yang dapat di-boot

1. Lakukan boot dari media yang dapat di-boot.
2. Pulihkan sistem.

Penting
Data yang dicadangkan dipulihkan sebagai non-enkripsi.

3. Boot ulang sistem yang dipulihkan.
4. Aktifkan perangkat lunak enkripsi.

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 dapat memulihkan partisi sistem terenkripsi hanya dengan 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

Dengan Acronis Cyber Protect, Anda dapat menggunakan perangkat Dell EMC Data Domain sebagai penyimpanan cadangan. Kunci retensi (Mode tata kelola) didukung.

Jika kunci retensi diaktifkan, Anda perlu menambahkan variabel lingkungan `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 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**.
7. Di jendela **Variabel Lingkungan**, klik **OK**.
8. Mulai ulang mesin.

Untuk menambahkan variabel 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.

Untuk menambahkan variabel dalam alat virtual

1. Masuk sebagai administrator ke mesin 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.

Persyaratan sistem

Tabel berikut ini merangkum ruang disk dan persyaratan memori untuk kasus instalasi tipikal. Instalasi dilakukan dengan pengaturan default.

Komponen yang akan diinstal	Ruang disk diperlukan untuk instalasi	Konsumsi memori minimum
Agen untuk Windows	850 MB	150 MB
Agen untuk Windows dan salah satu agen berikut: • Agen untuk SQL • Agen untuk Exchange	950 MB	170 MB
Agen untuk Windows dan salah satu agen berikut: • Agen untuk VMware (Windows) • Agen untuk Hyper-V	1170 MB	180 MB
Agen untuk Office 365	500 MB	170 MB
Agen untuk Linux	2,0 GB	130 MB
Agen untuk Mac	500 MB	150 MB
Hanya untuk penyebaran di lokasi		

Server Manajemen di Windows	1,7 GB	200 MB
Server Manajemen di Linux	1,5 GB	200 MB
Server Manajemen dan Agen untuk Windows	2,4 GB	360 MB
Server Manajemen dan agen pada mesin yang menjalankan Windows, Microsoft SQL Server, Microsoft Exchange Server, dan Layanan Domain Active Directory	3,35 GB	400 MB
Server Manajemen dan Agen untuk Linux	4,0 GB	340 MB
Simpul Penyimpanan dan Agen untuk Windows • Hanya platform 64-bit • Untuk menggunakan deduplikasi, diperlukan minimum 8 GB RAM. Untuk informasi lebih lanjut, lihat "Praktik terbaik deduplikasi" (hlm. 616).	1,1 GB	330 MB

Saat mencadangkan, agen biasanya mengonsumsi sekitar 350 MB memori (diukur selama pencadangan volume 500-GB). Konsumsi puncak dapat mencapai 2 GB, tergantung pada jumlah dan jenis data yang sedang diproses.

Mencadangkan ke set cadangan besar (600 GB atau lebih) membutuhkan sekitar 1 GB RAM per 1 TB set cadangan.

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.

Server manajemen dengan satu beban kerja terdaftar menghabiskan memori 200 MB. Beban kerja adalah semua jenis sumber daya yang dilindungi – misalnya, mesin fisik, mesin virtual, kotak surat, atau instans basis data. Setiap beban kerja tambahan menambahkan sekitar 2 MB. Dengan demikian, server dengan 100 beban kerja terdaftar menghabiskan sekitar 400 MB di atas sistem operasi dan menjalankan aplikasi.

Jumlah maksimum beban kerja terdaftar adalah 900-1000. Batasan ini berasal dari basis data SQLite tertanam server manajemen.

Untuk mengatasi batasan ini, tentukan instans Microsoft SQL Server eksternal saat Anda menginstal server manajemen. Dengan database SQL eksternal, Anda dapat mendaftarkan hingga 8000 beban kerja ke server manajemen, tanpa penurunan kinerja yang signifikan. Dengan 8000 beban kerja terdaftar, instans SQL Server akan menggunakan sekitar 8 GB RAM.

Untuk kinerja pencadangan yang lebih baik, kelola beban kerja berdasarkan grup, hingga 500 beban kerja di setiap grup.

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. Pembatasan berlaku untuk agen dan media yang dapat di-boot.

<table>
<tr><th rowspan="2">Sistem file</th><th colspan="4">Didukung oleh</th><th rowspan="2">Pembatasan</th></tr>
<tr><th>Agen</th><th>Media yang dapat di-boot WinPE</th><th>Media yang dapat di-boot berbasis Linux</th><th>Media yang dapat di-boot Mac</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Semua agen</td><td>+</td><td>+</td><td>+</td><td rowspan="4">Tidak ada pembatasan</td></tr>
<tr><td>NTFS</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td><td>+</td><td>-</td></tr>
<tr><td>HFS+</td><td rowspan="2">Agen untuk Mac</td><td>-</td><td>-</td><td>+</td></tr>
<tr><td>APFS</td><td>-</td><td>-</td><td>+</td><td>• Didukung mulai dengan macOS High Sierra 10.13
• Konfigurasi disk harus dibuat ulang secara manual ketika memulihkan ke mesin non-asli atau bare metal.</td></tr>
</table>

JFS	Agen untuk Linux	-	+	-	• File tidak dapat dikecualikan dari cadangan disk • Pencadangan inkremental/diferensial cepat tidak dapat diaktifkan
ReiserFS3		-	+	-	
ReiserFS4		-	+	-	• File tidak dapat dikecualikan dari cadangan disk • Pencadangan inkremental/diferensial cepat tidak dapat diaktifkan • Volume tidak dapat diubah ukurannya selama pemulihan
ReFS	Semua agen	+	+	+	
XFS		+	+	+	• File tidak dapat dikecualikan dari cadangan disk • Pencadangan inkremental/diferensial cepat tidak dapat diaktifkan • Volume tidak dapat diubah ukurannya selama pemulihan • Memulihkan file dari cadangan yang disimpan pada pita tidak didukung
Linux swap	Agen	-	+	-	Tidak ada pembatasan

	untuk Linux				
exFAT	Semua agen	+	+ Media yang dapat di-boot tidak dapat digunakan untuk pemulihan jika cadangan *disimpan di* exFAT	+	• Hanya cadangan disk/volume yang didukung • File tidak dapat dikecualikan dari pencadangan • 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. 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.

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 Penyedia Acronis VSS. 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 Acronis Backup.

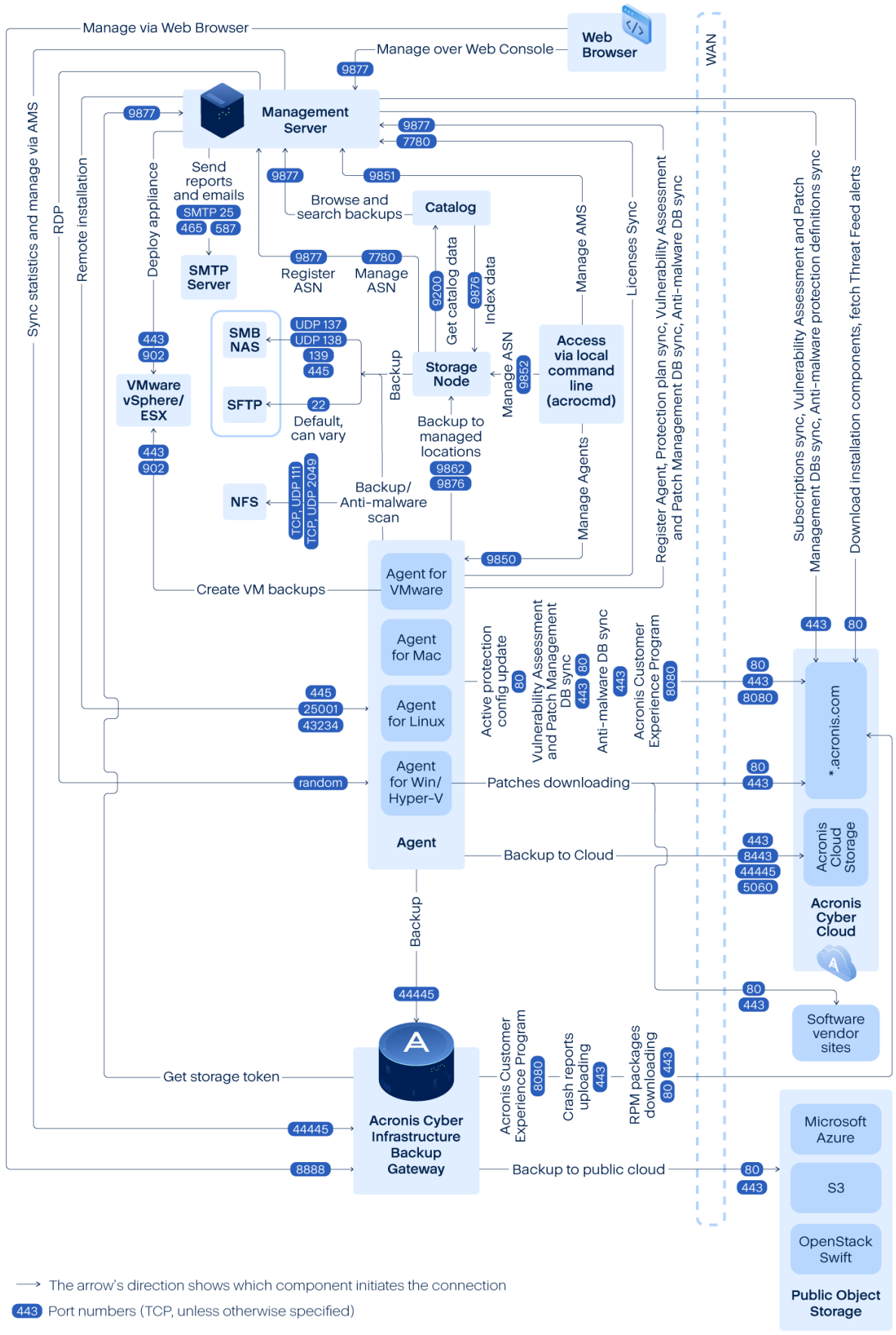
Diagram koneksi jaringan untuk Acronis Cyber Protect

Topik ini berisi diagram koneksi untuk Acronis Cyber Protect.

Kunjungi Basis Pengetahuan kami untuk mengetahui daftar port, layanan, dan proses yang Acronis Cyber Protect menggunakan:

- Untuk Windows, lihat Layanan dan proses Windows (65663).
- Untuk Linux, lihat Komponen, layanan, dan proses Linux (67276).

Diagram koneksi jaringan - Cyber Protect proses



Penting
Port keluar dalam diagram jaringan bersifat dinamis. Beberapa layanan juga dapat menggunakan port dinamis untuk koneksi masuk. Saat Anda memecahkan masalah jaringan, pastikan lalu lintas melalui port dinamis diizinkan.

Port dinamis dikelola oleh sistem operasi dan ditetapkan secara acak. Rentang port dinamis default di Windows adalah 49152 – 65535. Rentang ini dapat bervariasi sesuai dengan sistem operasi dan dapat diubah secara manual.

Server manajemen adalah komponen utama dari Acronis Cyber Protect. Ini memperlihatkan dua port TCP: 7780 dan 9877. Port 9877, dilindungi dengan TLS, digunakan untuk menyediakan REST API dan antarmuka pengguna berbasis web. Titik akhir REST API mengautentikasi permintaan dengan menggunakan token JWT yang direpresentasikan sebagai header HTTP terpisah atau dikodekan sebagai cookie HTTP. Port 7780 mengimplementasikan protokol ZeroMQ dengan autentikasi dan enkripsi ZMTP CURVE. Port 7780 digunakan oleh agen dan node penyimpanan untuk bertukar pesan manajemen dengan server manajemen secara asinkron. Server manajemen juga berkomunikasi dengan layanan awan untuk mengunduh pembaruan melalui port HTTP dan HTTPS standar.

Simpul penyimpanan adalah komponen penyimpanan Acronis Cyber Protect. Ini memperlihatkan port TCP 9876. Port ini digunakan untuk mengirim dan menerima data cadangan. Transportasi dilindungi dengan TLS dan autentikasi dilakukan menggunakan TLS bersama. Protokol tingkat aplikasi berpemilik Acronis. Node penyimpanan berkomunikasi dengan sistem penyimpanan backend dengan menggunakan protokol dan mekanisme otentikasi yang sesuai.

Katalog adalah komponen pendukung dari Acronis Cyber Protect. Ini mengindeks data pada node penyimpanan, mengaksesnya pada port 9876 dan mengekspos indeks pada port 9200.

Gateway cadangan mengimplementasikan protokol akses data Acronis berpemilik generasi berikutnya. Komponen yang sama digunakan di Acronis Cyber Cloud, jika pelanggan ikut serta dalam pencadangan awan. Port TCP 44445, terdaftar di IANA, digunakan oleh gateway. Perlindungan data dilakukan melalui TLS dan autentikasi dilakukan menggunakan TLS bersama. Gateway cadangan juga dapat menggunakan port 8888 untuk layanan manajemen berbasis HTTPS.

Agen berkomunikasi dengan server manajemen, node penyimpanan, dan gateway cadangan melalui port, seperti dijelaskan di atas. Agen juga dapat berkomunikasi dengan layanan file berbasis standar (SMB, NFS) saat digunakan sebagai tujuan pencadangan. Port standar dan protokol otentikasi yang sesuai digunakan dalam kasus ini. Agen untuk VMware menggunakan VMware vSphere API melalui port yang ditentukan oleh VMware vSphere saat fungsionalitas tersebut dikonfigurasi.

Penilaian kerentanan untuk Linux diimplementasikan melalui layanan CVSS yang disebarkan di Acronis Cyber Cloud. Agen perlindungan memilih pusat data terdekat secara dinamis dengan menyematkan dari daftar https://cloud.acronis.com/services.json.

Penyebaran di lokasi

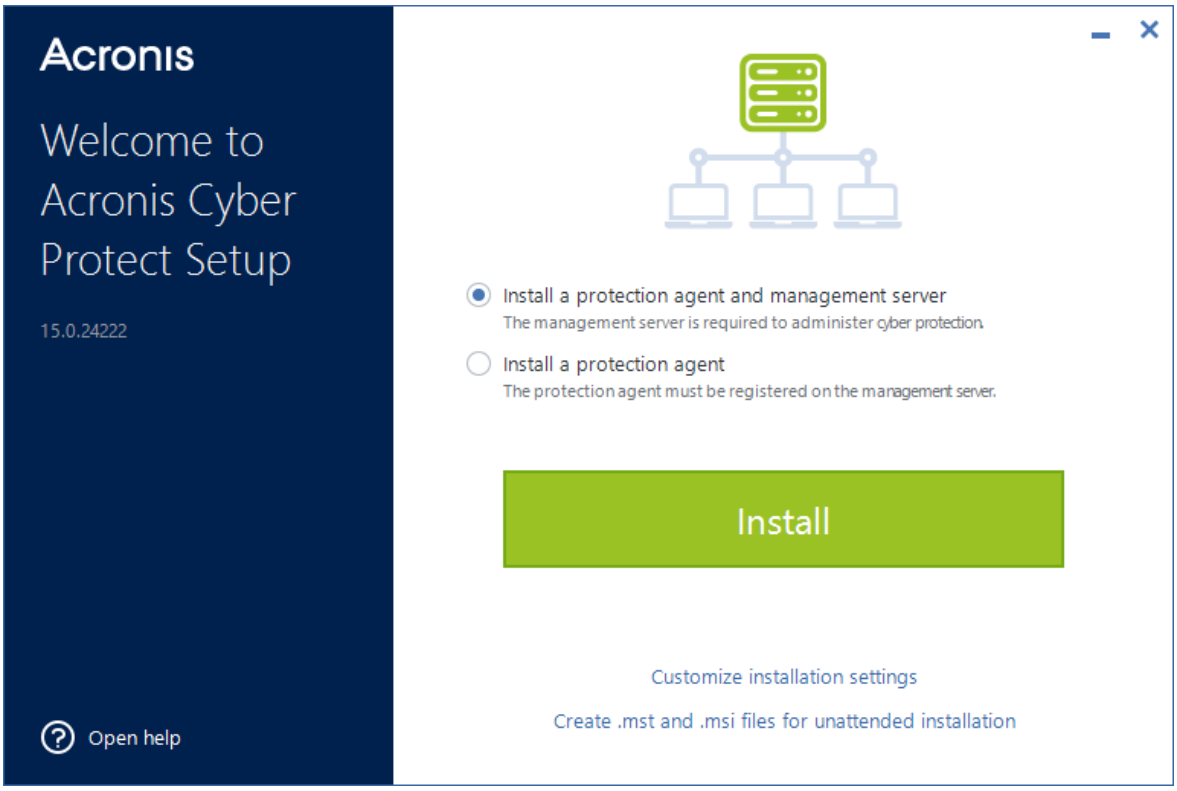
Penyebaran di lokasi mencakup sejumlah komponen perangkat lunak yang dijelaskan di bagian "Komponen" (hlm. 47). Untuk perincian tentang interaksi antara komponen ini dan port yang diperlukan, lihat "Diagram koneksi jaringan untuk Acronis Cyber Protect" (hlm. 78).

Menginstal server manajemen

Instalasi di Windows

Untuk menginstal server manajemen

1. Masuk sebagai administrator dan mulai program penyiapan Acronis Cyber Protect.
2. [Opsional] Untuk mengubah bahasa program penyiapan, klik **Pengaturan bahasa**.
3. Terima persyaratan perjanjian lisensi dan pernyataan privasi, lalu klik **Lanjutkan**.
4. Biarkan pengaturan default apa adanya, **Instal agen perlindungan dan server manajemen**.



5. Lakukan yang berikut ini:
   - Klik **Instal**.

     Ini adalah cara termudah untuk menginstal produk. Sebagian besar parameter instalasi akan ditetapkan ke nilai standarnya.

     Komponen berikut akan diinstal:

- Server Manajemen
- Komponen untuk Instalasi Jarak Jauh
- Agen untuk Windows
- Agen lainnya (Agen untuk Hyper-V, Agen untuk Exchange, Agen untuk SQL, dan Agen untuk Active Directory), jika masing-masing hypervisor atau aplikasi terdeteksi pada mesin
- Pembangun Media Yang Dapat Di-Boot
- Command-Line Tool
- Monitor Cyber Protect

- Klik **Sesuaikan pengaturan instalasi** untuk mengonfigurasi pengaturan.
  Anda akan dapat memilih komponen yang akan diinstal dan menentukan parameter tambahan. Untuk perincian, lihat "Menyesuaikan pengaturan instalasi" (hlm. 84).
- Klik **Buat file .mst dan .msi untuk instalasi tanpa pengawasan** agar dapat mengekstrak rencana instalasi. Tinjau atau modifikasi pengaturan instalasi yang akan ditambahkan ke file .mst, lalu klik **Hasilkan**. Langkah lebih lanjut dari prosedur ini tidak diperlukan.
  Jika Anda ingin menyebarkan agen melalui Kebijakan Grup, lihat "Menyebarkan agen melalui Kebijakan Grup" (hlm. 175).

6. Lanjutkan instalasi.
7. Setelah instalasi selesai, klik **Tutup**.

Untuk mulai menggunakan server manajemen Anda, aktifkan dengan masuk ke akun Acronis Anda atau melalui file aktivasi.

Menyesuaikan pengaturan instalasi

Bagian ini menjelaskan pengaturan yang dapat diubah selama instalasi.

Komponen-komponen yang akan diinstal

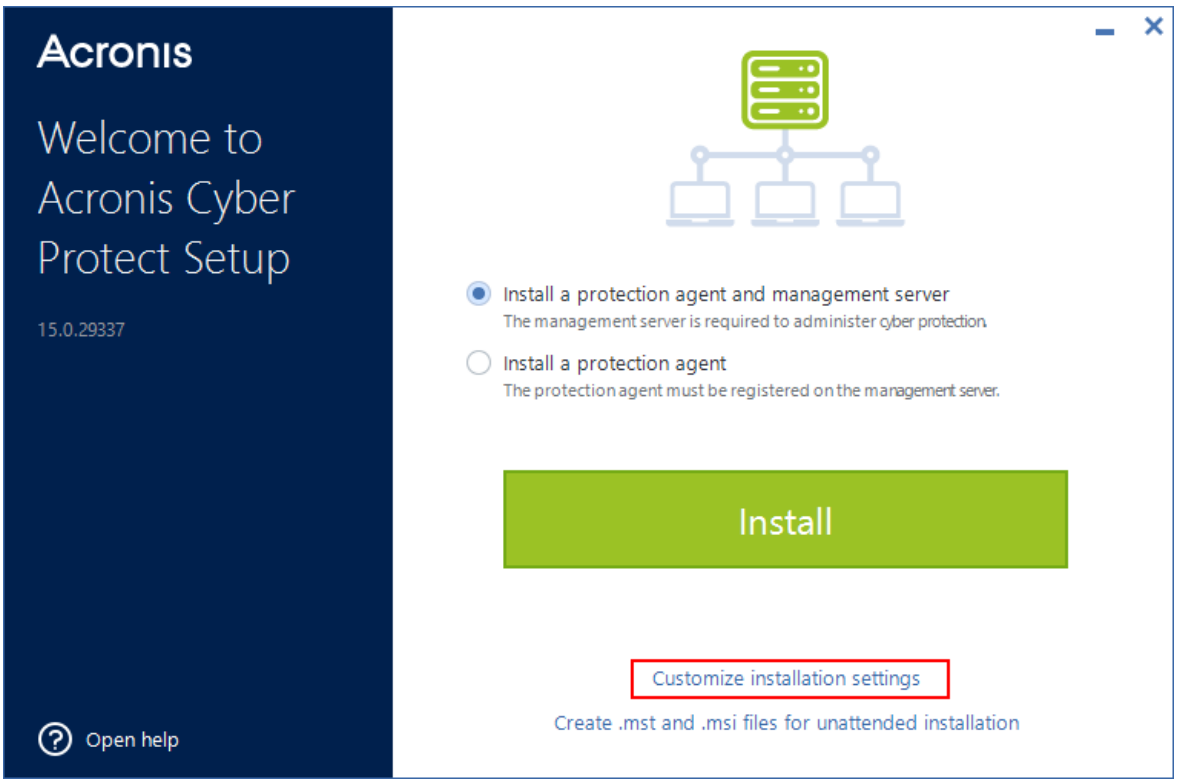
Bergantung pada apakah Anda menginstal server manajemen dan agen proteksi, atau agen proteksi saja, komponen di bawah ini dipilih secara default:

Server manajemen dan agen proteksi	Agen proteksi saja
Server Manajemen	Agen untuk Windows
Komponen untuk Instalasi Jarak Jauh	Pembangun Media Yang Dapat Di-Boot
Agen untuk Windows	Command-Line Tool
Pembangun Media Yang Dapat Di-Boot	Monitor Cyber Protect
Command-Line Tool	
Monitor Cyber Protect	

Untuk daftar lengkap komponen yang tersedia, lihat "Komponen" (hlm. 47).

Untuk menginstal komponen opsional

1. Di wizard penginstalan, klik **Kustomisasi pengaturan instalasi**.



2. Di **Apa yang diinstal**, klik **Ubah**.
3. Pilih komponen yang diinginkan, lalu klik **Selesai**.
4. Jika diminta, konfigurasikan pengaturan untuk komponen yang dipilih.
5. Klik **Instal**.

Akun masuk layanan

Anda dapat mengubah akun di mana agen atau layanan manajemen akan dijalankan dengan menggunakan opsi masing-masing **Akun masuk untuk layanan agen** dan **Akun masuk untuk layanan server manajemen**.

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 opsi ini adalah kebijakan keamanan domain yang tidak memengaruhi hak pengguna akun ini. Secara default, agen berjalan di bawah akun **Sistem Lokal**.
- **CBuat akun baru** (default untuk layanan server manajemen dan layanan simpul penyimpanan)

  Nama akun akan berupa **Acronis Agent User**, **AMS User**, dan **ASN User** masing-masing untuk agen, server manajemen, dan layanan simpul penyimpanan.
- **Gunakan akun berikut**

Jika Anda menginstal produk pada pengontrol domain, program penyiapan akan meminta Anda menentukan akun yang ada (atau akun yang sama) untuk setiap layanan. Untuk alasan keamanan, program penyiapan 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 penginstalan agen pada pengontrol domain hanya baca, lihat artikel basis pengetahuan ini.

Selain itu, memilih **Gunakan akun berikut** memungkinkan Anda untuk menggunakan autentikasi Windows untuk Microsoft SQL Server jika Anda mengonfigurasi server manajemen dengan database SQL.

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 terkait mungkin bekerja secara tidak semestinya atau tidak berfungsi.

Hak pengguna yang diperlukan untuk akun masuk layanan

Agen proteksi berjalan sebagai **Managed Machine Service** (MMS) pada mesin Windows. Akun di mana agen akan berjalan harus memiliki hak berikut ini agar agen bekerja dengan benar:

1. Pengguna MMS harus termasuk dalam grup **Operator Pencadangan** dan **Administrator**. Pada pengontrol domain, pengguna harus dimasukkan dalam grup **Admin Domain**.
2. Pengguna MMS harus diberi izin **Kontrol Penuh** pada folder `%PROGRAMDATA%\Acronis` (pada Windows XP dan Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) dan pada subfoldernya.
3. Pengguna MMS harus diberi izin **Kontrol Penuh** pada kunci registri tertentu dengan kunci berikut: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Pengguna MMS harus diberi hak pengguna berikut di Windows:
   - **Masuk sebagai layanan**
   - **Sesuaikan kuota memori untuk suatu proses**
   - **Ganti token level proses**
   - **Modifikasi nilai lingkungan firmware**

Pengguna ASN harus memiliki hak administrator lokal pada mesin yang menginstal Simpul Penyimpanan Acronis.

Untuk menetapkan hak pengguna di Windows

Catatan
Prosedur ini menggunakan hak pengguna **Masuk sebagai layanan** sebagai contoh. Langkah-langkah untuk hak pengguna lainnya sama.

1. Masuk ke komputer sebagai administrator.
2. Di **Kontrol Panel**, buka **Alat Bantu Administratif**. Atau, tekan Win+R pada keyboard, ketik **control admintools**, lalu tekan Enter.
3. Buka **Kebijakan Keamanan Lokal**.
4. Perluas **Kebijakan Lokal**, lalu klik **Penetapan Hak Pengguna**.
5. Di panel kanan, klik kanan **Masuk sebagai layanan**, dan pilih **Properti**.
6. Klik **Tambahkan Pengguna atau Grup...** untuk menambahkan pengguna baru.
7. Di jendela **Pilih Pengguna atau Grup**, temukan pengguna yang ingin Anda masukkan, lalu klik **OK**.
8. Di jendela **Masuk sebagai Properti layanan**, klik **OK** untuk menyimpan perubahan.

Catatan
Pengguna yang Anda tambahkan ke hak pengguna **Masuk sebagai layanan** tidak tercantum dalam kebijakan **Tolak masuk sebagai layanan** di **Kebijakan Keamanan Lokal**.

Penting
Kami tidak menyarankan mengubah akun masuk secara manual setelah instalasi selesai.

Database untuk server manajemen

Anda dapat mengonfigurasi server manajemen dengan database berikut ini:

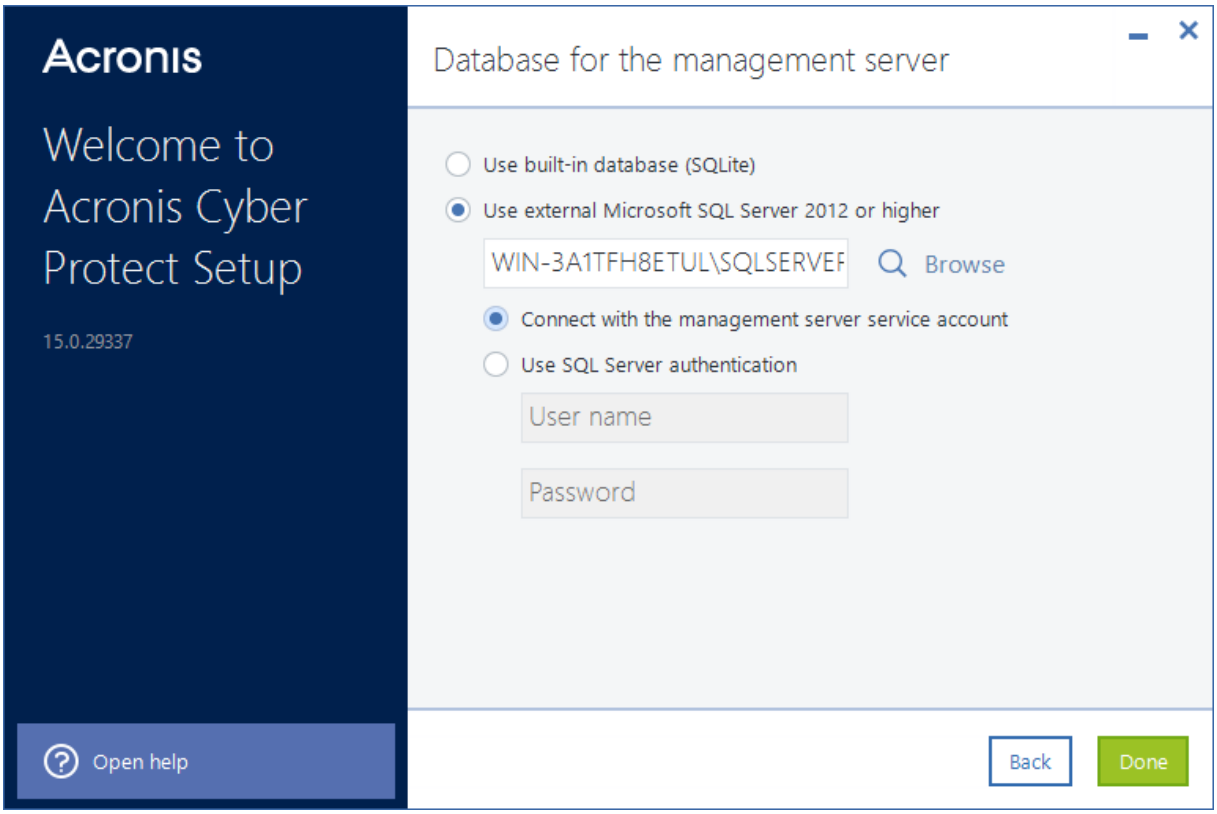
- SQLite

  Secara default, server manajemen menggunakan database SQLite bawaan. Ini memungkinkan pendaftaran sekitar 900-1000 beban kerja di server manajemen. SQLite tidak kompatibel dengan Layanan Pemindaian.
- Microsoft SQL

  Microsoft SQL memungkinkan pendaftaran hingga 8000 beban kerja ke server manajemen, tanpa penurunan kinerja yang signifikan. Instans Microsoft SQL yang sama dapat digunakan oleh server manajemen, oleh Layanan Pemindaian, dan oleh program lainnya.

  Versi MS SQL Server berikut didukung:
  - Microsoft SQL Server 2019 (berjalan di Windows)
  - Microsoft SQL Server 2017 (berjalan di Windows)
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2012

Jika instans Microsoft SQL adalah instans default, yaitu **MSSQLSERVER**, Anda hanya dapat menentukan nama mesin tempat instans ini berjalan. Jika instans memiliki nama kustom, Anda harus menentukannya menggunakan format berikut: `nama mesin\nama instans`.



Catatan
Pastikan bahwa Layanan Browser SQL Server dan protokol TCP/IP diaktifkan di mesin yang menjalankan instans Microsoft SQL. Untuk informasi lebih lanjut tentang cara memulai Layanan Browser SQL Server, kunjungi http://msdn.microsoft.com/en-us/library/ms189093.aspx. Anda dapat mengaktifkan protokol TCP/IP dengan menggunakan prosedur serupa.

Untuk terhubung ke instans Microsoft SQL yang ditentukan, Anda dapat menggunakan metode autentikasi berikut ini:

- Autentikasi Windows (**Hubungkan saya dengan akun layanan server manajemen**)
  Anda dapat menggunakan metode ini jika Anda mengonfigurasi akun masuk untuk layanan server manajemen dengan menggunakan opsi **Gunakan akun berikut**, misalnya dengan menentukan `<NAMA MESIN>\Administrator`. Akun yang ditentukan harus mempunyai peran **dbcreator** atau **sysadmin** dalam Microsoft SQL Server.
  Untuk informasi lebih lanjut tentang akun masuk, lihat "Hak pengguna yang diperlukan untuk akun masuk layanan" (hlm. 86).
- Autentikasi SQL Server
  Anda dapat selalu menggunakan metode ini. Akun yang ditentukan harus mempunyai peran **dbcreator** atau **sysadmin** dalam Microsoft SQL Server.

Layanan Pemindaian

Layanan Pemindaian adalah komponen opsional yang memungkinkan pemindaian antimalware pada pencadangan di penyimpanan awan, atau di folder lokal atau jaringan. Layanan Pemindaian mengharuskan server manajemen diinstal di mesin yang sama.

Menginstal Layanan Pemindaian memberikan akses ke fungsionalitas berikut ini:

- Rencana pemindaian cadangan
- Widget detail pemindaian cadangan
- Daftar putih perusahaan
- Pemulihan aman
- Kolom **Status** dalam daftar cadangan

Anda dapat menginstal Layanan Pemindaian selama instalasi server manajemen, atau Anda dapat menambahkan Layanan Pemindaian nanti, dengan memodifikasi instalasi yang ada. Untuk informasi lebih lanjut tentang cara menginstal komponen opsional sebagai Layanan Pemindaian, lihat "Untuk menginstal komponen opsional" (hlm. 85).

Penting
Layanan Pemindaian tidak kompatibel dengan database SQLite default yang digunakan server manajemen.

Anda dapat mengonfigurasi Layanan Pemindaian dengan Microsoft SQL atau database PostgreSQL. Untuk informasi lebih lanjut tentang cara memilih salah satu, lihat "Basis data untuk Layanan Pemindaian" (hlm. 90).

Basis data untuk Layanan Pemindaian

Layanan Pemindaian tidak kompatibel dengan SQLite, yang merupakan database default untuk server manajemen.

Jika server manajemen Anda menggunakan SQLite, Anda hanya dapat mengonfigurasi Layanan Pemindaian dengan database PostgreSQL. PostgreSQL 9.6 dan yang lebih baru didukung.

Jika server manajemen Anda menggunakan Microsoft SQL Server, Anda dapat mengonfigurasi Layanan Pemindaian dengan database yang sama, tanpa pengaturan tambahan. Anda juga dapat mengonfigurasi Layanan Pemindaian dengan database PostgreSQL.

Untuk mengonfigurasi Layanan Pemindaian dengan database PostgreSQL

1. Di wizard penginstalan, di dalam **Database untuk layanan pemindaian**, klik **Ubah**.
2. Pilih **Database PostgreSQL Server**.
3. Tentukan nama host instans PostgreSQL, atau alamat IP dan port.
4. Tentukan kredensial pengguna yang memiliki hak istimewa **CREATEDB** atau yang merupakan superuser.

   Catatan
   Metode autentikasi SCRAM-SHA-256 di PostgreSQL 10 dan yang lebih baru tidak didukung.

5. Klik **Selesai**.

Port

Anda dapat menyesuaikan port yang akan digunakan oleh browser web untuk mengakses server manajemen (secara default, 9877) dan port yang akan digunakan untuk komunikasi antara komponen produk (secara default, 7780). Mengubah port yang terakhir disebut setelah instalasi akan memerlukan pendaftaran ulang semua komponen.

Windows Firewall dikonfigurasi secara otomatis selama instalasi. Jika Anda menggunakan firewall lain, pastikan port terbuka untuk permintaan masuk dan keluar melalui firewall tersebut.

Server proksi

Anda dapat memilih apakah agen perlindungan menggunakan server proxy HTTP saat mencadangkan dan memulihkan dari penyimpanan awan.

Selain itu, gunakan server proxy yang sama untuk komunikasi antar komponen Acronis Cyber Protect yang berbeda.

Untuk menggunakan server proxy, tentukan nama host atau alamat IP-nya, dan nomor portnya. Jika server proxy Anda memerlukan autentikasi, tentukan kredensial akses.

Catatan
Memperbarui definisi perlindungan (definisi antivirus dan antimalware, definisi deteksi lanjutan, penilaian kerentanan dan definisi manajemen patch) tidak mungkin dilakukan saat menggunakan server proxy.

Instalasi di Linux

Persiapan

1. Jika Anda ingin menginstal Agen untuk Linux bersama dengan manajemen server, pastikan bahwa paket Linux yang diperlukan sudah diinstal pada mesin.
2. Pilih database yang akan digunakan oleh server manajemen.

Batasan

Server manajemen yang berjalan pada mesin Linux tidak mendukung instalasi jarak jauh agen perlindungan, yang digunakan, misalnya, dalam prosedur autodiscovery. Untuk informasi lebih lanjut tentang kemungkinan solusi, lihat basis pengetahuan kami: https://kb.acronis.com/content/69553.

Instalasi

Untuk menginstal server manajemen, Anda memerlukan minimal 4 GB ruang bebas dalam disk.

Untuk menginstal server manajemen

1. Sebagai pengguna root, navigasi ke direktori dengan file instalasi, buat file yang dapat dieksekusi, lalu jalankan.

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

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

2. Terima persyaratan perjanjian lisensi.
3. [Opsional] Pilih komponen yang ingin Anda instal.
   Secara default, komponen berikut akan diinstal:
   - Server Manajemen
   - Agen untuk Linux
   - Pembangun Media Yang Dapat Di-Boot
4. Tentukan port yang akan digunakan oleh browser web untuk mengakses server manajemen. Nilai default adalah 9877.
5. Tentukan port yang akan digunakan untuk komunikasi antara komponen produk. Nilai defaultnya adalah 7780.
6. Klik **Berikutnya** untuk melanjutkan instalasi.

7. Setelah instalasi selesai, pilih **Buka konsol web**, lalu klik **Keluar**. Konsol web Cyber Protect akan terbuka di browser web default Anda.

Untuk mulai menggunakan server manajemen Anda, aktifkan dengan masuk ke akun Acronis Anda atau melalui file aktivasi.

Alat Acronis Cyber Protect

Dengan alat Acronis Cyber Protect, Anda dapat dengan mudah memperoleh mesin virtual dengan perangkat lunak berikut:

- CentOS
- Komponen Acronis Cyber Protect:
  - Server Manajemen
  - Agen untuk Linux
  - Agen untuk VMware (Linux)

Alat ini disediakan sebagai arsip .zip. Arsip berisi file .ovf dan .iso. Anda dapat menyebarkan file .ovf ke host ESXi atau menggunakan file .iso untuk mem-boot mesin virtual yang ada. Arsip juga berisi file .vmdk yang harus ditempatkan di direktori yang sama dengan .ovf.

Catatan
Klien Host VMware (klien web yang digunakan untuk mengelola ESXi 6.0+ yang berdiri sendiri) tidak mengizinkan penyebaran templat OVF dengan image ISO di dalamnya. Jika ini terjadi, buat mesin virtual yang memenuhi persyaratan di bawah ini, lalu gunakan file .iso untuk menginstal perangkat lunak.

Persyaratan untuk alat virtual adalah sebagai berikut:

- Persyaratan sistem minimum:
  - 2 CPU
  - RAM 6 GB
  - Satu disk virtual 10 GB (disarankan 40 GB)
- Di pengaturan mesin virtual VMware, klik tab **Opsi** > **Umum** > **Parameter Konfigurasi**, kemudian pastikan bahwa nilai parameter `disk.EnableUUID` adalah `true`.

Batasan

Server manajemen yang berjalan pada mesin Linux, termasuk peralatan Acronis Cyber Protect, tidak mendukung instalasi jarak jauh agen perlindungan yang digunakan, misalnya, dalam prosedur autodiscovery. Untuk informasi lebih lanjut tentang kemungkinan solusi, lihat basis pengetahuan kami: https://kb.acronis.com/content/69553.

Menginstal perangkat lunak

1. Lakukan salah satu langkah berikut:
   - Sebarkan alat dari .ovf. Setelah penyebaran selesai, hidupkan mesin yang dihasilkan.
   - Boot mesin virtual yang ada dari .iso.
2. Pilih **Instal atau perbarui Acronis Cyber Protect**, lalu tekan **Enter**. Tunggu jendela pengaturan awal muncul.
3. [Opsional] Untuk mengubah pengaturan instalasi, pilih **Ubah pengaturan**, lalu tekan **Enter**. Anda dapat menentukan pengaturan berikut:
   - Nama host alat (secara default, `AcronisAppliance-<komponen acak>`).
   - Kata sandi akun "root" yang akan digunakan untuk masuk ke konsol web Cyber Protect (secara default, **tidak ditentukan**).

     Jika Anda mengosongkan nilai default, setelah Acronis Cyber Protect diinstal, Anda akan diminta untuk menentukan kata sandi. Tanpa kata sandi ini, Anda tidak akan dapat masuk ke konsol web Cyber Protect dan konsol web Cockpit.
   - Pengaturan jaringan kartu antarmuka jaringan:
     - **Gunakan DHCP** (secara default)
     - **Atur alamat IP statis**

     Jika mesin memiliki beberapa kartu antarmuka jaringan, perangkat lunak akan memilih salah satunya secara acak dan menerapkan pengaturan ini untuknya.
4. Pilih **Instal dengan pengaturan saat ini**.

Hasilnya, CentOS dan Acronis Cyber Protect akan diinstal pada mesin.

Tindakan selanjutnya

Setelah instalasi selesai, perangkat lunak akan menampilkan tautan ke konsol web Cyber Protect dan konsol web Cockpit. Hubungkan ke konsol web Cyber Protect untuk mulai menggunakan Acronis Cyber Protect: tambahkan perangkat lainnya, buat rencana pencadangan, dan sebagainya.

Untuk menambahkan mesin virtual ESXi, klik **Tambah** > **VMware ESXi**, lalu tentukan alamat dan kredensial untuk Server vCenter atau host ESXi yang berdiri sendiri.

Tidak ada pengaturan Acronis Cyber Protect yang dikonfigurasikan di konsol web Cockpit. Konsol disediakan untuk kemudahan dan pemecahan masalah.

Memperbarui perangkat lunak

1. Unduh dan buka rencana arsip .zip dengan versi peralatan yang baru.
2. Boot mesin dari iso. yang dibuka di langkah sebelumnya.
   a. Simpan .iso ke penyimpanan data vSphere Anda.
   b. Hubungkan .iso ke drive CD/DVD mesin.

c. Mulai ulang mesin.

d. [Hanya selama pembaruan pertama] Tekan **F2**, lalu ubah urutan boot sehingga drive CD/DVD menjadi yang pertama.

3. Pilih **Instal atau perbarui Acronis Cyber Protect**, lalu tekan **Enter**.
4. Pilih **Pembaruan**, lalu tekan **Enter**.
5. Setelah pembaruan selesai, lepaskan .iso dari drive CD/DVD mesin.

Hasilnya, Acronis Cyber Protect akan diperbarui. Jika versi CentOS dalam file .iso juga merupakan lebih baru daripada versi yang ada di disk, sistem operasi akan diperbarui sebelum memperbarui Acronis Cyber Protect.

Menambahkan mesin dari konsol web Cyber Protect

Anda dapat menambahkan mesin dengan salah satu cara berikut:

- Dengan mengunduh program penyiapan dan menjalankannya secara lokal di mesin target.
- Dengan menginstal agen perlindungan dari jarak jauh di mesin target.

Pembatasan

- Instalasi jarak jauh hanya tersedia dengan server manajemen yang berjalan di mesin Windows. Mesin target juga harus menjalankan Windows.
- Instalasi jarak jauh tidak didukung pada mesin yang menjalankan Windows XP.
- Instalasi jarak jauh tidak didukung pada pengontrol domain. Untuk mempelajari cara menginstal agen perlindungan pada pengontrol domain, lihat "Instalasi di Windows" (hlm. 103). Pastikan Anda menyesuaikan pengaturan instalasi dengan memilih **Gunakan akun berikut** di bagian **Akun masuk untuk layanan agen**. Untuk mempelajari lebih lanjut tentang opsi ini, lihat "Hak pengguna yang diperlukan untuk akun masuk layanan" (hlm. 86).

Menambahkan mesin yang menjalankan Windows

Anda dapat menambahkan mesin Windows dengan menginstal agen perlindungan secara jarak jauh, di konsol web Cyber Protect, atau dengan mengunduh dan menjalankan program penyiapan secara lokal.

Untuk menginstal agen secara jarak jauh

Penting
Sebelum memulai instalasi, pastikan prasyarat untuk instalasi jarak jauh terpenuhi dan setidaknya terdapat satu agen di lingkungan Anda yang dapat digunakan sebagai agen penyebaran. Untuk informasi lebih lanjut, lihat "Prasyarat untuk instalasi jarak jauh" (hlm. 96) dan "Agen penyebaran" (hlm. 97).

1. Di konsol web Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Klik **Tambah**.
3. [Untuk menginstal Agen untuk Windows] Klik **Windows**.
4. [Untuk menginstal agen yang didukung lainnya] Klik tombol yang sesuai dengan aplikasi yang ingin Anda lindungi.

   Agen berikut tersedia:
   - Agen untuk Hyper-V
   - Agen untuk SQL + Agen untuk Windows
   - Agen untuk Exchange + Agen untuk Windows

     Jika Anda mengeklik **Server Microsoft Exchange** > **Kotak surat Exchange**, dan setidaknya satu Agen untuk Exchange sudah terdaftar, lanjutkan ke langkah 9.
   - Agen untuk Active Directory + Agen untuk Windows
   - Agen untuk Office 365
5. Di panel yang terbuka, pilih agen penyebaran.
6. Tentukan nama host atau alamat IP mesin target, serta kredensial akun dengan hak administratif pada mesin tersebut.

   Sebaiknya Anda menggunakan akun Administrator bawaan. Untuk menggunakan akun lain, tambahkan akun tersebut ke grup Administrator dan ubah registri mesin target seperti yang dijelaskan di artikel berikut: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.
7. Pilih nama atau alamat IP server manajemen yang akan digunakan agen untuk mengakses server tersebut.

   Secara default, nama server dipilih. Anda mungkin harus memilih alamat IP jika server manajemen Anda memiliki lebih dari satu antarmuka jaringan atau jika Anda menghadapi masalah DNS yang mengakibatkan kegagalan registrasi agen.
8. Klik **Instal**.
9. [Jika Anda memilih **Server Microsoft Exchange** > **Kotak surat Exchange** di langkah 4], tentukan mesin tempat peran server **Akses Klien** (CAS) pada Server Microsoft Exchange diaktifkan. Untuk informasi lebih lanjut, lihat "Pencadangan kotak surat" (hlm. 445).

Untuk mengunduh dan menginstal agen secara lokal

1. Di konsol web Cyber Protect, klik ikon akun di pojok kanan atas, lalu klik **Unduhan**.
2. Klik nama penginstal Windows yang Anda butuhkan.

   Program penyiapan diunduh ke mesin Anda.
3. Jalankan program penyiapan di mesin yang ingin Anda lindungi. Untuk informasi lebih lanjut, lihat "Instalasi di Windows" (hlm. 103).

Prasyarat untuk instalasi jarak jauh

- Agar berhasil menginstal pada mesin jarak jauh yang menjalankan Windows 7 atau versi lebih baru, opsi **Panel kontrol** > **Opsi folder** > **Lihat** > **Gunakan Wizard Bersama** 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, lihat "Untuk menonaktifkan UAC" (hlm. 97).
- 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, lihat "Untuk menonaktifkan batasan jarak jauh UAC" (hlm. 97).
- File dan Printer bersama harus *diaktifkan* pada mesin jarak jauh. Untuk mengakses opsi ini:
  - [Di mesin yang menjalankan Windows 2003 Server] Buka **Panel kontrol** > **Windows Firewall** > **Pengecualian** > **File dan Printer Bersama**.
  - [Di 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**.
- Acronis Cyber Protect 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.

Catatan
Instalasi jarak jauh tidak didukung pada mesin yang menjalankan Windows XP.

Catatan
Instalasi jarak jauh tidak didukung pada pengontrol domain. Untuk mempelajari cara menginstal agen perlindungan pada pengontrol domain, lihat "Instalasi di Windows" (hlm. 103). Pastikan Anda menyesuaikan pengaturan instalasi dengan memilih **Gunakan akun berikut** di bagian **Akun masuk untuk layanan agen**. Untuk mempelajari lebih lanjut tentang opsi ini, lihat "Hak pengguna yang diperlukan untuk akun masuk layanan" (hlm. 86).

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
Untuk alasan keamanan, disarankan setelah menyelesaikan operasi manajemen – misalnya instalasi jarak jauh, kedua setelan dikembalikan ke keadaan semula: **EnableLUA**=**1** and **LocalAccountTokenFilterPolicy**=**0**.

Agen penyebaran

Untuk menginstal agen atau mesin jarak jauh dari konsol web Cyber Protect, setidaknya satu agen harus sudah diinstal di lingkungan Anda. Agen ini akan berfungsi sebagai agen penyebaran untuk instalasi jarak jauh, dan akan terhubung ke server manajemen dan mesin target jarak jauh.

Biasanya, agen perlindungan pertama di lingkungan adalah agen yang Anda instal bersama dengan server manajemen. Akan tetapi, Anda dapat memilih setiap Agen untuk Windows di lingkungan untuk menjadi agen penyebaran.

Catatan
Saat Anda menggunakan penemuan otomatis untuk menginstal agen perlindungan di beberapa mesin, agen penyebaran disebut agen penemuan.

Cara kerja agen penyebaran

1. Agen penyebaran menghubungkan server manajemen dan mengunduh file `web_installer.exe`.
2. Agen penyebaran terhubung ke mesin jarak jauh dengan menggunakan nama host atau alamat IP mesin tersebut dan kredensial administrator yang Anda tentukan, lalu mengunggah file `web_installer.exe` ke mesin tersebut.
3. File `web_installer.exe` berjalan di mesin jarak jauh dalam mode tanpa pengawasan.
4. Bergantung pada cakupan instalasi yang diperlukan, penginstal web mengambil paket instalasi tambahan dari folder `installation_files` di server manajemen, lalu menginstalnya ke mesin target menggunakan perintah `msiexec`.
   Folder `installation_files` berada di:
   - Windows: `\Program Files\Acronis\RemoteInstallationFiles\`
   - Linux: `/usr/lib/Acronis/RemoteInstallationFiles/`
5. Setelah instalasi selesai, agen terdaftar di server manajemen.

Komponen untuk instalasi jarak jauh

Komponen untuk instalasi jarak jauh diinstal secara default saat Anda menginstal server manajemen.

Bergantung pada sistem operasi mesin tempat berjalannya server manajemen, Anda dapat menemukan komponen-komponen ini di lokasi berikut:

- Windows: `%Program Files%\Acronis\RemoteInstallationFiles\installation_files`
- Linux: `/usr/lib/Acronis/RemoteInstallationFiles/installation_files`

Lokasi-lokasi ini mungkin tidak tersedia jika Anda meningkatkan dari versi lama Acronis Cyber Protect atau dengan sengaja mengecualikan **Komponen untuk Instalasi jarak jauh** saat Anda menginstal server manajemen. Dalam hal ini, Anda perlu menambahkan komponen untuk instalasi jarak jauh secara manual, dengan memperbarui dan memodifikasi instalasi Acronis Cyber Protect yang sudah ada.

Untuk menambahkan komponen instalasi jarak jauh secara manual ke instalasi yang sudah ada

1. Unduh file instalasi terbaru untuk Acronis Cyber Protect dari situs web Acronis.
   Pilih file instalasi yang sesuai dengan bit sistem operasi Anda. Umumnya, Anda akan memerlukan file instalasi **Windows 64-bit**. Jika Anda perlu menginstal agen perlindungan dari jarak jauh pada mesin 32-bit, unduh file instalasi **Windows 32/64-bit**.
2. Di mesin tempat server manajemen berjalan, mulai file instalasi, lalu pilih **Perbarui**.

3. Setelah pembaruan selesai, mulai file instalasi lagi, lalu pilih **Modifikasi instalasi saat ini**.
4. Pilih **Komponen untuk Instalasi jarak jauh**, lalu klik **Selesai**.

   Setelah instalasi selesai, Anda akan dapat menginstal agen perlindungan pada mesin jarak jauh dari konsol web Cyber Protect.

Menambahkan mesin yang menjalankan Linux

Anda dapat menambahkan mesin Linux hanya dengan menginstal agen perlindungan secara lokal. Instalasi jarak jauh tidak didukung.

Untuk menambahkan mesin yang menjalankan Linux

1. Di konsol web Cyber Protect, klik **Semua perangkat** > **Tambahkan**.
2. Klik **Linux**.
   Program penyiapan diunduh ke mesin Anda.
3. Jalankan program penyiapan di mesin yang ingin Anda lindungi. Untuk informasi lebih lanjut, lihat "Instalasi di Linux" (hlm. 105).

Menambahkan mesin yang menjalankan macOS

Anda dapat menambahkan mesin macOS hanya dengan menginstal agen perlindungan secara lokal. Instalasi jarak jauh tidak didukung.

Untuk menambahkan mesin yang menjalankan macOS

1. Di konsol web Cyber Protect, klik **Semua perangkat** > **Tambahkan**.
2. Klik **Mac**.
   Program penyiapan diunduh ke mesin Anda.
3. Jalankan program penyiapan di mesin yang ingin Anda lindungi. Untuk informasi lebih lanjut, lihat "Instalasi di MacOS" (hlm. 106).

Menambahkan vCenter atau host ESXi

Ada empat metode penambahan vCenter atau host ESXi yang berdiri sendiri ke server manajemen:

- Menyebarkan Agen untuk VMware (Virtual Appliance)
  Metode ini disarankan dalam banyak kasus. Alat virtual akan secara otomatis disebarkan untuk setiap host yang dikelola oleh vCenter yang Anda tentukan. Anda dapat memilih host dan menyesuaikan pengaturan alat virtual.
- Menginstal Agen untuk VMware (Windows)
  Anda mungkin perlu menginstal Agen untuk VMware di mesin fisik yang menjalankan Windows untuk tujuan pencadangan offloaded atau bebas LAN.
  - **Cadangan offloaded**
    Gunakan jika host ESXi produksi Anda dimuat dengan sangat berat sehingga host menjalankan peralatan virtual tidak diinginkan.

- **Pencadangan bebas 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. Untuk instruksi mendetail, lihat "Pencadangan bebas LAN".

Jika server manajemen berjalan di Windows, agen akan secara otomatis disebarkan untuk mesin yang Anda tentukan. Jika tidak, Anda harus menginstal agen secara manual.

- Mendaftarkan Agen untuk VMware yang sudah diinstal

  Ini adalah langkah yang diperlukan setelah Anda menginstal ulang server manajemen. Anda juga dapat mendaftar dan mengonfigurasi Agen untuk VMware (Virtual Appliance) yang disebarkan dari templat OVF.
- Mengonfigurasi Agen untuk VMware yang sudah terdaftar

  Ini adalah langkah yang diperlukan setelah Anda menginstal Agen untuk VMware (Windows) secara manual atau menyebarkan alat Acronis Cyber Protect. Selain itu, Anda juga dapat mengaitkan Agen untuk VMware yang sudah dikonfigurasi dengan vCenter Server lain atau host ESXi yang berdiri sendiri.

Menyebarkan Agen untuk VMware (Virtual Appliance) melalui antarmuka web

1. Klik **Semua perangkat** > **Tambah**.
2. Klik **VMware ESXi**.
3. Pilih **Sebarkan sebagai alat virtual ke setiap host vCenter**.
4. Tentukan alamat dan kredensial akses untuk vCenter Server atau host ESXi yang berdiri sendiri. Kami sarankan untuk menggunakan akun yang memiliki peran **Administrator**. Jika tidak, sediakan akun dengan privilese yang diperlukan pada vCenter Server atau ESXi.
5. Pilih nama atau alamat IP server manajemen yang akan digunakan agen untuk mengakses server tersebut.

   Secara default, nama server dipilih. Anda mungkin harus memilih alamat IP jika server manajemen Anda memiliki lebih dari satu antarmuka jaringan atau jika Anda menghadapi masalah DNS yang mengakibatkan kegagalan registrasi agen.
6. [Opsional] Klik **Pengaturan** untuk menyesuaikan pengaturan penyebaran:
   - ESXi host yang Anda ingin sebarkan dengan agen (hanya jika Server vCenter ditentukan pada langkah sebelumnya).
   - Nama alat virtual.
   - Penyimpanan data lokasi alat akan ditempatkan.
   - Pool sumber daya atau vApp yang akan berisi alat.
   - Jaringan yang akan dihubungkan dengan adaptor jaringan alat virtual.
   - Pengaturan jaringan alat virtual. Anda dapat memilih konfigurasi otomatis DHCP atau menentukan nilai secara manual, termasuk alamat IP statis.
7. Klik **Sebarkan**.

Menginstal Agen untuk VMware (Windows)

Persiapan

Ikuti langkah-langkah persiapan yang dijelaskan di bagian "Menambahkan mesin yang menjalankan Windows".

Instalasi

1. Klik **Semua perangkat** > **Tambah**.
2. Klik **VMware ESXi**.
3. Pilih **Instal dari jauh di mesin yang menjalankan Windows**.
4. Pilih agen penyebaran.
5. Tentukan nama host atau alamat IP mesin target, serta kredensial akun dengan hak istimewa administratif pada mesin tersebut.
6. Pilih nama atau alamat IP server manajemen yang akan digunakan agen untuk mengakses server tersebut.
   Secara default, nama server dipilih. Anda mungkin harus memilih alamat IP jika server manajemen Anda memiliki lebih dari satu antarmuka jaringan atau jika Anda menghadapi masalah DNS yang mengakibatkan kegagalan registrasi agen.
7. Klik **Hubungkan**.
8. Tentukan alamat dan kredensial untuk vCenter Server atau host ESXi yang berdiri sendiri, lalu klik **Sambungkan**. Kami sarankan untuk menggunakan akun yang memiliki peran **Administrator**. Jika tidak, sediakan akun dengan privilese yang diperlukan pada vCenter Server atau ESXi.
9. Klik **Instal** untuk menginstal agen.

Mendaftarkan Agen untuk VMware yang sudah diinstal

Bagian ini menjelaskan cara mendaftarkan Agen untuk VMware melalui antarmuka web.

Metode pendaftaran alternatif:

- Anda dapat mendaftarkan Agen untuk VMware (Virtual Appliance) dengan menentukan server manajemen di UI alat virtual. Lihat langkah 3 pada "Mengonfigurasi alat virtual" di "Menyebarkan Agen untuk VMware (Virtual Appliance) dari Templat OVF".
- Agen untuk VMware (Windows) terdaftar selama instalasi lokal.

Untuk mendaftarkan Agen untuk VMware

1. Klik **Semua perangkat** > **Tambah**.
2. Klik **VMware ESXi**.
3. Pilih **Daftarkan agen yang sudah diinstal**.

4. Pilih agen penyebaran.
5. Jika Anda mendaftarkan *Agen untuk VMware (Windows)*, tentukan nama host atau alamat IP mesin tempat agen diinstal, dan kredensial akun dengan privilese administratif pada mesin tersebut.
   Jika Anda mendaftarkan *Agen untuk VMware (Virtual Appliance)*, tentukan nama host atau alamat IP alat virtual, dan kredensial untuk Server vCenter atau host ESXi yang berdiri sendiri tempat alat berjalan.
6. Pilih nama atau alamat IP server manajemen yang akan digunakan agen untuk mengakses server tersebut.
   Secara default, nama server dipilih. Anda mungkin harus memilih alamat IP jika server manajemen Anda memiliki lebih dari satu antarmuka jaringan atau jika Anda menghadapi masalah DNS yang mengakibatkan kegagalan registrasi agen.
7. Klik **Hubungkan**.
8. Tentukan nama host atau alamat IP vCenter Server atau host ESXi, dan kredensial untuk mengaksesnya, lalu klik **Sambungkan**. Kami sarankan untuk menggunakan akun yang memiliki peran **Administrator**. Jika tidak, sediakan akun dengan privilese yang diperlukan pada vCenter Server atau ESXi.
9. Klik **Daftar** untuk mendaftarkan agen.

Mengonfigurasi Agen untuk VMware yang sudah terdaftar

Bagian ini menjelaskan cara mengaitkan Agen untuk VMware dengan vCenter Server atau ESXi di antarmuka web. Agen untuk VMware (Virtual Appliance)

Sebagai alternatif, Anda dapat melakukannya di konsol Agen untuk VMware (Virtual Appliance). Atau, Anda juga dapat melakukan ini di konsol Agen untuk VMware (Virtual Appliance) atau dengan mengklik **Pengaturan** > **Agen** > agen > **Detail** > **vCenter/ESXi**.

Untuk mengonfigurasi Agen untuk VMware

1. Klik **Semua perangkat** > **Tambah**.
2. Klik **VMware ESXi**.
3. Perangkat lunak ini menunjukkan Agen untuk VMware yang tidak dikonfigurasi yang muncul pertama kali secara alfabetis.
   Jika semua agen yang terdaftar di server manajemen dikonfigurasikan, klik **Konfigurasi agen yang sudah terdaftar**, dan perangkat lunak akan menunjukkan agen yang muncul pertama kali secara alfabetis.
4. Jika perlu, klik **Mesin dengan agen**, lalu pilih agen yang akan dikonfigurasi.
5. Tentukan atau ubah nama host atau alamat IP vCenter Server atau host ESXi, dan kredensial untuk mengaksesnya. Kami sarankan untuk menggunakan akun yang memiliki peran **Administrator**. Jika tidak, sediakan akun dengan privilese yang diperlukan pada vCenter Server atau ESXi.
6. Klik **Konfigurasi** untuk menyimpan perubahan.

Menambahkan klaster Scale Computing HC3

Untuk menambahkan klaster Scale Computing HC3 ke server manajemen Cyber Protect

1. Menyebarkan Agen untuk Scale Computing HC3 (Alat Virtual) di klaster.
2. Konfigurasikan koneksinya ke klaster ini dan ke server manajemen Cyber Protect.

Menginstal agen secara lokal

Instalasi di Windows

Untuk menginstal Agen untuk Windows, Agen untuk Hyper-V, Agen untuk Exchange, Agen untuk SQL, atau Agen untuk Active Directory

1. Masuk sebagai administrator dan mulai program penyiapan Acronis Cyber Protect.
2. [Opsional] Untuk mengubah bahasa program penyiapan, klik **Pengaturan bahasa**.
3. Terima persyaratan perjanjian lisensi dan pernyataan privasi, lalu klik **Lanjutkan**.
4. Pilih **Instal agen perlindungan**.
5. Lakukan yang berikut ini:
   - Klik **Instal**.

     Ini adalah cara termudah untuk menginstal produk. Sebagian besar parameter instalasi akan ditetapkan ke nilai standarnya.

     Komponen berikut akan diinstal:
     - Agen untuk Windows
     - Agen lainnya (Agen untuk Hyper-V, Agen untuk Exchange, Agen untuk SQL, dan Agen untuk Active Directory), jika masing-masing hypervisor atau aplikasi terdeteksi pada mesin
     - Pembangun Media Yang Dapat Di-Boot
     - Command-Line Tool
     - Monitor Cyber Protect
   - Klik **Sesuaikan pengaturan instalasi** untuk mengonfigurasi pengaturan.

     Anda akan dapat memilih komponen yang akan diinstal dan menentukan parameter tambahan. Untuk perincian, lihat "Menyesuaikan pengaturan instalasi" (hlm. 84).
   - Klik **Buat file .mst dan .msi untuk instalasi tanpa pengawasan** agar dapat mengekstrak rencana instalasi. Tinjau atau modifikasi pengaturan instalasi yang akan ditambahkan ke file .mst, lalu klik **Hasilkan**. Langkah lebih lanjut dari prosedur ini tidak diperlukan.

     Jika Anda ingin menyebarkan agen melalui Kebijakan Grup, lanjutkan seperti yang dijelaskan dalam "Menyebarkan agen melalui Kebijakan Grup" (hlm. 175).
6. Tentukan server manajemen tempat mesin dengan agen akan didaftarkan:
   a. Tentukan nama host atau alamat IP mesin tempat server manajemen diinstal.
   b. Tentukan kredensial administrator server manajemen atau token registrasi.

Untuk informasi lebih lanjut tentang cara membuat token pendaftaran, lihat "Langkah 1: Membuat token pendaftaran" (hlm. 176).

c. Klik **Selesai**.

7. Jika diminta, pilih apakah mesin dengan agen akan ditambahkan ke organisasi atau ke salah satu unit.

   Permintaan ini akan muncul jika Anda mengelola lebih dari satu unit, atau organisasi dengan setidaknya satu unit. Jika tidak, mesin akan secara otomatis ditambahkan ke unit atau organisasi yang Anda kelola. Untuk informasi lebih lanjut, lihat "Unit dan akun administratif" (hlm. 635).

8. Lanjutkan instalasi.
9. Setelah instalasi selesai, klik **Tutup**.
10. Jika Anda menginstal Agen untuk Exchange, Anda akan dapat mencadangkan database Exchange. Jika Anda ingin mencadangkan kotak surat Exchange, buka konsol web Cyber Protect, klik **Tambah** > **Microsoft Exchange Server** > **Kotak surat Exchange**, lalu tentukan mesin tempat peran server **Akses Klien** (CAS) Microsoft Exchange Server diaktifkan. Untuk informasi lebih lanjut, lihat "Pencadangan kotak surat" (hlm. 445).

Untuk menginstal Agen untuk VMware (Windows), Agen untuk Office 365, Agen untuk Oracle, atau Agen untuk Exchange pada mesin tanpa Microsoft Exchange Server

1. Masuk sebagai administrator dan mulai program penyiapan Acronis Cyber Protect.
2. [Opsional] Untuk mengubah bahasa program penyiapan, klik **Pengaturan bahasa**.
3. Terima persyaratan perjanjian lisensi dan pernyataan privasi, lalu klik **Lanjutkan**.
4. Pilih **Instal agen perlindungan**, lalu klik **Sesuaikan pengaturan instalasi**.
5. Di sebelah **Apa yang diinstal**, klik **Ubah**.
6. Pilih kotak centang untuk agen yang ingin Anda instal.Pilih kotak centang yang sesuai dengan agen yang ingin Anda instal. Kosongkan kotak centang untuk komponen yang tidak ingin Anda instal. Klik **Selesai** untuk melanjutkan.
7. Tentukan server manajemen tempat mesin dengan agen akan didaftarkan:
   a. Di sebelah **Server Manajemen Acronis Cyber Protect**, klik **Tentukan**.
   b. Tentukan nama host atau alamat IP mesin tempat server manajemen diinstal.
   c. Tentukan kredensial administrator server manajemen atau token registrasi.

      Untuk informasi lebih lanjut tentang cara membuat token pendaftaran, lihat "Langkah 1: Membuat token pendaftaran" (hlm. 176).

   d. Klik **Selesai**.
8. Jika diminta, pilih apakah mesin dengan agen akan ditambahkan ke organisasi atau ke salah satu unit.

   Permintaan ini akan muncul jika Anda mengelola lebih dari satu unit, atau organisasi dengan setidaknya satu unit. Jika tidak, mesin akan secara otomatis ditambahkan ke unit atau organisasi yang Anda kelola. Untuk informasi lebih lanjut, lihat "Unit dan akun administratif" (hlm. 635).

9. [Opsional] Ubah pengaturan instalasi lain seperti yang dijelaskan dalam "Menyesuaikan pengaturan instalasi" (hlm. 84).
10. Klik **Instal** untuk melanjutkan instalasi.
11. Setelah instalasi selesai, klik **Tutup**.
12. [Hanya ketika menginstal Agen untuk VMware (Windows)] Lakukan prosedur yang dijelaskan dalam "Mengonfigurasi Agen untuk VMware yang sudah terdaftar" (hlm. 102).
13. [Hanya ketika menginstal Agen untuk Exchange] Buka konsol web Cyber Protect, klik **Tambah** > **Microsoft Exchange Server** > **Kotak surat Exchange**, lalu tentukan mesin tempat peran server **Akses Klien** (CAS) Microsoft Exchange Server diaktifkan. Untuk informasi lebih lanjut, lihat "Pencadangan kotak surat" (hlm. 445).

Instalasi di Linux

Persiapan

1. Pastikan bahwa paket Linux yang diperlukan sudah diinstal pada mesin.
2. 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 web 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.

Untuk menginstal Agen untuk Linux

1. Sebagai pengguna root, navigasi ke direktori dengan file instalasi (file .i686 atau .x86_64), buat file yang dapat dieksekusi, lalu jalankan.

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

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

2. Terima persyaratan perjanjian lisensi.
3. Tentukan komponen yang akan dipasang:
   a. Kosongkan kotak centang **Server Manajemen Acronis Cyber Protect**.
   b. Pilih kotak centang untuk agen yang ingin Anda instal. Agen berikut tersedia:
      - **Agen untuk Linux**
      - **Agen untuk Oracle**

      Agen untuk Oracle mengharuskan Agen untuk Linux untuk diinstal juga.
   c. Klik **Berikutnya**.

4. Tentukan server manajemen tempat mesin dengan agen akan didaftarkan:
   a. Tentukan nama host atau alamat IP mesin tempat server manajemen diinstal.
   b. Tentukan nama pengguna dan kata sandi administrator server manajemen.
   c. Klik **Berikutnya**.
5. Jika diminta, pilih apakah mesin dengan agen akan ditambahkan ke organisasi atau ke salah satu unit, lalu tekan **Enter**.

   Perintah ini muncul jika akun yang ditentukan pada langkah sebelumnya mengelola lebih dari satu unit atau organisasi dengan setidaknya satu unit.
6. Jika UEFI Secure Boot diaktifkan pada mesin, akan diinformasikan bahwa Anda harus memulai ulang sistem setelah instalasi. 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.
7. Setelah instalasi selesai, lakukan salah satu langkah berikut:
   - Klik **Mulai Kembali**, jika Anda disarankan untuk memulai kembali sistem di langkah sebelumnya.

     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

Instalasi di MacOS

Untuk menginstal Agen untuk Mac

1. Klik dua kali pada file instalasi (.dmg).
2. Tunggu saat sistem operasi melakukan mounting profil disk instalasi.
3. Klik dua kali pada **Instal**, lalu klik **Lanjutkan**.
4. [Opsional] Klik **Ubah lokasi instalasi** untuk mengubah disk tempat perangkat lunak akan diinstal. Secara default, disk startup sistem dipilih.
5. Klik **Instal**. Jika diminta, masukkan nama pengguna dan kata sandi administrator.
6. Tentukan server manajemen tempat mesin dengan agen akan didaftarkan:

a. Tentukan nama host atau alamat IP mesin tempat server manajemen diinstal.

b. Tentukan nama pengguna dan kata sandi administrator server manajemen.

c. Klik **Daftar**.

7. Jika diminta, pilih apakah mesin dengan agen akan ditambahkan ke organisasi atau ke salah satu unit, lalu klik **Selesai**.
   Perintah ini muncul jika akun yang ditentukan pada langkah sebelumnya mengelola lebih dari satu unit atau organisasi dengan setidaknya satu unit.
8. Setelah instalasi selesai, klik **Tutup**.

Instalasi atau penghapusan instalasi tanpa pengawasan

Instalasi atau penghapusan instalasi tanpa pengawasan di Windows

Bagian ini menjelaskan cara menginstal atau menghapus instalasi Acronis Cyber Protect dalam mode tanpa pengawasan pada mesin yang menjalankan Windows, menggunakan Windows Installer (program `msiexec`). Dalam domain Active Directory, cara lain untuk melakukan instalasi tanpa pengawasan adalah melalui Kebijakan Grup— lihat "Menyebarkan agen melalui Kebijakan Grup" (hlm. 175).

Selama instalasi, Anda dapat menggunakan file yang dikenal sebagai **transformasi** (file.mst). Transformasi adalah file dengan parameter instalasi. Sebagai alternatif, Anda dapat menentukan parameter instalasi langsung di baris perintah.

Membuat transformasi .mst dan mengekstrak paket instalasi

1. Masuk sebagai administrator dan mulai program penyiapan.
2. Klik **Buat file .mst dan .msi untuk instalasi tanpa pengawasan**.
3. [Tidak tersedia di semua program penyiapan] Dalam **Bit komponen**, pilih **32-bit** atau **64-bit**.
4. Di **Apa yang diinstal**, pilih komponen yang ingin Anda instal, lalu klik **Selesai**.
   Paket instalasi untuk komponen-komponen ini akan diekstrak dari program pengaturan.
5. Dalam **Server Manajemen Acronis Cyber Protect**, 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 "Langkah 1: Membuat token pendaftaran" (hlm. 176).
6. [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 penginstalan agen pada pengontrol domain hanya baca, lihat artikel basis pengetahuan ini.

7. Tinjau atau modifikasi pengaturan instalasi lain yang akan ditambahkan ke file .mst, lalu klik **Lanjutkan**.
8. Pilih folder di mana transform .mst akan dibuat dan paket instalasi .msi dan .cab akan diekstrak, lalu klik **Hasilkan**.

Hasilnya, transformasi .mst dibuat dan paket instalasi .msi dan .cab akan diekstraksi ke folder yang Anda tentukan.

Menginstal produk menggunakan transformasi .mst

Pada baris perintah, jalankan perintah berikut:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Di mana:

- `<nama paket>` adalah nama file .msi. Nama ini adalah **AB.msi** atau **AB64.msi**, tergantung pada bitness sistem operasi.
- `<mengubah nama>` adalah nama transformasi. Nama ini adalah **AB.msi.mst** atau **AB64.msi.mst**, tergantung pada bitness sistem operasi.

Misalnya, `msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`

Menginstal atau menghapus instalasi produk dengan menentukan parameter secara manual

Pada baris perintah, jalankan perintah berikut:

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Di sini, `<nama paket>` adalah nama file .msi. Nama ini adalah **AB.msi** atau **AB64.msi**, tergantung pada bitness sistem operasi.

Parameter yang tersedia beserta nilainya dijelaskan dalam "Parameter umum" (hlm. 109).

Contoh

- Menginstal Server Manajemen dan Komponen untuk Instalasi Jarak Jauh.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature
TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1
```

- Menginstal Agen untuk Windows, Alat Baris Perintah, dan Monitor Cyber Protect. Mendaftarkan mesin dengan agen di server manajemen yang diinstal sebelumnya.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
AGREEMENT=1 MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
```

- Memperbarui Server Manajemen, Node Penyimpanan, Layanan Katalog, dan agen perlindungan.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AcronisCentralizedManagementServer,BackupAndRecoveryAgent,AgentsCoreComponen
ts,StorageServer,CatalogBrowser CATALOG_DATA_MIGRATION_PATH="C:\MyFolder\tmp"
```

Parameter pemasangan atau penghapusan instalasi tanpa pengawasan

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

Selain parameter tesebut, Anda juga dapat menggunakan parameter lain dari `msiexec`, seperti yang dijelaskan di https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Parameter instalasi

Parameter umum

`ADDLOCAL=<list of components>`

Komponen yang akan diinstal, dipisahkan dengan koma tanpa karakter spasi. Semua komponen yang ditentukan harus diekstraksi dari program pengaturan sebelum instalasi.

Daftar lengkap komponen adalah sebagai berikut.

Komponen	Harus diinstal bersama	Bitness	Nama komponen / deskripsi
AcronisCentralizedManagementServer	WebConsole	32-bit/64-bit	Server Manajemen
WebConsole	AcronisCentralizedManagementServer	32-bit/64-	Web Console

		bit	
ComponentRegisterFeature	AcronisCentralizedManagement Server	32-bit/64-bit	Komponen untuk Instalasi Jarak Jauh
AtpScanService	AcronisCentralizedManagement Server	32-bit/64-bit	Layanan Pemindaian
AgentsCoreComponents		32-bit/64-bit	Komponen inti untuk agen
BackupAndRecoveryAgent	AgentsCoreComponents	32-bit/64-bit	Agen untuk Windows
ArxAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agen untuk Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agen untuk SQL
ARADAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agen untuk Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agen untuk Oracle
ArxOnlineAgentFeature	AgentsCoreComponents	32-bit/64-bit	Agen untuk Office 365
AcronisESXSupport	AgentsCoreComponents	32-bit/64-bit	Agen untuk VMware (Windows)
HyperVAgent	AgentsCoreComponents	32-bit/64-bit	Agen untuk Hyper-V
ESXVirtualAppliance		32-	Agen untuk

		bit/64-bit	VMware (Virtual Appliance)
ScaleVirtualAppliance		32-bit/64-bit	Agen untuk Scale Computing HC3 (Alat Virtual)
CommandLineTool		32-bit/64-bit	Command-Line Tool
TrayMonitor	BackupAndRecoveryAgent	32-bit/64-bit	Monitor Cyber Protect
BackupAndRecoveryBootableComponents		32-bit/64-bit	Pembangun Media Yang Dapat Di-Boot
PXEServer		32-bit/64-bit	Server PXE
StorageServer	BackupAndRecoveryAgent	64-bit	Simpul Penyimpanan
CatalogBrowser	JRE 8 Update 111 ke atas	64-bit	Layanan Katalog

`TARGETDIR=<path>`

Folder tempat produk akan diinstal.

`REBOOT=ReallySuppress`

Jika parameter ditentukan, reboot mesin tidak diperbolehkan.

`CURRENT_LANGUAGE=<language ID>`

Bahasa produk. Nilai yang tersedia adalah sebagai berikut: `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`.

`ACEP_AGREEMENT={0,1}`

Jika nilainya `1`, mesin akan berpartisipasi dalam Acronis Customer Experience Program (ACEP).

`REGISTRATION_ADDRESS=<host name or IP address>:<port>`

Nama host atau alamat IP mesin tempat server manajemen diinstal. Agen, Simpul Penyimpanan, dan Layanan Katalog yang ditentukan dalam parameter `ADDLOCAL` akan didaftarkan di server manajemen ini. Nomor port wajib diisi jika berbeda dari nilai default (9877).

Dengan parameter ini, Anda harus menentukan parameter `REGISTRATION_TOKEN`, atau parameter `REGISTRATION_LOGIN`, dan `REGISTRATION_PASSWORD`.

`REGISTRATION_TOKEN=<token>`

Token registrasi yang dibuat di konsol web Cyber Protect seperti yang dijelaskan di Menyebarkan agen melalui Kebijakan Grup.

`REGISTRATION_LOGIN=<user name>, REGISTRATION_PASSWORD=<password>`

Nama pengguna dan kata sandi administrator server manajemen.

`REGISTRATION_TENANT=<unit ID>`

Unit dalam organisasi. Agen, Simpul Penyimpanan, dan Layanan Katalog yang ditentukan dalam parameter `ADDLOCAL` akan ditambahkan ke unit ini.

Untuk mempelajari ID unit, di konsol web Cyber Protect, klik **Pengaturan** > **Akun**, pilih unit, lalu klik **Detail**.

Parameter ini tidak berfungsi tanpa `REGISTRATION_TOKEN`, atau `REGISTRATION_LOGIN` dan `REGISTRATION_PASSWORD`. Dalam kasus ini, komponen akan ditambahkan ke organisasi.

Tanpa parameter ini, komponen akan ditambahkan ke organisasi.

`REGISTRATION_REQUIRED={0,1}`

Hasil instalasi jika pendaftaran gagal. Jika nilainya `1`, instalasi akan gagal. Jika nilainya `0`, instalasi akan berhasil diselesaikan meskipun komponen tidak terdaftar.

`REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY=<public key value>`

Parameter yang saling berhubungan ini menentukan metode pemeriksaan sertifikat server manajemen selama pendaftaran. Periksa sertifikat jika Anda ingin memverifikasi keaslian server manajemen untuk mencegah serangan MITM.

Jika nilainya `1`, verifikasi akan menggunakan sistem CA, atau bundel CA yang disertakan bersama produk. Apabila kunci publik yang disematkan ditentukan, verifikasinya akan menggunakan kunci ini. Jika nilainya `0` atau parameternya tidak ditentukan, verifikasi sertifikat tidak dilakukan, tetapi lalu lintas registrasi tetap dienkripsi.

`/l*v <log file>`

Jika parameternya ditentukan, log instalasi dalam mode verbose akan disimpan ke file yang ditentukan. File log dapat digunakan untuk menganalisis masalah instalasi.

Parameter instalasi server manajemen

`WEB_SERVER_PORT=<port number>`

Port yang akan digunakan oleh browser web untuk mengakses server manajemen. Secara default, 9877.

`AMS_ZMQ_PORT=<port number>`

Port yang akan digunakan untuk komunikasi antara komponen produk. Secara default, 7780.

`SQL_INSTANCE=<instance>`

Database yang akan digunakan oleh server manajemen. Anda dapat memilih edisi Microsoft SQL Server 2012, Microsoft SQL Server 2014, atau Microsoft SQL Server 2016. Instans yang Anda pilih juga dapat digunakan oleh program lain.

Tanpa parameter ini, database SQLite bawaan akan digunakan.

`SQL_USER_NAME=<user name>` dan `SQL_PASSWORD=<password>`

Kredensial akun masuk Microsoft SQL Server. Server manajemen akan menggunakan kredensial ini agar untuk terhubung ke instans SQL Server yang dipilih. Tanpa parameter ini, server manajemen akan menggunakan kredensial akun layanan server manajemen (**Pengguna AMS**).

Akun yang di bawahnya layanan server manajemen akan berjalan

Tentukan salah satu parameter berikut:

- `AMS_USE_SYSTEM_ACCOUNT={0,1}`
  Jika nilainya `1`, akun sistem akan digunakan.
- `AMS_CREATE_NEW_ACCOUNT={0,1}`
  Jika nilainya `1`, akun baru akan dibuat.
- `AMS_SERVICE_USERNAME=<user name>` dan `AMS_SERVICE_PASSWORD=<password>`
  Akun yang ditentukan akan digunakan.

Parameter instalasi agen

`HTTP_PROXY_ADDRESS=<IP address>` dan `HTTP_PROXY_PORT=<port>`

Server proksi HTTP yang akan digunakan oleh agen. Tanpa parameter ini, tidak ada server proksi yang akan digunakan.

`HTTP_PROXY_LOGIN=<login>` dan `HTTP_PROXY_PASSWORD=<password>`

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

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

Jika nilainya `0`, atau parameter tidak ditentukan, agen akan menggunakan server proxy hanya untuk pencadangan dan pemulihan dari awan. Jika nilainya `1`, agen juga akan terhubung ke server manajemen melalui server proxy.

`SET_ESX_SERVER={0,1}`

Jika nilainya `0`, Agen untuk VMware yang diinstal tidak akan terhubung ke vCenter Server atau host ESXi. Setelah instalasi, lanjutkan seperti yang dijelaskan dalam "Mengkonfigurasi Agen yang sudah terdaftar untuk VMware".

Jika nilainya `1`, tentukan parameter berikut:

`ESX_HOST=<host name or IP address>`

Nama host atau alamat IP dari Server vCenter atau host ESXi.

`ESX_USER=<user name>` dan `ESX_PASSWORD=<password>`

Kredensial untuk mengakses vCenter Server atau host ESXi.

Akun yang di bawahnya layanan agen akan berjalan

Tentukan salah satu parameter berikut:

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`
  Jika nilainya `1`, akun sistem akan digunakan.
- `MMS_CREATE_NEW_ACCOUNT={0,1}`
  Jika nilainya `1`, akun baru akan dibuat.
- `MMS_SERVICE_USERNAME=<user name>` dan `MMS_SERVICE_PASSWORD=<password>`
  Akun yang ditentukan akan digunakan.

Parameter instalasi simpul penyimpanan

Akun yang di bawahnya layanan simpul penyimpanan akan dijalankan

Tentukan salah satu parameter berikut:

- `ASN_USE_SYSTEM_ACCOUNT={0,1}`
  Jika nilainya `1`, akun sistem akan digunakan.
- `ASN_CREATE_NEW_ACCOUNT={0,1}`
  Jika nilainya `1`, akun baru akan dibuat.
- `ASN_SERVICE_USERNAME=<user name>` dan `ASN_SERVICE_PASSWORD=<password>`
  Akun yang ditentukan akan digunakan.

Parameter pemasangan layanan katalog

`CATALOG_DATA_MIGRATION_PATH=<path>`

Gunakan parameter ini untuk memigrasikan data katalog ke versi baru layanan katalog di Acronis Cyber Protect 15 Update 4. Tentukan jalur ke folder sementara tempat data katalog akan diekspor.

`SKIP_CATALOG_DATA_MIGRATION=1`

Gunakan parameter ini untuk melewati migrasi data katalog.

Parameter `SKIP_CATALOG_DATA_MIGRATION` dan `CATALOG_DATA_MIGRATION_PATH` sama-sama eksklusif.

Parameter penghapusan instalasi

`REMOVE={<list of components>|ALL}`

Komponen yang akan dihapus, dipisahkan dengan koma tanpa karakter spasi.

Komponen yang tersedia sebelumnya sudah dijelaskan di bagian ini.

Jika nilainya `ALL`, semua komponen produk akan dihapus instalasinya. Selain itu, Anda juga dapat menentukan parameter berikut:

`DELETE_ALL_SETTINGS={0, 1}`

Jika nilainya `1`, log produk, tugas, dan pengaturan konfigurasi akan dihapus.

Instalasi atau penghapusan tanpa pengawasan di Linux

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

Untuk menginstal atau menghapus instalasi produk

1. Buka Terminal.
2. Jalankan perintah berikut:

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

   Di sini, `<nama paket>` adalah nama paket instalasi (file .i686 atau .x86_64).
3. [Hanya ketika menginstal Agen untuk Linux] Jika UEFI Secure Boot diaktifkan pada mesin, akan diinformasikan bahwa Anda harus memulai ulang sistem setelah instalasi. Pastikan untuk mengingat kata sandi apa (kata sandi 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.

Parameter instalasi

Parameter umum

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

Komponen yang akan diinstal, dipisahkan dengan koma tanpa karakter spasi.

Komponen berikut ini tersedia untuk instalasi:

Komponen	Deskripsi komponen
AcronisCentralizedManagementServer	Server Manajemen
BackupAndRecoveryAgent	Agen untuk Linux
BackupAndRecoveryBootableComponents	Pembangun Media Yang Dapat Di-Boot

Tanpa parameter ini, semua komponen di atas akan diinstal.

`--language=<language ID>`

Bahasa produk. Nilai yang tersedia adalah sebagai berikut: `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`.

`{-d|--debug}`

Jika parameternya ditentukan, log instalasi akan ditulis dalam mode verbose. Log berada di file **/var/log/trueimage-setup.log**.

`{-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}`

Jika parameter ditentukan, ketidakadaan paket Linux yang diperlukan akan diabaikan selama instalasi.

Parameter instalasi server manajemen

`{-W |--web-server-port=}<port number>`

Port yang akan digunakan oleh browser web untuk mengakses server manajemen. Secara default, 9877.

`--ams-tcp-port=<port number>`

Port yang akan digunakan untuk komunikasi antara komponen produk. Secara default, 7780.

Parameter instalasi agen

Tentukan salah satu parameter berikut:

- `--skip-registration`
  - Jangan mendaftarkan agen pada server manajemen.

- `{-C |--ams=}<host name or IP address>`
  - Nama host atau alamat IP mesin tempat server manajemen diinstal. Agen akan terdaftar di server manajemen ini.

Jika Anda menginstal agen dan server manajemen dalam satu perintah, agen akan terdaftar di server manajemen ini, apa pun parameter `-C`-nya.

Dengan parameter ini, Anda harus menentukan parameter `token`, atau parameter `masuk` dan `kata sandi`.

`--token=<token>`

Token registrasi yang dibuat di konsol web Cyber Protect seperti yang dijelaskan di Menyebarkan agen melalui Kebijakan Grup.

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

Kredensial administrator server manajemen.

`--unit=<unit ID>`

Unit dalam organisasi. Agen akan ditambahkan ke unit ini.

Untuk mempelajari ID unit, di konsol web Cyber Protect, klik **Pengaturan** > **Akun**, pilih unit, lalu klik **Detail**.

Tanpa parameter ini, agen akan ditambahkan ke organisasi.

`--reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}`

Metode pemeriksaan sertifikat server manajemen selama pendaftaran. Periksa sertifikat jika Anda ingin memverifikasi keaslian server manajemen untuk mencegah serangan MITM.

Jika nilainya `https` atau parameter tidak ditentukan, pemeriksaan sertifikat tidak dilakukan, tetapi lalu lintas registrasi tetap dienkripsi. Jika nilainya *bukan*`https`, pemeriksaan menggunakan sistem CA, atau bundel CA yang disertakan bersama produk atau kunci publik yang disematkan.

`--reg-transport-pinned-public-key=<public key value>`

Nilai kunci publik yang disematkan. Parameter ini harus ditentukan bersama atau sebagai ganti dari parameter `--reg-transport=https-pinned-public-key`.

- `--http-proxy-host=<IP address>` dan `--http-proxy-port=<port>`
  - Server proksi HTTP yang akan digunakan agen untuk pencadangan dan pemulihan dari awan dan untuk koneksi ke server manajemen. Tanpa parameter ini, tidak ada server proksi yang akan digunakan.
- `--http-proxy-login=<login>` dan `--http-proxy-password=<password>`
  - Kredensial untuk server proksi HTTP. Gunakan parameter ini jika server memerlukan autentikasi.

- `--no-proxy-to-ams`
  - Agen perlindungan akan menyambungkan ke server manajemen tanpa menggunakan server proxy yang ditentukan oleh parameter `--http-proxy-host` dan `--http-proxy-port`.

Parameter penghapusan instalasi

`{-u|--uninstall}`

Menghapus instalasi produk.

`--purge`

Menghapus log, tugas, dan pengaturan konfigurasi produk.

Parameter informasi

`{-?|--help}`

Menampilkan deskripsi parameter.

`--usage`

Menampilkan deskripsi singkat tentang penggunaan perintah.

`{-v|--version}`

Menampilkan versi paket instalasi.

`--product-info`

Menunjukkan nama produk dan versi paket instalasi.

Contoh

- Menginstal Server Manajemen.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Menginstal Server Manajemen, menentukan port kustom.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --
web-server-port 6543 --ams-tcp-port 8123
```

- Menginstal Agen untuk Linux dan mendaftarkannya di Server Manajemen yang ditentukan.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456
```

- Menginstal Agen untuk Linux dan mendaftarkannya di Server Manajemen yang ditentukan, di unit yang ditentukan.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456 -unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

Instalasi atau 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. Untuk informasi tentang cara mengunduh file instalasi (.dmg), lihat "Menambahkan mesin yang menjalankan macOS".

Untuk menginstal Agen untuk Mac

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

   ```
   mkdir <dmg_root>
   ```

   Di sini, `<dmg_root>` adalah nama yang Anda pilih.
2. Pasang file .dmg.

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

   Di sini, `<dmg_file>` adalah nama file instalasi. Misalnya, **AcronisCyberProtect_15_MAC.dmg**.
3. Jalankan penginstal.

   ```
   sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
   ```
4. Lepaskan file instalasi (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Contoh

- ```
  mkdir mydirectory
  ```

  ```
  hdiutil attach /Users/JohnDoe/AcronisCyberProtect_15_MAC.dmg -mountpoint mydirectory
  ```

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

  ```
  hdiutil detach mydirectory
  ```

Untuk mendaftarkan Agen untuk Mac

Lakukan salah satu langkah berikut:

- Daftarkan agen dengan akun administrator tertentu.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  <management server address:port> -u <user name> -p <password>
  ```
  ```

Bidang `<alamat server manajemen:port>` adalah nama host atau alamat IP mesin tempat Server Manajemen Acronis Cyber Protect diinstal. Nomor port wajib diisi jika berbeda dari default (9877).

`<nama pengguna>` dan `<kata sandi>` adalah kredensial untuk akun administrator tempat agen akan didaftarkan.

- Daftarkan agen di unit spesifik.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent  -o register -a
<management server address:port> -u <user name> -p <password> --tenant <unit ID>
```

Untuk mempelajari ID unit, di konsol web Cyber Protect, klik **Pengaturan** > **Akun**, pilih unit yang diinginkan, lalu klik **Detail**.

Penting
Administrator dapat mendaftarkan agen dengan menentukan ID unit hanya di tingkat hierarki organisasi mereka. Administrator unit dapat mendaftarkan mesin di unit mereka sendiri dan subunitnya. Administrator organisasi dapat mendaftarkan mesin di semua unit. Untuk informasi selengkapnya tentang akun administrator yang berbeda, lihat "Mengelola akun pengguna dan unit organisasi".

- Daftarkan agen dengan menggunakan token registrasi.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> --token <token>
```

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

Penting
Di macOS 10.14 atau versi setelahnya, Anda perlu memberikan akses disk penuh pada agen perlindungan. Untuk melakukannya, tuju **Aplikasi** >**utilitas**, dan lalu jalankan **Asisten Agen Perlindungan Cyber**. Selanjutnya, ikuti petunjuk dalam jendela aplikasi.

Contoh

Mendaftarkan dengan nama pengguna dan kata sandi.

-
```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

Registrasi dengan ID unit dan kredensial administrator.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 4dd941c1-c03f-11ea-
  86d8-005056bdd3a0
  ```

Mendaftarkan dengan token.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 --token D91D-DC46-4F0B
  ```

Untuk menghapus instalasi Agen untuk Mac

Jalankan perintah berikut:

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

Untuk menghapus instalan Agen untuk Mac 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
  ```

Mendaftarkan mesin secara manual

Selain mendaftarkan mesin di server manajemen Cyber Protect selama instalasi agen, Anda juga dapat mendaftarkannya menggunakan antarmuka baris perintah. Anda mungkin perlu melakukannya jika Anda telah menginstal agen tetapi pendaftaran otomatis gagal, misalnya, atau jika Anda ingin mendaftarkan mesin yang ada di bawah akun baru.

Untuk mendaftarkan mesin

Pada saran perintah dari mesin tempat agen diinstal, jalankan salah satu dari perintah berikut ini:

- Untuk mendaftarkan mesin dengan akun administrator tertentu:

  ```
  <path to the registration tool> -o register -a <management server address:port> -u
  <user name> -p <password>
  ```

  `<Jalur ke alat bantu registrasi>` adalah:
  - di Windows: `%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe`
  - di Linux: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
  - di macOS: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`

Bidang `<alamat server manajemen:port>` adalah nama host atau alamat IP mesin tempat Server Manajemen Acronis Cyber Protect diinstal. Jika menggunakan port default 9877, Anda tidak wajib untuk menentukannya secara eksplisit.

`<nama pengguna>` dan `<kata sandi>` adalah kredensial untuk akun administrator tempat agen akan didaftarkan.

- Untuk mendaftarkan mesin di unit tertentu, tentukan ID unit:

```
<path to the registration tool> -o register -a <management server address:port> u
<user name> -p <password> --tenant <unit ID>
```

Untuk mempelajari ID unit, di konsol web Cyber Protect, klik **Pengaturan** > **Akun**, pilih unit yang diinginkan, lalu klik **Detail**.

Penting
Administrator hanya dapat mendaftarkan agen di tingkat hierarki organisasi mereka. Administrator unit dapat mendaftarkan agen di unit mereka sendiri dan subunitnya. Administrator organisasi dapat mendaftarkan agen di semua unit. Untuk informasi selengkapnya tentang akun administrator yang berbeda, lihat "Mengelola akun pengguna dan unit organisasi".

- Untuk mendaftarkan mesin dengan menggunakan token registrasi:

```
<path to the registration tool> -o register -a <management server address:port> --
token <token>
```

  - Token pendaftaran adalah rangkaian dari 12 karakter, yang dipisahkan oleh tanda hubung dalam tiga segmen. Untuk informasi lebih lanjut tentang cara membuat token tersebut, lihat "Menyebarkan agen melalui Kebijakan Grup".

Untuk membatalkan pendaftaran mesin

Pada saran perintah dari mesin tempat agen diinstal, jalankan perintah:

```
<path to the registration tool> -o unregister
```

Contoh

Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD
```

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

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --token 34F6-8C39-4A5C
```

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

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 --token 9DBF-3DA9-4DAB
```

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

Kata sandi dengan karakter spesial atau spasi kosong

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

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <"password">
```

Contoh (untuk Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p "johns password"
```

Jika Anda masih menerima kesalahan:

1. Kodekan kata sandi Anda ke dalam format base64 di https://www.base64encode.org/.
2. Pada baris perintah, tentukan kata sandi yang dikodekan dengan menggunakan parameter -b atau --base64.

Contoh (untuk Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

Memeriksa pembaruan perangkat lunak

Fungsi ini hanya tersedia untuk administrator organisasi.

Setiap kali Anda masuk ke konsol web Cyber Protect, Acronis Cyber Protect akan memeriksa apakah versi baru tersedia di situs web Acronis. Jika ada, konsol web Cyber Protect akan menampilkan tautan pengunduhan untuk versi baru di bagian bawah setiap halaman pada tab **Perangkat**, **Rencana**, dan **Penyimpanan cadangan**. Tautan ini juga tersedia di halaman **Pengaturan** > **Agen**.

Untuk mengaktifkan atau menonaktifkan pemeriksaan otomatis untuk pembaruan, ubah pengaturan sistem **Pembaruan**.

Untuk memeriksa pembaruan secara manual, klik ikon tanda tanya di sudut kanan atas > **Tentang** > **Cek pembaruan** atau ikon tanda tanya > **Cek pembaruan**.

Memigrasikan server manajemen

Anda dapat memigrasikan server manajemen yang berjalan di mesin Windows ke mesin Windows lain di lingkungan yang sama.

Proses migrasi terdiri atas fase-fase berikut:

1. "Operasi di mesin sumber" (hlm. 125)

   Pada fase ini, Anda menyiapkan data di server manajemen asli untuk migrasi.
2. "Operasi di mesin target" (hlm. 126)

   Pada fase ini, Anda menginstal dan mengonfigurasi server manajemen baru, lalu menyalin data dari server manajemen asli ke yang baru.

Prasyarat

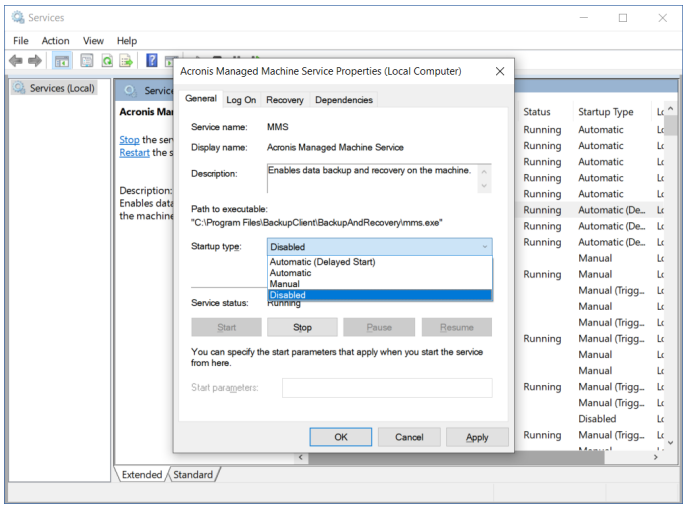
- Server manajemen menggunakan database Microsoft SQL Server eksternal. Instans Microsoft SQL Server berjalan di mesin khusus.
- Agen perlindungan terdaftar di server manajemen dengan menggunakan nama hostnya, bukan alamat IP-nya.
- Versi server manajemen adalah Acronis Cyber Protect Pembaruan 4 (build 29486) atau lebih baru.
- Versi server manajemen yang sama diinstal di mesin sumber dan target.

Operasi di mesin sumber

Di fase ini, Anda menyiapkan data dari server manajemen asli untuk migrasi.

Untuk menyiapkan data migrasi

1. Di mesin server manajemen asli, hentikan semua layanan Acronis.
   a. Buka **Layanan**, lalu nonaktifkan pengaktifan layanan Acronis, kecuali untuk **Layanan Acronis Active Protection** dan **Layanan Acronis Cyber Protection**.



   b. Buka **Regedit**, lalu nonaktifkan **Layanan Acronis Active Protection** dan **Layanan Acronis Cyber Protection**, dengan mengedit kuncinya:
      - Di kunci `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisCyberProtectionService`, buka nilai **Mulai**, lalu atur data nilai ke 4.

- Di kunci `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisActiveProtectionService`, buka nilai **Mulai**, lalu atur data nilai ke 4.

2. Mulai ulang mesin server manajemen, lalu verifikasi bahwa layanan Acronis yang dinonaktifkan tidak berjalan.

   Catatan
   Dua layanan, yaitu **Acronis Scheduler Service Helper** dan **Acronis TIB Mounter Monitor**, mungkin masih berjalan. Anda dapat mengabaikannya dengan aman.

3. [Jika komponen Monitor Cyber Protect diinstal di mesin server manajemen] Keluar dari Monitor Acronis Cyber Protect.
4. Di Saran Perintah Windows, ubah pemilik folder `%ProgramData%\Acronis` dan `%ProgramFiles%\Acronis`, dengan menjalankan perintah berikut:

   ```
   takeown /f "%ProgramData%\Acronis" /r /d y
   ```

   ```
   takeown /f "%ProgramFiles%\Acronis" /r /d y
   ```

5. Edit izin akses ke folder dan subfoldernya dengan menjalankan perintah berikut:

   ```
   icacls "%ProgramData%\Acronis" /grant everyone:F /t
   ```

   ```
   icacls "%ProgramFiles%\Acronis" /grant everyone:F /t
   ```

6. Salin folder `%ProgramData%\Acronis` dan `%ProgramFiles%\Acronis` ke jaringan bersama yang dapat diakses mesin server manajemen baru.
7. Matikan mesin server manajemen asli.

Berikutnya, ikuti prosedur di "Operasi di mesin target" (hlm. 126).

Operasi di mesin target

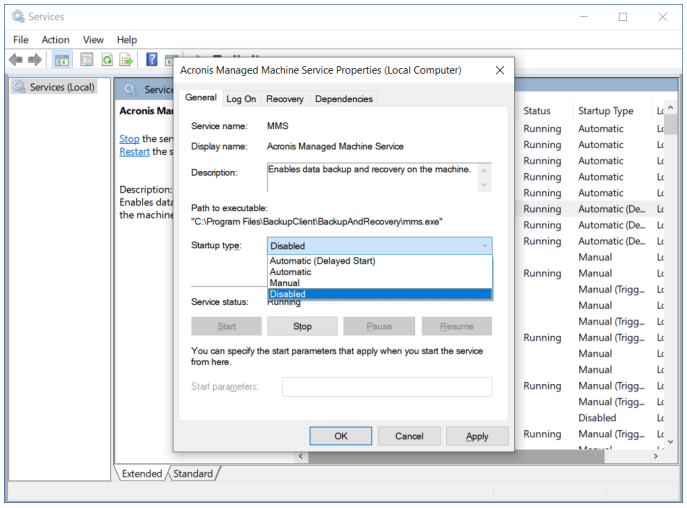
Pada fase ini, Anda menginstal dan mengonfigurasi server manajemen baru, lalu memigrasikan data ke server tersebut.

Sebelum melakukan operasi pada mesin target, pastikan Anda telah menyelesaikan prosedur di "Operasi di mesin sumber" (hlm. 125).

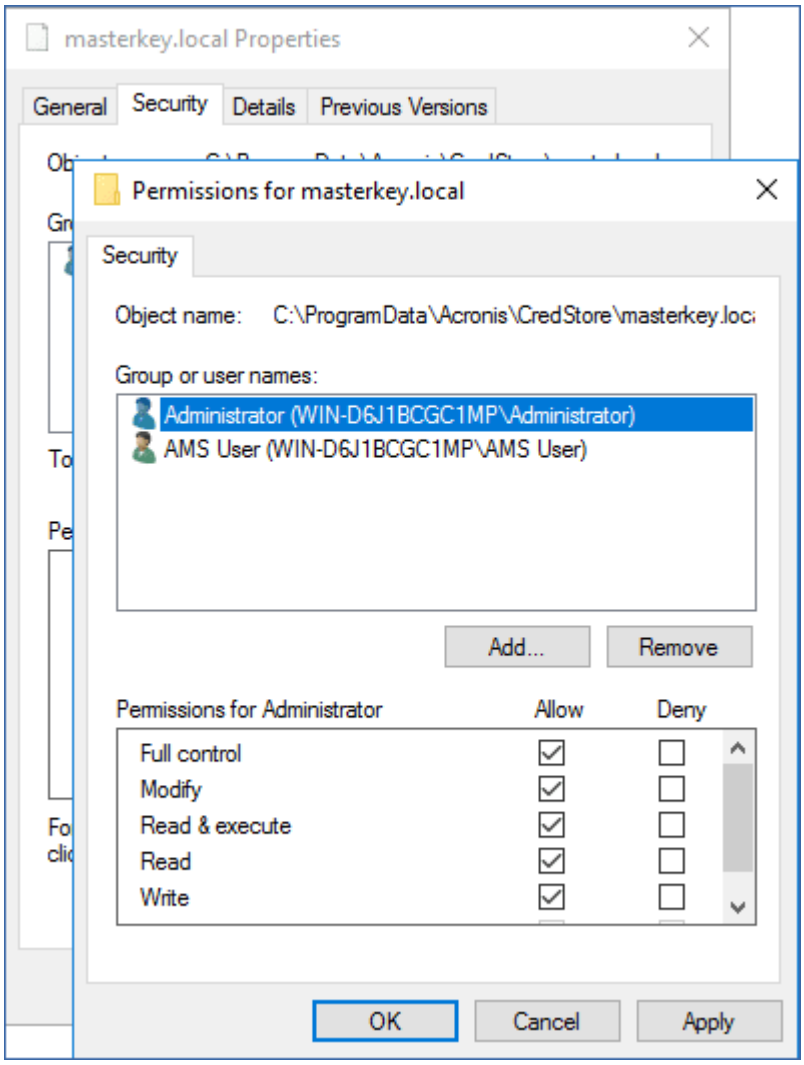
Untuk memigrasikan data ke server manajemen baru

1. Tetapkan nama host mesin tempat Anda akan menginstal server manajemen baru. Nama ini harus sama dengan nama mesin dengan server manajemen asli.
2. Buat aturan firewall untuk memblokir semua lalu lintas di port TCP 9877.

3. Jalankan program penyiapan Acronis Cyber Protect.
   a. Terima persyaratan perjanjian lisensi dan pernyataan privasi, lalu klik **Lanjutkan**.
   b. Klik **Sesuaikan pengaturan instalasi**.
   c. Pada bagian **Apa yang diinstal**, hanya pilih komponen berikut, lalu klik **Selesai**.
      - Server Manajemen
      - Komponen untuk Instalasi Jarak Jauh
      - Pembangun Media Yang Dapat Di-Boot
      - Command-Line Tool
   d. Pada bagian **Database untuk server manajemen**, pertahankan opsi default **Gunakan SQLite bawaan**.
   e. Pada **Akun masuk untuk layanan server manajemen**, gunakan opsi yang sama seperti server manajemen asli.
4. Hentikan semua layanan Acronis.
   a. Buka **Layanan**, lalu nonaktifkan pengaktifan semua layanan Acronis.



   b. Mulai ulang mesin, lalu verifikasi bahwa layanan Acronis yang dinonaktifkan tidak berjalan.
5. Buka `%ProgramData%\Acronis\CredStore`, lalu sesuaikan izin untuk file `masterkey.local`, sebagai berikut:
   a. Berikan kepemilikan file ke akun pengguna **Administrator**.
   b. Berikan akun pengguna **Administrator** izin **Kontrol penuh**.



6. Arahkan ke `%ProgramData%\Acronis\AMS\AccessVault\config`, lalu berikan akun pengguna **Administrator** izin **Kontrol penuh** untuk file berikutnya:
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred`
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json`
7. Ganti folder berikut dengan folder yang Anda salin dari mesin server manajemen asli ke jaringan bersama:
   - `%ProgramData%\Acronis`
   - `%ProgramFiles%\Acronis`

   Penting
   Timpa folder yang ada tanpa menghapusnya terlebih dahulu.

   Catatan
   Jika melihat pesan bahwa folder `%ProgramFiles%\Acronis\ShellExtentions` tidak dapat diganti, Anda dapat dengan aman melewati folder ini.
8. Pulihkan izin untuk file berikut:

- `%ProgramData%\Acronis\CredStore\masterkey.local` – Hapus akun pengguna **Administrator** dari daftar pengguna dengan izin.
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred` – Berikan akun pengguna **Administrator** hanya izin **Baca**.
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json` – Berikan akun pengguna **Administrator** hanya izin **Baca**.

9. Buat persimpangan direktori untuk folder `NGMP\latest`.
   - Di Saran Perintah Windows, arahkan ke `%ProgramData%\Acronis\NGMP`, lalu hapus folder `terbaru`.

     ```
     cd %ProgramData%\Acronis\NGMP
     ```

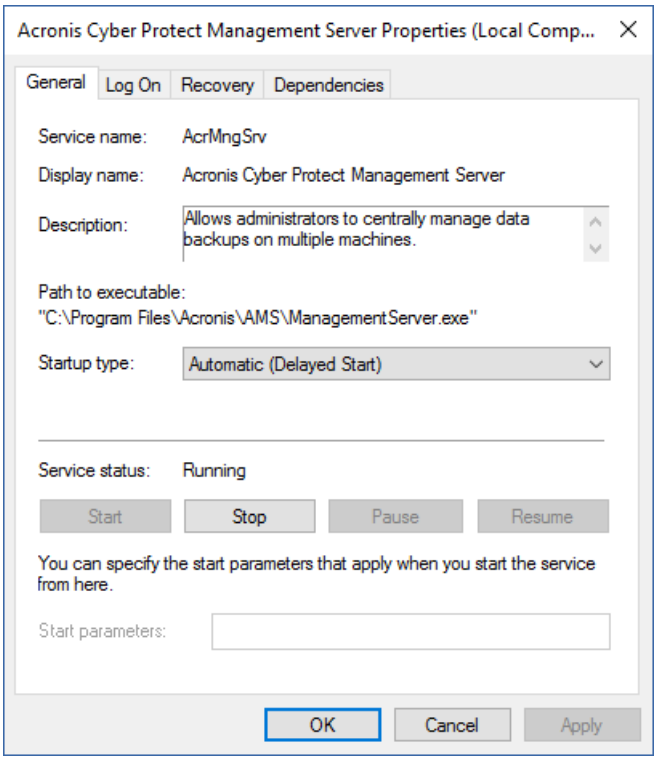
     ```
     rmdir latest
     ```

   - Buat persimpangan direktori `terbaru` dan arahkan ke folder yang diberi nama menurut versi NGMP saat ini, misalnya:

     ```
     mklink /j latest C:\ProgramData\Acronis\NGMP\1.0.2653.0
     ```

10. Arahkan server manajemen baru ke database Microsoft SQL Server yang digunakan server manajemen asli.
    a. Buka **Regedit**.
    b. Di kunci `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\AMS\Settings`, ubah nilai `AmsDmlDbProtocol`, dengan mengubah datanya ke `config://C:\ProgramData\Acronis\AMS\mssql\dml_mssql.config`.
11. Buka **Layanan**, lalu nonaktifkan semua layanan Acronis.

    Atur jenis pengaktifan **Server Manajemen Acronis Cyber Protect** ke **Otomatis (Mulai Tunda)** dan jenis pengaktifan semua layanan Acronis lainnya ke **Otomatis**.



12. Di firewall, izinkan semua lalu lintas di Port TCP 9877.
13. Mulai ulang mesin, lalu pastikan semua layanan Acronis berjalan.
14. Jalankan program penyiapan Acronis Cyber Protect dan instal item berikut:
    - Agen untuk Windows
    - [Opsional] Monitor Cyber Protect
15. Mulai ulang mesin.

Penyebaran awan

Mengaktifkan akun

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

- **Tautan aktivasi akun.** Klik tautan dan atur kata sandi untuk akun tersebut. Ingat masuk Anda yang ditampilkan pada halaman aktivasi akun.
- **Tautan ke halaman masuk konsol web Cyber Protect.** Gunakan tautan ini untuk mengakses konsol di lain waktu. Masuk dan kata sandi sama seperti pada langkah sebelumnya.

Persiapan

Langkah 1

Pilih agen, tergantung pada apa yang akan Anda buat cadangannya. Untuk informasi tentang agen, lihat "Komponen" (hlm. 47).

Langkah 2

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

Halaman **Tambahkan perangkat** 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. 175).

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

Instalasi di Linux dan macOS dilakukan dari program penyiapan biasa.

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

Langkah 3

Sebelum instalasi, pastikan firewall dan komponen lain dari sistem keamanan jaringan Anda (seperti server proksi) memungkinkan koneksi inbound dan outbound melalui port TCP berikut:

- Port **443** dan **8443**
  Port ini digunakan untuk mengakses konsol web 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 "Pengaturan server proksi" (hlm. 133) 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.

  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.

Langkah 4

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.

Layanan Active Protection sedang mendengarkan di port TCP **6109**. Verifikasi bahwa layanan tidak digunakan oleh proses lain.

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.

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

Pengaturan server proksi

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 mendaftar sendiri di awan selama instalasi, pengaturan server proksi harus disediakan selama instalasi atau sebelum instalasi.

Di Windows

Jika server proksi dikonfigurasi di Windows (**Panel kontrol** > **Opsi Internet** > **Koneksi**, program penyiapan akan membaca pengaturan server proksi dari registri dan menggunakannya secara otomatis. Selain itu, Anda juga dapat memasukkan pengaturan proksi selama instalasi, atau menentukannya terlebih dahulu menggunakan prosedur yang dijelaskan di bawah ini. Untuk mengubah pengaturan proksi setelah instalasi, gunakan prosedur yang sama.

Untuk menentukan pengaturan proksi di Windows

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 perlindungan belum diinstal, Anda dapat menginstalnya sekarang. Jika tidak, lakukan langkah berikut untuk memulai kembali agen:
   a. Pada menu **Start**, klik **Run**, lalu ketik: **cmd**
   b. Klik **OK**.
   c. Jalankan perintah berikut:

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

Di Linux

Jalankan file instalasi dengan parameter `--http-proxy-host=ALAMAT --http-proxy-port=PORT --http-proxy-login=MASUK--http-proxy-password=KATA SANDI`. Untuk mengubah pengaturan proksi setelah instalasi, gunakan prosedur yang di jelaskan di bawah ini.

Untuk mengubah pengaturan proksi di Linux

1. Buka file **/etc/Acronis/Global.config** dalam editor teks.
2. 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>`.
3. Ganti `ALAMAT` 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 `KATA SANDI` dengan kredensial server proksi. Atau, hapus baris ini dari file.
5. Simpan file.
6. Mulai kembali agen dengan mengeksekusi perintah berikut di direktori mana pun:

```
sudo service acronis_mms restart
```

Di macOS

Anda dapat memasukkan pengaturan proxy selama instalasi, atau menentukannya terlebih dahulu menggunakan prosedur yang dijelaskan di bawah ini. Untuk mengubah pengaturan proksi setelah

instalasi, gunakan prosedur yang sama.

Untuk menentukan pengaturan proksi di macOS

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.
5. Simpan file.
6. Jika agen perlindungan belum diinstal, Anda dapat menginstalnya sekarang. Jika tidak, lakukan langkah berikut untuk memulai kembali agen:
   a. Buka **Aplikasi** > **Utilitas** > **Terminal**
   b. Jalankan perintah berikut:
   ```
   sudo launchctl stop acronis_mms
   sudo launchctl start acronis_mms
   ```

Di media yang dapat di-boot

Saat bekerja di bawah media yang dapat di-boot, Anda dapat memerlukan akses ke penyimpanan awan via server proxy. Untuk menentukan pengaturan server proksi, klik **Alat** > **Server proksi**, lalu tentukan nama host server proksi/alamat IP, port, dan kredensial.

Menginstal agen

Di Windows

1. Pastikan mesin terhubung ke Internet.
2. Masuk sebagai administrator dan mulai program penyiapan.
3. [Opsional] Klik **Sesuaikan pengaturan instalasi** dan buat perubahan sesuai keinginan Anda:

- Untuk mengubah komponen yang akan diinstal (khususnya, untuk menonaktifkan instalasi Monitor Cyber Protect dan Alat Baris Perintah).
- Untuk mengubah metode pendaftaran mesin di layanan Perlindungan Cyber. Anda dapat beralih dari **Gunakan konsol Cyber Protect** (default) ke **Gunakan kredensial**, atau **Gunakan token registrasi**.
- Untuk mengubah jalur instalasi.
- Untuk mengubah akun untuk layanan agen.
- 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 ketika menginstal Agen untuk VMware] Tentukan alamat dan kredensial akses untuk vCenter Server atau host ESXi yang berdiri sendiri yang mesin virtualnya akan dicadangkan oleh agen, lalu klik **Selesai**. Kami sarankan untuk menggunakan akun yang memiliki peran **Administrator**. Jika tidak, sediakan akun dengan privilese yang diperlukan pada vCenter Server atau ESXi.
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 penginstalan agen pada pengontrol domain hanya baca, lihat artikel basis pengetahuan ini.
7. Jika Anda mempertahankan metode registrasi default **Gunakan konsol Cyber Protect** pada langkah 3, tunggu hingga layar registrasi muncul, lalu lanjutkan ke langkah berikutnya. Jika tidak, tidak diperlukan tindakan lainnya.
8. Lakukan salah satu langkah berikut:
   - Klik **Daftarkan mesin**. Di jendela browser yang terbuka, masuk ke konsol web Cyber Protect, tinjau detail registrasi, kemudian klik **Konfirmasikan registrasi**.
   - Klik **Tampilkan info pendaftaran**. Program penyiapan menampilkan tautan pendaftaran dan kode pendaftaran. Anda dapat menyalin tautan pendaftaran dan melakukan langkah pendaftaran pada mesin yang berbeda. 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**.

9. **Catatan**
   Jangan keluar dari program penyiapan sampai Anda mengonfirmasi pendaftaran. Untuk memulai kembali pendaftaran, Anda harus memulai ulang program penyiapan, lalu klik **Daftarkan mesin**.

   Hasilnya, mesin akan ditetapkan ke akun yang digunakan untuk masuk ke konsol web Cyber Protect.

Di Linux

1. Pastikan mesin terhubung ke Internet.
2. Sebagai pengguna root, jalankan file instalasi.
   Jika server proxy diaktifkan di jaringan Anda, ketika menjalankan file, tentukan nama host server/alamat IP dan port dalam format berikut: `--http-proxy-host=ALAMAT --http-proxy-port=PORT --http-proxy-login=MASUK--http-proxy-password=KATA SANDI`.
   Jika Anda ingin mengubah metode default untuk mendaftarkan mesin di layanan Perlindungan Cyber, jalankan file instalasi dengan salah satu parameter berikut:
   - `--register-with-credentials` - untuk meminta nama pengguna dan kata sandi selama instalasi
   - `--token=STRING` - untuk menggunakan token registrasi
   - `--skip-registration` - untuk melewati registrasi
3. Pilih kotak centang untuk agen yang ingin Anda instal. Agen berikut tersedia:
   - **Agen untuk Linux**
   - **Agen untuk Virtuozzo**

   Agen untuk Virtuozzo tidak dapat diinstal tanpa Agen untuk Linux.
4. Jika Anda mempertahankan metode pendaftaran default di langkah 2, lanjutkan ke langkah berikutnya. Jika tidak, masukkan nama pengguna dan kata sandi untuk layanan Perlindungan Cyber, atau tunggu hingga mesin akan didaftarkan menggunakan token.
5. Lakukan salah satu langkah berikut:
   - Klik **Daftarkan mesin**. Di jendela browser yang terbuka, masuk ke konsol web Cyber Protect, tinjau detail registrasi, kemudian klik **Konfirmasikan registrasi**.
   - Klik **Tampilkan info pendaftaran**. Program penyiapan menampilkan tautan pendaftaran dan kode pendaftaran. Anda dapat menyalin tautan pendaftaran dan melakukan langkah pendaftaran pada mesin yang berbeda. 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**.

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

   Hasilnya, mesin akan ditetapkan ke akun yang digunakan untuk masuk ke konsol web Cyber Protect.
7. Jika UEFI Secure Boot diaktifkan pada mesin, akan diinformasikan bahwa Anda harus memulai ulang sistem setelah instalasi. Pastikan untuk mengingat kata sandi apa (kata sandi dari pengguna akar atau "acronis") yang harus digunakan.

   Catatan
   Selama instalasi, kunci baru dihasilkan, digunakan untuk masuk ke modul `snapapi`, dan terdaftar sebagai Machine Owner Key (MOK). Diwajibkan untuk mulai kembali untuk dapat mendaftarkan kunci ini. Tanpa mendaftarkan kunci, agen tidak akan bisa dioperasikan. Jika Anda mengaktifkan UEFI Secure Boot setelah instalasi agen, ulangi instalasi termasuk langkah 6.

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

Di macOS

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 proxy 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:
   - Klik **Daftarkan mesin**. Di jendela browser yang terbuka, masuk ke konsol web Cyber Protect, tinjau detail registrasi, kemudian klik **Konfirmasikan registrasi**.
   - Klik **Tampilkan info pendaftaran**. Program penyiapan menampilkan tautan pendaftaran dan kode pendaftaran. Anda dapat menyalin tautan pendaftaran dan melakukan langkah pendaftaran pada mesin yang berbeda. 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**.
10. **Tips** Jangan keluar dari program penyiapan hingga Anda mengonfirmasi registrasi. Untuk memulai kembali pendaftaran, Anda harus memulai ulang program penyiapan dan mengulangi prosedur instalasi.

Hasilnya, mesin akan ditetapkan ke akun yang digunakan untuk masuk ke konsol web Cyber Protect.

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 penginstalan 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
   - 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 tidak disarankan untuk mengubah akun masuk secara manual setelah instalasi selesai.

Instalasi atau penghapusan instalasi tanpa pengawasan

Instalasi atau penghapusan instalasi tanpa pengawasan di Windows

Bagian ini menjelaskan cara menginstal atau menghapus instalasi agen perlindungan dalam mode tanpa pengawasan pada mesin yang menjalankan Windows, menggunakan Windows Installer (program `msiexec`). Dalam domain Active Directory, cara lain untuk melakukan instalasi tanpa pengawasan adalah melalui Kebijakan Grup— lihat "Menyebarkan agen melalui Kebijakan Grup" (hlm. 175).

Selama instalasi, Anda dapat menggunakan file yang dikenal sebagai **transformasi** (file.mst). Transformasi adalah file dengan parameter instalasi. Sebagai alternatif, Anda dapat menentukan parameter instalasi langsung pada baris perintah.

Membuat transformasi .mst dan mengekstrak paket instalasi

1. Masuk sebagai administrator dan mulai program penyiapan.
2. Klik **Buat file .mst dan .msi untuk instalasi tanpa pengawasan**.
3. Di **Apa yang diinstal**, pilih komponen yang ingin Anda instal, lalu klik **Selesai**.
   Paket instalasi untuk komponen-komponen ini akan diekstrak dari program pengaturan.
4. Dalam **Pengaturan registrasi**, pilih **Gunakan kredensial** atau **Gunakan token pendaftaran**.
   Untuk informasi lebih lanjut tentang cara membuat token pendaftaran, lihat "Langkah 1: Membuat token pendaftaran" (hlm. 176).
5. [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 penginstalan agen pada pengontrol domain hanya baca, lihat artikel basis pengetahuan ini.
6. Tinjau atau modifikasi pengaturan instalasi lain yang akan ditambahkan ke file .mst, lalu klik **Lanjutkan**.
7. Pilih folder di mana transform .mst akan dibuat dan paket instalasi .msi dan .cab akan diekstrak, lalu klik **Hasilkan**.

Menginstal produk menggunakan transformasi .mst

Pada baris perintah, jalankan perintah berikut.

Templat perintah:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Di mana:

- `<nama paket>` adalah nama file .msi.
- `<mengubah nama>` adalah nama transformasi.

Contoh perintah:

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

Menginstal atau menghapus instalasi produk dengan menentukan parameter secara manual

Pada baris perintah, jalankan perintah berikut.

Templat perintah (menginstal):

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Di sini, `<nama paket>` adalah nama file .msi. Semua parameter yang tersedia beserta nilainya dijelaskan dalam "Parameter dasar" (hlm. 142).

Templat perintah (menghapus instalasi):

```
msiexec /x <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Paket .msi harus versi yang sama dengan produk yang instalasinya ingin Anda hapus.

Parameter pemasangan atau penghapusan instalasi tanpa pengawasan

Bagian ini menjelaskan parameter yang digunakan selama instalasi atau penghapusan instalasi tanpa pengawasan di Windows. Selain parameter tesebut, Anda juga dapat menggunakan parameter lain dari `msiexec`, seperti yang dijelaskan di https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Parameter instalasi

Parameter dasar

`ADDLOCAL= <list of components>`

Komponen yang akan diinstal, dipisahkan dengan koma dan tanpa karakter spasi. Semua komponen yang ditentukan harus diekstraksi dari program pengaturan sebelum instalasi.

Daftar lengkap komponen adalah sebagai berikut:

Komponen	Harus diinstal bersama	Bitness	Nama komponen / deskripsi
MmsMspComponents		32-bit/64-bit	Komponen inti untuk agen
BackupAndRecoveryAgent	MmsMspComponents	32-bit/64-bit	Agen untuk Windows
ArxAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agen untuk Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agen untuk SQL
ARADAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agen untuk Active Directory
ArxOnlineAgentFeature	MmsMspComponents	32-bit/64-bit	Agen untuk Office 365
OracleAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agen untuk Oracle
AcronisESXSupport	MmsMspComponents	64-bit	Agen untuk VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	32-bit/64-bit	Agen untuk Hyper-V
CommandLineTool		32-bit/64-bit	Command-Line Tool
TrayMonitor	BackupAndRecoveryAgent	32-bit/64-bit	Monitor Cyber Protect

`TARGETDIR= <path>`

Folder tempat produk akan diinstal. Secara default, folder ini: `C:\Program Files\BackupClient`.

`REBOOT=ReallySuppress`

Jika parameter ditentukan, reboot mesin tidak diperbolehkan.

`/l*v <log file>`

Jika parameternya ditentukan, log instalasi dalam mode verbose akan disimpan ke file yang ditentukan. File log dapat digunakan untuk menganalisis masalah instalasi.

`CURRENT_LANGUAGE= <language ID>`

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

`REGISTRATION_ADDRESS`

Ini adalah URL untuk layanan Cyber Protect. Anda dapat menggunakan parameter ini baik dengan parameter `REGISTRATION_LOGIN` dan `REGISTRATION_PASSWORD` , atau dengan `REGISTRATION_TOKEN`.

- Saat Anda menggunakan `REGISTRATION_ADDRESS` dengan paramenter `REGISTRATION_LOGIN` dan `REGISTRATION_PASSWORD` , tentukan alamat yang Anda gunakan **untuk masuk** ke layanan Cyber Protect. Misalnya, `https://cloud.company.com`:

- Saat Anda menggunakan `REGISTRATION_ADDRESS` dengan parameter `REGISTRATION_TOKEN` , tentukan alamat pusat data yang tepat. Ini adalah URL yang Anda lihat **setelah Anda masuk** ke layanan Cyber Protect. Misalnya, `https://eu2-cloud.company.com`.

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

`REGISTRATION_LOGIN` dan `REGISTRATION_PASSWORD`

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

`REGISTRATION_PASSWORD_ENCODED`

Kata sandi untuk akun yang akan menjadi tempat agen terdaftar di layanan Cyber Protect, yang dikodekan dalam base64. Untuk informasi lebih lanjut tentang cara mengodekan kata sandi Anda ini, lihat "Mendaftarkan mesin secara manual".

`REGISTRATION_TOKEN`

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

`REGISTRATION_REQUIRED={0,1}`

Menentukan bagaimana instalasi akan selesai jika pendaftaran gagal. Jika nilainya `1`,instalasi juga akan gagal. Nilai default adalah `0`, jadi jika Anda tidak menentukan parameter ini, instalasi selesai dengan sukses meskipun agen tidak terdaftar.

Parameter tambahan

Untuk menentukan akun masuk untuk layanan agen di Windows, gunakan salah satu dari parameter berikut:

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`

  Jika nilainya `1`, agen akan berjalan di bawah akun **Sistem Lokal**.
- `MMS_CREATE_NEW_ACCOUNT={0,1}`

  Jika nilainya `1`, agen akan berjalan di bawah akun yang baru dibuat bernama **Acronis Agent User**.
- `MMS_SERVICE_USERNAME= <user name>` dan `MMS_SERVICE_PASSWORD=<password>`

  Gunakan parameter ini untuk menentukan akun yang ada di mana agen akan berjalan.

Untuk informasi lebih lanjut mengenai akun masuk, lihat "Mengubah akun masuk pada mesin Windows".

`SET_ESX_SERVER={0,1}`

- Jika nilainya `0`, Agen untuk VMware yang diinstal tidak akan terhubung ke vCenter Server atau host ESXi. Jika nilainya `1`, tentukan parameter berikut:
  - `ESX_HOST= <host name>`

    Nama host atau alamat IP dari Server vCenter atau host ESXi.
  - `ESX_USER= <user name>` dan `ESX_PASSWORD=<password>`

    Kredensial untuk mengakses vCenter Server atau host ESXi.

`HTTP_PROXY_ADDRESS= <IP address>` dan `HTTP_PROXY_PORT=<port>`

Server proksi HTTP yang akan digunakan oleh agen. Tanpa parameter ini, tidak ada server proksi yang akan digunakan.

`HTTP_PROXY_LOGIN= <login>` dan `HTTP_PROXY_PASSWORD=<password>`

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

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

Jika nilainya `0`, atau parameter tidak ditentukan, agen akan menggunakan server proxy hanya untuk pencadangan dan pemulihan dari awan. Jika nilainya `1`, agen juga akan terhubung ke server manajemen melalui server proxy.

Parameter penghapusan instalasi

`REMOVE={ <list of components> |ALL}`

Komponen yang akan dihapus, dipisahkan dengan koma dan tanpa karakter spasi. Jika nilainya `ALL`, semua komponen produk akan dihapus instalasinya.

Selain itu, Anda juga dapat menentukan parameter berikut:

`DELETE_ALL_SETTINGS={0, 1}`

Jika nilainya `1`, log produk, tugas, dan pengaturan konfigurasi akan dihapus.

Contoh

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

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
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 Pemantauan Perlindungan Cyber. Membuat akun masuk baru untuk layanan agen di Windows. Mendaftarkan mesin di layanan Cyber Protect 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 Pemantauan Perlindungan Cyber. Mendaftarkan mesin di layanan Cyber Protect dengan menggunakan nama pengguna dan dikodekan dalam kata sandi base64.

```
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 Pemantauan Perlindungan Cyber. Mendaftarkan mesin di layanan Cyber Protect 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
```

- Menghapus instalasi semua agen dan menghapus log, tugas, dan pengaturan konfigurasi.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt REMOVE=ALL DELETE_ALL_
SETTINGS=1 REBOOT=ReallySuppress
```

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 atau menghapus instalasi agen perlindungan

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, `<nama paket>` adalah nama paket instalasi (file .i686 atau .x86_64). Semua parameter yang tersedia beserta nilainya dijelaskan dalam "Parameter instalasi atau penghapusan instalasi tanpa pengawasan".
- 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 yang diinginkan, misalnya:

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

  atau

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

```
-a
--language
en
```

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 untuk 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.

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.

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

Tanpa parameter ini, semua komponen di atas akan diinstal.

Kedua Agen untuk Virtuozzo dan Agen untuk Oracle memerlukan Agen untuk Linux untuk 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 Protect, 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=` `<location>`

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

`--language=` `<language ID>`

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=}` `<user name>` dan `{-w|--password=}`<password>

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

- `--token=` `<token>`

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

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

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

    URL layanan Cyber Protect.

    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 Protect. 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 Protect. 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 Protect. Ini bukan akun administrator mitra.

- `--skip-registration`

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

Parameter tambahan

`--http-proxy-host=<IP address>` 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=<login>` dan `--http-proxy-password=<password>`

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

`--tmp-dir=<location>`

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. Tidak direkomendasikan 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}`

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=}` `<path>`

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.

```
./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, dan 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. Untuk informasi tentang cara mengunduh file instalasi (.dmg), lihat "Menambahkan mesin yang menjalankan macOS".

Untuk menginstal Agen untuk Mac

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

```
mkdir <dmg_root>
```

Di sini, <dmg_root> adalah nama yang Anda pilih.

2. Pasang file .dmg.

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

Di sini, <dmg_file> adalah nama file instalasi. Misalnya, **AcronisAgentMspMacOSX64.dmg**.

3. Jalankan penginstal.

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

4. Lepaskan file instalasi (.dmg).

```
hdiutil detach <dmg_root>
```

Contoh

-

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/AcronisAgentMspMacOSX64.dmg -mountpoint mydirectory
```

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

```
hdiutil detach mydirectory
```

Untuk mendaftarkan Agen untuk Mac

Lakukan salah satu langkah berikut:

- Mendaftarkan agen di bawah akun yang ditentukan, dengan menggunakan nama pengguna dan kata sandi.

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

Di sini:

Bidang <alamat layanan Cyber Protect> adalah alamat yang Anda gunakan untuk **masuk** ke layanan Cyber Protect. Misalnya:

<Nama pengguna> dan <kata sandi> adalah kredensial untuk akun tempat agen akan didaftarkan. Ini bukan akun administrator mitra.

- Daftarkan agen dengan menggunakan token registrasi.

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

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

Saat Anda menggunakan token registrasi, Anda harus menentukan alamat pusat data yang tepat. Ini adalah URL yang Anda lihat **setelah Anda masuk** ke layanan Cyber Protect. Misalnya:

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

Contoh

Mendaftarkan dengan nama pengguna dan kata sandi.

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

Mendaftarkan dengan token.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  https://eu2-cloud company.com --token D91D-DC46-4F0B
  ```

Untuk menghapus instalasi Agen untuk Mac

Jalankan perintah berikut:

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

Untuk menghapus semua log, tugas, dan pengaturan konfigurasi selama penghapusan instalasi, jalankan perintah berikut:

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

Mendaftarkan mesin secara manual

Selain mendaftarkan mesin di layanan Cyber Protect selama instalasi agen, Anda juga dapat mendaftarkannya dengan menggunakan antarmuka baris perintah. Anda mungkin perlu melakukannya jika Anda telah menginstal agen tetapi pendaftaran otomatis gagal, misalnya, atau jika Anda ingin mendaftarkan mesin yang ada di bawah akun baru.

Untuk mendaftarkan mesin

Pada saran perintah dari mesin tempat agen diinstal, jalankan salah satu dari perintah berikut ini:

- Perintah untuk mendaftarkan mesin di akun saat ini:

  ```
  <path to the registration tool> -o register -s mms -t cloud --update
  ```

  - Di sini, `<path ke alat bantu registrasi>` adalah:
    - di Windows: `%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe`
    - di Linux: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
    - di macOS: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`
- Untuk mendaftarkan mesin di akun lain:

  ```
  <path to the registration tool> -o register -t cloud -a <service address> -u <user name> -p <password>
  ```

  - Di sini, `<nama pengguna>` dan `<kata sandi>` adalah kredensial untuk akun tertentu tempat agen akan didaftarkan. Ini bukan akun administrator mitra.

    Bidang `<alamat layanan>` adalah URL yang Anda gunakan untuk **masuk** ke layanan Cyber Protect. Misalnya, `https://cloud.company.com`.

- Untuk mendaftarkan mesin dengan token registrasi:

  ```
  <path to the registration tool> -o register -t cloud -a <service address> --token <token>
  ```

  - Token pendaftaran adalah rangkaian dari 12 karakter, yang dipisahkan oleh tanda hubung dalam tiga segmen. Untuk informasi lebih lanjut tentang cara membuat token tersebut, lihat "Menyebarkan agen melalui Kebijakan Grup".

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

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

Untuk membatalkan pendaftaran mesin

Pada saran perintah dari mesin tempat agen diinstal, jalankan perintah:

```
<path to the registration tool> -o unregister
```

Contoh

Windows

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -s mms -t
cloud --update
```

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

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

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

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t cloud --
update
```

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

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

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

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -s mms -t cloud --update
```

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

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

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

Kata sandi dengan karakter spesial atau spasi kosong

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

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <"password">
```

Contoh (untuk Windows):

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

Jika Anda masih menerima kesalahan:

- Kodekan kata sandi Anda ke dalam format base64 di https://www.base64encode.org/.
- Pada baris perintah, tentukan kata sandi yang dikodekan dengan menggunakan parameter -b atau --base64.

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-b -p <encoded password>
```

Contoh (untuk Windows):

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

Menyebarkan Agen untuk oVirt (Alat Virtual)

Untuk informasi tentang cara menyebarkan dan mengonfigurasi Agen untuk oVirt (Alat Virtual), lihat: Dokumentasi Cyber Protection Cloud.

Menyebarkan Agen untuk Virtuozzo Hybrid Infrastructure (Alat Virtual)

Untuk informasi tentang cara menyebarkan dan mengonfigurasi Agen untuk Virtuozzo Hybrid Infrastructure (Alat Virtual), lihat Dokumentasi Cyber Protection Cloud.

Penemuan manual mesin

Dengan penemuan otomatis, Anda dapat:

- Mengotomatiskan instalasi agen perlindungan dan registrasi mesin ke server manajemen 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

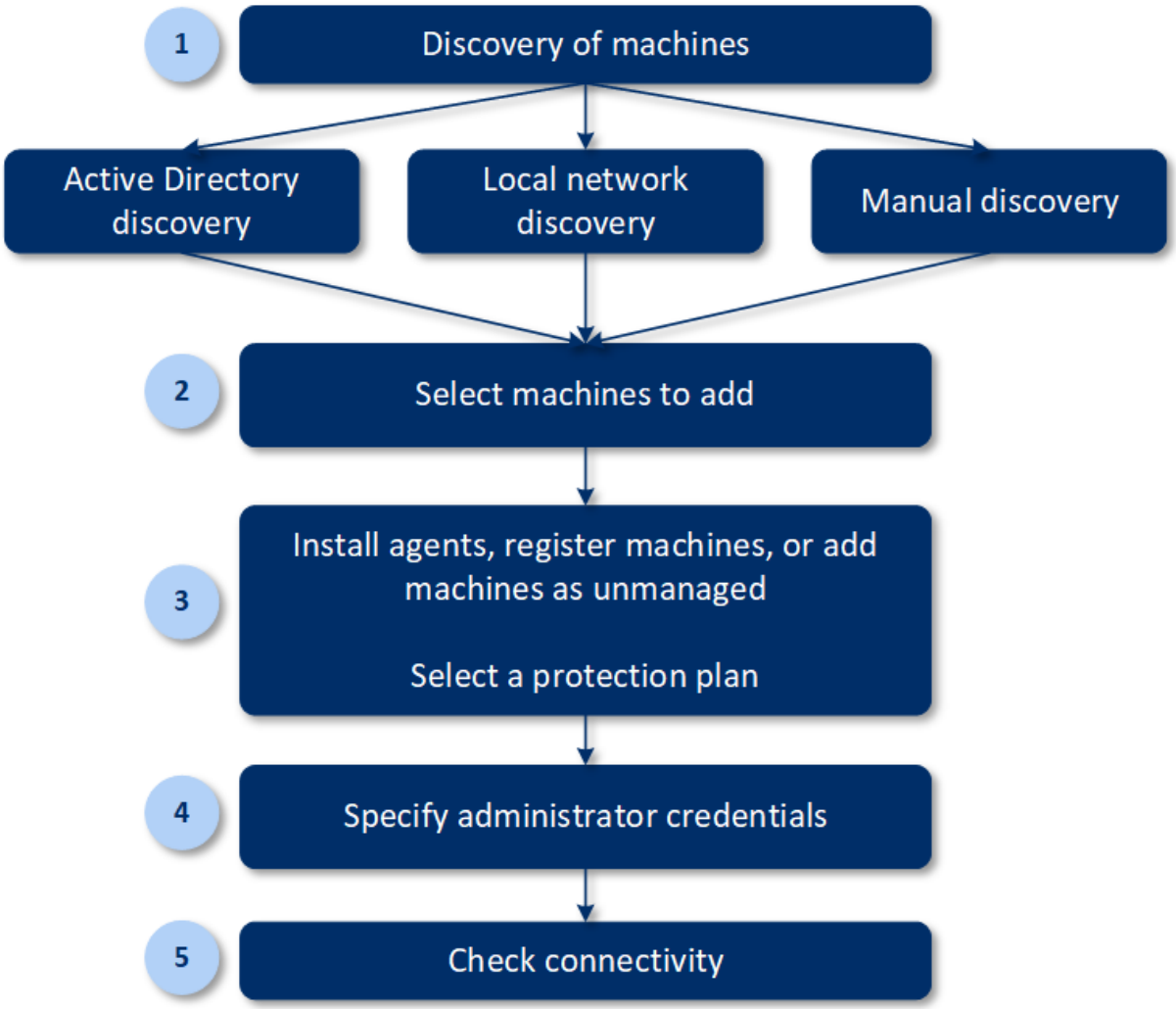
Selama penemuan jaringan lokal, agen penemuan mengumpulkan informasi berikut untuk setiap mesin di jaringan, menggunakan NetBIOS discovery, Web Service Discovery (WSD), dan tabel Address Resolution Protocol (ARP):

- Nama (nama host pendek/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
   - 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 semuanya di konsol web.
   - Daftarkan mesin di konsol web (jika agen perlindungan sudah diinstal).
   - Tambahkan mesin ke konsol web sebagai mesin **Tidak dikelola**, tanpa menginstal agen perlindungan.

   Anda juga dapat menerapkan rencana perlindungan yang ada ke mesin tempat Anda memasang agen perlindungan atau yang Anda daftarkan di konsol web.
4. Berikan kredensial administrator untuk mesin yang dipilih.
5. Pilih nama atau alamat IP server manajemen yang akan digunakan agen untuk mengakses server tersebut.

   Secara default, nama server dipilih. Anda mungkin harus memilih alamat IP jika server manajemen Anda memiliki lebih dari satu antarmuka jaringan atau jika Anda menghadapi masalah DNS yang mengakibatkan kegagalan registrasi agen.
6. Verifikasi bahwa Anda dapat terhubung ke mesin menggunakan kredensial yang ditentukan.

Mesin yang ditampilkan di konsol web 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.

Penemuan otomatis dan penemuan manual

Sebelum memulai penemuan, pastikan bahwa prasyarat sudah terpenuhi.

Untuk menemukan mesin

1. Di konsol web, buka **Perangkat** > **Semua perangkat**.
2. Klik **Tambah**.
3. Di **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.
8. [Jika metode penemuan Active Directory atau jaringan lokal dipilih] Gunakan daftar untuk memilih mesin yang ingin Anda tambah.

   [Jika metode penemuan Manual dipilih] Tentukan alamat IP mesin atau nama host, atau impor daftar mesin dari file teks. File harus berisi alamat IP/nama host, satu per baris. Ini adalah contoh file:

   ```
   156.85.34.10
   156.85.53.32
   156.85.53.12
   EN-L00000100
   EN-L00000101
   ```

   Setelah menambahkan alamat mesin secara manual atau mengimpornya dari file, agen akan mencoba melakukan ping ke mesin yang ditambahkan dan menentukan ketersediaannya.
9. Pilih yang harus dilakukan setelah penemuan:
   - **Instal agen dan daftarkan mesin**. Anda dapat memilih komponen apa untuk diinstal pada mesin dengan mengeklik **Pilih komponen**. Untuk detail selengkapnya, lihat "Memilih komponen untuk instalasi". Anda dapat menginstal hingga 100 agen secara bersamaan.

     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.

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.

- **Daftarkan mesin dengan agen yang terinstal**. Opsi ini digunakan jika agen sudah diinstal di mesin dan Anda hanya perlu mendaftarkannya di Cyber Protect. Jika di dalam mesin tidak ditemukan agen, mesin akan ditambahkan sebagai mesin yang **Tidak dikelola**.
- **Tambahkan sebagai mesin yang tidak dikelola**. Agen tidak akan diinstal pada mesin. Anda dapat melihatnya di konsol web dan menginstal atau mendaftarkan agen nanti.

[Jika tindakan pasca-penemuan **Instal agen dan daftarkan mesin** yang dipilih] **Mulai ulang mesin jika diperlukan** – jika opsi tersebut diaktifkan, mesin akan dimulai ulang sesering mungkin yang diperlukan untuk menyelesaikan instalasi.

Memulai ulang mesin mungkin perlu dilakukan pada salah satu kasus berikut:

- Instalasi prasyarat selesai dan mulai ulang perlu dilakukan untuk melanjutkan instalasi.
- Instalasi selesai tetapi mulai ulang perlu dilakukan karena beberapa file terkunci selama instalasi.
- Instalasi selesai tetapi mulai ulang perlu dilakukan untuk perangkat lunak lain yang diinstal sebelumnya.

[Jika **Mulai ulang mesin jika diperlukan** dipilih] **Jangan mulai ulang jika pengguna sedang login** – jika opsi ini diaktifkan, mesin tidak akan dimulai ulang secara otomatis jika pengguna sudah login ke sistem. Contohnya, jika pengguna sedang bekerja saat instalasi meminta mulai ulang, sistem tidak akan dimulai ulang.

Jika prasyarat sudah diinstal dan boot ulang belum dilakukan karena ada pengguna yang masuk, untuk menyelesaikan instalasi agen Anda harus boot ulang mesin dan memulai instalasi lagi.

Jika agen sudah diinstal tapi boot ulang belum dilakukan, Anda harus melakukan boot ulang mesin.

[Jika ada unit di organisasi Anda] **Unit tempat mendaftarkan mesin** – pilih unit tempat mesin akan didaftarkan.

Jika Anda sudah memilih salah satu dari dua tindakan pasca penemuan pertama, terdapat juga opsi untuk menerapkan rencana proteksi pada mesin. Jika memiliki beberapa rencana proteksi, Anda dapat memilih yang mana yang akan digunakan.

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

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 kredensial administrator kustom, Anda harus melakukan persiapan manual tambahan seperti yang dijelaskan di Menambahkan mesin yang menjalankan Windows > Persiapan.

11. Pilih nama atau alamat IP server manajemen yang akan digunakan agen untuk mengakses server tersebut.

    Secara default, nama server dipilih. Anda mungkin harus memilih alamat IP jika server manajemen Anda memiliki lebih dari satu antarmuka jaringan atau jika Anda menghadapi masalah DNS yang mengakibatkan kegagalan registrasi agen.

12. 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 **Dasbor** > **Aktivitas** > aktivitas **Menemukan mesin**.

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.
Komponen tambahan	
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 Office 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 Protect	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.
Alat Baris Perintah	Cyber Protect mendukung antarmuka baris perintah dengan utilitas acrocmd. acrocmd tidak berisi alat bantu apa pun yang mengeksekusi perintah secara fisik. Alat ini hanya menyediakan antarmuka baris perintah untuk komponen - agen Cyber Protect dan server manajemen. Agen ini akan diinstal jika dipilih.
Pembangun Media Yang Dapat Di-Boot	Komponen ini memungkinkan pengguna untuk membuat media yang dapat di-boot dan akan diinstal di mesin Windows, jika dipilih.

Mengelola mesin yang ditemukan

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

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 Protect dengan memilih mesin dalam daftar dan mengeklik **Instal dan daftarkan**.

Wizard yang terbuka juga memungkinkan Anda untuk menetapkan rencana proteksi pada sekumpulan mesin.

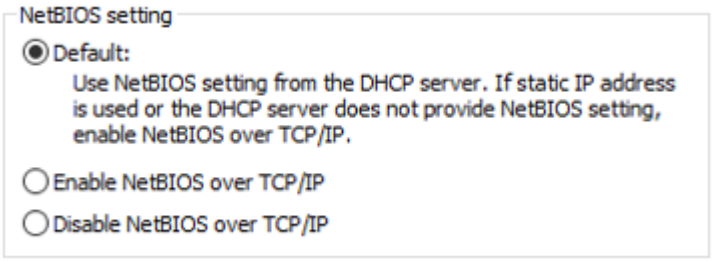
Setelah agen perlindungan diinstal pada mesin, mesin tersebut akan ditampilkan di bagian **Perangkat** > **Mesin dengan agen**.

Untuk memeriksa status proteksi Anda, buka **Dasbor** > **Ikhtisar** dan tambahkan widget **Status proteksi** atau widget **Mesin yang ditemukan**.

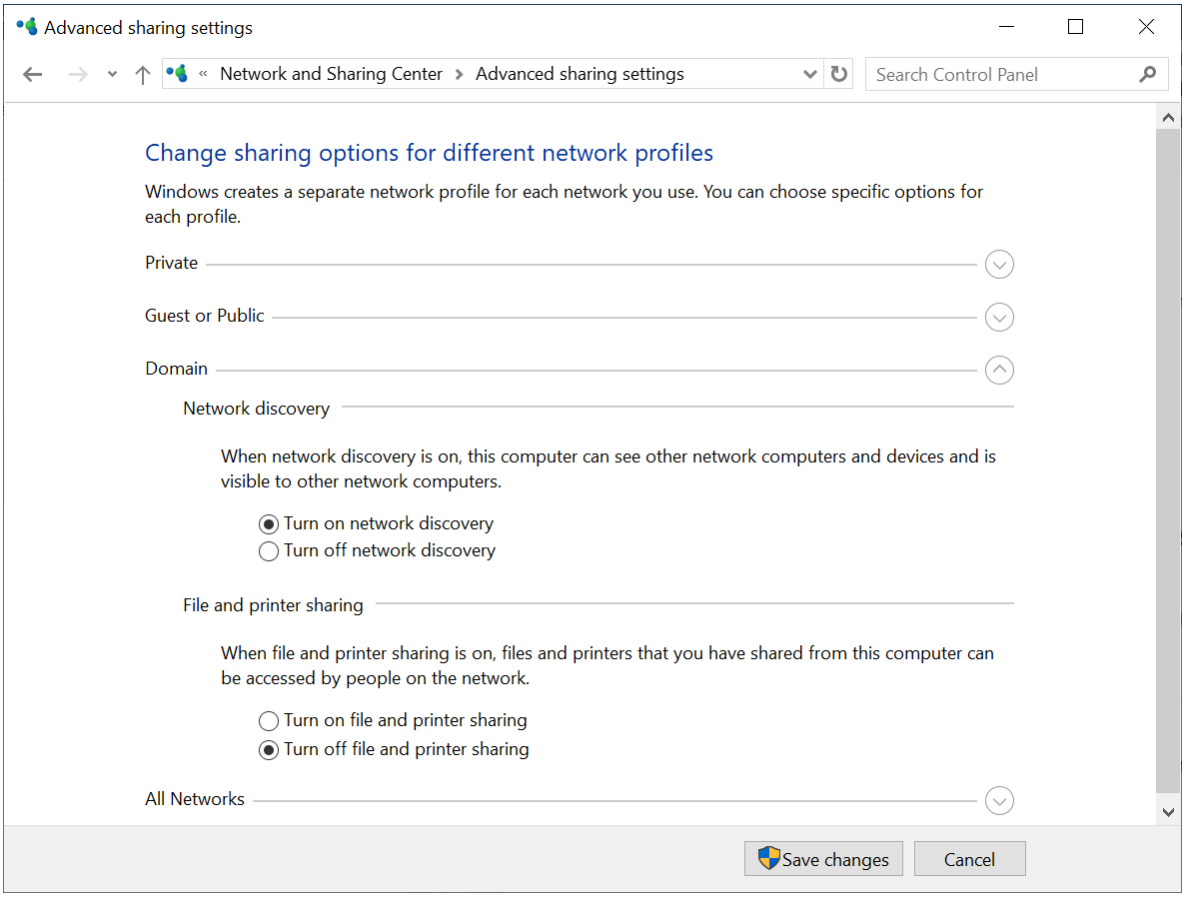
Penyelesaian masalah

Jika Anda memiliki masalah apa pun dengan fungsi penemuan otomatis, coba langkah berikut:

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



- Di **Kontrol Panel** > **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.

Menyebarkan Agen untuk VMware (Perlengkapan Virtual) dari templat OVF

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. Kami sarankan untuk menambah sumber daya ini menjadi 8 GB RAM dan 4 vCPU jika bandwidth lalu lintas pencadangan diperkirakan melebihi 100 MB per detik (misalnya, pada jaringan 10-Gbit), untuk meningkatkan performa pencadangan.

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

Catatan
API vStorage harus diinstal pada host ESXi untuk mengaktifkan cadangan mesin virtual. Lihat https://kb.acronis.com/content/14931.

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 merekomendasikan penggunaan penyimpanan yang terpasang secara lokal (yaitu menyimpan cadangan pada disk virtual yang ditambahkan pada alat virtual) jika Anda memiliki lebih dari satu agen. Untuk pertimbangan selanjutnya, lihat "Menggunakan penyimpanan yang terpasang secara lokal".

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**.

Menyebarkan templat OVF

Lokasi templat OVF

Templat OVF terdiri dari satu file .ovf dan dua file .vmdk.

Dalam penyebaran di lokasi

Setelah server manajemen diinstal, paket OVF alat virtual akan berada di folder **%ProgramFiles%\Acronis\ESXAppliance** (di Windows) atau **/usr/lib/Acronis/ESXAppliance** (di Linux).

Di penerapan awan

1. Klik **Semua perangkat** > **Tambah** > **VMware ESXi** > **Alat Virtual (OVF)**.
   Arsip .zip diunduh ke mesin Anda.
2. Ekstrak arsip .zip.

Menyebarkan templat OVF

1. Pastikan file templat OVF dapat diakses dari mesin yang menjalankan Klien vSphere.
2. Mulai vSphere Client dan masuk ke vCenter Server.
3. Sebarkan templat OVF.
   - Ketika mengonfigurasi penyimpanan, pilih penyimpanan data bersama, jika ada. Format disk tebal atau tipis tidak masalah, karena tidak memengaruhi performa alat.
   - Saat mengonfigurasi koneksi jaringan dalam penyebaran awan, pastikan untuk memilih jaringan yang memungkinkan koneksi Internet, sehingga agen dapat otomatis terdaftar dengan benar di awan. Saat mengonfigurasi koneksi jaringan dalam penyebaran di lokasi, pilih jaringan yang menyertakan server manajemen.

Mengonfigurasi alat virtual

1. **Memulai alat virtual**
   Pada vSphere Client, tampilkan **Inventaris**, klik kanan nama alat virtual, lalu pilih **Daya** > **Nyalakan**. Pilih tab **Konsol**.
2. **Server proksi**
   Jika server proksi diaktifkan pada jaringan Anda:

a. Untuk memulai command shell, tekan CTRL+SHIFT+F2 saat berada di UI alat virtual.

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 `ALAMAT` 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 `KATA SANDI` 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 **`boot ulang`**.

Jika tidak, lewati langkah ini.

3. **Pengaturan jaringan**

   Koneksi jaringan agen dikonfigurasi secara otomatis menggunakan Dynamic Host Configuration Protocol (DHCP). Untuk mengubah konfigurasi default, pada **Opsi agen**, di **eth0**, klik **Ubah** dan tentukan pengaturan jaringan yang diinginkan.

4. **vCenter/ESX(i)**

   Pada **Opsi agen**, di **vCenter/ESX(i)**, klik **Ubah** dan tentukan nama vCenter Server atau alamat IP. Agen akan dapat mencadangkan dan memulihkan mesin virtual yang dikelola oleh vCenter Server.

   Jika Anda tidak menggunakan vCenter Server, tentukan nama atau alamat IP host ESXi yang mesin virtualnya ingin Anda cadangkan dan pulihkan. Normalnya, pencadangan berjalan lebih cepat saat agen mencadangkan mesin virtual yang dihosting di mesinnya sendiri.

Tentukan kredensial yang akan digunakan agen untuk terhubung ke vCenter Server atau ESXi. Kami sarankan untuk menggunakan akun yang memiliki peran **Administrator**. Jika tidak, sediakan akun dengan privilese yang diperlukan pada vCenter Server atau ESXi.

Anda dapat mengklik **Periksa sambungan** untuk memastikan kredensial akses sudah benar.

5. **Server manajemen**
   a. Pada **Opsi agen**, di **Server Manajemen**, klik **Ubah**.
   b. Di **Name/IP Server**, lakukan salah satu langkah berikut:
      - Untuk penyebaran di lokasi, pilih **Lokal**. Tentukan nama host atau alamat IP mesin tempat server manajemen diinstal.
      - Untuk penyebaran awan, pilih **Awan**. Perangkat lunak menampilkan alamat layanan Perlindungan Cyber. Jangan ubah alamat ini kecuali diperintahkan.
   c. Di **Nama pengguna** dan **Kata Sandi**, lakukan salah satu langkah berikut:
      - Untuk penyebaran di lokasi, tentukan nama pengguna dan kata sandi administrator server manajemen.
      - Untuk penyebaran awan, tentukan nama pengguna dan kata sandi untuk layanan Perlindungan Cyber. Agen dan mesin virtual yang dikelola oleh agen akan didaftarkan dalam akun ini.
6. **Zona waktu**

   Pada **Mesin virtual**, di **Zona waktu**, klik **Ubah**. Pilih zona waktu lokasi Anda untuk memastikan operasi terjadwal berjalan pada waktu yang tepat.
7. **[Opsional] Penyimpanan lokal**

   Anda dapat melampirkan disk tambahan ke alat virtual sehingga Agen untuk VMware dapat mencadangkan ke penyimpanan terlampir secara lokal ini.

   Tambahkan disk dengan mengedit pengaturan mesin virtual dan klik **Refresh**. Tautan **Buat penyimpanan** akan tersedia. Klik tautan ini, pilih disk, lalu tentukan label untuknya.

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

Saat menyebarkan alat virtual, Anda dapat memilih antara berbagai kombinasi vCPU dan RAM. 2 vCPU dan RAM 4 GiB sudah optimal dan memadai untuk sebagian besar operasi. Kami sarankan untuk menambah sumber daya ini menjadi 4 vCPU dan RAM 8 GiB jika bandwidth lalu lintas

pencadangan diperkirakan melebihi 100 MB per detik (misalnya, pada jaringan 10-Gbit), untuk meningkatkan kinerja pencadangan.

Disk virtual milik alat memerlukan tidak lebih dari 6 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.

Jika Anda memiliki lebih dari satu agen dalam klaster, mesin virtual secara otomatis membagi dengan adil antara para agen, sehingga setiap agen mengelola mesin dalam jumlah yang sama.

Redistribusi otomatis terjadi ketika ketidakseimbangan beban di antara agen mencapai 20 persen. Hal ini dapat terjadi, misalnya, ketika mesin atau agen ditambahkan atau dihapus. 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 untuk agen akan diredistribusikan di antara agen yang tersisa. Namun, hal ini tidak akan terjadi jika agen rusak atau dihapus secara manual dari klaster Scale Computing HC3. Redistribusi hanya akan dimulai setelah Anda menghapus agen tersebut dari antarmuka web Cyber Protect.

Anda dapat melihat hasil dari distribusi otomatis:

- Di kolom **Agen** untuk setiap mesin virtual di bagian **Semua perangkat**
- Di bagian **Mesin virtual yang ditetapkan** pada panel **Detail** ketika agen dipilih di bagian **Pengaturan** > **Agen**

Menyebarkan alat virtual

1. Masuk ke akun Cyber Protect Anda.
2. Klik **Perangkat** > **Semua perangkat** > **Tambahkan** > **Scale Computing HC3**.
3. Pilih jumlah alat virtual yang ingin Anda sebarkan.
4. Tentukan alamat IP atau nama host klaster Scale Computing HC3.
5. Tentukan kredensial akun yang memiliki peran **Buat/Edit VM** yang ditugaskan di klaster ini.
6. Tentukan berbagi jaringan yang akan digunakan untuk penyimpanan file profil sementara bagi alat virtual. Diperlukan ruang bebas minimal 2 GB.
7. Tentukan kredensial dari akun yang telah membaca dan menulis akses ke berbagi jaringan ini.
8. Klik **Sebarkan**.

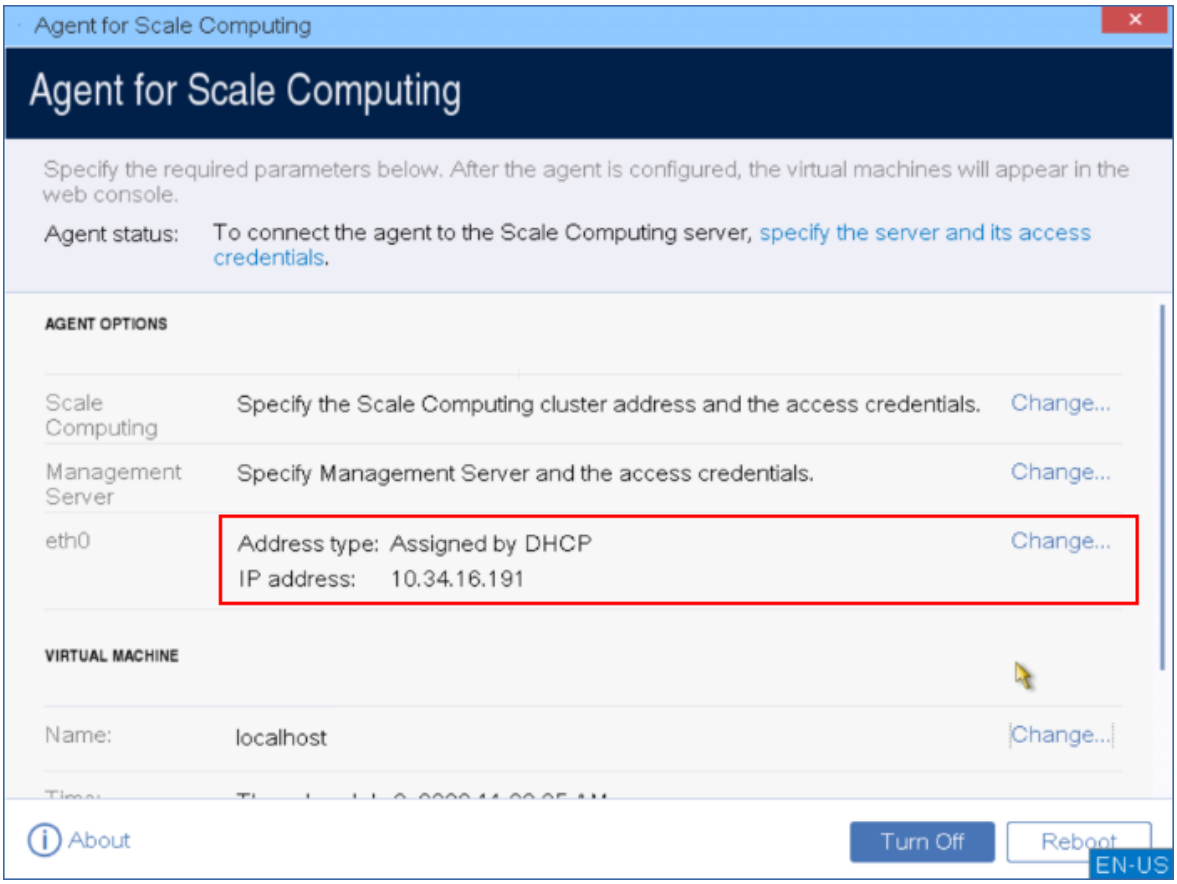
Setelah penyebaran selesai, konfigurasi alat virtual.

Mengonfigurasi alat virtual

Setelah menyebarkan alat virtual, Anda harus mengonfigurasikannya agar dapat menjangkau klaster Scale Computing HC3 yang akan dilindunginya dan server manajemen Cyber Protect.

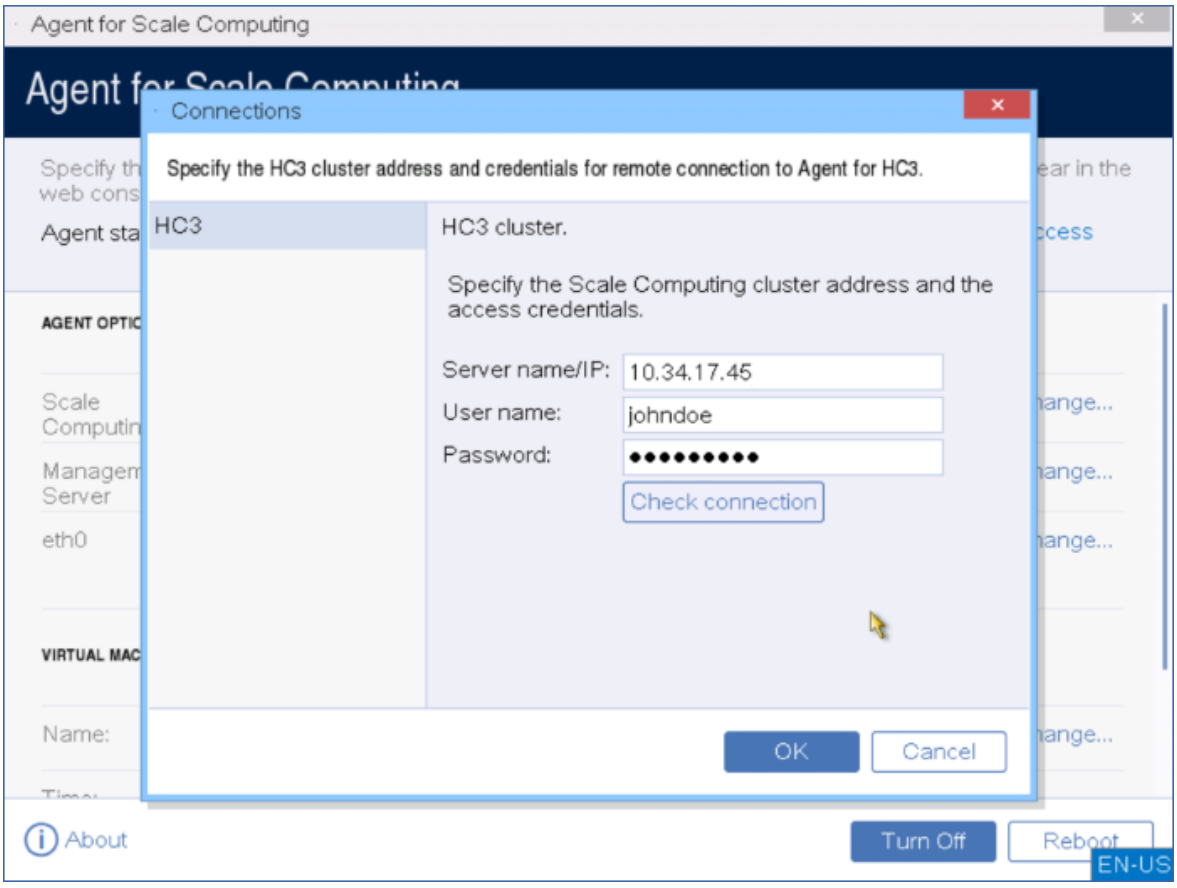
Untuk mengonfigurasi alat virtual

1. Masuk ke akun Scale Computing HC3.
2. Pilih mesin virtual dengan agen yang harus Anda konfigurasi, kemudian klik **Konsol**.
3. Konfigurasi antarmuka jaringan pada alat. Mungkin ada satu atau beberapa antarmuka untuk dikonfigurasi – bergantung pada jumlah jaringan yang digunakan alat. Pastikan alamat DHCP yang ditetapkan secara otomatis (jika ada) valid dalam jaringan yang digunakan mesin virtual Anda, atau tetapkan secara manual.

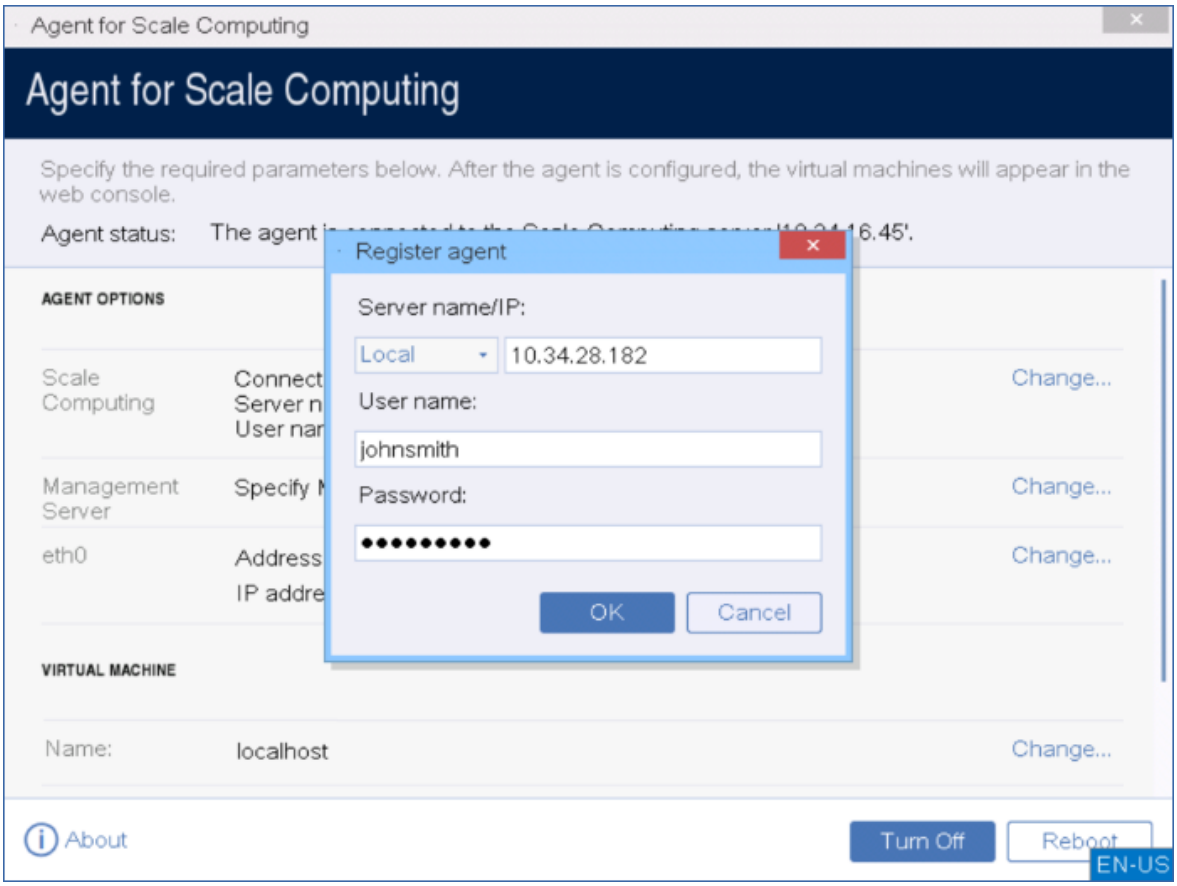


4. Tentukan alamat dan kredensial klaster Scale Computing HC3:
   - Nama DNS atau alamat IP klaster.
   - Di bidang **Nama pengguna** dan **Kata sandi**, masukkan kredensial untuk akun Scale Computing HC3 dengan peran yang sesuai.

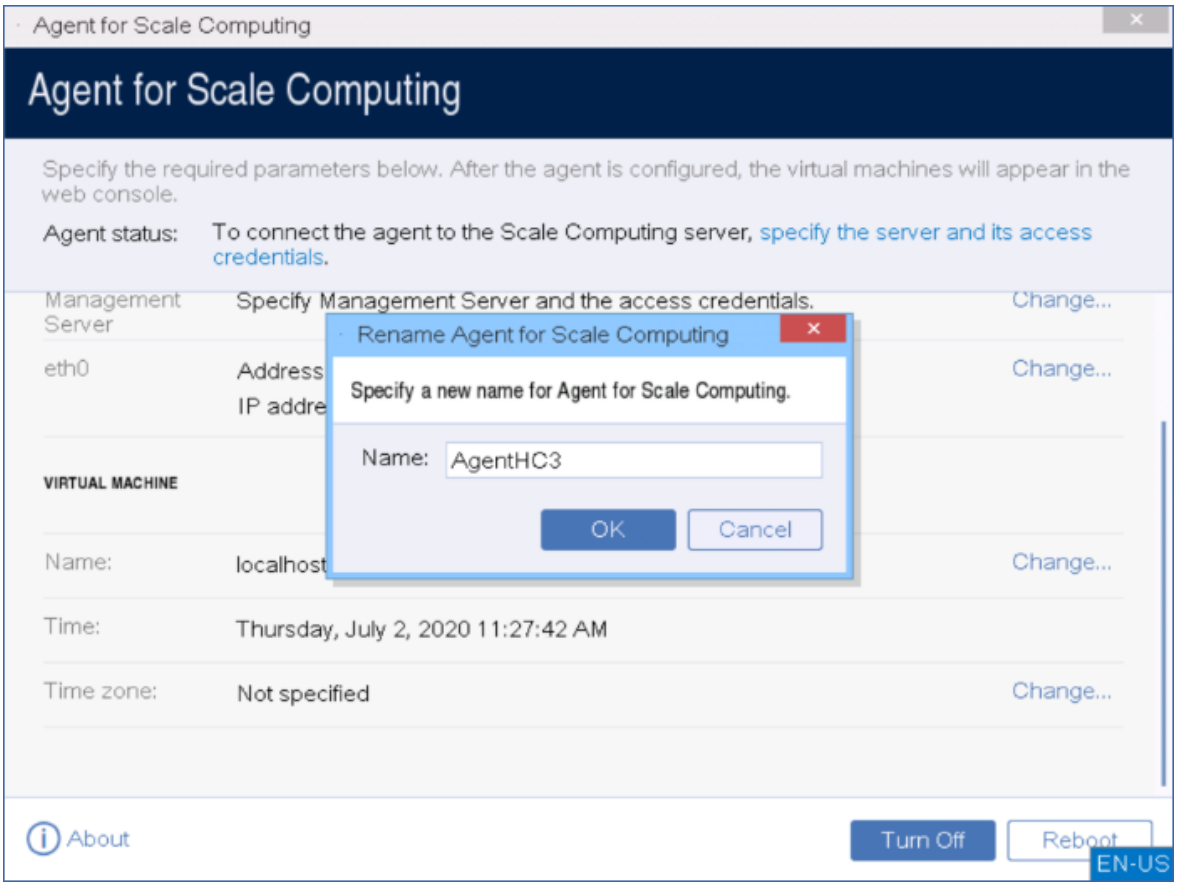
   Anda dapat mengklik **Periksa sambungan** untuk memastikan kredensial akses sudah benar.



5. Tentukan alamat server manajemen dan kredensial Cyber Protect untuk mengaksesnya.



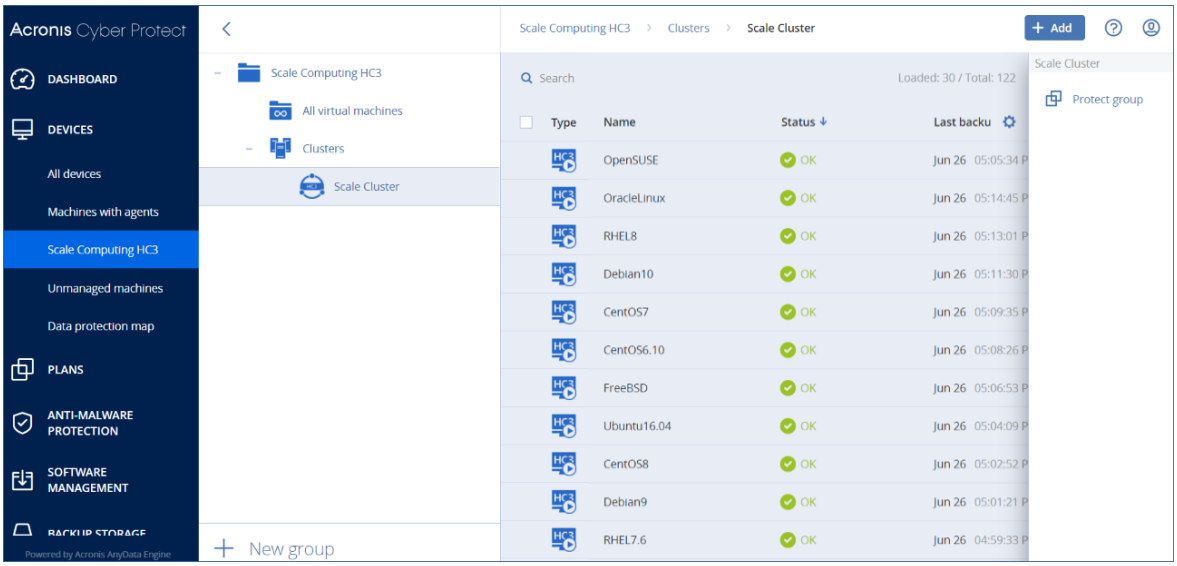
6. [Opsional] Tentukan nama untuk agen. Nama ini akan ditampilkan di konsol web Cyber Protect.



7. [Opsional] Pilih zona waktu lokasi Anda untuk memastikan operasi terjadwal berjalan pada waktu yang tepat.

Untuk melindungi mesin virtual dalam klaster Scale Computing HC3

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



Agen untuk Scale Computing HC3 – peran yang diperlukan

Bagian ini menjelaskan tentang peran yang diperlukan untuk operasi dengan mesin virtual Scale Computing HC3 dan, untuk penyebaran alat virtual.

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

Menyebarkan agen melalui Kebijakan Grup

Anda dapat menginstal (atau menyebarkan) Agen secara terpusat untuk Windows ke mesin yang menjadi anggota domain Active Directory menggunakan Kebijakan Grup.

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

Sebelum melanjutkan penyebaran agen, pastikan:

- Anda memiliki domain Active Directory dengan pengontrol domain yang menjalankan Microsoft Windows Server 2003 ke atas.
- Anda adalah anggota grup **Admin Domain** di dalam domain.

- Anda telah mengunduh program penyiapan **Semua agen untuk instalasi di Windows**. Tautan unduhan tersedia di halaman **Tambah perangkat** di konsol web Cyber Protect.

Langkah 1: Membuat token pendaftaran

Token registrasi mengirimkan identitas Anda ke program penyiapan tanpa menyimpan identitas masuk dan kata sandi Anda untuk konsol web Cyber Protect. Hal ini memungkinkan Anda untuk mendaftarkan sejumlah mesin dengan akun Anda. Agar lebih aman, token memiliki masa aktif yang terbatas.

Untuk membuat token pendaftaran

1. Masuk ke konsol web Cyber Protect menggunakan kredensial akun yang akan ditetapkan mesin untuknya.
2. Klik **Semua perangkat** > **Tambah**.
3. Gulir ke bawah sampai **Token pendaftaran**, lalu klik **Hasilkan**.
4. Tentukan masa aktif token, lalu klik **Hasilkan token**.
5. Salin atau tulis token. Pastikan untuk menyimpan token jika Anda membutuhkannya untuk digunakan lebih lanjut.

   Anda dapat mengklik **Kelola token aktif** untuk melihat dan mengelola token yang sudah dibuat. Perlu diketahui bahwa karena alasan keamanan, tabel ini tidak menampilkan nilai token lengkap.

Langkah 2: Membuat transform .mst dan mengekstrak paket instalasi

1. Masuk sebagai administrator pada mesin apa pun di dalam domain.
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. Mulai program penyiapan.
4. Klik **Buat file .mst dan .msi untuk instalasi tanpa pengawasan**.
5. Tinjau atau modifikasi pengaturan instalasi yang akan ditambahkan ke file .mst. Saat menentukan metode koneksi ke server manajemen, pilih **Gunakan token pendaftaran**, lalu masukkan token yang Anda hasilkan.
6. Klik **Memproses**.
7. Pada bagian **Simpan file ke**, tentukan jalur ke folder yang Anda buat.
8. Klik **Hasilkan**.

Hasilnya, transform .mst akan dibuat dan paket instalasi .msi dan .cab akan diekstrak ke folder yang Anda buat.

Langkah 3: Menyiapkan objek Kebijakan Grup

1. Masuk ke pengontrol domain sebagai administrator domain; jika domain memiliki lebih dari satu pengendali domain, masuk ke salah satunya sebagai administrator domain.
2. Jika Anda berencana untuk menyebarkan agen di unit organisasi, pastikan unit organisasi ada di domain. Jika tidak, lewati langkah ini.
3. Pada menu **Start** , arahkan ke **Administrative Tools**, lalu klik **Active Directory Users and Computers** (di Windows Server 2003) atau **Group Policy Management** (di Windows Server 2008 ke atas).
4. Di Windows Server 2003:
   - Klik kanan nama domain atau unit organisasi, lalu klik **Properti**. Di kotak dialog, klik tab **Kebijakan Grup**, lalu klik **Baru**.

   Di Windows Server 2008 ke atas:
   - Klik kanan nama domain atau unit organisasi, lalu klik **Buat GPO di domain ini, dan Tautkan di sini**.
5. Beri nama objek Kebijakan Grup baru **Agen untuk Windows.**
6. Buka objek Kebijakan Grup **Agen untuk Windows** untuk mengedit, dengan langkah sebagai berikut:
   - Di Windows Server 2003, klik objek Kebijakan Grup, lalu klik **Edit**.
   - Di Windows Server 2008 ke atas, pada **Group Policy Objects**, klik kanan objek Kebijakan Grup, lalu klik **Edit**.
7. Pada snap-in editor objek Kebijakan Grup, perluas **Konfigurasi Komputer**.
8. Di Windows Server 2003 dan Windows Server 2008:
   - Perluas **Pengaturan Perangkat Lunak**.

   Di Windows Server 2012 ke atas:
   - Perluas **Kebijakan** > **Pengaturan Perangkat Lunak**.
9. Klik kanan **Instalasi perangkat lunak**, arahkan ke **Baru**, lalu klik **Paket**.
10. Pilih paket instalasi .msi agen di folder bersama yang Anda buat sebelumnya, lalu klik **Buka**.
11. Di kotak dialog **Sebarkan Perangkat Lunak**, klik **Lanjutan**, lalu klik **OK**.
12. Di tab **Modifikasi**, klik **Tambah**, lalu pilih perubahan pertama yang Anda buat sebelumnya.
13. Klik **OK** untuk menutup kotak dialog **Sebarkan Perangkat Lunak**.

Memperbarui alat virtual

Penyebaran di lokasi

Untuk memperbarui alat virtual (Agen untuk VMware atau Agen untuk Scale Computing HC3) yang memiliki versi di bawah 15.24426 (dirilis pada September 2020), ikuti prosedur dalam

"Memperbarui agen" (hlm. 178).

Untuk memperbarui versi alat virtual 15.24426 atau versi setelahnya

1. Unduh paket pembaruan seperti yang dijelaskan dalam http://kb.acronis.com/terakhir.
2. Simpan file `tar.bz` di direktori mesin server manajemen berikut:
   - Windows: `C:\Program Files\Acronis\VirtualAppliances\va-updates`
   - Linux: `/usr/lib/Acronis/VirtualAppliances/va-updates`
3. Di konsol web Cyber Protect, klik **Pengaturan** > **Agen**.
   Perangkat lunak menampilkan daftar mesin. Mesin dengan alat virtual yang kedaluwarsa ditandai dengan tanda seru berwarna oranye.
4. Pilih mesin yang ingin Anda perbarui alat virtualnya. Mesin ini harus online.
5. Klik **Perbarui agen**.
6. Pilih agen penyebaran.
7. Tentukan kredensial akun dengan hak istimewa administratif pada mesin target.
8. Pilih nama atau alamat IP yang akan digunakan agen untuk mengakses server manajemen.
   Secara default, nama server dipilih. Anda mungkin perlu mengubah pengaturan ini jika server DNS tidak dapat menyelesaikan nama ke alamat IP, yang mengakibatkan kegagalan selama registrasi alat virtual.

Progres pembaruan ditunjukkan pada tab **Aktivitas**.

Catatan
Selama pembaruan, pencadangan apa pun yang sedang berjalan, akan gagal.

Penyebaran awan

Untuk informasi tentang memperbarui alat virtual dalam penyebaran awan, lihat Memperbarui agen di dokumentasi awan.

Memperbarui agen

Prasyarat

Pada mesin Windows, fitur Cyber Protect memerlukan Microsoft Visual C++ 2017 Redistributable. Harap pastikan bahwa ini sudah diinstal di mesin Anda atau installah sebelum memperbarui agen. Setelah instalasi, mulai ulang mungkin perlu dilakukan. Paket Microsoft Visual C++ Redistributable dapat ditemukan di sini https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Untuk menemukan versi agen, pilih mesin, lalu klik **Detail**.

Anda dapat memperbarui agen dengan konsol web Cyber Protect atau mengulangi instalasinya dengan cara apa pun yang tersedia. Untuk memperbarui beberapa agen secara bersamaan, gunakan prosedur berikut.

Untuk memperbarui agen menggunakan konsol web Cyber Protect

1. [Hanya pada penyebaran di lokasi] Perbarui server manajemen.
2. [Hanya pada penyebaran di lokasi] Pastikan paket instalasi ada pada mesin dengan server manajemen. Untuk langkah tepatnya, lihat "Menambahkan mesin yang menjalankan Windows" > "Paket instalasi".
3. Di konsol web Cyber Protect, klik **Pengaturan** > **Agen**.
   Perangkat lunak menampilkan daftar mesin. Versi mesin agen yang kedaluwarsa ditandai dengan tanda seru berwarna oranye.
4. Pilih mesin yang ingin Anda perbarui agennya. Mesin harus online.
5. Klik **Perbarui agen**.
6. Pilih agen penyebaran.
7. Tentukan kredensial akun dengan hak istimewa administratif pada mesin target.
8. Pilih nama atau alamat IP server manajemen yang akan digunakan agen untuk mengakses server tersebut.
   Secara default, nama server dipilih. Anda mungkin harus memilih alamat IP jika server manajemen Anda memiliki lebih dari satu antarmuka jaringan atau jika Anda menghadapi masalah DNS yang mengakibatkan kegagalan registrasi agen.
9. [Hanya pada penyebaran di lokasi] Progres pembaruan ditunjukkan pada tab **Aktivitas**.

Catatan
Selama pembaruan, pencadangan apa pun yang sedang berjalan, akan gagal.

Untuk memperbarui definisi Cyber Protect pada mesin

1. Klik **Pengaturan** > **Agen-Agen**.
2. Pilih mesin tempat Anda ingin memperbarui definisi Cyber Protect, lalu 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 di bagian **definisi Cyber Protect** , aktifkan **Gunakan agen ini untuk mengunduh serta mendistribusikan patch dan pembaruan**.

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**.

Meningkatkan ke Acronis Cyber Protect 15

Anda dapat meningkatkan produk sebelumnya ke Acronis Cyber Protect 15 dengan cara berikut:

- Langsung, tanpa menguninstall produk sebelumnya.

  Opsi ini hanya tersedia untuk Acronis Backup 12.5 Update 5 (build 16180) dan versi yang lebih baru.
- Dengan mencopot pemasangan produk sebelumnya dan memasang salinan baru Acronis Cyber Protect 15.

  Opsi ini tersedia untuk semua produk yang memenuhi syarat. Untuk informasi lebih lanjut tentang produk ini, lihat artikel basis pengetahuan ini.

Catatan
Kami menyarankan agar Anda mencadangkan sistem sebelum melakukan peningkatan versi. Ini akan memungkinkan Anda untuk memutar kembali ke konfigurasi awal jika upgrade Anda gagal.

Untuk memulai peningkatan versi, jalankan installer dan ikuti petunjuk pada layar.

Server manajemen dalam Acronis Cyber Protect 15 kompatibel dengan versi sebelumnya dan mendukung agen versi 12.5. Meski demikian, agen ini tidak mendukung fitur Cyber Protect.

Meningkatkan agen tidak mengganggu set cadangan yang ada dan pengaturannya.

Menghapus instalasi produk

Jika Anda ingin menghapus komponen produk individual dari mesin, jalankan program pengaturan, pilih untuk memodifikasi produk, dan hapus pilihan komponen yang ingin Anda hapus. Tautan ke program pengaturan ada di halaman **Unduhan** (klik ikon akun di sudut kanan atas > **Unduhan**).

Jika Anda ingin menghapus semua komponen produk dari mesin, ikuti langkah yang dijelaskan di bawah ini.

Peringatan!
Untuk penyebaran di lokasi, berhati-hatilah saat memilih komponen yang akan dihapus instalasinya.

Jika Anda menghapus instalasi server manajemen secara tidak disengaja, konsol web Cyber Protect tidak tersedia lagi dan tidak bisa lagi mencadangkan dan memulihkan mesin yang terdaftar di server manajemen yang dihapus ini.

Di Windows

1. Masuk sebagai administrator.
2. Buka **Panel kontrol**, lalu pilih **Program dan Fitur** (**Tambah atau Hapus Program** di Windows XP) > **Acronis Cyber Protect** > **Hapus instalasi**.
3. [Opsional] Pilih kotak centang **Hapus log dan pengaturan konfigurasi**.

   Jika Anda menghapus instalasi agen dan berencana menginstalnya kembali, biarkan kotak centang ini kosong. Jika Anda memilih kotak centang, mesin dapat diduplikasi di konsol web Cyber Protect dan cadangan mesin lama mungkin tidak akan terkait dengan mesin baru.
4. Konfirmasi keputusan Anda.

Di Linux

1. Sebagai pengguna root, jalankan **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Opsional] Pilih kotak centang **Bersihkan semua jejak produk (Hapus log, tugas, kubah, dan pengaturan konfigurasi produk)**.

   Jika Anda menghapus instalasi agen dan berencana menginstalnya kembali, biarkan kotak centang ini kosong. Jika Anda memilih kotak centang, mesin dapat diduplikasi di konsol web Cyber Protect dan cadangan mesin lama mungkin tidak akan terkait dengan mesin baru.
3. Konfirmasi keputusan Anda.

Di macOS

1. Klik dua kali pada file instalasi (.dmg).
2. Tunggu saat sistem operasi melakukan mounting profil disk instalasi.
3. Di dalam gambar, klik dua kali pada **Hapus instalasi**.
4. Jika diminta, berikan kredensial administrator.
5. Konfirmasi keputusan Anda.

Menghapus Agen untuk VMware (Alat Virtual)

1. Mulai vSphere Client dan masuk ke vCenter Server.
2. Jika alat virtual dihidupkan, klik kanan, lalu klik **Daya** > **Matikan**. Konfirmasi keputusan Anda.
3. Jika VA menggunakan penyimpanan yang terpasang secara lokal di disk virtual dan Anda ingin mempertahankan data pada disk tersebut, lakukan hal berikut:
   a. Klik kanan VA, lalu klik **Edit Pengaturan**.
   b. Pilih disk dengan penyimpanan, lalu klik **Hapus**. Di **Opsi Penghapusan**, klik **Hapus dari mesin virtual**.
   c. 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.

Menghapus mesin dari konsol web Cyber Protect

Setelah instalasi agen dihapus, agen akan dibatalkan registrasinya dari server manajemen, dan mesin tempat agen diinstal akan otomatis dihapus dari konsol web Cyber Protect.

Namun, jika koneksi ke server manajemen terputus selama operasi ini, misalnya – karena masalah jaringan, instalasi agen mungkin dihapus tetapi mesinnya mungkin masih ditampilkan di konsol web. Apabila hal ini terjadi, Anda perlu menghapus mesin dari konsol web secara manual.

Untuk menghapus mesin dari konsol web secara manual

1. Di konsol web Cyber Protect, buka **Pengaturan** > **Agen**.
2. Pilih mesin tempat agen diinstal.
3. Klik **Hapus**.

Mengakses konsol web Cyber Protect

Untuk mengakses konsol web Cyber Protect, masukkan alamat halaman masuk ke biMasuklah alamat browser web, lalu masuk seperti yang dijelaskan di bawah ini.

Penyebaran di lokasi

Alamat halaman masuk adalah alamat IP atau nama mesin tempat server manajemen diinstal.

Protokol HTTP dan HTTPS didukung pada port TCP yang sama, sehingga dapat dikonfigurasi selama instalasi server manajemen. Port defaultnya adalah 9877.

Anda dapat mengonfigurasi server manajemen untuk melarang akses konsol web Cyber Protect melalui HTTP dan untuk menggunakan sertifikat SSL pihak ketiga.

Di Windows

Jika server manajemen diinstal di Windows, ada dua cara untuk masuk ke konsol web Cyber Protect:

- Klik **Masuk** untuk masuk sebagai pengguna Windows saat ini.
  Ini adalah cara termudah untuk masuk dari mesin yang sama di mana server manajemen diinstal.
  Jika server manajemen diinstal pada mesin yang berbeda, metode ini berfungsi dengan ketentuan bahwa:
  - Mesin tempat Anda masuk berada dalam domain Active Directory yang sama dengan server manajemen.
  - Anda masuk sebagai pengguna domain.

  Kami menyarankan konfigurasi browser web Anda untuk Autentikasi Windows Terintegrasi. Jika tidak, browser akan meminta nama pengguna dan kata sandi. Namun, Anda dapat menonaktifkan opsi ini.
- Klik **Masukkan nama pengguna dan kata sandi**, lalu tentukan nama pengguna dan kata sandi.

Bagaimanapun, akun Anda harus ada dalam daftar administrator server manajemen. Secara default, daftar ini berisi grup **Administrator** pada mesin yang menjalankan server manajemen. Untuk informasi lebih lanjut, lihat "Administrator dan unit".

Untuk menonaktifkan opsi Masuk sebagai pengguna Windows saat ini

1. Pada mesin tempat server manajemen diinstal, buka `C:\Program Files\Acronis\AccountServer`.
2. Buka file **account_server.json** untuk pengeditan.
3. Buka bagian "connectors", lalu hapus baris berikut:

```
{
"type": "sspi",
"name": "1 Windows Integrated Logon",
"id": "sspi",
```

```
"config": {}
},
```

4. Arahkan ke bagian "checksum", lalu ubah nilai "sum" sebagai berikut:

```
"sum": "FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbjpzU="
```

5. Mulai ulang Acronis Layanan Manajer Layanan seperti yang dijelaskan dalam "Menggunakan sertifikat yang diterbitkan oleh otoritas sertifikat tepercaya".

Di Linux

Jika server manajemen diinstal di Linux, tentukan nama pengguna dan kata sandi akun yang ada dalam daftar administrator server manajemen. Secara default, daftar ini hanya berisi pengguna **root** pada mesin yang menjalankan server manajemen. Untuk informasi lebih lanjut, lihat "Administrator dan unit".

Penyebaran awan

Alamat halaman masuk adalah https://backup.acronis.com/. Nama pengguna dan kata sandi adalah yang Anda gunakan di akun Acronis.

Jika akun Anda dibuat oleh administrator pencadangan, Anda harus mengaktifkan akun dan mengatur kata sandi dengan mengklik tautan di email aktivasi Anda.

Mengganti bahasa

Saat masuk, Anda dapat mengganti bahasa antarmuka web dengan mengklik ikon akun di sudut kanan atas.

Mengonfigurasi browser web untuk Autentikasi Windows Terintegrasi

Autentikasi Windows Terintegrasi mungkin dilakukan jika Anda mengakses konsol web Cyber Protect dari mesin yang menjalankan Windows dan semua browser yang didukung.

Kami menyarankan konfigurasi browser web Anda untuk Autentikasi Windows Terintegrasi. Jika tidak, browser akan meminta nama pengguna dan kata sandi.

Mengonfigurasi Internet Explorer, Microsoft Edge, Opera, dan Google Chrome

Jika mesin yang menjalankan browser berada dalam domain Active Directory yang sama dengan mesin yang menjalankan server manajemen, tambahkan halaman masuk konsol ke daftar situs **Intranet lokal**.

Jika tidak, tambahkan halaman masuk konsol ke daftar **Situs tepercaya** dan aktifkan **Log masuk otomatis dengan pengaturan nama pengguna dan kata sandi saat ini**.

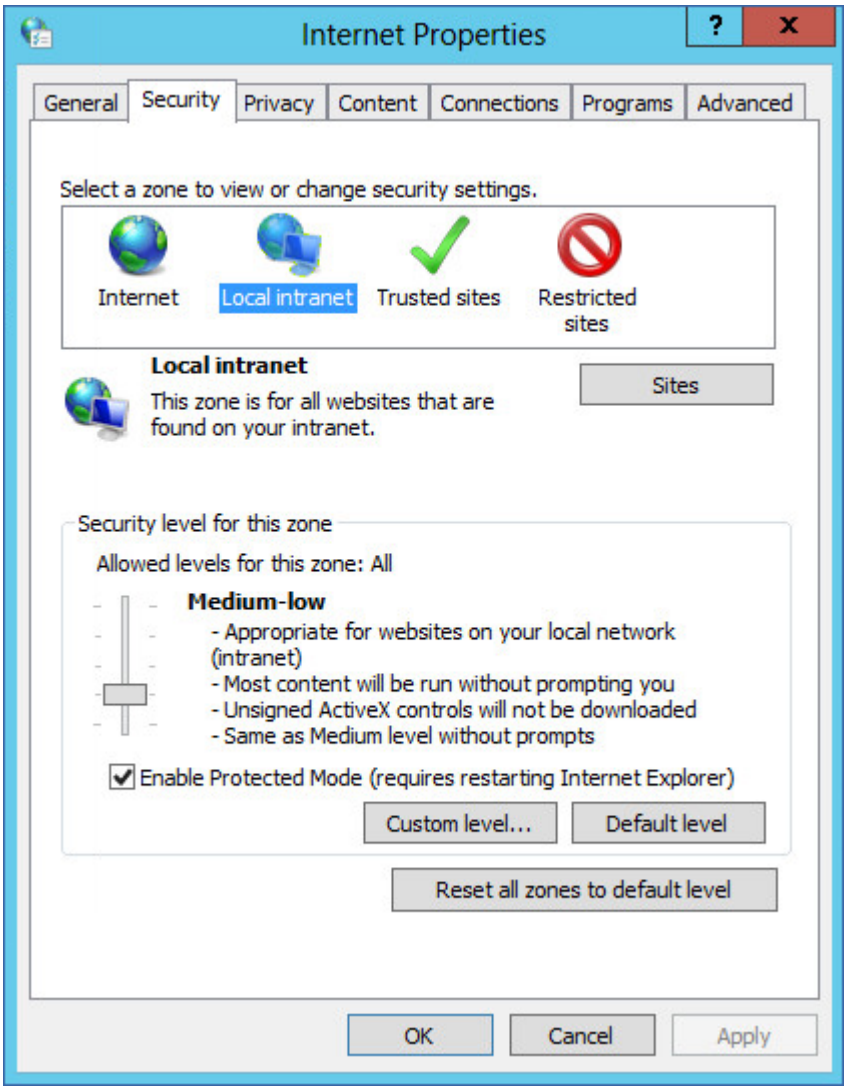
Petunjuk langkah demi langkah tersedia di bagian ini selanjutnya. Karena browser ini menggunakan pengaturan Windows, Anda juga dimungkinkan untuk mengonfigurasinya menggunakan Kebijakan Grup di domain Active Directory.

Mengonfigurasi Mozilla Firefox

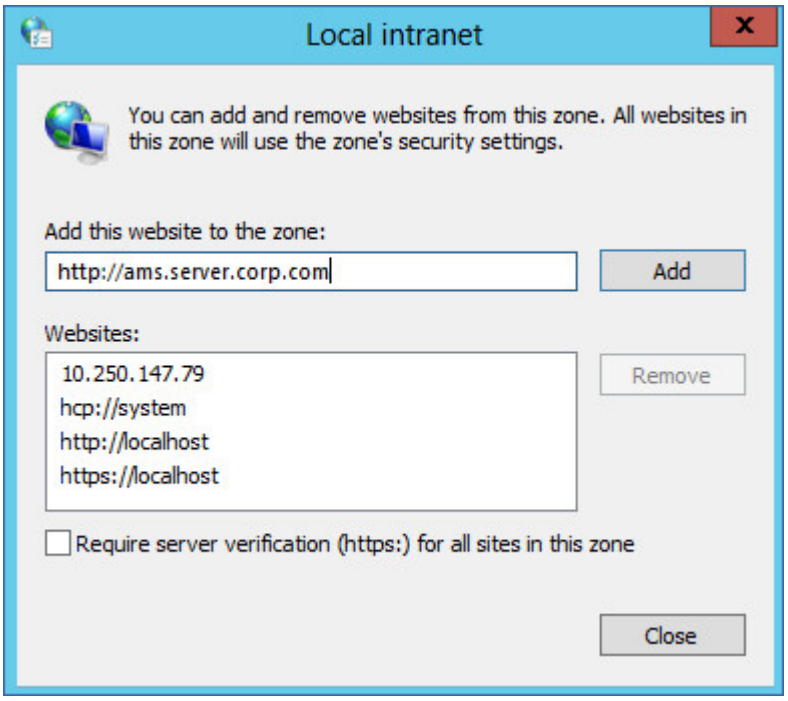
1. Di Firefox, navigasikan ke URL `about:config`, lalu klik tombol **Saya menerima risiko**.
2. Dalam bidang **Pencarian**, cari preferensi `network.negotiate-auth.trusted-uris`.
3. Klik preferensi dua kali, lalu masukkan alamat halaman masuk konsol web Cyber Protect.
4. Ulangi langkah 2-3 untuk preferensi `network.automatic-ntlm-auth.trusted-uris`.
5. Tutup jendela `about:config`.

Menambahkan konsol ke daftar situs intranet lokal

1. Buka **Panel Kontrol** > **Opsi Internet**.
2. Pada tab **Keamanan**, pilih **Intranet lokal**.



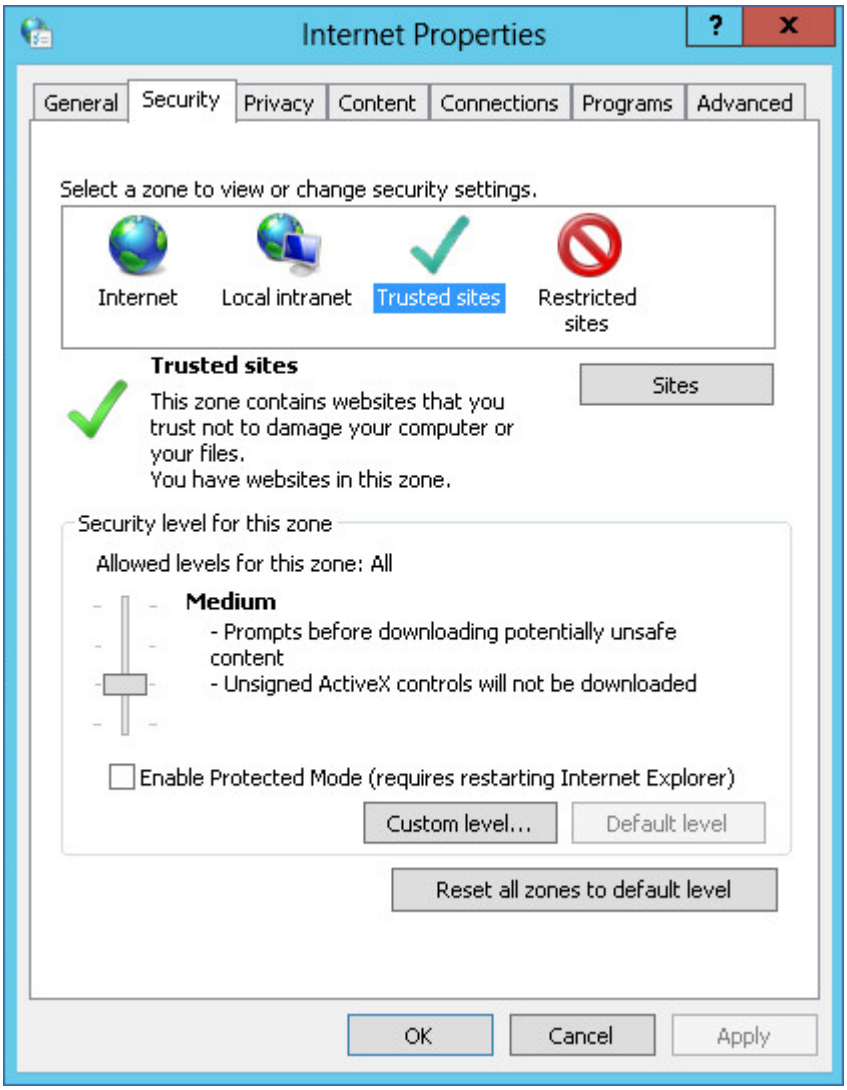
3. Klik **Situs**.
4. Di bidang **Tambahkan situs web ini ke zona**, masukkan alamat halaman masuk konsol web Cyber Protect, lalu klik **Tambah**.



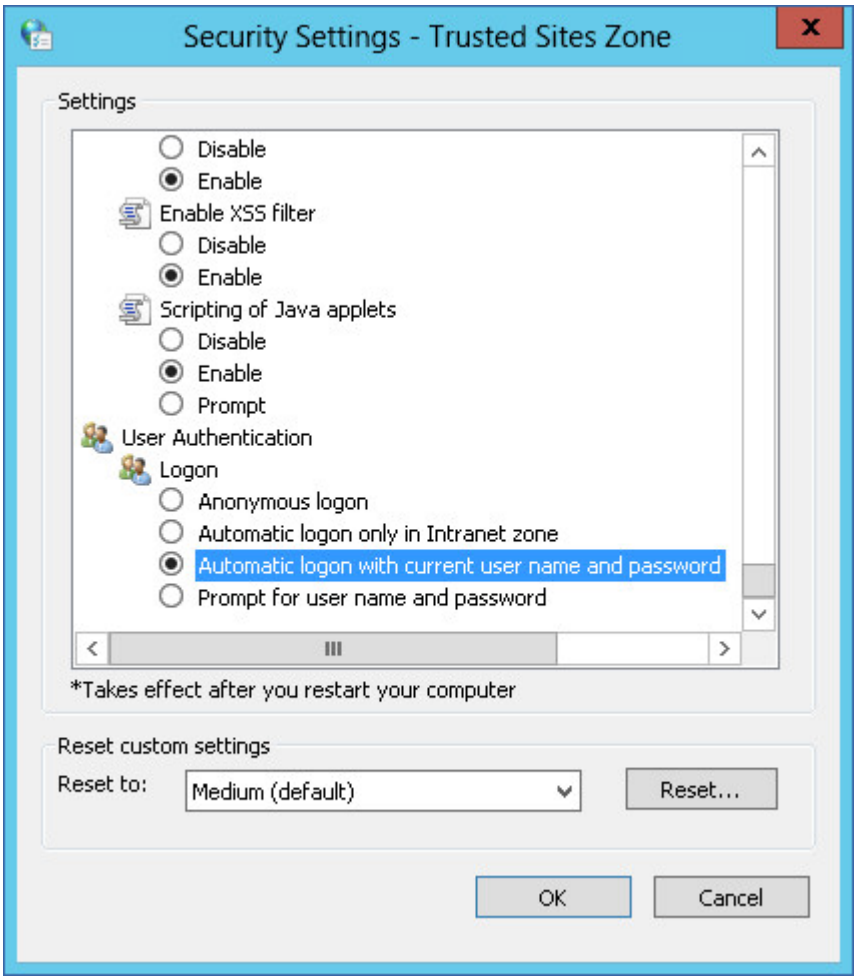
5. Klik **Tutup**.
6. Klik **OK**.

Menambahkan konsol ke daftar situs tepercaya

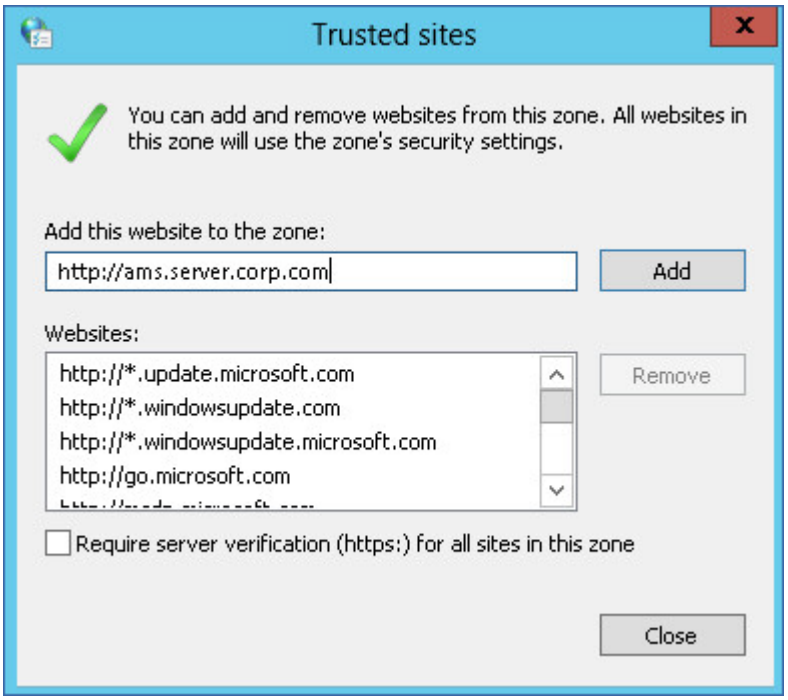
1. Buka **Panel Kontrol** > **Opsi Internet**.
2. Pada tab **Keamanan**, pilih **Situs tepercaya**, lalu klik **Level Kustom**.



3. Di **Masuk**, pilih **Log masuk otomatis dengan nama pengguna dan kata sandi saat ini**, lalu klik **OK**.



4. Pada tab **Keamanan**, dengan **Situs tepercaya** yang masih dipilih, klik **Situs**.
5. Di bidang **Tambahkan situs web ini ke zona**, masukkan alamat halaman masuk konsol web Cyber Protect, lalu klik **Tambah**.



6. Klik **Tutup**.
7. Klik **OK**.

Hanya mengizinkan koneksi HTTPS ke konsol web

Untuk alasan keamanan, Anda dapat mencegah pengguna mengakses konsol web Cyber Protect melalui protokol HTTP, dan hanya mengizinkan koneksi HTTPS.

Untuk hanya mengizinkan koneksi HTTPS ke konsol web

1. Di mesin yang menjalankan server manajemen, buka file konfigurasi berikut dengan editor teks:
   - Di Windows: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - Di Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`
2. Temukan bagian berikut:

   ```
   "tls": {
     "auto_redirect" : false,
     "cert_file": "cert.pem",
   ```

3. Ubah nilai `"auto_redirect"` dari `false` menjadi `true`.

   Jika baris `"auto_redirect"` tidak ada, tambahkan secara manual:

   ```
   "auto_redirect": true,
   ```

4. Simpan file `api_gateway.json`.

Penting
Berhati-hatilah dan jangan sampai menghapus tanda koma, tanda kurung, dan tanda kutip dalam file konfigurasi.

5. Mulai ulang Layanan Acronis Service Manager seperti yang dijelaskan di bawah ini.

Untuk memulai ulang Acronis Layanan Manajer Layanan di Windows

Di Windows

1. Pada menu **Start**, klik **Run**, lalu ketik: **cmd**
2. Klik **OK**.
3. Jalankan perintah berikut:

```
net stop asm
net start asm
```

Di Linux

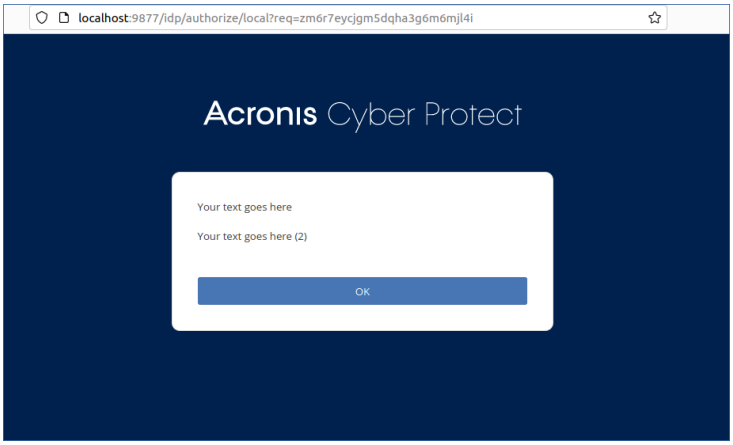
1. **Terminal** Terbuka.
2. Jalankan perintah berikut di direktori mana pun:

```
sudo service acronis_asm restart
```

Menambahkan pesan kustom ke konsol web

Anda dapat menambahkan pesan kustom ke konsol web Cyber Protect.

Pesan ini akan ditampilkan sebelum setiap upaya masuk.



Prasyarat

Jika ada rencana proteksi yang diterapkan pada mesin yang menjalankan server manajemen, pastikan fitur perlindungan mandiri dinonaktifkan. Jika tidak, Anda tidak akan bisa mengedit file

konfigurasi.

Untuk informasi lebih lanjut tentang cara menonaktifkan atau mengaktifkan fitur perlindungan mandiri, lihat "Perlindungan diri" (hlm. 506).

Untuk menambahkan pesan kustom ke konsol web

Di Windows

1. Masuk ke mesin tempat server manajemen diinstal. Akun Anda harus memiliki hak administrator.
2. Arahkan ke `%Program Files%\Acronis\AccountServer`.
3. [Opsional] Buat salinan cadangan file `AccountServer.zip`.
4. Arahkan ke `%Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale`.
5. Ekstrak file JSON yang sesuai dengan bahasa yang Anda gunakan di konsol web Cyber Protect. Misalnya, jika Anda menggunakan bahasa Inggris, ekstrak file `en.json`.

   Catatan
   Agar dapat mengedit file, Anda harus mengekstraknya, bukan hanya membuka file dengan mengeklik dua kali.

6. Buka file yang diekstrak untuk mengedit. Anda dapat menggunakan editor teks, seperti Notepad atau Notepad++.
7. Arahkan ke baris berikut, lalu tambahkan koma di akhir:

   ```
   "APP_LOGINFORM_LOGIN_BUTTON": "Log in",
   ```

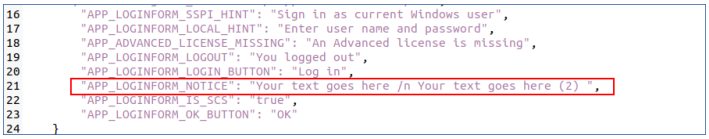
8. Di bawah baris `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"`, tambahkan baris berikut:

   ```
   "APP_LOGINFORM_NOTICE": "<Type your custom message here>",
   ```

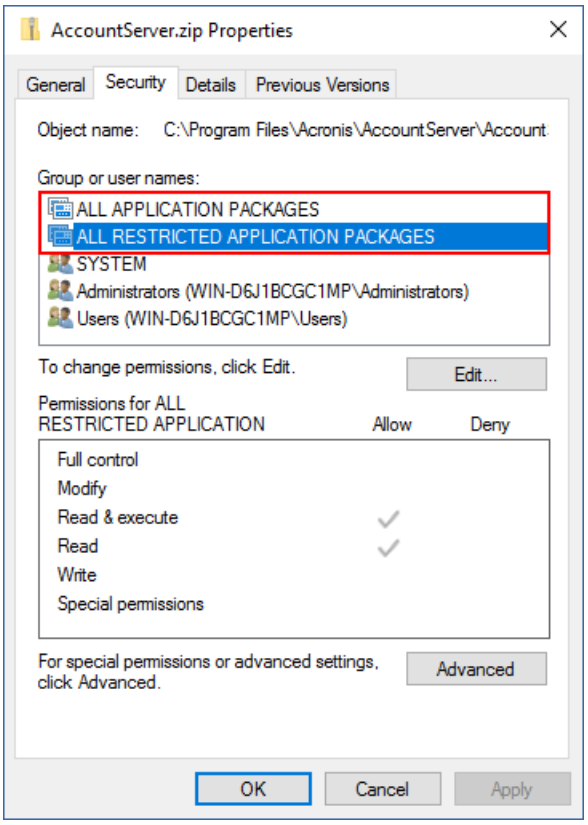
   ```
   "APP_LOGINFORM_IS_SCS": "true",
   ```

   ```
   "APP_LOGINFORM_OK_BUTTON": "OK"
   ```

   Misalnya:

9. Simpan perubahannya, lalu kembalikan file JSON yang sudah diedit di `%Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale`.
10. Klik kanan file `AccountServer.zip`, lalu arahkan ke **Properti** > **Keamanan** untuk memverifikasi bahwa `SEMUA PAKET APLIKASI` dan `SEMUA PAKET APLIKASI TERBATAS` ditambahkan di bawah **Nama grup atau pengguna** dengan hak **Baca** dan **Baca & Jalankan**.



Catatan
Jika `SEMUA PAKET APLIKASI TERBATAS` hilang, hapus `SEMUA PAKET APLIKASI` dari daftar itu, lalu tambahkan lagi. `SEMUA PAKET APLIKASI TERBATAS` akan muncul saat Anda menambahkan `SEMUA PAKET APLIKASI`.

11. Mulai ulang **Layanan Acronis Service Manager** seperti yang dijelaskan di "Untuk memulai ulang Layanan Acronis Service Manager" (hlm. 197).

Di Linux

1. Masuk ke mesin tempat server manajemen diinstal.
2. Arahkan ke `/usr/lib/Acronis/AccountServer`.
3. Pastikan Anda memiliki izin tulis untuk file `AccountServer.zip`.
4. [Opsional] Buat salinan cadangan file `AccountServer.zip`.
5. Arahkan ke `/usr/lib/Acronis/AccountServer/static/locale`.
6. Ekstrak file JSON yang sesuai dengan bahasa yang Anda gunakan di konsol web Cyber Protect. Misalnya, jika Anda menggunakan bahasa Inggris, ekstrak file `en.json`.
7. Buka file yang diekstrak untuk mengedit.
8. Arahkan ke baris berikut, lalu tambahkan koma di akhir:

```
"APP_LOGINFORM_LOGIN_BUTTON": "Log in",
```

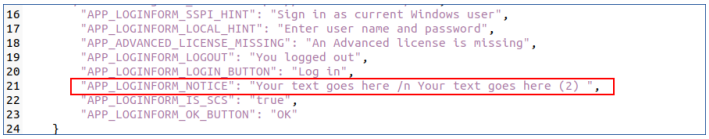
9. Di bawah baris `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"`, tambahkan baris berikut:

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

```
"APP_LOGINFORM_IS_SCS": "true",
```

```
"APP_LOGINFORM_OK_BUTTON": "OK"
```

Contoh:



10. Simpan perubahannya, lalu kembalikan file JSON yang sudah diedit di `/usr/lib/Acronis/AccountServer/static/locale`.
11. Mulai ulang **Layanan Acronis Service Manager** seperti yang dijelaskan di "Untuk memulai ulang Layanan Acronis Service Manager" (hlm. 197).

Pengaturan sertifikat SSL

Bagian ini menjelaskan cara:

- Mengonfigurasi agen perlindungan yang menggunakan sertifikat Secure Socket Layer (SSL) yang ditandatangani sendiri yang dikeluarkan oleh server manajemen.
- Mengubah sertifikat SSL yang ditandatangani sendiri yang dikeluarkan oleh server manajemen menjadi sertifikat yang diterbitkan oleh otoritas sertifikat tepercaya, seperti GoDaddy, Comodo, atau GlobalSign. Jika Anda melakukan ini, sertifikat yang digunakan oleh server manajemen akan dipercaya pada mesin apa pun. Peringatan keamanan browser tidak akan muncul saat masuk ke konsol web Cyber Protect menggunakan protokol HTTPS.

Secara opsional, Anda dapat mengonfigurasi server manajemen untuk melarang akses ke konsol web Cyber Protect melalui HTTP, dengan mengarahkan semua pengguna ke HTTPS.

Menggunakan sertifikat yang ditandatangani sendiri

Untuk mengonfigurasi agen perlindungan di Windows

1. Di mesin dengan agen, buka Editor Registri.
2. Temukan kunci registri berikut: **HKEY_LOCAL_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions.**
3. Atur nilai **VerifyPeer** ke **0**.
4. Pastikan bahwa nilai **VerifyHost** diatur ke **0**.
5. Mulai Ulang Managed Machine Service (MMS):
   a. Di **menu Start**, klik **Run**, lalu ketik: **cmd**
   b. Klik **OK**.

c. Jalankan perintah berikut:

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

Untuk mengonfigurasi agen perlindungan di Linux

1. Pada mesin dengan agen, buka file **/etc/Acronis/BackupAndRecovery.config** untuk pengeditan**.**
2. Arahkan ke kunci **CurlOptions** dan atur nilai untuk **VerifyPeer** ke **0.** Pastikan nilai untuk **VerifyHost** juga diatur ke **0.**
3. Simpan editan Anda.
4. Mulai ulang Managed Machine Service (MMS) dengan menjalankan perintah berikut di direktori mana pun:

```
sudo service acronis_mms restart
```

Untuk mengonfigurasi agen perlindungan di macOS

1. Pada mesin dengan agent, hentikan Managed Machine Service (MMS):
   a. Buka **Aplikasi** > **Utilitas** > **Terminal**
   b. Jalankan perintah berikut:

```
sudo launchctl stop acronis_mms
```

2. Buka file **/Library/Application Support/Acronis/Registry/BackupAndRecovery.config** untuk mengedit.
3. Arahkan ke kunci **CurlOptions** dan atur nilai untuk **VerifyPeer** ke **0**. Pastikan nilai untuk **VerifyHost** juga diatur ke **0**.
4. Simpan editan Anda.
5. Mulai Managed Machine Service (MMS), dengan menjalankan perintah berikut di Terminal:

```
sudo launchctl starts acronis_mms
```

Menggunakan sertifikat yang diterbitkan oleh otoritas sertifikat tepercaya

Untuk mengonfigurasi pengaturan sertifikat SSL

1. Pastikan Anda memiliki semua syarat berikut ini:

Jika Anda menggunakan sertifikat dan file kunci	Jika Anda menggunakan file PFX
File sertifikat (dalam format .pem)	File PFX
File dengan kunci pribadi untuk sertifikat (biasanya dalam format .key)	
Kata sandi kunci pribadi (jika kunci tersebut dilindungi dengan kata sandi)	Kata sandi untuk file PFX, jika file dilindungi kata sandi

2. Salin file ke mesin yang menjalankan server manajemen.
3. Pada mesin ini, buka file konfigurasi berikut dengan editor teks:
   - Di Windows: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - Di Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`
4. Temukan bagian berikut:

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
```

5. Di antara tanda kutip di baris `"cert_file"`, tentukan jalur lengkap ke file sertifikat atau file PFX.
   Contoh:

Sistem operasi	Jika Anda menggunakan sertifikat dan pasangan kunci	Jika Anda menggunakan file .pfx
Windows (perhatikan garis miring)	`"cert_file": "C:/certificate/local-domain.ams.pem"`	`"cert_file": "C:/certificate/local-domain.ams.pfx"`
Linux	`"cert_file": "/home/user/local-domain.ams.pem"`	`"cert_file": "/home/user/local-domain.ams.pfx"`

6. Di antara tanda kutip di baris `"key_file"`, tentukan jalur lengkap ke file kunci pribadi atau file PFX yang berisi kunci sertifikat.
   Biasanya, file PFX mencakup sertifikat dan kuncinya. Dalam hal ini, di baris `"key_file"`, tentukan jalur yang sama seperti langkah sebelumnya.
   Contoh:

Sistem operasi	Jika Anda menggunakan sertifikat dan pasangan kunci	Jika Anda menggunakan file .pfx
Windows (perhatikan garis miring)	`"key_file": "C:/certificate/private.key"`	`"cert_file": "C:/certificate/local-domain.ams.pfx"`
Linux	`"key_file": "/home/user/private.key"`	`"cert_file": "/home/user/local-domain.ams.pfx"`

7. [Opsional] Jika kunci pribadi atau file PFX dilindungi kata sandi, di antara tanda kutip di baris `"passphrase"`, tentukan kata sandi.
   Misalnya: `"passphrase": "my password"`

   Catatan
   Jika baris `"passphrase": ""`, tidak ada di file konfigurasi `api_gateway.json`, tambahkan secara manual.
   Misalnya:

   ```
   "tls": {
       "cert_file": "cert.pem",
       "key_file": "key.pem",
       "passphrase": "my password",
   }
   ```

8. Simpan file `api_gateway.json`.

   Penting
   Berhati-hatilah dan jangan sampai menghapus tanda koma, tanda kurung, dan tanda kutip dalam file konfigurasi.

9. Mulai ulang Layanan Acronis Service Manager seperti yang dijelaskan di bawah ini.

Untuk memulai ulang Layanan Acronis Service Manager

Di Windows

1. Pada menu **Start**, klik **Run**, lalu ketik: **cmd**
2. Klik **OK**.
3. Jalankan perintah berikut:

   ```
   net stop asm
   net start asm
   ```

Di Linux

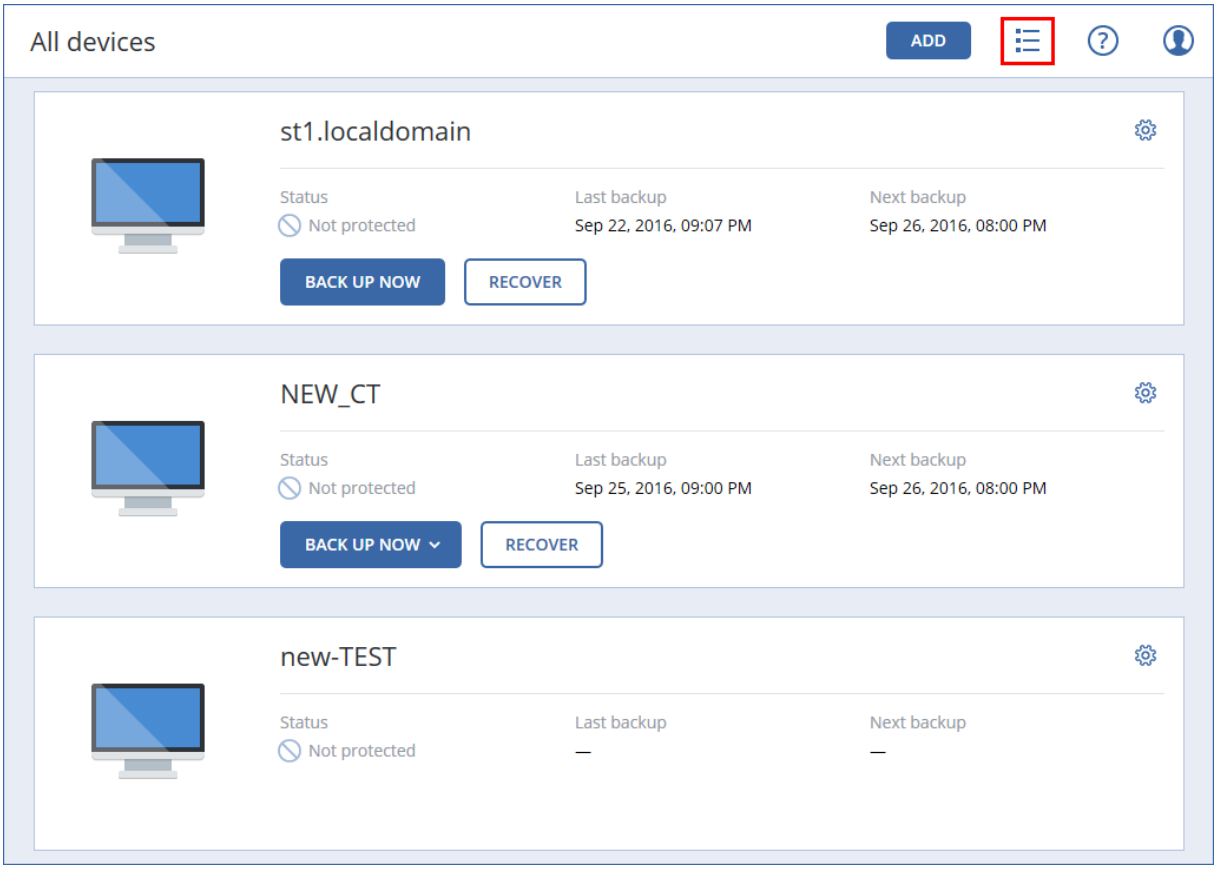
1. **Terminal** Terbuka.
2. Jalankan perintah berikut di direktori mana pun:

```
sudo service acronis_asm restart
```

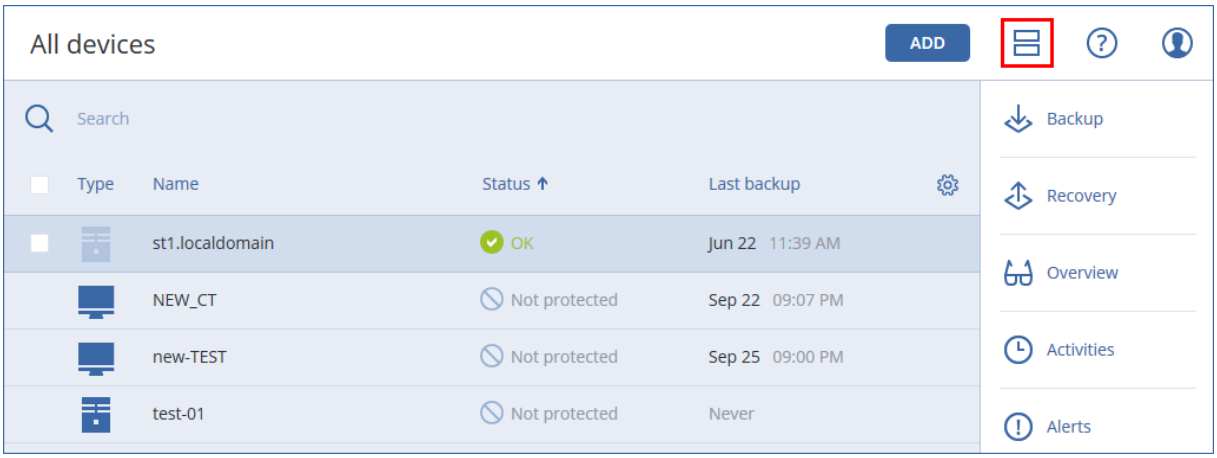
Tampilan konsol web Cyber Protect

Konsol web Cyber Protect memiliki dua tampilan: tampilan sederhana dan tampilan tabel. Untuk beralih antar tampilan, klik ikon yang sesuai di sudut kanan atas.

Tampilan sederhana mendukung mesin dalam jumlah sedikit.



Tampilan tabel diaktifkan secara otomatis jika jumlah mesin menjadi lebih banyak.



Kedua tampilan tersebut memberikan akses ke fitur dan operasi yang sama. Dokumen ini menjelaskan akses ke operasi dari tampilan tabel.

Saat mesin online atau offline, diperlukan beberapa waktu untuk mengubah statusnya di Cyber Protect konsol web.

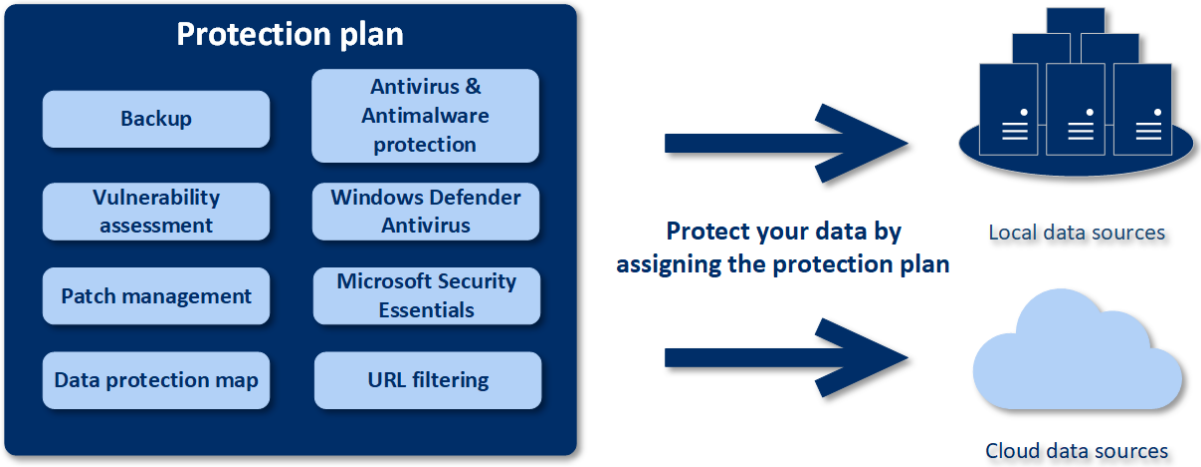
Status mesin diperiksa setiap menit. Jika agen yang diinstal pada mesin ini tidak mentransfer data dan tidak ada jawaban selama lima pemeriksaan berturut-turut, mesin akan ditampilkan sebagai offline. Mesin ditampilkan sebagai kembali online saat menjawab pemeriksaan status atau mulai mentransfer data.

Rencana proteksi dan modul

Rencana proteksi adalah rencana yang menggabungkan beberapa modul perlindungan data termasuk

- Pencadangan – memungkinkan Anda untuk mencadangkan sumber data Anda ke penyimpanan lokal atau awan.
- Perlindungan Antivirus & Antimalware – memungkinkan Anda untuk memeriksa mesin Anda dengan solusi antimalware bawaan.
- Pemfilteran URL – memungkinkan Anda untuk melindungi mesin dari ancaman dari internet dengan memblokir akses ke URL dan konten berbahaya yang akan diunduh.
- Windows Defender Antivirus – memungkinkan Anda untuk mengelola pengaturan Windows Defender Antivirus guna melindungi lingkungan Anda.
- Microsoft Security Essentials – memungkinkan Anda untuk mengelola pengaturan Microsoft Security Essentials guna melindungi lingkungan Anda.
- Penilaian kerentanan – secara otomatis memeriksa kerentanan pada produk Microsoft dan produk pihak ketiga yang diinstal di mesin Anda dan mengeluarkan pemberitahuan tentang hal tersebut.
- Manajemen patch – memungkinkan Anda untuk menginstal patch dan pembaruan untuk produk Microsoft dan produk pihak ketiga pada mesin Anda guna menutup kerentanan yang ditemukan.
- Peta perlindungan data – memungkinkan Anda untuk menemukan data guna memantau status proteksi file-file penting.

Rencana proteksi memungkinkan Anda untuk melindungi sumber data Anda sepenuhnya dari ancaman internal dan eksternal. Dengan mengaktifkan dan menonaktifkan modul yang berbeda-beda dan menetapkan pengaturan modul, Anda dapat membuat rencana yang fleksibel untuk memenuhi berbagai kebutuhan bisnis.



Membuat rencana proteksi

Rencana proteksi dapat diterapkan pada beberapa mesin pada saat pembuatannya, atau di lain waktu. Saat Anda membuat rencana, sistem memeriksa jenis sistem operasi dan perangkat (contohnya, stasiun kerja, mesin virtual, dll.) dan hanya menunjukkan modul rencana yang berlaku bagi perangkat Anda.

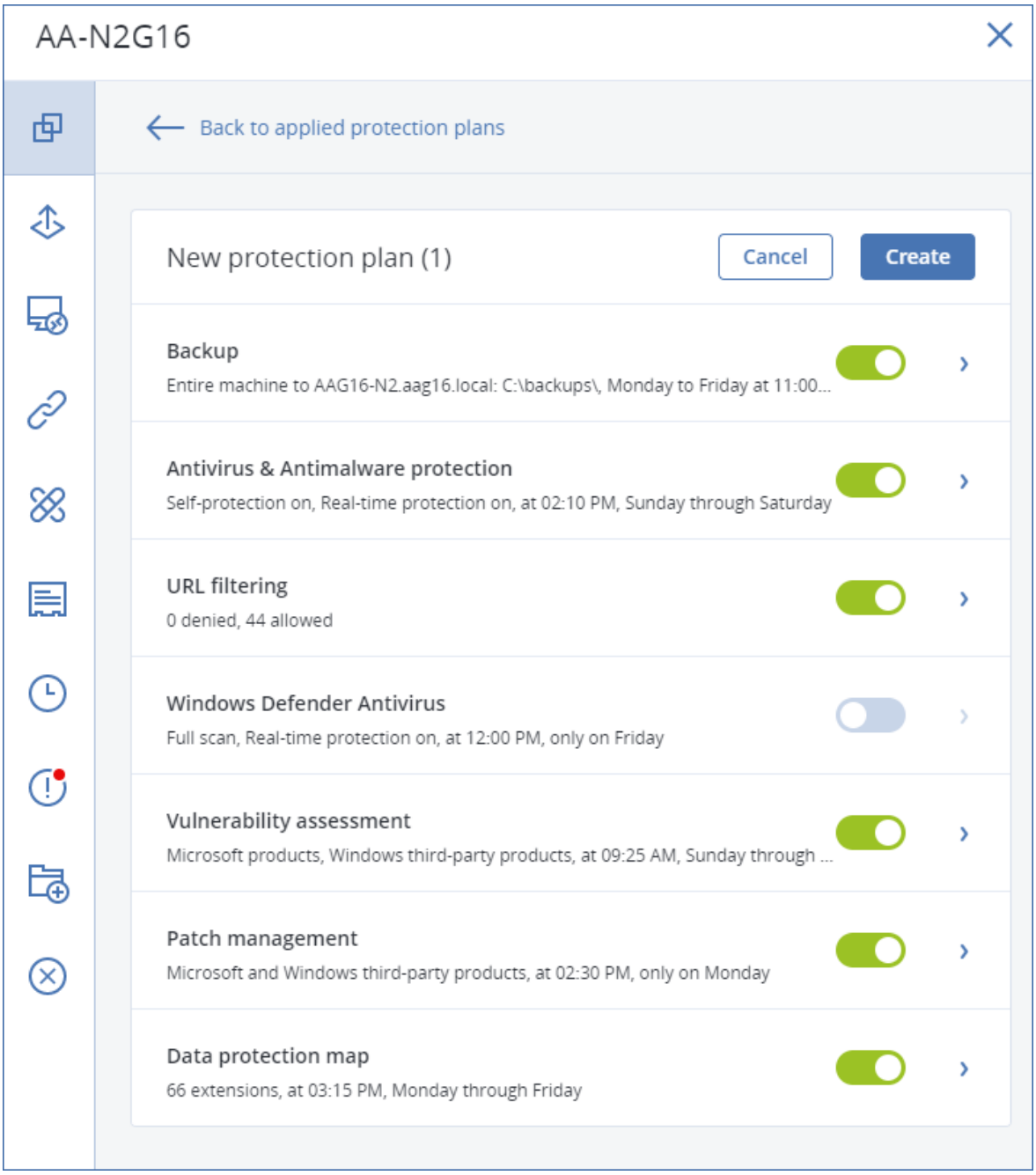
Rencana proteksi dapat dibuat dengan dua cara:

- Di bagian **Perangkat** – jika Anda memilih perangkat atau beberapa perangkat untuk dilindungi lalu membuat rencana untuk perangkat tersebut.
- Di bagian **Rencana** – jika Anda membuat rencana lalu memilih mesin tempat diterapkannya rencana.

Pertimbangkanlah cara pertama.

Untuk membuat rencana proteksi pertama

1. Di konsol web Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih mesin yang ingin Anda lindungi.
3. Klik **Lindungi**, lalu klik **Buat rencana**. Anda akan melihat rencana proteksi dengan pengaturan default.



4. [Opsional] Untuk memodifikasi nama rencana proteksi, klik ikon pensil di samping nama.
5. [Opsional] Untuk mengaktifkan atau menonaktifkan modul rencana proteksi, klik switch di sebelah nama modul.
6. [Opsional] Untuk mengonfigurasi parameter modul, klik bagian yang sesuai pada bagian rencana proteksi.
7. Ketika sudah siap, klik **Buat**.

Modul Pencadangan, Perlindungan Antivirus & Antimalware, Penilaian kerentanan, Manajemen patch, dan Peta perlindungan data dapat dijalankan sesuai permintaan dengan mengeklik **Jalankan sekarang**.

Menyelesaikan pertentangan rencana

Rencana proteksi dapat berada dalam status berikut:

- **Aktif** – rencana yang ditetapkan untuk perangkat dan dieksekusi di perangkat tersebut.
- **Tidak aktif** – rencana yang ditetapkan untuk perangkat tapi dinonaktifkan dan tidak dieksekusi di perangkat tersebut.

Menerapkan beberapa rencana proteksi pada perangkat

Anda dapat menerapkan beberapa rencana proteksi pada suatu perangkat. Hasilnya, Anda akan mendapat kombinasi beberapa rencana proteksi yang ditetapkan untuk suatu perangkat. Misalnya, Anda mungkin menerapkan rencana yang hanya mengaktifkan modul perlindungan Antivirus & Antimalware, dan rencana lain yang hanya berisi modul Cadangan. Rencana-rencana proteksi dapat digabungkan hanya jika kesemuanya tidak memiliki modul yang berpotongan. Jika modul yang sama diaktifkan di lebih dari satu rencana proteksi, Anda harus menyelesaikan pertentangan di antara rencana proteksi.

Menyelesaikan pertentangan rencana

Pertentangan rencana dengan rencana yang sudah diterapkan

Jika Anda membuat rencana baru di perangkat atau beberapa perangkat dengan rencana yang sudah diinstal yang bertentangan dengan rencana baru, Anda dapat menyelesaikan pertentangan dengan salah satu cara berikut:

- Buat rencana baru, terapkan, dan nonaktifkan semua rencana bertentangan yang sudah diterapkan.
- Buat rencana baru dan nonaktifkan rencana tersebut.

Jika Anda mengedit rencana pada perangkat atau beberapa perangkat dengan rencana yang sudah diinstal yang bertentangan dengan perubahan yang diterapkan, Anda dapat menyelesaikan pertentangan dengan salah satu cara berikut:

- Simpan perubahan pada rencana dan menonaktifkan semua rencana bertentangan yang sudah diterapkan.
- Simpan perubahan pada rencana dan nonaktifkan rencana.

Rencana perangkat bertentangan dengan rencana grup

Jika perangkat disertakan dalam grup perangkat dengan rencana grup yang sudah ditetapkan, Anda dapat mencoba menetapkan rencana baru ke perangkat, lalu sistem akan meminta Anda untuk menyelesaikan konflik dengan melakukan salah satu hal berikut:

- Hapus perangkat dari grup dan tetapkan rencana baru untuk perangkat.
- Terapkan rencana baru pada keseluruhan grup atau edit rencana grup terkini.

Masalah lisensi

Kuota yang ditetapkan pada perangkat harus sesuai untuk rencana proteksi yang akan dijalankan, diperbarui, atau diterapkan. Untuk menyelesaikan masalah lisensi, lakukan salah satu hal berikut:

- Nonaktifkan modul yang tidak didukung oleh kuota yang ditetapkan dan lanjutkan menggunakan rencana proteksi.
- Mengubah secara manual kuota yang ditetapkan: buka **Perangkat** > **<Perangkat tertentu>** > **Detail** > **Layanan kuota**. Kemudian, batalkan kuota yang ada dan tetapkan kuota baru.

Operasi dengan rencana proteksi

Untuk informasi tentang cara membuat rencana proteksi, lihat "Membuat rencana proteksi".

Tindakan yang tersedia dengan rencana proteksi

Anda dapat melakukan tindakan berikut dengan rencana proteksi:

- Ganti nama rencana
- Aktifkan/nonaktifkan modul dan edit setiap pengaturan modul
- Aktifkan/nonaktifkan rencana

  Rencana yang dinonaktifkan tidak akan dijalankan pada perangkat tempatnya diterapkan.

  Tindakan ini memudahkan administrator yang nantinya ingin melindungi perangkat yang sama dengan rencana yang sama. Rencananya tidak dicabut dari perangkat dan untuk memulihkan perlindungannya, administrator hanya perlu mengaktifkannya kembali.
- Terapkan rencana pada perangkat atau sekumpulan perangkat
- Batalkan rencana dari perangkat

  Rencana yang dibatalkan tidak lagi diterapkan ke perangkat.

  Tindakan ini memudahkan administrator yang tidak perlu segera melindungi perangkat yang sama dengan rencana yang sama lagi. Untuk memulihkan perlindungan rencana yang dibatalkan, administrator harus mengetahui nama rencana ini, memilihnya dari daftar rencana yang tersedia, lalu menerapkannya kembali ke perangkat yang diinginkan.
- Impor/ekspor rencana

  Catatan
  Anda hanya dapat mengimpor rencana proteksi yang dibuat di Acronis Cyber Protect 15. Rencana proteksi yang dibuat di versi produk sebelumnya tidak kompatibel dengan Acronis Cyber Protect 15.
- Hapus rencana

Untuk menerapkan rencana proteksi yang sudah ada

1. Pilih mesin yang ingin Anda lindungi.
2. Klik **Lindungi**. Jika rencana proteksi sudah diterapkan pada mesin yang dipilih, klik **Tambah rencana**.
3. Perangkat lunak menampilkan rencana proteksi yang telah dibuat sebelumnya.
4. Pilih proteksi yang Anda butuhkan, kemudian klik **Terapkan**.

Untuk mengedit rencana proteksi

1. Jika Anda ingin mengedit rencana proteksi untuk semua mesin yang padanya rencana diterapkan, pilih salah satu dari mesin ini. Atau, pilih mesin yang rencana proteksinya ingin Anda edit.
2. Klik **Lindungi**.
3. Pilih rencana proteksi yang ingin Anda edit.
4. Klik ikon elipsis di samping nama rencana proteksi, lalu klik **Edit**.
5. Untuk memodifikasi parameter rencana, klik bagian yang sesuai pada panel rencana proteksi.
6. Klik **Simpan perubahan**.
7. Untuk mengubah rencana proteksi bagi semua mesin yang untuknya rencana diterapkan, klik **Terapkan perubahan ke rencana proteksi ini**. Atau, klik **Buat rencana proteksi tambahan untuk mesin perangkat**.

Untuk mencabut rencana proteksi dari mesin

1. Pilih mesin yang ingin Anda cabut rencana proteksinya.
2. Klik **Lindungi**.
3. Jika beberapa rencana proteksi diterapkan pada mesin, pilih rencana proteksi yang ingin Anda cabut.
4. Klik ikon elipsis di samping nama rencana proteksi, lalu klik **Cabut**.

Untuk menghapus rencana proteksi

1. Pilih mesin mana pun yang menerapkan rencana proteksi yang ingin Anda hapus.
2. Klik **Lindungi**.
3. Jika beberapa rencana proteksi diterapkan pada mesin, pilih rencana proteksi yang ingin Anda hapus.
4. Klik ikon elipsis di samping nama rencana proteksi, lalu klik **Hapus**.
   Hasilnya, rencana proteksi akan dicabut dari semua mesin dan dihapus sepenuhnya dari antarmuka web.

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.

Catatan
Pada penyebaran lokal, apabila hanya lisensi Standar yang ada di server manajemen, rencana proteksi tidak dapat diterapkan pada beberapa mesin fisik. Setiap mesin fisik harus memiliki rencana proteksi sendiri.

Untuk membuat rencana proteksi pertama dengan modul Pencadangan yang diaktifkan

1. Pilih mesin yang ingin Anda cadangkan.
2. Klik **Lindungi**.

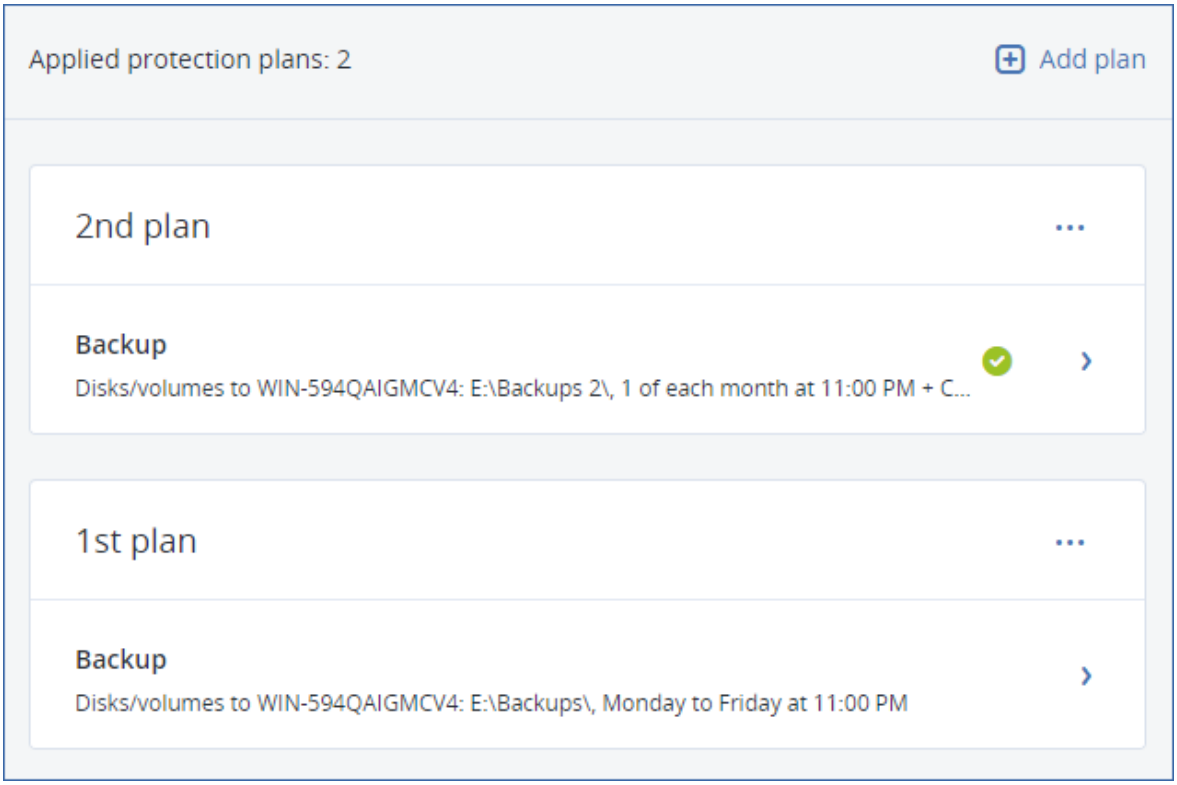
   Perangkat lunak menampilkan rencana proteksi yang diterapkan pada mesin. Jika mesin tidak memiliki rencana yang sudah ditetapkan padanya, Anda akan melihat rencana proteksi default yang dapat diterapkan. Anda dapat menyesuaikan pengaturan bila diperlukan dan menerapkan

rencana ini atau membuat rencana baru.

3. Untuk membuat rencana baru, klik **Buat rencana**. Aktifkan modul **Cadangan** dan buka Pengaturan.
4. [Opsional] Untuk mengubah nama rencana proteksi, klik nama default.
5. [Opsional] Untuk memodifikasi parameter modul Cadangan, klik bagian 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.



3. Pilih rencana proteksi untuk diterapkan.
4. Klik **Terapkan**.

Referensi cepat modul cadangan

Penting
Beberapa fitur yang dijelaskan dalam bagian ini hanya tersedia untuk penyebaran lokal.

Tabel berikut merangkum parameter modul Cadangan 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 (bukan untuk Awan)	BERAPA LAMA AKAN DISIMPAN

Disk/volume (mesin fisik)	Pemilihan langsung Aturan kebijakan Filter file	Awan Folder lokal Folder jaringan Server SFTP* NFS* Secure Zone* Lokasi yang dikelola* Perangkat pita*	Selalu inkremental (File tunggal)* Selalu penuh Mingguan penuh, kenaikan Harian Penuh bulanan, Diferensial mingguan, Inkremental harian (GFS) Kustom (F-D-I)	Berdasarkan umur cadangan (aturan tunggal/per set cadangan) Berdasarkan jumlah cadangan Berdasarkan ukuran total cadangan* Simpan tanpa batas waktu
Disk/volume (mesin virtual)	Aturan kebijakan Filter file	Awan Folder lokal Folder jaringan Server SFTP* NFS* Lokasi yang dikelola* Perangkat pita*		
File (hanya mesin fisik)	Pemilihan langsung Aturan kebijakan Filter file	Awan Folder lokal Folder jaringan Server SFTP* NFS* Secure Zone* Lokasi yang dikelola* Perangkat pita	Selalu penuh Mingguan penuh, kenaikan Harian Penuh bulanan, Diferensial mingguan, Inkremental harian (GFS) Selalu inkremental (File tunggal)* Kustom (F-D-I)	
Konfigurasi ESXi	Pemilihan langsung	Folder lokal Folder jaringan Server SFTP NFS*		
Status sistem (hanya untuk penyebaran awan)	Pemilihan langsung	Awan Folder lokal Folder jaringan	Selalu penuh Mingguan penuh, kenaikan	

Database SQL	Pemilihan langsung	Awan Folder lokal Folder jaringan Lokasi yang dikelola* Perangkat pita	Harian Kustom (F-I)	
Basis data Exchange	Pemilihan langsung			
Kotak surat Exchange	Pemilihan langsung	Awan Folder lokal Folder jaringan Lokasi yang dikelola*	Selalu inkremental (file tunggal)	Berdasarkan umur cadangan (aturan tunggal/per set cadangan) Berdasarkan jumlah cadangan Simpan tanpa batas waktu
Kotak surat Microsoft 365	Pemilihan langsung			

* Lihat batasan di bawah ini.

Pembatasan

Server SFTP dan perangkat pita

- Lokasi ini tidak dapat menjadi tujuan untuk pencadangan mesin yang menjalankan macOS.
- Lokasi ini tidak dapat dijadikan tujuan untuk pencadangan keberadaan aplikasi
- Skema pencadangan **Selalu inkremental (file tunggal** tidak tersedia saat mencadangkan ke lokasi tersebut.
- Aturan retensi **Berdasarkan ukuran total cadangan** tidak tersedia untuk lokasi tersebut.

NFS

- Pencadangan ke NFS tidak tersedia di Windows.
- Skema pencadangan **Selalu inkremental (file tunggal)** untuk File (mesin fisik) tidak tersedia saat mencadangkan ke bagian NFS.

Secure Zone

- Secure Zone tidak dapat dibuat di Mac.

Lokasi yang dikelola

- Lokasi yang dikelola dengan deduplikasi atau enkripsi yang diaktifkan tidak dapat dipilih sebagai tujuan:
  - Jika skema pencadangan diatur ke **Selalu inkremental (file tunggal)**
  - Jika format pencadangan diatur ke **Versi 12**
  - Untuk pencadangan level disk mesin yang menjalankan macOS
  - Untuk cadangan kotak surat Exchange dan kotak surat Microsoft 365.
- Aturan retensi **Berdasarkan ukuran total cadangan** tidak tersedia untuk lokasi yang dikelola dengan deduplikasi yang diaktifkan.

Selalu inkremental (file tunggal)

- Skema pencadangan **Selalu inkremental (file tunggal)** tidak tersedia ketika mencadangkan ke server SFTP atau perangkat pita.
- Skema pencadangan **Selalu inkremental (file tunggal)** untuk File (mesin fisik) hanya tersedia saat lokasi cadangan primer adalah Acronis Cloud.

Berdasarkan ukuran total cadangan

- Aturan retensi **Berdasarkan ukuran total cadangan** tidak tersedia:
  - Jika skema pencadangan diatur ke **Selalu inkremental (file tunggal)**
  - Saat mencadangkan ke server SFTP, perangkat pita, atau lokasi yang dikelola dengan deduplikasi yang diaktifkan.

Memilih data yang akan dicadangkan

Memilih keseluruhan mesin

Cadangan keseluruhan mesin berarti cadangan dari semua disk-nya yang tidak dapat dilepas.

Untuk mengonfigurasi cadangan tersebut, di **Apa yang akan dicadangkan**, pilih **Seluruh mesin**.

Penting
Drive eksternal, seperti drive flash USB atau hard drive USB, tidak disertakan dalam cadangan **Seluruh mesin**. Untuk mencadangkan drive ini, konfigurasikan cadangan **Disk/volume**. Untuk informasi lebih lanjut tentang cadangan disk, lihat "Memilih disk/volume" (hlm. 213).

Memilih disk/volume

Cadangan tingkat disk berisi salinan disk atau volume dalam bentuk paket. Anda dapat memulihkan disk, volume, atau file individual dari cadangan tingkat disk. Cadangan keseluruhan mesin berarti cadangan dari semua disk-nya yang tidak dapat dilepas.

Catatan
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 di arsip.

Ada dua cara untuk memilih disk/volume: langsung pada setiap mesin atau menggunakan aturan kebijakan. Anda dapat mengecualikan file dari cadangan disk dengan mengatur filter file.

Pemilihan langsung

Pemilihan langsung hanya tersedia untuk mesin fisik. Untuk mengaktifkan pilihan langsung disk dan volume pada mesin virtual, Anda harus menginstal agen perlindungan dalam sistem operasi tamunya.

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 mesin yang termasuk dalam rencana proteksi, pilih kotak centang di sebelah disk atau volume yang akan dicadangkan.
5. Klik **Selesai**.

Gunakan 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.

   Aturan kebijakan akan diterapkan pada semua mesin yang termasuk dalam rencana proteksi. Jika tidak ada data yang memenuhi setidaknya satu aturan ditemukan pada mesin saat

pencadangan dimulai, pencadangan pada mesin akan gagal.

5. Klik **Selesai**.

Aturan untuk Windows, Linux, dan macOS

- `[Semua volume]` memilih semua volume pada mesin yang menjalankan Windows dan semua volume terpasang pada mesin yang menjalankan Linux atau macOS.

Aturan untuk Windows

- Huruf drive (misalnya **C:**) memilih volume dengan huruf drive yang ditentukan.
- `[Volume Tetap (mesin fisik)]` memilih semua volume mesin fisik, selain media yang dapat dilepas. Volume tetap mencakup volume pada perangkat SCSI, ATAPI, ATA, SSA, SAS, dan SATA, dan pada array RAID.
- `[BOOT+SYSTEM]` memilih boot dan volume sistem. Kombinasi ini adalah set data minimal yang memastikan pemulihan sistem operasi dari cadangan.
- `[BOOT+SYSTEM DISK (mesin fisik)]` memilih semua volume disk di tempat boot dan volume sistem berada. Jika booting dan volume sistem tidak berada di disk yang sama, tidak ada yang akan dipilih. Ketentuan ini berlaku hanya untuk mesin fisik.
- `[Disk 1]` memilih disk pertama mesin, termasuk semua volume pada disk tersebut. Untuk memilih disk lain, ketik nomor yang sesuai.

Aturan untuk Linux

- `/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.

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, masukkan:

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

Aturan untuk macOS

- `[Disk 1]` Memilih disk pertama mesin, termasuk semua volume pada disk tersebut. Untuk memilih disk lain, ketik nomor yang sesuai.

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 7, Titik Pengembalian Windows tidak dicadangkan.
  - Jika opsi pencadangan **Layanan Volume Shadow Copy (VSS)** diaktifkan, file dan folder yang ditentukan dalam kunci registri **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**.

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.

Memilih file/folder

Pencadangan tingkat file tersedia untuk mesin fisik dan mesin virtual yang dicadangkan oleh agen yang terinstal di sistem tamu.

Pencadangan tingkat file tidak cukup untuk memulihkan sistem operasi. Pilih cadangan file jika Anda berencana hanya melindungi data tertentu (misalnya, proyek saat ini). Cara ini akan mengurangi ukuran cadangan, sehingga menghemat ruang penyimpanan.

Catatan
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 di arsip.

Ada dua cara untuk memilih file: langsung pada setiap mesin atau menggunakan aturan kebijakan. Metode apa pun memungkinkan Anda untuk lebih menyempurnakan pemilihan dengan mengatur filter file.

Pemilihan langsung

1. Di **Apa yang akan dicadangkan**, pilih **File/folder**.
2. Klik **Item untuk dicadangkan**.
3. Di **Pilih item untuk dicadangkan**, pilih **Secara langsung**.
4. Untuk setiap mesin yang termasuk dalam rencana proteksi:
   a. Klik **Pilih file dan folder**.
   b. Klik **Folder lokal** atau **Folder jaringan**.
      Berbagi harus dapat diakses dari mesin yang dipilih.
   c. Jelajahi file/folder yang diperlukan atau masukkan jalur dan klik tombol panah. Jika diminta, tentukan nama pengguna dan kata sandi untuk folder bersama.
      Mencadangkan folder dengan akses anonim tidak didukung.

d. Pilih file/folder yang diperlukan.

e. Klik **Selesai**.

Gunakan aturan kebijakan

1. Di **Apa yang akan dicadangkan**, pilih **File/folder**.
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.

   Aturan kebijakan akan diterapkan pada semua mesin yang termasuk dalam rencana proteksi. Jika tidak ada data yang memenuhi setidaknya satu aturan ditemukan pada mesin saat pencadangan dimulai, pencadangan pada mesin akan gagal.
5. Klik **Selesai**.

Pemilihan aturan untuk Windows

- Jalur lengkap ke file atau folder, misalnya **D:\Work\Text.doc** atau **C:\Windows**.
- Templat:
  - `[Semua File]` memilih semua file pada semua volume mesin.
  - `[Semua Folder Profil]` memilih folder yang berisi semua profil pengguna (biasanya, **C:\Users** atau **C:\Documents and Settings**).
- Variabel lingkungan:
  - `%ALLUSERSPROFILE%` memilih folder yang berisi data umum semua profil pengguna (biasanya, **C:\ProgramData** atau **C:\Documents and Settings\All Users**).
  - `%PROGRAMFILES%` memilih folder File Program (misalnya, **C:\Program Files**).
  - `%WINDIR%` memilih folder yang berisi Windows (misalnya, **C:\Windows**).

  Anda dapat menggunakan variabel lingkungan lain atau kombinasi variabel lingkungan dan teks. Misalnya, untuk memilih folder Java di folder File Program, ketik: **%PROGRAMFILES%\Java**.

Pemilihan aturan untuk Linux

- Jalur lengkap ke file atau direktori. Misalnya, untuk mencadangkan **file.txt** di volume **/dev/hda3** yang di-mount di **/home/usr/docs**, tentukan **/dev/hda3/file.txt** atau **/home/usr/docs/file.txt**.
  - `/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.
- Templat:

- `[Semua Folder Profil]` memilih **/home**. Ini adalah folder yang berisi semua profil pengguna secara default.

Pemilihan aturan untuk macOS

- Jalur lengkap ke file atau direktori.
- Templat:
  - `[Semua Folder Profil]` memilih **/Users**. Ini adalah folder yang berisi semua profil pengguna secara default.

Contoh:

- Untuk mencadangkan **file.txt** di desktop Anda, tentukan **/Users/<username>/Desktop/file.txt**, di mana <username> adalah nama pengguna Anda.
- Untuk mencadangkan direktori asal semua pengguna, tentukan **/Users**.
- Untuk mencadangkan direktori di mana aplikasi diinstal, tentukan **/Applications**.

Memilih status sistem

Pencadangan status sistem tersedia untuk mesin yang menjalankan Windows 7 dan versi lebih baru.

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).
- Ekstensi dan patch diinstal atau ditempel pada host.
- File log.

Prasyarat

- SSH harus diaktifkan di **Security Profile** konfigurasi host ESXi.
- Untuk mencadangkan konfigurasi ESXi, Agen untuk VMware menggunakan koneksi SSH ke host ESXi di Port TCP 22. Pastikan firewall Anda tidak memblokir koneksi ini.
- Anda harus mengetahui kata sandi untuk akun 'root' di host ESXi.

Pembatasan

- Pencadangan konfigurasi ESXi tidak didukung untuk VMware vSphere 7.0.
- 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 **Cadangkan**.
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)

Pencadangan biasanya dilakukan pada interval berkala tapi cukup lama karena alasan performa. Jika sistem tiba-tiba rusak, perubahan data antara pencadangan terakhir dan kegagalan sistem akan hilang.

Fungsi **Perlindungan data berkelanjutan** memungkinkan Anda mencadangkan perubahan pada data yang dipilih antara pencadangan terjadwal secara berkelanjutan:

- Dengan melacak perubahan dalam file/folder yang ditentukan
- Dengan melacak perubahan pada file yang dimodifikasi oleh aplikasi yang ditentukan

Anda dapat memilih file tertentu untuk perlindungan data berkelanjutan dari data yang dipilih untuk cadangan. Sistem akan mencadangkan setiap perubahan pada file-file ini. Anda dapat memulihkan file ini ke waktu perubahan terakhir.

Saat ini, fungsi **Perlindungan data berkelanjutan** didukung oleh sistem operasi berikut:

- Windows 7 dan versi lebih baru
- Windows Server 2008 R2 dan versi lebih baru

Sistem file yang didukung: Hanya NTFS, hanya folder lokal (folder bersama tidak didukung).

Opsi **Perlindungan data berkelanjutan** tidak kompatibel dengan opsi **Cadangan aplikasi**.

Catatan
Fiturnya bervariasi pada setiap edisi. Beberapa fitur yang dijelaskan di dokumentasi ini mungkin tidak tersedia dengan lisensi Anda. Untuk informasi detail mengenai fitur yang disertakan dalam setiap edisi, lihat Perbandingan Edisi Acronis Cyber Protect 15 termasuk Penyebaran awan.

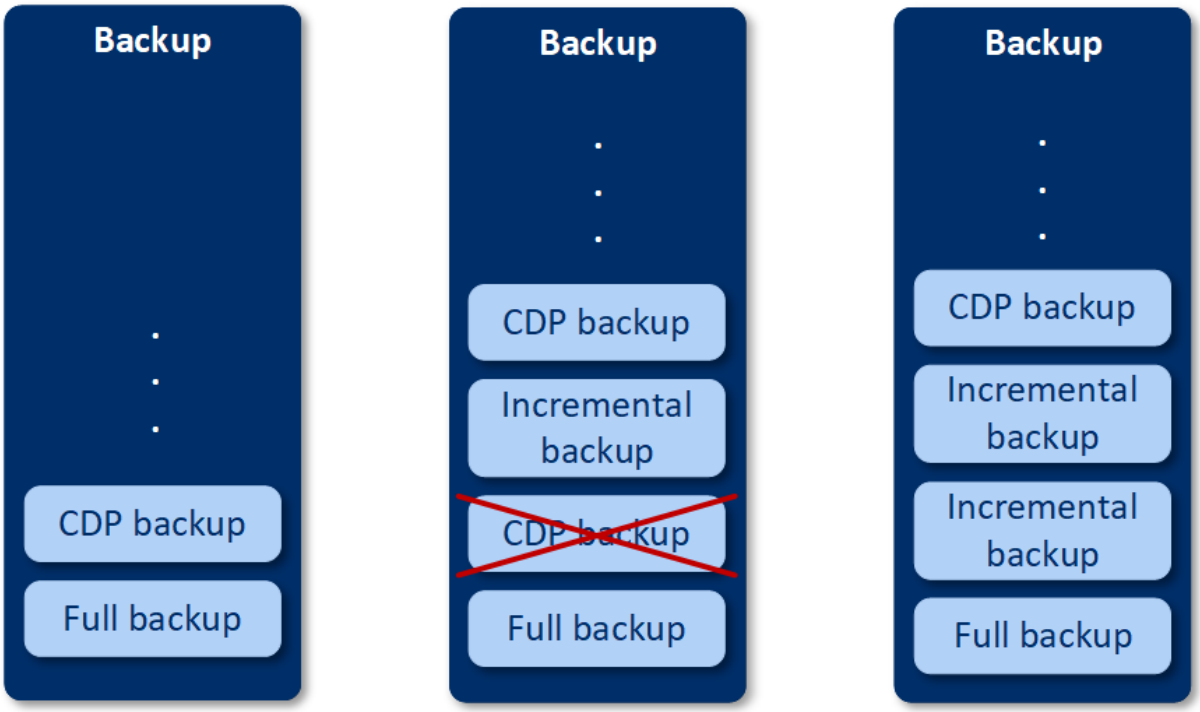
Cara kerjanya

Ambillah cadangan yang dibuat secara berkelanjutan cadangan CDP. Agar cadangan CDP dibuat, cadangan penuh atau cadangan bertahap harus dibuat sebelumnya.

Saat Anda pertama kali menjalankan rencana proteksi dengan modul Cadangan dan **Perlindungan data berkelanjutan** diaktifkan, cadangan penuh dibuat terlebih dahulu. Tepat setelahnya, cadangan CDP untuk file/folder yang dipilih atau diubah akan dibuat. Cadangan CDP selalu berisi data yang Anda pilih dalam kondisi terbaru. Jika Anda menerapkan perubahan pada file/folder yang dipilih, tidak ada cadangan CDP baru yang dibuat, semua perubahan dicatat pada cadangan CDP yang sama.

Jika waktunya tiba untuk pencadangan inkremental terjadwal, cadangan CDP dilepaskan, dan cadangan CDP baru dibuat setelah pencadangan inkremental selesai.

Jadi, cadangan CDP selalu menjadi cadangan terbaru dalam rantai cadangan dengan status aktual terbaru dalam file/folder yang dilindungi.



Jika Anda sudah memiliki rencana proteksi dengan modul Cadangan diaktifkan dan Anda memutuskan untuk mengaktifkan **Perlindungan data berkelanjutan**, cadangan CDP akan dibuat tepat setelah mengaktifkan opsi karena rantai cadangan sudah memiliki cadangan penuh.

Sumber data yang didukung dan tujuan untuk perlindungan data berkelanjutan

Untuk pekerjaan perlindungan data berkelanjutan yang baik, Anda harus menentukan item berikut untuk sumber data berikut:

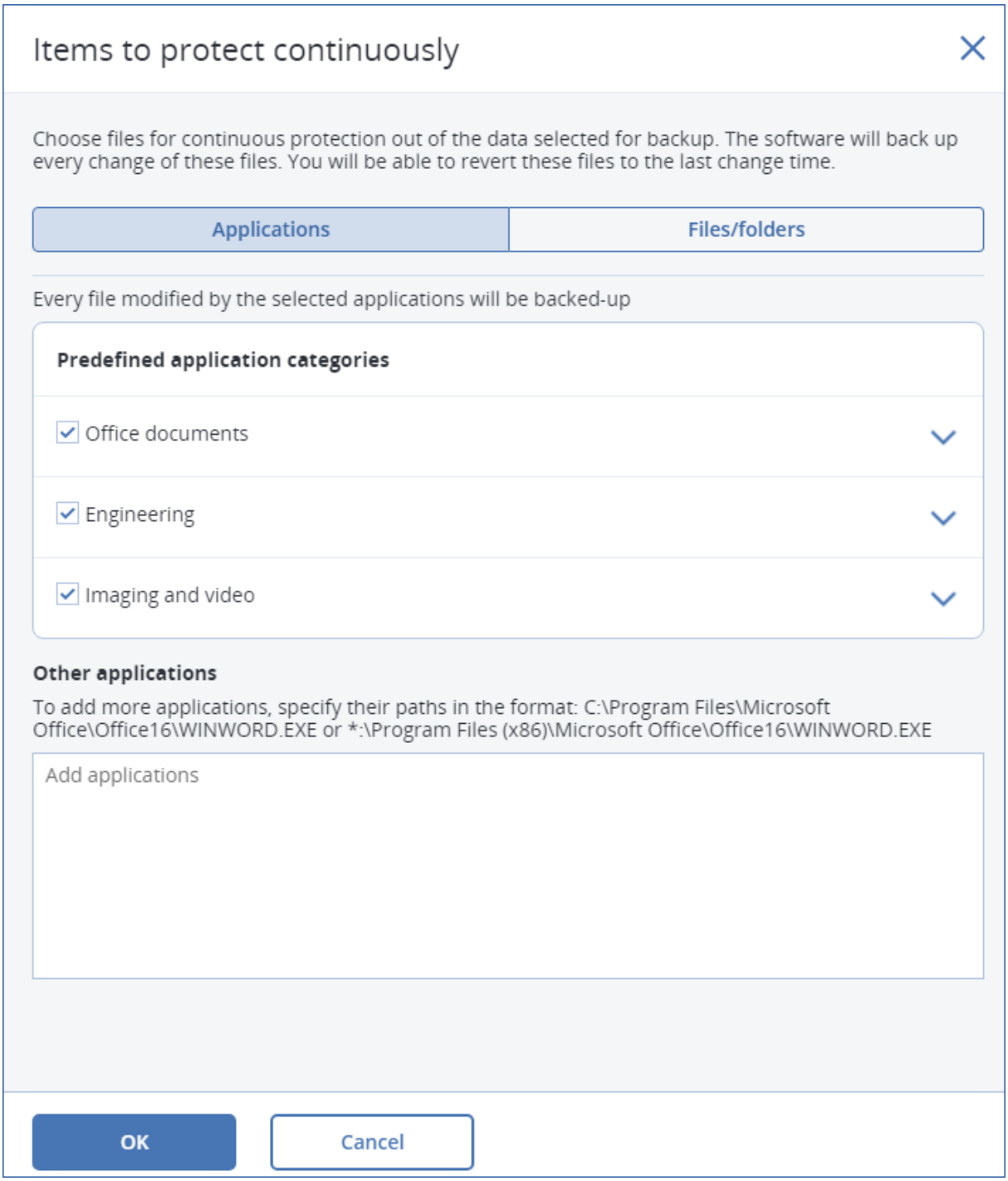
Apa yang harus dicadangkan	Item untuk dicadangkan
Seluruh mesin	File/folder atau aplikasi harus ditentukan
Disk/volume	Disk/volume dan file/folder atau aplikasi harus ditentukan
File/folder	File/folder harus ditentukan Aplikasi dapat ditentukan (tidak wajib)

Tujuan pencadangan berikut didukung untuk perlindungan data berkelanjutan:

- Folder lokal
- Folder jaringan
- Lokasi ditentukan oleh skrip
- Penyimpanan awan
- Acronis Cyber Infrastructure

Untuk melindungi perangkat dengan perlindungan data berkelanjutan

1. Di konsol web Cyber Protect, buat rencana proteksi dengan mengaktifkan modul **Cadangan**.
2. Aktifkan opsi **Perlindungan data berkelanjutan (CDP)**.
3. Tentukan **Item untuk dilindungi secara berkelanjutan**:
   - **Aplikasi** (setiap file yang dimodifikasi oleh aplikasi terpilih akan dicadangkan). Kami menyarankan untuk menggunakan opsi ini guna melindungi dokumen Office Anda dengan cadangan CDP.



- Anda dapat memilih aplikasi dari kategori yang sudah ditetapkan sebelumnya atau tentukan aplikasi lain dengan menetapkan jalur ke file aplikasi yang dapat dieksekusi. Gunakan salah satu format berikut:

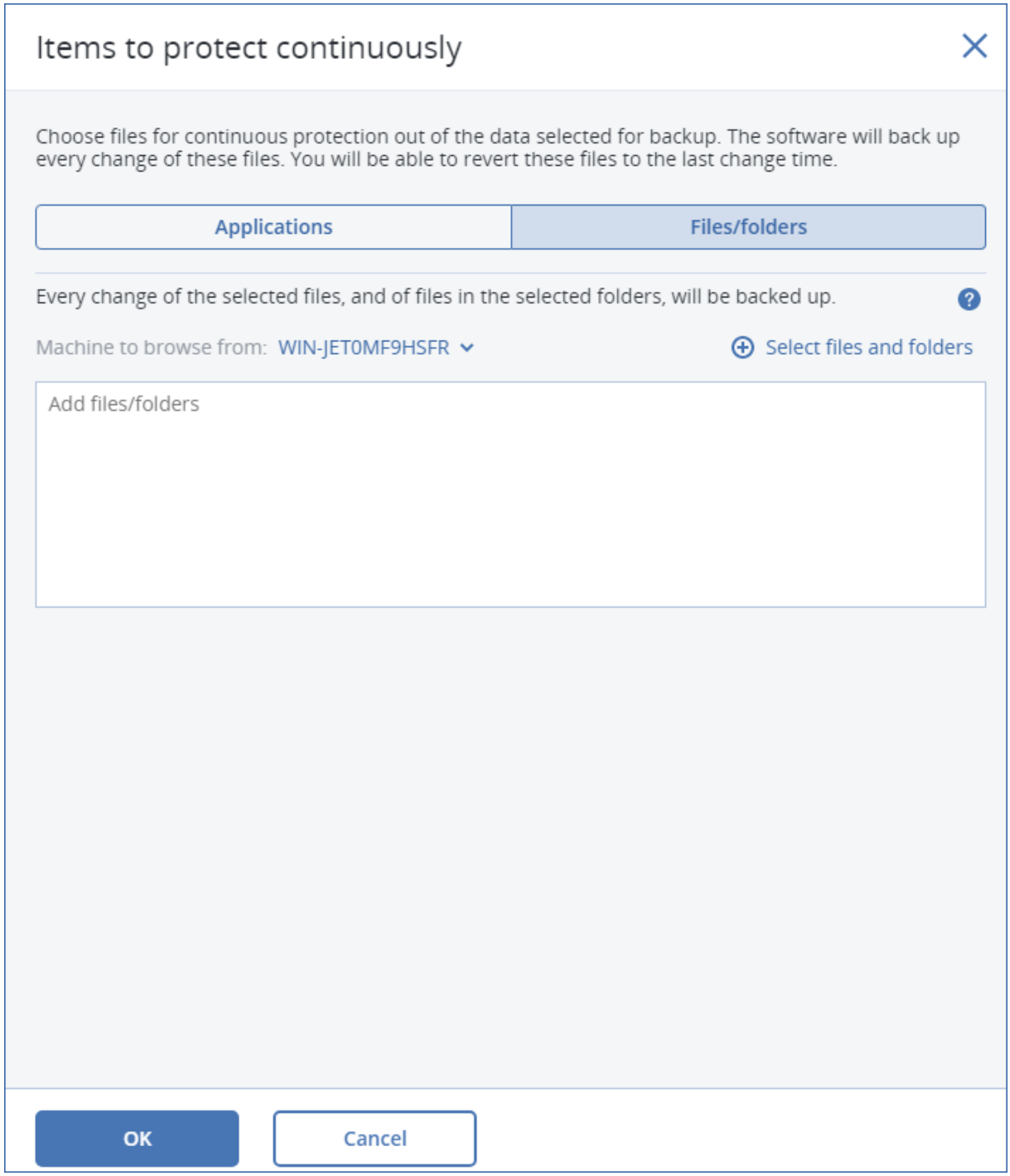
  `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

  OR

  `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

  - **File/folder** (setiap file yang dimodifikasi di lokasi yang ditentukan akan dicadangkan). Kami

merekomendasikan untuk menggunakan opsi ini guna melindungi file dan folder tersebut yang terus berubah.



1. **Mesin untuk menelusuri** – tentukan mesin yang file/foldernya ingin Anda pilih untuk perlindungan data berkelanjutan.

   Klik **Pilih file dan folder** untuk memilih file/folder di mesin yang ditentukan.

Penting
Jika Anda menentukan secara manual seluruh folder yang file-nya akan dicadangkan secara berkelanjutan, gunakanlah mask, misalnya:
Jalur yang benar: D:\Data*
Jalur yang salah: D:\Data\

Di bidang teks, Anda juga dapat menetapkan aturan untuk memilih file/folder yang akan dicadangkan. Untuk keterangan lebih lanjut tentang cara menetapkan aturan, lihat "Memilih file/folder". Ketika sudah siap, klik **Selesai**.

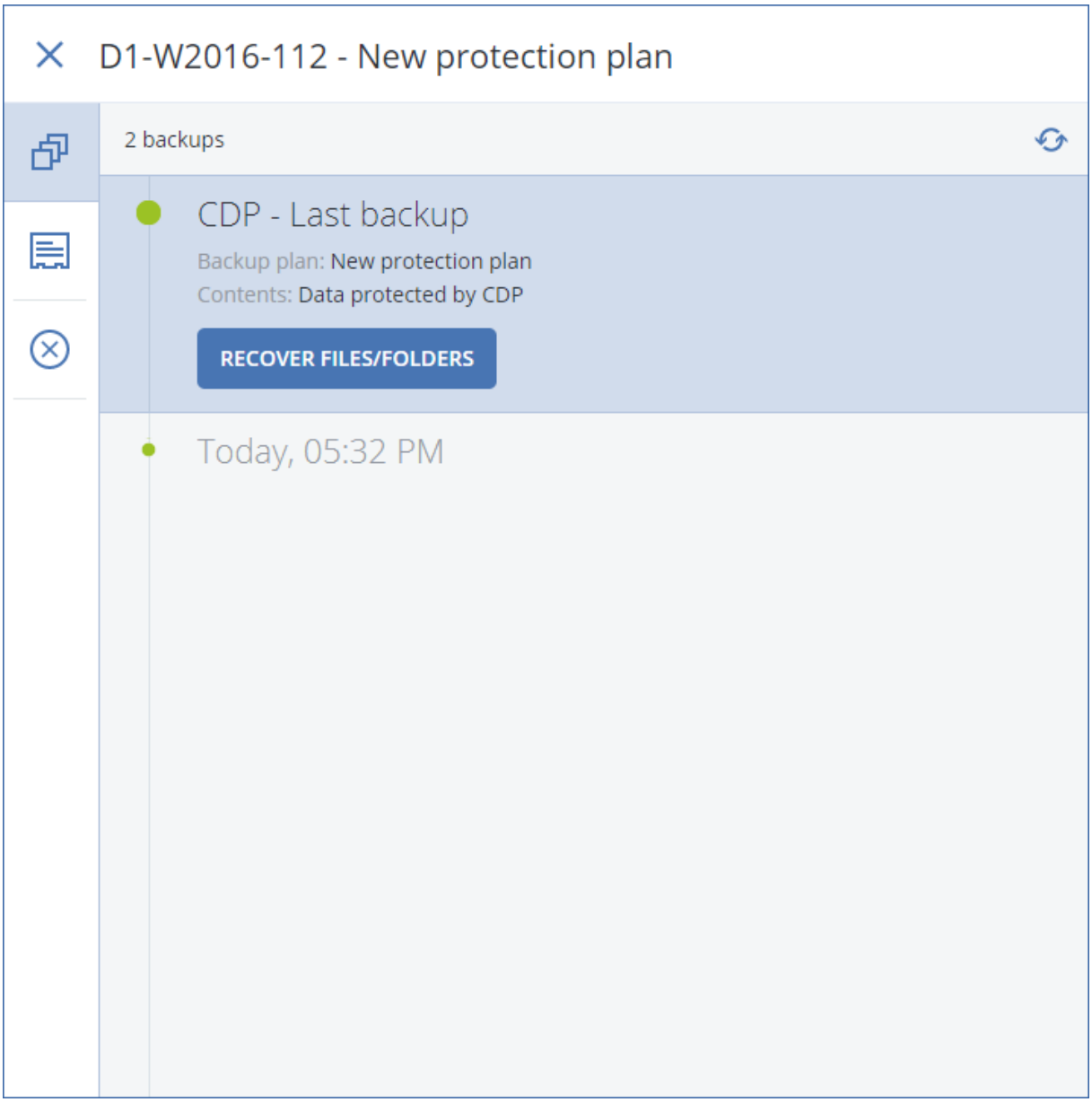
2. Klik **Buat**.

Hasilnya, rencana proteksi dengan perlindungan data berkelanjutan yang diaktifkan akan ditetapkan untuk mesin terpilih. Setelah pencadangan reguler pertama, cadangan dengan salinan terbaru dari data CDP yang dilindungi akan dibuat secara berkelanjutan. Data yang ditetapkan melalui Aplikasi dan File/Folder akan dicadangkan.

Data yang terus-menerus dicadangkan disimpan sesuai dengan kebijakan penyimpanan yang ditentukan untuk modul Cadangan.

Cara membedakan cadangan yang dilindungi secara berkelanjutan

Cadangan yang dicadangkan secara berkelanjutan memiliki prefiks CDP.



Cara memulihkan keseluruhan mesin Anda ke status terbaru

Jika Anda ingin dapat memulihkan seluruh mesin ke status terbaru, Anda dapat menggunakan opsi **Perlindungan data berkelanjutan (CDP)** di modul Cadangan rencana proteksi.

Anda dapat memulihkan keseluruhan mesin atau file/folder dari cadangan CDP. Pada kasus pertama, Anda akan mendapatkan keseluruhan mesin dalam status terbaru, pada kasus kedua – file/folder dalam status terbaru.

Memilih tujuan

Penting
Beberapa fitur yang dijelaskan dalam bagian ini hanya tersedia untuk penyebaran lokal.

Untuk memilih lokasi pencadangan

1. Klik **Tempat menyimpan cadangan**.
2. Lakukan salah satu langkah berikut:
   - Pilih lokasi pencadangan yang sebelumnya digunakan atau sudah ditentukan
   - Klik **Tambah lokasi**, lalu tentukan lokasi pencadangan baru.

Lokasi yang didukung

- **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`

  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.
- **Acronis Infrastruktur Cyber**

  Acronis Infrastruktur Cyber dapat digunakan sebagai penyimpanan yang ditentukan perangkat lunak yang sangat andal dengan redundansi data dan penyembuhan otomatis. Penyimpanan dapat dikonfigurasikan sebagai gateway untuk menyimpan cadangan di Microsoft Azure atau di salah satu dari berbagai solusi penyimpanan yang kompatibel dengan S3 atau Swift. Penyimpanan juga dapat menggunakan NFS back-end. Untuk informasi lebih lanjut, lihat "Tentang Acronis Infrastruktur Cyber".

  Penting
  Pencadangan Acronis Infrastruktur Cyber tidak tersedia untuk mesin macOS.
- **Folder NFS** (tersedia untuk mesin yang menjalankan Linux atau macOS)

  Verifikasi bahwa paket nfs-utils diinstal di mesin Linux tempat 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.

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".

- **SFTP**

  Ketikkan nama atau alamat server SFTP. Notasi berikut didukung:

  `sftp://<server>`

  `sftp://<server>/<folder>`

  Setelah memasukkan nama pengguna dan kata sandi, Anda dapat menjelajahi folder server.

  Di kedua notasi tersebut, Anda juga dapat menentukan port, nama pengguna, dan kata sandi:

  `sftp://<server>:<port>/<folder>`

  `sftp://<nama pengguna>@<server>:<port>/<folder>`

  `sftp://<nama pengguna>:<kata sandi>@<server>:<port>/<folder>`

  Jika nomor port tidak ditentukan, port 22 akan digunakan.

  Pengguna, yang untuknya akses SFTP tanpa kata sandi dikonfigurasikan, tidak dapat mencadangkan ke SFTP.

  Pencadangan ke server FTP tidak didukung.

Opsi penyimpanan lanjutan

- **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:

  - Skrip **JScript** berikut menampilkan lokasi cadangan untuk mesin dalam format `\\bkpsrv\<nama mesin>`:

    ```
    WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject
    ("WScript.Network").ComputerName);
    ```

  - Skrip **JScript** berikut menampilkan lokasi pencadangan dalam folder di mesin tempat skrip dijalankan:

    ```
    WScript.Echo("C:\\Backup");
    ```

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 web Cyber Protect. Selain itu, gunakan huruf besar untuk huruf drive.

- Skrip **VBScript** 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**.

- **Simpul penyimpanan**
  Simpul penyimpanan adalah server yang dirancang untuk mengoptimalkan penggunaan berbagai sumber daya (seperti kapasitas penyimpanan perusahaan, bandwidth jaringan, dan beban CPU server produksi) yang diperlukan untuk melindungi data perusahaan. Tujuan ini dapat dicapai dengan mengatur dan mengelola lokasi yang berfungsi sebagai penyimpanan khusus cadangan perusahaan (lokasi yang dikelola).
  Anda dapat memilih lokasi yang dibuat sebelumnya atau membuat yang baru dengan mengklik **Tambah lokasi** > **Simpul penyimpanan**. Untuk informasi tentang pengaturan, lihat "Menambahkan lokasi yang dikelola".
  Anda mungkin diminta menentukan nama pengguna dan kata sandi untuk simpul penyimpanan. Anggota grup Windows pada mesin di mana simpul penyimpanan diinstal berikut memiliki akses ke semua lokasi yang dikelola pada simpul penyimpanan:
  - **Administrator**
  - **Pengguna Jarak Jauh ASN Acronis**
    Grup ini otomatis dibuat ketika simpul penyimpanan diinstal. Secara default, grup ini kosong. Anda dapat menambahkan pengguna ke grup ini secara manual.
- **Pita**
  Jika perangkat pita terpasang ke mesin atau ke simpul penyimpanan yang dicadangkan, daftar lokasi akan menunjukkan pool pita default. Pool ini dibuat secara otomatis.
  Anda dapat memilih pool standar atau membuat yang baru dengan mengklik **Tambah lokasi** > **Pita**. Untuk informasi tentang pengaturan pool, lihat "Membuat pool".

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).
- 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.

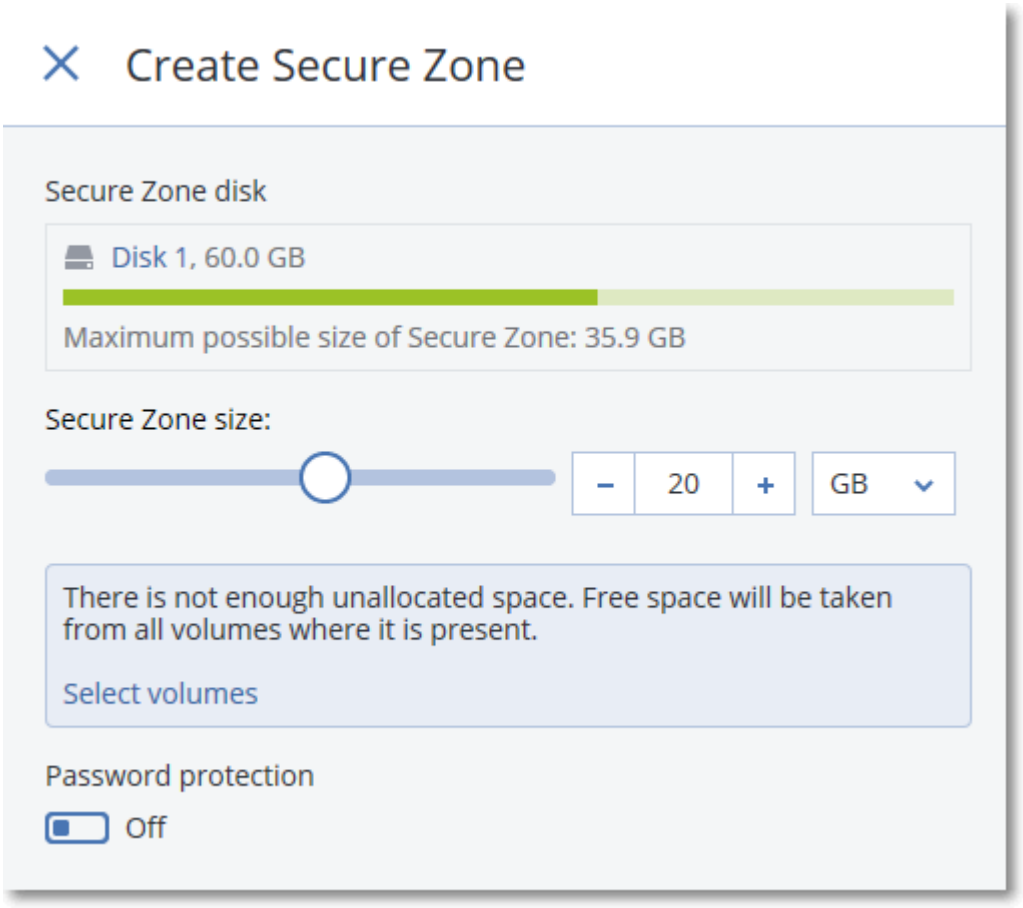
Penting
Memindahkan atau mengubah ukuran volume yang darinya sistem di-boot memerlukan reboot.

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.



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.
   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.

Tentang Acronis Infrastruktur Cyber

Acronis Cyber Protect 15 mendukung integrasi dengan Pembaruan 5 Acronis Infrastruktur Cyber 3.5 atau versi setelahnya.

Pencadangan Acronis Infrastruktur Cyber tidak tersedia untuk mesin macOS.

Penyebaran

Agar dapat menggunakan Acronis Infrastruktur Cyber, sebarkan di bagian logam di lokasi Anda. Setidaknya lima server fisik disarankan agar dapat memaksimalkan produk. Jika Anda hanya memerlukan fungsionalitas gateway, Anda dapat menggunakan satu server fisik atau virtual, atau mengonfigurasi klaster gateway dengan sebanyak mungkin server yang Anda inginkan.

Pastikan pengaturan waktu disinkronkan antara server manajemen dan Acronis Infrastruktur Cyber. Pengaturan waktu untuk Acronis Infrastruktur Cyber dapat dikonfigurasi selama penyebaran. Sinkronisasi waktu melalui Network Time Protocol (NTP) diaktifkan secara default.

Anda dapat menyebarkan beberapa instans Acronis Infrastruktur Cyber dan mendaftarkannya di server manajemen yang sama.

Pendaftaran

Registrasi dilakukan di antarmuka web Acronis Infrastruktur Cyber. Acronis Infrastruktur Cyber hanya dapat didaftarkan oleh administrator organisasi dan hanya di organisasi itu. Setelah didaftarkan, penyimpanan akan tersedia untuk semua unit organisasi. Penyimpanan dapat ditambahkan sebagai lokasi pencadangan ke unit apa pun atau ke organisasi.

Operasi terbalik (deregistrasi) dilakukan di antarmuka Acronis Cyber Protect. Klik **Pengaturan** > **Simpul penyimpanan**, klik Acronis Infrastruktur Cyber yang diperlukan, lalu klik **Hapus**.

Menambahkan lokasi pencadangan

Hanya satu lokasi cadangan pada setiap instans Acronis Infrastruktur Cyber yang dapat ditambahkan ke unit atau organisasi. Lokasi yang ditambahkan pada level unit tersedia untuk unit ini dan administrator organisasi. Lokasi yang ditambahkan di level organisasi hanya tersedia untuk administrator organisasi.

Saat menambahkan lokasi, Anda membuat dan memasukkan namanya. Jika Anda perlu menambahkan lokasi yang ada ke server manajemen yang baru atau berbeda, pilih **Gunakan lokasi yang ada...**, centang kotak, klik **Jelajahi**, lalu pilih lokasi dari daftar.

Jika beberapa instans Acronis Infrastruktur Cyber terdaftar di server manajemen, Anda dapat memilih instans Infrastruktur Cyber saat menambahkan lokasi.

Skema pencadangan, operasi, dan batasan

Akses langsung ke Acronis Infrastruktur Cyber dari media yang dapat di-boot tidak tersedia. Untuk bekerja menggunakan Acronis Infrastruktur Cyber, daftarkan media di server manajemen dan kelola melalui konsol web Cyber Protect.

Akses ke Acronis Infrastruktur Cyber melalui antarmuka baris perintah tidak tersedia.

Dalam hal skema dan operasi pencadangan yang tersedia dengan cadangan, Acronis Infrastruktur Cyber mirip dengan penyimpanan awan. Satu-satunya perbedaan adalah bahwa cadangan dapat direplikasi *dari* Acronis Infrastruktur Cyber selama eksekusi rencana proteksi.

Dokumentasi

Set lengkap dokumentasi Acronis Infrastruktur Cyber tersedia di situs web Acronis.

Jadwal

Penting
Beberapa fitur yang dijelaskan dalam bagian ini hanya tersedia untuk penyebaran lokal.

Jadwal menggunakan pengaturan waktu (termasuk zona waktu) dari sistem operasi di mana agen diinstal. Zona waktu Agen untuk VMware (Alat Virtual) dapat dikonfigurasi di dalam antarmuka agen.

Misalnya, jika jadwal rencana pencadangan dijalankan pada pukul 21.00 dan diterapkan pada beberapa mesin yang berada di zona waktu berbeda, pencadangan akan dimulai di setiap mesin pada pukul 21.00 waktu setempat.

Parameter penjadwalan bergantung tujuan pencadangan.

Saat mencadangkan ke penyimpanan awan

Secara default, pencadangan dilakukan setiap hari, Senin hingga Jumat. Anda dapat memilih waktu untuk menjalankan pencadangan.

Jika Anda ingin mengubah frekuensi pencadangan, geser slider, lalu tentukan jadwal pencadangan.

Anda dapat menjadwalkan pencadangan untuk dijalankan berdasarkan event, bukan waktu. Untuk melakukannya, pilih jenis event pada pemilih jadwal. Untuk informasi lebih lanjut, lihat "Jadwal berdasarkan event".

Penting
Cadangan pertama penuh, artinya pencadangan ini paling menghabiskan waktu. Semua pencadangan berikutnya bersifat inkremental dan memerlukan waktu yang jauh lebih sedikit.

Ketika mencadangkan ke lokasi lain

Anda dapat memilih salah satu skema pencadangan yang sudah ditentukan sebelumnya atau membuat skema kustom. Skema pencadangan adalah bagian dari rencana proteksi yang mencakup jadwal pencadangan dan metode pencadangan.

Di **Skema cadangan**, pilih salah satu opsi berikut:

- **Selalu inkremental (file tunggal)**

  Secara default, pencadangan dilakukan setiap hari, Senin hingga Jumat. Anda dapat memilih waktu untuk menjalankan pencadangan.

  Jika Anda ingin mengubah frekuensi pencadangan, geser slider, lalu tentukan jadwal pencadangan.

  Pencadangan menggunakan format cadangan file tunggal[1] baru.

  Skema ini tidak tersedia saat mencadangkan ke alat rekaman atau server SFTP.
- **Selalu penuh**

  Secara default, pencadangan dilakukan setiap hari, Senin hingga Jumat. Anda dapat memilih waktu untuk menjalankan pencadangan.

[1]Format cadangan baru, di mana cadangan penuh awal dan inkremental selanjutnya akan disimpan ke file .tib tunggal, bukan rantai file. 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, misalnya server SFTP.

Jika Anda ingin mengubah frekuensi pencadangan, geser slider, lalu tentukan jadwal pencadangan.

Semua cadangan penuh.

- **Mingguan penuh, kenaikan Harian**

  Secara default, pencadangan dilakukan setiap hari, Senin hingga Jumat. Anda dapat memodifikasi hari dan waktu untuk menjalankan pencadangan.

  Pencadangan penuh dibuat sekali seminggu. Semua pencadangan lainnya bersifat inkremental. Hari saat pencadangan penuh dibuat tergantung pada opsi **Pencadangan mingguan** (klik ikon roda gigi, lalu **Opsi cadangan** > **Pencadangan mingguan**).
- **Penuh bulanan, Diferensial mingguan, Inkremental harian (GFS)**

  Secara default, pencadangan inkremental dilakukan setiap hari, Senin hingga Jumat; pencadangan diferensial dilakukan setiap hari Sabtu; pencadangan penuh dilakukan pada hari pertama setiap bulannya. Anda dapat mengubah jadwal dan waktu untuk menjalankan pencadangan.

  Skema pencadangan ini ditampilkan sebagai skema **Kustom** pada panel rencana proteksi.
- **Kustom**

  Tentukan jadwal untuk pencadangan penuh, diferensial dan inkremental.

  Pencadangan diferensial tidak tersedia ketika mencadangkan data SQL, data Exchange, atau status sistem.

Dengan skema pencadangan apa pun, Anda dapat menjadwalkan pencadangan untuk dijalankan berdasarkan event, bukan waktu. Untuk melakukannya, pilih jenis event pada pemilih jadwal. Untuk informasi lebih lanjut, lihat "Jadwal berdasarkan event".

Opsi penjadwalan tambahan

Dengan tujuan apa pun, Anda dapat melakukan hal berikut:

- Tentukan kondisi mulai pencadangan, sehingga pencadangan terjadwal hanya dilakukan jika syaratnya terpenuhi. Untuk informasi lebih lanjut, lihat "Syarat mulai".
- Menetapkan rentang tanggal kapan jadwal akan berlaku efektif. Pilih kotak centang **Jalankan rencana dalam kisaran tanggal**, lalu tentukan rentang tanggal.
- Nonaktifkan jadwal. Saat jadwal dinonaktifkan, aturan retensi tidak diterapkan kecuali pencadangan dimulai secara manual.
- Masukkan 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.

  Klik ikon roda gigi, lalu **Opsi cadangan** > **Penjadwalan**. Pilih **Distribusikan waktu mulai pencadangan dalam sebuah jendela waktu**, lalu tentukan penundaan maksimal. 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.

Catatan
Pada penyebaran awan, opsi ini diaktifkan secara default, dengan penundaan maksimum yang ditetapkan ke 30 menit. Pada penyebaran di lokasi, secara default semua cadangan dimulai tepat seperti yang dijadwalkan.

- Klik **Tampilkan lebih banyak** untuk mengakses opsi berikut:
  - **Jika mesin dimatikan, jalankan tugas yang tertinggal pada saat mesin dinyalakan** (dinonaktifkan secara default)
  - **Cegah mode tidur atau hibernasi selama pencadangan** (diaktifkan secara default)
    Opsi ini hanya efektif untuk mesin yang menjalankan Windows.
  - **Bangun dari mode tidur atau hibernasi untuk memulai pencadangan terjadwal** (dinonaktifkan secara default)
    Opsi ini hanya efektif untuk mesin yang menjalankan Windows. Opsi ini tidak efektif ketika mesin dimatikan, misalnya Opsi tidak menggunakan fungsionalitas Wake-on-LAN.

Jadwalkan berdasarkan event

Ketika mengatur jadwal untuk rencana proteksi, Anda dapat memilih jenis event pada pemilih jadwal. Pencadangan akan diluncurkan segera setelah event terjadi.

Anda dapat memilih salah satu event berikut:

- **Sejak waktu pencadangan terakhir**
  Ini adalah waktu sejak pencadangan terakhir yang berhasil dalam rencana proteksi yang sama. Anda dapat menentukan durasi waktunya.

Catatan
Karena jadwal didasarkan pada peristiwa pencadangan yang berhasil, jika pencadangan gagal, penjadwal tidak akan menjalankan pekerjaan lagi hingga operator menjalankan rencana secara manual dan proses selesai dengan sukses.

- **Ketika pengguna masuk ke sistem**
  Secara default, setiap pengguna yang masuk akan memulai pencadangan. Anda dapat mengubah setiap pengguna menjadi akun pengguna spesifik.
- **Ketika pengguna keluar dari sistem**
  Secara default, setiap pengguna yang keluar akan memulai pencadangan. Anda dapat mengubah setiap pengguna menjadi akun pengguna spesifik.

Catatan
Pencadangan tidak akan berjalan pada saat sistem mati karena mematikan sistem tidak sama dengan keluar dari sistem.

- **Pada startup sistem**
- **Pada sistem shutdown**

- **Pada event Windows Event Log**

  Anda harus menentukan properti event.

Tabel di bawah ini berisi peristiwa yang tersedia untuk berbagai data di Windows, Linux, dan macOS.

APA YANG AKAN DICADANGKAN	Sejak waktu pencadangan terakhir	Ketika pengguna masuk ke sistem	Ketika pengguna keluar dari sistem	Pada startup sistem	Pada sistem shutdown	Pada event Windows Event Log
Disk/volume atau file (mesin fisik)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Disk/volume (mesin virtual)	Windows, Linux	–	–	–	–	–
Konfigurasi ESXi	Windows, Linux	–	–	–	–	–
Kotak surat Microsoft 365	Windows	–	–	–	–	Windows
Database dan kotak surat Exchange	Windows	–	–	–	–	Windows
Database SQL	Windows	–	–	–	–	Windows

Pada event Windows Event Log

Anda dapat menjadwalkan pencadangan untuk dimulai ketika event Windows tertentu telah direkam di salah satu log event, seperti log **Aplikasi**, **Keamanan**, atau **Sistem**.

Misalnya, Anda mungkin ingin mengatur rencana proteksi yang secara otomatis akan melakukan pencadangan penuh darurat terhadap data Anda segera setelah Windows menemukan bahwa hard disk Anda akan rusak.

Untuk menjelajahi event dan melihat properti event, gunakan snap-in **Event Viewer** yang tersedia di konsol **Manajemen Komputer**. Agar dapat membuka log **Keamanan**, Anda harus menjadi anggota grup **Administrator**.

Properti event

Nama log

Menentukan nama log. Pilih nama log standar (**Aplikasi**, **Keamanan**, atau **Sistem**) dari daftar, atau ketik nama log—misalnya: **Sesi Microsoft Office**

Sumber peristiwa

Menentukan sumber event, yang biasanya menunjukkan program atau komponen sistem yang menyebabkan event tersebut—misalnya: **disk**

Sumber peristiwa apa pun yang berisi string yang ditentukan akan memicu pencadangan terjadwal. Opsi ini tidak peka huruf besar dan kecil. Jadi, jika Anda menetapkan **layanan** string, kedua sumber peristiwa **Service Control Manager** dan **Time-Service** akan memicu pencadangan.

Jenis event

Menentukan jenis event: **Kesalahan**, **Peringatan**, **Informasi**, **Audit berhasil**, atau **Audit gagal**.

ID peristiwa

Menentukan jumlah event, yang biasanya menunjukkan jenis event tertentu di antara event dari sumber yang sama.

Misalnya, peristiwa **Kesalahan** dengan sumber Peristiwa **berupa disk** dan ID Peristiwa **7** terjadi saat Windows menemukan blok yang buruk pada disk, sedangkan peristiwa **Kesalahan** dengan sumber Peristiwa **berupa disk** dan ID Peristiwa **15** terjadi saat disk belum siap diakses.

Contoh: Pencadangan darurat "Blok buruk"

Satu atau beberapa blok buruk yang tiba-tiba muncul di hard disk biasanya menjadi pertanda bahwa drive hard disk akan segera rusak. Apabila situasi ini terjadi, Anda harus segera membuat rencana proteksi yang akan mencadangkan data hard disk.

Ketika Windows mendeteksi blok buruk di hard disk, Windows akan merekam event dengan sumber event **disk** dan nomor event **7** ke dalam log **Sistem** ; jenis event ini adalah **Eror**.

Saat membuat rencana, ketik atau pilih item berikut di bagian **Jadwal**:

- **Nama log**: **Sistem**
- **Sumber peristiwa**: **disk**
- **Jenis event**: **Eror**
- **ID peristiwa**: **7**

Penting
Untuk memastikan bahwa pencadangan tersebut akan selesai meskipun terdapat blok buruk, Anda harus membuat pencadangan yang mengabaikan blok buruk. Untuk melakukannya, di **Opsi cadangan**, masuk ke **Penanganan eror**, lalu pilih kotak centang **Abaikan sektor buruk**.

Persyaratan untuk memulai

Pengaturan ini menambahkan fleksibilitas lebih pada penjadwal, yang memungkinkan eksekusi pencadangan dengan syarat tertentu. Dengan banyaknya syarat, semuanya harus dipenuhi secara simultan untuk memulai pencadangan. Syarat awal tidak efektif jika pencadangan dijalankan secara manual.

Untuk mengakses pengaturan ini, klik **Tampilkan lebih banyak** saat mengatur jadwal untuk rencana proteksi.

Jika satu syarat (atau beberapa syarat) tidak terpenuhi, perilaku penjadwal akan ditentukan oleh opsi pencadangan Syarat mulai pencadangan. Untuk menangani situasi ketika syarat tidak terpenuhi dalam waktu yang sangat lama dan penundaan pencadangan menjadi berisiko, Anda dapat menentukan interval waktu di mana pencadangan akan berjalan tanpa memperhatikan syarat.

Tabel di bawah ini berisi syarat awal yang tersedia untuk berbagai data di Windows, Linux, dan macOS.

APA YANG AKAN DICADANGKAN	Disk/volume atau file (mesin fisik)	Disk/volume (mesin virtual)	Konfigurasi ESXi	Kotak surat Microsoft 365	Database dan kotak surat Exchange	Database SQL
Pengguna idle	Windows	–	–	–	–	–
Host lokasi cadangan tersedia	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Pengguna telah keluar	Windows	–	–	–	–	–
Sesuai interval waktu	Windows, Linux, macOS	Windows, Linux	–	–	–	–
Hemat daya baterai	Windows	–	–	–	–	–
Jangan dimulai ketika memakai koneksi bermeter	Windows	–	–	–	–	–

Jangan dimulai ketika terkoneksi ke jaringan Wi-Fi berikut	Windows	–	–	–	–	–
Cek alamat IP perangkat	Windows	–	–	–	–	–

Pengguna idle

"Pengguna idle" berarti bahwa screen saver berjalan di mesin atau mesin terkunci.

Contoh

Jalankan pencadangan pada mesin setiap hari pada pukul 21:00, lebih baik bila pengguna idle. 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 sampai syarat terpenuhi, Tetap mulai pencadangan setelah 2** jam.

Hasilnya,

(1) Jika pengguna idle pada pukul 21:00, pencadangan akan dimulai pada pukul 21:00.

(2) jika pengguna idle antara pukul 21:00 dan 23:00, pencadangan akan segera dimulai setelah pengguna idle.

(3) Jika pengguna masih aktif pada pukul 23:00, pencadangan akan dimulai pada pukul 23:00.

Host lokasi cadangan tersedia

"Host lokasi cadangan tersedia" artinya mesin yang menjadi host tujuan penyimpanan cadangan tersedia dalam jaringan.

Syarat ini efektif untuk folder jaringan, penyimpanan awan, dan lokasi yang dikelola oleh simpul penyimpanan.

Syarat 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

Data dicadangkan ke folder jaringan setiap hari kerja pada pukul 21:00. Jika saat itu mesin yang menjadi host folder tidak tersedia (misalnya karena adanya pekerjaan pemeliharaan), Anda perlu

melewati pencadangan dan menunggu jadwal pencadangan berikutnya dimulai 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:

(1) Jika tiba pukul 21:00 dan host tersedia, pencadangan akan segera dimulai.

(2) Jika tiba pukul 21:00 namun host tidak tersedia, pencadangan akan dimulai pada hari kerja berikutnya jika host tersedia.

(3) Jika host tidak pernah tersedia di hari kerja pada pukul 21:00, pencadangan tidak akan pernah dimulai.

Pengguna telah keluar

Memungkinkan Anda untuk menunda pencadangan sampai semua pengguna keluar dari Windows.

Contoh

Jalankan pencadangan pada pukul 20:00 setiap Jumat, sebaiknya ketika semua pengguna telah keluar. Jika salah satu pengguna masih masuk pada pukul 23:00, tetap jalankan pencadangan.

- Jadwal: Mingguan, pada hari Jumat. Mulai pada: **20:00**.
- Syarat: **Pengguna telah keluar**.
- Syarat mulai pencadangan: **Tunggu sampai syarat terpenuhi**, **Tetap mulai pencadangan setelah 3** jam.

Hasilnya:

(1) Jika pengguna sudah keluar pada pukul 20:00, pencadangan akan dimulai pada pukul 20:00.

(2) jika pengguna keluar antara pukul 20:00 dan 23:00, pencadangan akan segera dimulai setelah pengguna keluar.

(3) Jika pengguna masih masuk pada pukul 23:00, pencadangan akan dimulai pada pukul 23:00.

Sesuai interval waktu

Batasi waktu mulai pencadangan dengan interval tertentu.

Contoh

Perusahaan menggunakan lokasi yang berbeda pada penyimpanan terpasang-jaringan yang sama untuk mencadangkan data dan server pengguna. Hari kerja dimulai pukul 08:00 dan berakhir pukul 17:00. Data pengguna harus dicadangkan segera setelah pengguna keluar, namun tidak boleh lebih awal dari pukul 16:30. Setiap hari pukul 23:00 server perusahaan akan dicadangkan. Jadi, semua

data pengguna sebaiknya dicadangkan sebelum waktu ini, untuk mengosongkan bandwidth jaringan. Perkiraan waktu pencadangan data pengguna tidak lebih dari satu jam, jadi waktu mulai pencadangan terakhir adalah 22:00. Jika pengguna masih masuk dalam interval waktu yang ditentukan, atau keluar di waktu lain – jangan mencadangkan data pengguna, yaitu, lewati eksekusi pencadangan.

- Event: **Ketika pengguna keluar dari sistem**. Tentukan akun pengguna: **Pengguna mana pun**.
- Syarat: **Sesuai interval waktu** dari **16:30** hingga **22:00**.
- Syarat mulai pencadangan: **Lewati jadwal pencadangan**.

Hasilnya:

(1) jika pengguna keluar antara pukul 16:30 dan 22:00, pencadangan akan segera dimulai setelah keluar.

(2) jika pengguna keluar pada waktu lain, pencadangan akan dilewati.

Hemat daya baterai

Mencegah pencadangan jika perangkat (laptop atau tablet) tidak terhubung ke sumber daya. Tergantung nilai opsi pencadangan Syarat mulai pencadangan, cadangan yang dilewati akan atau tidak akan dimulai setelah perangkat terhubung ke sumber daya. Opsi berikut tersedia:

- **Jangan dimulai ketika memakai daya baterai**
  Pencadangan hanya akan mulai jika perangkat terhubung ke sumber daya.
- **Mulai ketika memakai daya baterai jika level baterai lebih tinggi dari**
  Pencadangan akan dimulai jika perangkat terhubung ke sumber daya atau jika tingkat baterai lebih tinggi dari nilai yang ditentukan.

Contoh

Data dicadangkan setiap hari kerja pada pukul 21:00. Jika perangkat tidak terhubung ke sumber daya (misalnya, pengguna menghadiri rapat di sore hari), Anda ingin melewatkan pencadangan untuk menghemat daya baterai dan menunggu sampai pengguna menghubungkan perangkat ke sumber daya.

- 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:

(1) Jika tiba pukul 21:00 dan perangkat terhubung ke sumber daya, pencadangan akan segera dimulai.

(2) Jika tiba pukul 21:00 dan perangkat berjalan dengan daya baterai, pencadangan akan segera dimulai setelah perangkat terhubung ke sumber daya.

Jangan dimulai ketika memakai koneksi bermeter

Cegah pencadangan (termasuk pencadangan ke disk lokal) jika perangkat terhubung ke Internet menggunakan koneksi yang ditetapkan sebagai 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.

Sebagai langkah tambahan untuk mencegah pencadangan melalui hotspot seluler, jika Anda mengaktifkan syarat **Jangan dimulai ketika memakai koneksi bermeter**, syarat **Jangan dimulai ketika terkoneksi ke jaringan Wi-Fi berikut** akan diaktifkan secara otomatis. Nama jaringan berikut ditentukan secara default: "android", "phone", "mobile", dan "modem". Anda dapat menghapus nama tersebut dari daftar dengan mengklik tanda X.

Contoh

Data dicadangkan setiap hari kerja pada pukul 21:00. Jika perangkat dihubungkan ke Internet menggunakan koneksi bermeter (misalnya, pengguna sedang dalam perjalanan bisnis), Anda akan melewati pencadangan untuk menyimpan lalu lintas jaringan dan menunggu jadwal untuk memulai 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:

(1) Jika tiba pukul 21:00 dan perangkat tidak terhubung ke internet menggunakan koneksi bermeter, pencadangan akan segera dimulai.

(2) Jika tiba pukul 21:00 dan perangkat terhubung ke internet menggunakan koneksi bermeter, pencadangan akan dimulai pada hari kerja berikutnya.

(3) Jika perangkat selalu terhubung ke Internet menggunakan koneksi bermeter di hari kerja pada pukul 21:00, pencadangan tidak akan pernah dimulai.

Jangan dimulai ketika terkoneksi ke jaringan Wi-Fi berikut

Cegah pencadangan (termasuk pencadangan ke disk lokal) jika perangkat terhubung ke salah satu jaringan nirkabel yang ditetapkan. Anda dapat menentukan nama jaringan Wi-Fi, disebut juga sebagai service set identifier (SSID).

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, pencadangan tidak akan dimulai saat perangkat terhubung ke salah satu jaringan berikut: "John's iPhone", "phone_wifi", or "my_PHONE_wifi".

Syarat ini berguna untuk mencegah pencadangan ketika perangkat terhubung ke Internet menggunakan hotspot telepon genggam.

Sebagai langkah tambahan untuk mencegah pencadangan melalui hotspot seluler, syarat **Jangan dimulai ketika terhubung ke Wi-Fi berikut** diaktifkan secara otomatis ketika Anda mengaktifkan syarat **Jangan dimulai ketika memakai koneksi bermeter**. Nama jaringan berikut ditentukan secara default: "android", "phone", "mobile", dan "modem". Anda dapat menghapus nama tersebut dari daftar dengan mengklik tanda X.

Contoh

Data dicadangkan setiap hari kerja pada pukul 21:00. Jika perangkat terhubung ke Internet menggunakan hotspot seluler (misalnya, laptop dihubungkan dalam mode tethering), Anda akan melewati pencadangan dan menunggu jadwal untuk memulai 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:

(1) Jika tiba pukul 21:00 dan mesin tidak terhubung ke jaringan yang ditentukan, pencadangan akan segera dimulai.

(2) Jika tiba pukul 21:00 dan mesin terhubung ke jaringan yang ditentukan, pencadangan akan dimulai pada hari kerja berikutnya.

(3) Jika mesin selalu terhubung ke jaringan yang ditentukan di hari kerja pada pukul 21:00, pencadangan tidak akan pernah dimulai.

Cek alamat IP perangkat

Mencegah pencadangan (termasuk pencadangan ke disk lokal) jika alamat IP perangkat ada di dalam atau di luar rentang alamat IP yang telah ditentukan. 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.

Syarat ini berguna jika pengguna berada di luar negeri, untuk menghindari biaya transit data yang besar. Juga untuk membantu mencegah pencadangan melalui koneksi Jaringan Privat Virtual (VPN).

Contoh

Data dicadangkan setiap hari kerja pada pukul 21:00. Jika perangkat terhubung ke jaringan perusahaan menggunakan tunnel VPN (misalnya, pengguna bekerja dari rumah), Anda ingin melewati pencadangan dan menunggu sampai pengguna membawa perangkatnya ke kantor.

- Jadwal: Harian, Jalankan Senin hingga Jumat. Mulai pada: 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:

(1) Jika tiba pukul 21:00 dan alamat IP mesin tidak dalam rentang yang ditentukan, pencadangan akan segera dimulai.

(2) Jika tiba pukul 21:00 dan alamat IP mesin ada dalam rentang yang ditentukan, pencadangan akan segera dimulai begitu perangkat mendapatkan alamat IP non-VPN.

(3) Jika alamat IP mesin selalu dalam rentang yang ditentukan di hari kerja pada pukul 21:00, pencadangan tidak akan pernah dimulai.

Aturan retensi

Penting
Beberapa fitur yang dijelaskan dalam bagian ini hanya tersedia untuk penyebaran lokal.

1. Klik **Berapa lama akan disimpan**.
2. Di **Pembersihan**, Anda dapat memilih salah satu opsi berikut:
   - **Berdasarkan umur cadangan** (default)
     Tentukan berapa lama cadangan yang dibuat akan disimpan oleh rencana proteksi. Secara default, aturan retensi ditentukan untuk setiap set cadangan[1] secara terpisah. Jika Anda ingin menggunakan aturan tunggal untuk semua cadangan, klik **Beralih ke aturan tunggal untuk semua set cadangan**.
   - **Berdasarkan jumlah cadangan**
     Tentukan jumlah maksimum cadangan yang akan disimpan.
   - **Berdasarkan ukuran total cadangan**
     Tentukan ukuran total maksimum cadangan yang akan disimpan.

[1]Sejumlah cadangan yang untuknya aturan retensi individual dapat diterapkan. Untuk skema pencadangan Kustom, set cadangan sesuai dengan metode pencadangan (Penuh, Diferensial, dan Inkremental). Dalam semua kasus lainnya, set cadangannya adalah Bulanan, Harian, Mingguan, dan per Jam. Pencadangan bulanan adalah cadangan pertama yang dibuat pada awal suatu bulan. Pencadangan mingguan adalah cadangan pertama yang dibuat pada hari dalam minggu yang dipilih dalam opsi pencadangan Mingguan (klik ikon roda, lalu Opsi pencadangan > Cadangan mingguan). Apabila pencadangan mingguan adalah cadangan pertama yang dibuat setelah awal suatu bulan, cadangan ini dianggap sebagai cadangan bulanan. Dalam hal ini, pencadangan mingguan akan dibuat pada hari yang dipilih untuk minggu berikutnya. Pencadangan harian adalah cadangan pertama yang dibuat pada awal suatu hari, kecuali jika cadangan ini termasuk dalam definisi cadangan bulanan atau mingguan. Pencadangan per jam adalah cadangan yang pertama dibuat pada awal suatu jam, kecuali jika cadangan ini termasuk dalam definisi cadangan bulanan, mingguan, atau harian.

Pengaturan ini tidak tersedia dengan skema pencadangan **Selalu inkremental (file tunggal)**, atau saat membuat cadangan ke server SFTP maupun perangkat pita.

- **Simpan cadangan tanpa batas**

3. Pilih waktu untuk memulai pembersihan::
   - **Setelah pencadangan** (default)

     Aturan retensi akan diterapkan setelah cadangan baru dibuat.
   - **Sebelum pencadangan**

     Aturan retensi akan diterapkan sebelum cadangan baru dibuat.

     Pengaturan ini tidak tersedia saat mencadangkan klaster Microsoft SQL Server atau klaster Microsoft Exchange Server.

Apa saja yang perlu Anda ketahui

- Dalam semua kasus, cadangan terakhir yang dibuat oleh rencana proteksi disimpan, kecuali Anda mengonfigurasi aturan retensi untuk membersihkan cadangan sebelum memulai operasi pencadangan baru dan menyetel jumlah cadangan ke nol.

  Peringatan!
  Jika Anda menghapus satu-satunya cadangan yang Anda miliki dengan menerapkan aturan retensi dengan cara ini, jika pencadangan gagal, Anda tidak akan memiliki cadangan untuk memulihkan data karena tidak akan ada cadangan yang tersedia untuk digunakan.

- Cadangan yang disimpan di pita tidak akan dihapus sampai pita tersebut ditimpa.
- Jika, berdasarkan skema cadangan dan format cadangan, setiap cadangan disimpan sebagai file terpisah, file ini tidak dapat dihapus hingga masa berlaku semua cadangan dependen (inkremental dan diferensial) habis. Hal ini memerlukan ruang ekstra untuk menyimpan cadangan yang penghapusannya ditunda. Selain itu, usia cadangan, jumlah, atau ukuran cadangan juga dapat melebihi nilai yang Anda tentukan.

  Perilaku ini dapat diubah menggunakan opsi cadangan "Konsolidasi cadangan".
- Aturan retensi adalah bagian dari rencana proteksi. Aturan tersebut menghentikan operasi cadangan mesin segera setelah rencana proteksi dibatalkan atau dihapus dari mesin, atau mesin itu sendiri dihapus dari server manajemen. Jika Anda tidak lagi memerlukan rencana pembuatan cadangan, hapus seperti yang dijelaskan dalam "Menghapus cadangan".

Enkripsi

Kami menyarankan Anda untuk mengenkripsi semua cadangan yang disimpan dalam penyimpanan awan, terutama jika perusahaan tunduk pada kepatuhan peraturan.

Penting
Tidak ada cara untuk memulihkan cadangan terenkripsi jika Anda menghilangkan atau lupa kata sandi.

Enkripsi dalam rencana proteksi

Untuk mengaktifkan enkripsi, tentukan pengaturan enkripsi saat membuat rencana proteksi. Setelah rencana proteksi diterapkan, pengaturan enkripsi tidak dapat dimodifikasi. Untuk menggunakan pengaturan enkripsi yang berbeda, buat rencana proteksi baru.

Untuk menentukan pengaturan enkripsi dalam rencana proteksi

1. Pada panel rencana proteksi, aktifkan tombol **Enkripsi**.
2. Masukkan dan konfirmasi kata sandi enkripsi.
3. Pilih salah satu algoritma enkripsi berikut:
   - **AES 128** – cadangan akan dienkripsi menggunakan algoritma Advanced Encryption Standard (AES) dengan kunci 128-bit.
   - **AES 192** – cadangan akan dienkripsi menggunakan algoritma AES dengan kunci 192-bit.
   - **AES 256** – cadangan akan dienkripsi menggunakan algoritma AES dengan kunci 256-bit.
4. Klik **OK**.

Enkripsi sebagai properti mesin

Opsi ini ditujukan untuk administrator yang menangani cadangan beberapa mesin. Jika Anda memerlukan kata sandi enkripsi unik untuk setiap mesin atau jika Anda harus melakukan enkripsi cadangan apa pun terlepas dari pengaturan enkripsi rencana proteksinya, simpan pengaturan enkripsi pada setiap mesin secara individual. Pencadangan akan dienkripsi menggunakan algoritma AES dengan kunci 256-bit.

Menyimpan pengaturan enkripsi pada mesin akan memengaruhi 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 nanti.** Pengaturan enkripsi yang disimpan pada mesin akan mengesampingkan pengaturan enkripsi dalam rencana proteksi. Setiap cadangan akan dienkripsi, meskipun enkripsi dinonaktifkan dalam pengaturan rencana proteksi.

Opsi ini dapat digunakan pada mesin yang menjalankan Agen untuk VMware. Namun, berhati-hatilah jika Anda memiliki lebih dari satu Agen untuk VMware yang terhubung ke Server vCenter yang sama. Anda wajib menggunakan pengaturan enkripsi yang sama untuk semua agen, karena ada jenis penyeimbang pemuatan di antara mereka.

Setelah pengaturan enkripsi disimpan, pengaturan tersebut dapat diubah atau diatur ulang seperti yang dijelaskan di bawah.

Penting
Jika rencana proteksi yang berjalan di mesin ini sudah membuat cadangan, perubahan pengaturan enkripsi akan mengakibatkan kegagalan rencana ini. Untuk melanjutkan pencadangan, buat rencana baru.

Untuk menyimpan pengaturan enkripsi di mesin

1. Masuk sebagai administrator (di Windows) atau pengguna root (di Linux).
2. Jalankan skrip berikut:
   - Di Windows: `<jalur_instalasi>`**\PyShell\bin\acropsh.exe -m manage_creds --set-password** `<kata_sandi_enkripsi>`
     Di sini, `<jalur_instalasi>` adalah jalur instalasi agen perlindungan. Secara default, yaitu **%ProgramFiles%\BackupClient** dalam penyebaran awan dan **%ProgramFiles%\Acronis** dalam penyebaran lokal.
   - Di Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<kata_sandi_enkripsi>`

Untuk mengatur ulang pengaturan enkripsi di mesin

1. Masuk sebagai administrator (di Windows) atau pengguna root (di Linux).
2. Jalankan skrip berikut:
   - Di Windows: `<jalur_instalasi>`**\PyShell\bin\acropsh.exe -m manage_creds --reset**
     Di sini, `<jalur_instalasi>` adalah jalur instalasi agen perlindungan. Secara default, yaitu **%ProgramFiles%\BackupClient** dalam penyebaran awan dan **%ProgramFiles%\Acronis** dalam penyebaran lokal.
   - Di Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Untuk mengubah pengaturan enkripsi menggunakan Monitor Cyber Protect

1. Masuk sebagai administrator di Windows atau macOS.
2. Klik ikon **Monitor Cyber Protect** di area notifikasi (di Windows) atau bilah menu (di macOS).
3. Klik ikon roda gigi.
4. Klik **Enkripsi**.
5. Lakukan salah satu langkah berikut:
   - Pilih **Atur kata sandi khusus untuk mesin ini**. Masukkan dan konfirmasi kata sandi enkripsi.
   - Pilih **Gunakan pengaturan enkripsi yang ditentukan dalam rencana proteksi**.
6. Klik **OK**.

Cara kerja enkripsi

Algoritma kriptografi AES beroperasi dalam mode Cipher-block chaining (CBC) dan menggunakan kunci yang dihasilkan secara acak dengan ukuran yang ditentukan pengguna sebesar 128, 192, atau

256 bit. Semakin besar ukuran kunci, semakin lama waktu yang diperlukan program untuk mengenkripsi cadangan dan semakin aman pula data Anda.

Kunci enkripsi kemudian dienkripsi dengan AES-256 menggunakan SHA-256 hash dari kata sandi sebagai kunci. Kata sandi itu sendiri tidak disimpan di lokasi mana pun pada disk atau cadangan; hash kata sandi digunakan untuk tujuan verifikasi. Dengan keamanan dua tingkat ini, data cadangan akan terlindungi dari akses tidak berizin, namun tidak dapat memulihkan kata sandi yang hilang.

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 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
- Jika tujuan pencadangannya adalah lokasi yang dikelola dengan deduplikasi atau enkripsi yang diaktifkan

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.

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.

Konversi ke mesin virtual

Penting
Beberapa fitur yang dijelaskan dalam bagian ini hanya tersedia untuk penyebaran lokal.

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.

Metode konversi

- **Konversi reguler**

  Ada dua cara untuk mengonfigurasi konversi reguler:

  - **Jadikan konversi sebagai bagian dari rencana proteksi**

    Konversi akan dilakukan setelah setiap pencadangan (jika dikonfigurasi untuk lokasi utama) atau setelah setiap replikasi (jika dikonfigurasi untuk lokasi kedua dan yang berikutnya).
  - **Buat rencana konversi terpisah**

    Metode ini memungkinkan Anda untuk menentukan jadwal konversi terpisah.
- **Pemulihan ke mesin virtual baru**

  Metode ini memungkinkan Anda memilih disk untuk pemulihan dan menyesuaikan pengaturan untuk setiap disk virtual. Gunakan metode ini untuk melakukan konversi satu kali atau seweaktu-waktu, misalnya, untuk melakukan migrasi dari fisik ke virtual.

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 merangkum jenis mesin virtual yang dapat dibuat oleh agen:

Tipe VM	Agen untuk VMware	Agen untuk Hyper-V	Agen untuk Windows	Agen untuk Linux	Agen untuk Mac	Agen untuk Scale Computing HC3

VMware ESXi	+	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–
VMware Workstation	+	+	+	+	–	–
File VHDX	+	+	+	+	–	–
Scale Computing HC3	–	–	–	–	–	+

Pembatasan

- Agen untuk Windows, Agen untuk VMware (Windows), dan Agen untuk Hyper-V tidak dapat mengonversi cadangan yang disimpan di NFS.
- Cadangan yang disimpan di NFS atau di server SFTP tidak dapat dikonversi dalam rencana konversi terpisah.
- Cadangan yang disimpan di Secure Zone hanya dapat dikonversi oleh agen yang berjalan di mesin yang sama.
- Cadangan dapat dikonversi ke mesin virtual Scale Computing HC3 hanya dalam rencana konversi terpisah.
- 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 ESXi dan Hyper-V 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 membutuhkan sumber daya CPU dan memori. File dari mesin virtual akan secara konstan mengisi ruang di penyimpanan data (penyimpanan). Metode ini mungkin tidak praktis jika host produksi digunakan untuk konversi. Namun, kinerja mesin virtual hanya dibatasi oleh sumber daya host.

Dalam kasus kedua, sumber daya hanya dikonsumsi saat mesin virtual 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.

Konversi ke mesin virtual dalam rencana proteksi

Anda dapat mengonfigurasi konversi ke mesin virtual dari cadangan atau lokasi replikasi apa pun yang ada dalam rencana proteksi. Konversi akan dilakukan setelah setiap cadangan atau replikasi.

Untuk informasi tentang prasyarat dan batasan, silakan lihat "Yang perlu Anda ketahui tentang konversi".

Untuk mengatur konversi ke mesin virtual dalam rencana proteksi

1. Tentukan lokasi pencadangan asal Anda ingin melakukan konversi.
2. Pada panel rencana proteksi, klik **Konversi ke VM** pada lokasi ini.
3. Aktifkan switch **Konversi**.
4. Di **Konversi ke**, pilih jenis mesin virtual target. Anda dapat memilih salah satu dari tindakan berikut:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **File VHDX**
5. Lakukan salah satu langkah berikut:
   - Untuk VMware ESXi dan Hyper-V: 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. [Opsional] Klik **Agen yang akan melakukan konversi**, lalu pilih agen.

   Agen ini dapat berupa agen yang melakukan pencadangan (secara default) atau agen yang diinstal pada mesin lain. Jika agennya adalah yang diinstal di mesin lain, cadangan harus disimpan di lokasi bersama seperti folder jaringan, sehingga mesin lain dapat mengaksesnya.
7. [Opsional] Untuk VMware ESXi dan Hyper-V, Anda juga dapat melakukan langkah berikut:
   - Klik **Penyimpanan data** untuk ESXi atau **Jalur** untuk Hyper-V, lalu pilih penyimpanan data (penyimpanan) untuk mesin virtual.
   - Ubah mode provisi disk. Pengaturan default adalah **Tipis** untuk VMware ESXi dan **Memperluas secara dinamis** untuk Hyper-V.
   - Klik **Pengaturan VM** untuk mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual.
8. Klik **Selesai**.

Cara kerja konversi reguler ke VM

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 pada server virtualisasi:** saat mengonversi cadangan inkremental atau diferensial, perangkat lunak akan memperbarui mesin virtual yang ada, bukan membuatnya kembali. 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.

Snapshot intermediet

Agar dapat memperbarui mesin virtual, perangkat lunak akan menyimpan beberapa snapshot intermediet darinya. Snapshot tersebut akan dinamai **Backup...** dan **Replica...** dan harus disimpan. Snapshot yang tidak dibutuhkan akan dihapus secara otomatis.

Snapshot **Replica...** terbaru akan sesuai dengan hasil konversi terbaru. Anda dapat menuju ke snapshot ini jika Anda ingin mengembalikan mesin ke status tersebut; misalnya, jika Anda bekerja dengan mesin dan sekarang ingin membuang perubahan yang dibuat untuknya.

Snapshots lain adalah untuk penggunaan internal oleh perangkat lunak.

Replikasi

Penting
Beberapa fitur yang dijelaskan dalam bagian ini hanya tersedia untuk penyebaran lokal.

Bagian ini menjelaskan replikasi cadangan sebagai bagian dari rencana proteksi. Untuk informasi tentang membuat rencana replikasi terpisah, lihat "Pemrosesan data off-host".

Jika Anda mengaktifkan replikasi cadangan, setiap cadangan akan segera disalin ke lokasi lain setelah pembuatan. Jika cadangan sebelumnya tidak direplikasi (misalnya, koneksi jaringan hilang), perangkat lunak juga akan mereplikasi semua cadangan yang muncul setelah replikasi terakhir yang berhasil.

Cadangan yang direplikasi tidak bergantung pada cadangan yang tersisa di lokasi asli dan sebaliknya. Anda dapat memulihkan data dari cadangan apa pun, tanpa akses ke lokasi lain.

Contoh penggunaan

- **Pemulihan bencana yang dapat diandalkan**
  Simpan cadangan Anda di situs (untuk pemulihan cepat) dan di luar situs (untuk mengamankan cadangan dari kegagalan penyimpanan lokal atau bencana alam).
- **Menggunakan penyimpanan awan untuk melindungi data dari bencana alam**
  Mereplikasi cadangan ke penyimpanan awan dengan hanya mentransfer perubahan data.
- **Hanya menyimpan titik pemulihan terbaru**
  Menghapus cadangan lama dari penyimpanan cepat sesuai dengan aturan retensi, agar tidak terlalu banyak menggunakan ruang penyimpanan yang mahal.

Lokasi yang didukung

Anda dapat mereplikasi cadangan *dari* salah satu lokasi ini:

- Folder lokal
- Folder jaringan
- Secure Zone
- Server SFTP
- Lokasi dikelola oleh simpul penyimpanan

Anda dapat mereplikasi cadangan *ke* salah satu lokasi ini:

- Folder lokal
- Folder jaringan
- Penyimpanan awan
- Server SFTP

- Lokasi dikelola oleh simpul penyimpanan
- Perangkat pita

Untuk mengaktifkan replikasi cadangan

1. Pada panel rencana proteksi, klik **Tambah lokasi**.

   Kontrol **Tambahkan lokasi** hanya tersedia jika replikasi didukung *dari* lokasi pencadangan atau replikasi yang terakhir dipilih.
2. Tentukan lokasi di mana cadangan akan direplikasi.
3. [Opsional] Di **Berapa lama akan disimpan**, ubah aturan retensi untuk lokasi yang dipilih, seperti yang dijelaskan dalam "Aturan retensi".
4. [Opsional] Di **Konversi ke VM**, tentukan pengaturan untuk konversi ke mesin virtual, seperti yang dijelaskan dalam "Konversi ke mesin virtual".
5. [Opsional] Klik ikon roda gigi > **Jendela kinerja dan pencadangan**, lalu atur jendela pencadangan untuk lokasi yang dipilih, seperti dijelaskan dalam "Jendela kinerja dan pencadangan". Pengaturan ini akan menentukan performa replikasi.
6. [Opsional] Ulangi langkah 1-5 untuk semua lokasi di mana Anda ingin mereplikasi cadangan. Maksimum lima lokasi berturut-turut didukung, termasuk lokasi utama.

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 ketergantungan ini, gunakan paket terpisah untuk replikasi cadangan. Untuk informasi lebih lanjut tentang rencana spesifik ini, lihat "Replikasi cadangan" (hlm. 344).

Pertimbangan untuk pengguna dengan lisensi Lanjutan

Tips

Anda dapat mengatur replikasi cadangan *dari* penyimpanan awan dengan membuat rencana replikasi terpisah. Untuk informasi lebih lanjut, lihat "Pemrosesan data off-host".

Batasan

- Replikasi cadangan *dari* lokasi yang dikelola oleh simpul penyimpanan ke folder lokal tidak didukung. Folder lokal berarti folder pada mesin dengan agen yang membuat cadangan.
- Replikasi cadangan *ke* lokasi yang dikelola dengan deduplikasi yang diaktifkan tidak didukung untuk cadangan yang memiliki format cadangan **Versi 12**.

Mesin mana yang melakukan konversi?

Replikasi cadangan *dari* setiap lokasi diinisiasi oleh agen yang membuat cadangan dan dilakukan:

- Oleh agen tersebut, jika lokasi *tidak* dikelola oleh simpul penyimpanan.
- Oleh simpul penyimpanan yang sesuai, jika lokasi dikelola. Namun, replikasi cadangan dari lokasi yang dikelola ke penyimpanan awan akan dilakukan oleh agen yang mencadangkan.

Sebagai lanjutan dari uraian di atas, operasi hanya akan dilakukan jika mesin dengan agen dihidupkan.

Replikasi cadangan antara lokasi yang dikelola

Replikasi cadangan dari satu lokasi yang dikelola ke lokasi yang dikelola lainnya akan dilakukan oleh simpul penyimpanan.

Jika deduplikasi diaktifkan untuk lokasi target (mungkin pada simpul penyimpanan yang berbeda), simpul penyimpanan sumber hanya akan mengirimkan blok data yang tidak ada di lokasi target. Dengan kata lain, sama seperti agen, simpul penyimpanan akan melakukan deduplikasi pada sumbernya. Cara ini akan menghemat lalu lintas jaringan saat Anda mereplikasi data antara simpul penyimpanan yang terpisah secara geografis.

Memulai pencadangan secara manual

1. Pilih mesin yang memiliki setidaknya satu rencana proteksi yang diterapkan.
2. Klik **Cadangkan**.
3. Jika lebih dari satu rencana proteksi diterapkan, pilih rencana proteksi.
4. Lakukan salah satu langkah berikut:
   - Klik **Jalankan sekarang**. Cadangan bertahap akan dibuat.
   - Jika skema pencadangan mencakup beberapa metode pencadangan, Anda dapat memilih metode yang akan digunakan. Klik tanda panah pada tombol **Jalankan sekarang**, lalu pilih **Penuh, Inkremental**, atau **Diferensial**.

Cadangan pertama yang dibuat oleh rencana proteksi selalu penuh.

Progres pencadangan ditampilkan di kolom **Status** untuk mesin.

Opsi cadangan

Penting
Beberapa fitur yang dijelaskan dalam bagian ini hanya tersedia untuk penyebaran lokal.

Untuk memodifikasi opsi pencadangan, klik ikon roda di samping nama rencana proteksi, lalu klik **Opsi pencadangan**.

Ketersediaan opsi pencadangan

Set opsi pencadangan yang ada bergantung pada:

- 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**	**Scale Computing**	**Windows**
Peringatan	+	+	+	+	+	+	+	+	+	+
Konsolidasi cadangan	+	+	+	+	+	+	+	+	+	-
Nama file cadangan	+	+	+	+	+	+	+	+	+	+
Format cadangan	+	+	+	+	+	+	+	+	+	+
Validasi cadangan	+	+	+	+	+	+	+	+	+	+
Pelacakan perubahan blok (CBT)	+	-	-	-	-	-	+	+	+	+
Mode cadangan klaster	-	-	-	-	-	-	-	-	-	+
Tingkat kompresi	+	+	+	+	+	+	+	+	+	+
Notifikasi email	+	+	+	+	+	+	+	+	+	+
Penanganan eror										
Coba lagi jika terjadi kesalahan	+	+	+	+	+	+	+	+	+	+

Jangan menampilkan pesan dan dialog saat memproses (mode diam)	+	+	+	+	+	+	+	+	+	+
Abaikan sektor buruk	+	-	+	+	-	+	+	+	+	-
Coba lagi, jika kesalahan terjadi selama pembuatan snapshot VM	-	-	-	-	-	-	+	+	+	-
Cadangan inkremental/ diferensial cepat	+	+	+	-	-	-	-	-	-	-
Filter file	+	+	+	+	+	+	+	+	+	-
Snapshot pencadangan tingkat file	-	-	-	+	+	+	-	-	-	-
Pemotongan log	-	-	-	-	-	-	+	+	-	Hanya SQL
Membuat snapshot LVM	-	+	-	-	-	-	-	-	-	-
Titik mount	-	-	-	+	-	-	-	-	-	-
Snapshot multivolume	+	+	-	+	+	-	-	-	-	-
Jendela performa dan pencadangan	+	+	+	+	+	+	+	+	+	+
Pengiriman Data Fisik	+	+	+	+	+	+	+	+	+	-

Perintah pra/pasca	+	+	+	+	+	+	+	+	+	+
Perintah pengambilan data Pra/Pasca	+	+	+	+	+	+	+	-	-	+
Snapshot perangkat keras SAN	-	-	-	-	-	-	+	-	-	-
Penjadwalan										
Distribusikan waktu mulai dalam jendela waktu	+	+	+	+	+	+	+	+	+	+
Batasi jumlah pencadangan yang berjalan secara simultan	-	-	-	-	-	-	+	+	+	-
Pencadangan sektor demi sektor	+	+	-	-	-	-	+	+	+	-
Pembagian	+	+	+	+	+	+	+	+	+	+
Manajemen pita	+	+	+	+	+	+	+	+	+	+
Penanganan kegagalan tugas	+	+	+	+	+	+	+	+	+	+
Syarat mulai tugas	+	+	-	+	+	-	+	+	+	+
Layanan Volume Shadow Copy (VSS)	+	-	-	+	-	-	-	+	-	+
Layanan	-	-	-	-	-	-	+	+	+	-

Volume Shadow Copy (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.

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 adalah perangkat pita atau penyimpanan awan.
- Skema cadangan diatur ke **Selalu inkremental (file tunggal)**.
- Format cadangan diatur ke **Versi 12**.

Aktifkan pemulihan file dari cadangan disk yang disimpan pada pita 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. Cadangan yang disimpan pada pita akan hilang dari GUI hanya ketika pita tersebut ditimpa atau dihapus.

Nama file cadangan

Opsi ini menentukan nama file cadangan yang dibuat oleh rencana proteksi.

Nama-nama tersebut dapat dilihat di manajer file saat menjelajahi lokasi pencadangan.

Apa itu file cadangan?

Setiap rencana proteksi akan membuat satu atau beberapa file di lokasi pencadangan, tergantung 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 tradisional)

Format cadangan **Versi 12**	Satu file TIBX per rantai cadangan (cadangan penuh atau diferensial, dan semua cadangan bertahap yang bergantung padanya)

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 membuat atau mengedit rencana proteksi.

Catatan
Stempel waktu ditambahkan ke nama file cadangan hanya dalam format cadangan versi 11.

Setelah Anda mengubah nama file cadangan, cadangan berikutnya akan menjadi cadangan penuh, kecuali jika Anda menentukan nama file cadangan yang ada di mesin yang sama. Jika Anda menentukan nama file, cadangan penuh, inkremental, atau diferensial akan dibuat sesuai dengan jadwal rencana proteksi.

Perhatikan bahwa dimungkinkan untuk menetapkan nama file cadangan untuk lokasi yang tidak dapat diakses oleh manajer file (seperti penyimpanan awan atau perangkat pita). Hal ini wajar dilakukan jika Anda ingin melihat nama-nama kustom pada tab **Penyimpanan cadangan**.

Di mana saya dapat melihat nama file cadangan?

Pilih tab **Penyimpanan cadangan**, lalu pilih grup 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**.

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**).

Nama file cadangan default

Nama file cadangan default adalah `[Nama Mesin]-[ID Rencana]-[ID Unik]A`.

Nama file cadangan default untuk cadangan kotak surat adalah `[ID Kotak Surat]_mailbox_[ID Rencana]A`.

Nama terdiri dari variabel berikut:

- `[Nama Mesin]` Variabel ini diganti dengan nama mesin (nama yang sama yang ditampilkan di konsol web Cyber Protect) untuk semua jenis data yang dicadangkan, kecuali untuk kotak surat Microsoft 365. Untuk kotak surat Microsoft 365, nama diganti dengan nama utama pengguna kotak surat (UPN).
- `[ID Rencana]` Variabel ini diganti dengan pengidentifikasi unik rencana proteksi. Nilai ini tidak akan berubah jika nama rencana diubah.
- `[ID Unik]` Variabel ini diganti dengan pengidentifikasi unik dari mesin atau kotak surat yang dipilih. Nilai ini tidak berubah jika nama mesin diganti atau UPN kotak surat diubah.
- `[ID Kotak Surat]` Variabel ini diganti dengan UPN kotak surat.
- `"A"` adalah surat perlindungan yang ditambahkan untuk mencegah nama diakhiri dengan angka.

Diagram di bawah ini menunjukkan nama file cadangan default.

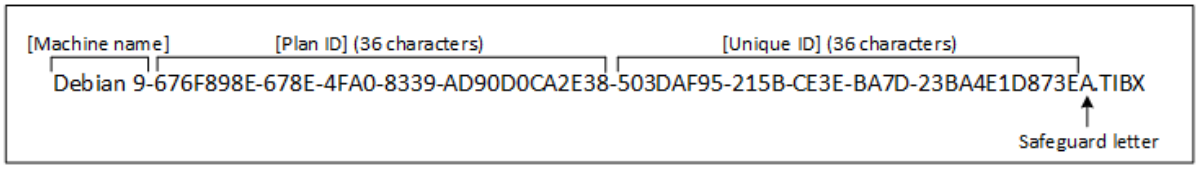
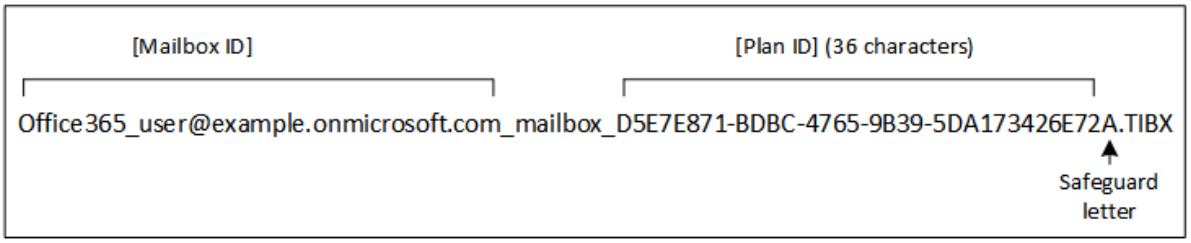


Diagram di bawah ini menunjukkan nama file cadangan default untuk kotak surat.



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
...
```

Untuk format versi 11 dengan skema pencadangan **Selalu inkremental (file tunggal)**:

```
MyBackup.xml
MyBackup.tib
```

Untuk format versi 11 dengan skema pencadangan lain:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

Menggunakan variabel

Selain variabel yang digunakan secara default, Anda juga dapat menggunakan variabel `[Nama rencana]`, yang diganti dengan nama rencana proteksi.

Jika beberapa mesin atau kotak surat dipilih untuk pencadangan, nama file cadangan harus berisi variabel `[Nama Mesin]`, `[ID Kotak Surat]`, atau `[ID Unik]`.

Nama file cadangan vs. penamaan file yang disederhanakan

Dengan teks polos dan/atau variabel, Anda dapat membuat nama file yang sama seperti pada versi Acronis Cyber Protect sebelumnya. Namun, nama file yang disederhanakan tidak dapat direkonstruksi—dalam versi 12, nama file akan memiliki stempel waktu kecuali jika format file tunggal digunakan.

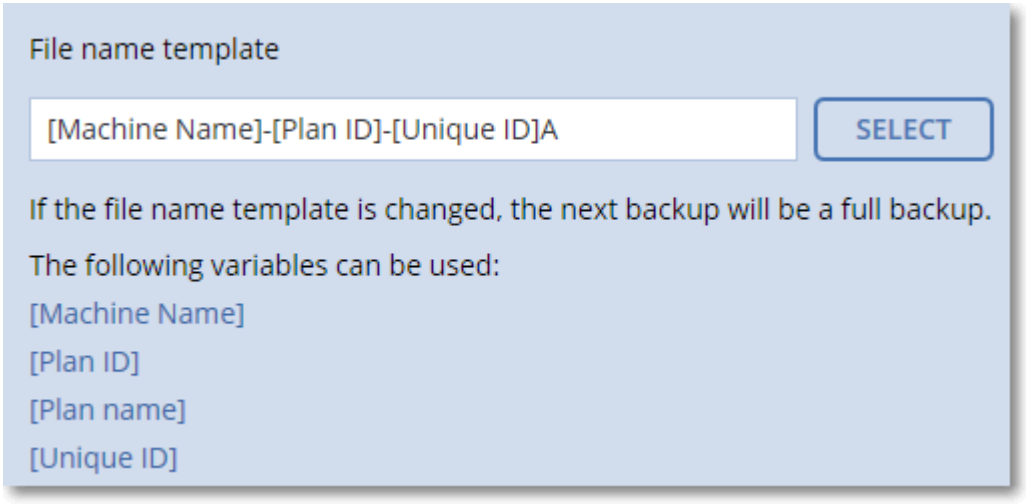
Contoh penggunaan

- **Lihat nama file yang mudah digunakan**

  Anda ingin membedakan cadangan dengan mudah saat menjelajahi lokasi pencadangan dengan manajer file.
- **Lanjutkan urutan cadangan yang ada**

  Anggap saja rencana proteksi diterapkan pada satu mesin, dan Anda harus menghapus mesin ini dari konsol web Cyber Protect atau menghapus instalasi agen beserta pengaturan konfigurasinya. Setelah mesin ditambahkan kembali atau agen diinstal ulang, Anda dapat memaksa rencana proteksi untuk terus mencadangkan ke cadangan atau urutan pencadangan yang sama. Untuk melakukan ini, dalam opsi pencadangan dari rencana proteksi, klik **Nama file cadangan**, lalu klik **Pilih** untuk memilih cadangan yang diinginkan.

  Tombol **Jelajahi** menunjukkan cadangan di lokasi yang dipilih di bagian **Tempat menyimpan cadangan** pada panel rencana proteksi. Tombol tersebut tidak dapat menjelajahi apa pun di luar lokasi ini.



- **Tingkatkan dari versi produk sebelumnya**
  Jika selama peningkatan versi rencana proteksi tidak bermigrasi secara otomatis, buat ulang rencana dan arahkan ke file cadangan lama. Jika hanya satu mesin yang dipilih untuk pencadangan, klik **Jelajahi**, lalu pilih cadangan yang diperlukan. Jika beberapa mesin dipilih untuk pencadangan, buat kembali nama file cadangan lama dengan menggunakan variabel.

Catatan
Tombol **Pilih** hanya tersedia untuk rencana proteksi yang dibuat untuk dan diterapkan pada suatu perangkat.

Format cadangan

Opsi ini menentukan format cadangan yang dibuat oleh rencana proteksi. Opsi ini hanya tersedia untuk rencana proteksi yang menggunakan format cadangan legasi versi 11. Dalam hal ini, Anda dapat mengubahnya ke format versi 12 yang baru. Setelah perubahan ini, opsi ini menjadi tidak dapat diakses.

Opsi ini *tidak* efektif untuk pencadangan kotak surat. Pencadangan kotak surat selalu memiliki format baru.

Nilai prasetelnya adalah: **Pemilihan otomatis**.

Anda dapat memilih salah satu dari tindakan berikut:

- **Pemilihan otomatis**
  Versi 12 akan digunakan kecuali jika rencana proteksi menambahkan cadangan pada rencana yang dibuat oleh versi produk sebelumnya.
- **Versi 12**
  Format baru disarankan dalam kebanyakan kasus untuk pencadangan dan pemulihan cepat. Tiap rantai cadangan (cadangan penuh atau diferensial, dan semua cadangan bertahap yang bergantung padanya) disimpan dalam file TIBX tunggal.
  Dengan format ini, aturan retensi **Berdasarkan ukuran total cadangan** tidak efektif.
- **Versi 11**

Format legasi yang dipertahankan untuk kompatibilitas mundur. Format ini memungkinkan Anda menambahkan cadangan pada rencana yang dibuat oleh versi produk sebelumnya.

Selain itu, gunakan format ini (dengan skema pencadangan apa pun kecuali untuk **Selalu inkremental (file tunggal)**) jika Anda ingin pencadangan penuh, inkremental, dan diferensial jadi file terpisah.

Format ini dipilih secara otomatis jika tujuan cadangan (atau tujuan replikasi) adalah lokasi terkelola dengan deduplikasi yang diaktifkan, atau lokasi terkelola dengan enkripsi yang diaktifkan. Jika Anda mengubah format ke **Versi 12**, pencadangan akan gagal.

Catatan
Anda tidak dapat mencadangkan Database Availability Group (DAG) dengan menggunakan format cadangan versi 11. Mencadangkan DAG hanya didukung dalam format versi 12.

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. Anda dapat menentukan nama file menggunakan opsi nama file cadangan. 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 tradisional)
Format cadangan **Versi 12**	Satu file TIBX per rantai cadangan (cadangan penuh atau diferensial, dan semua cadangan bertahap yang bergantung padanya)	

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.

- Jika tujuan cadangan (atau tujuan replikasi) adalah lokasi terkelola dengan deduplikasi yang diaktifkan, pencadangan akan gagal.

Deduplikasi dalam arsip

Format versi 12 mendukung deduplikasi dalam arsip.

Deduplikasi dalam arsip menggunakan deduplikasi sisi klien dan 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.

Validasi cadangan

Validasi adalah operasi untuk memeriksa kemungkinan pemulihan data dari cadangan. Ketika opsi ini diaktifkan, setiap cadangan yang dibuat oleh rencana proteksi akan langsung divalidasi setelah pembuatan. Operasi ini dilakukan oleh agen perlindungan.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Validasi akan menghitung checksum untuk tiap blok data yang dapat dipulihkan dari cadangan. Satu-satunya pengecualian adalah validasi cadangan tingkat file yang terletak di penyimpanan awan. Cadangan ini divalidasi dengan cara memeriksa konsistensi metadata yang tersimpan dalam cadangan.

Validasi adalah proses yang membutuhkan waktu cukup lama, bahkan untuk sebuah cadangan inkremental atau diferensial, yang ukurannya lebih kecil. Hal ini dikarenakan operasi bukan hanya memvalidasi data yang hanya ditampung secara fisik di dalam cadangan, namun semua data yang dapat dipulihkan dengan memilih cadangan. Proses ini membutuhkan akses ke cadangan yang sebelumnya telah dibuat.

Meskipun keberhasilan validasi menandakan tingginya kemungkinan keberhasilan pemulihan, proses validasi tidak memeriksa semua faktor yang memengaruhi proses pemulihan. Jika Anda mencadangkan sistem operasi, sebaiknya lakukan uji pemulihan menggunakan media yang dapat di-boot ke hard drive cadangan atau jalankan mesin virtual dari cadangan pada lingkungan ESXi atau Hyper-V.

Pelacakan perubahan blok (CBT)

Opsi ini efektif untuk pencadangan tingkat disk mesin virtual dan mesin fisik yang menjalankan Windows. Cara ini juga efektif untuk pencadangan database Microsoft SQL Server dan database

Microsoft Exchange Server.

Nilai prasetelnya adalah:**Aktif**.

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

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, 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.

Microsoft Exchange Server

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**
  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

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, tingkat 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.

Notifikasi email

Opsi ini memungkinkan Anda mengatur notifikasi email tentang peristiwa yang terjadi selama pencadangan.

Opsi ini hanya tersedia dalam penyebaran di lokasi. Dalam penyebaran awan, pengaturan dikonfigurasikan per akun ketika akun dibuat.

Nilai prasetelnya adalah: **Gunakan pengaturan sistem.**

Anda dapat menggunakan pengaturan kustom, atau menimpanya dengan nilai kustom yang akan spesifik untuk hanya untuk rencana ini. Pengaturan global dikonfigurasi seperti yang dijelaskan dalam "Notifikasi email".

Penting
Jika pengaturan sistem diubah, semua rencana proteksi yang menggunakan pengaturan sistem akan terpengaruh.

Sebelum mengaktifkan opsi ini, pastikan bahwa pengaturan **server Email** telah dikonfigurasi.

Untuk menyesuaikan notifikasi email bagi rencana proteksi

1. Pilih **Sesuaikan pengaturan untuk rencana proteksi ini**.
2. Di kolom **alamat email Penerima**, masukkan alamat email tujuan. Anda dapat memasukkan beberapa alamat yang dipisahkan dengan tanda titik koma.
3. [Opsional] Di **Subjek**, ubah subjek notifikasi email.
   Anda dapat menggunakan variabel berikut
   - `[Peringatan]` - ringkasan peringatan.
   - `[Perangkat]` - nama perangkat.
   - `[Rencana]` - nama rencana yang menghasilkan peringatan.
   - `[ManagementServer]` - nama host mesin tempat server manajemen diinstal.
   - `[Unit]` - nama unit tempat mesin tersebut berada.

   Subjek default adalah `[Peringatan]` **Perangkat:** `[Perangkat]` **Rencana:** `[Rencana]`
4. Pilih kotak centang untuk peristiwa yang ingin Anda terima notifikasinya. Anda dapat memilih dari daftar semua peringatan yang terjadi selama pencadangan, dikelompokkan berdasarkan tingkat keparahannya.

Penanganan eror

Opsi ini memungkinkan Anda untuk menentukan cara penanganan eror yang mungkin terjadi selama pencadangan.

Coba lagi, jika eror terjadi

Nilai prasetelnya adalah: **Aktif. 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.

Misalnya, jika tujuan pencadangan pada jaringan tidak tersedia atau tidak dapat dijangkau, program akan mencoba menjangkau tujuan setiap 30 detik, namun tidak lebih dari 30 kali. Upaya percobaan akan dihentikan begitu kembali terhubung ke jaringan ATAU jumlah percobaan yang ditentukan sudah habis, mana pun yang terlebih dahulu tercapai.

Penyimpanan awan

Jika penyimpanan awan dipilih sebagai tujuan cadangan, nilai opsi secara otomatis ditetapkan ke **Aktif**. **Jumlah percobaan: 300. Interval di antara percobaan: 30 detik.**

Dalam hal ini, jumlah percobaan yang sebenarnya adalah tidak terbatas, namun batas waktu sebelum pencadangan gagal dihitung sebagai berikut: (300 detik + **Interval di antara percobaan**) * (**Jumlah percobaan** + 1).

Contoh:

- Dengan nilai default, pencadangan akan gagal setelah (300 detik + 30 detik) * (300 + 1) = 99330 detik, atau ~27,6 jam.
- Jika Anda menetapkan **Jumlah percobaan** ke 1 dan **Interval di antara percobaan** ke 1 detik, pencadangan akan gagal setelah (300 detik + 1 detik) * (1 + 1) = 602 detik, atau ~10 menit.

Jika batas waktu yang dihitung melebihi 30 menit, dan transfer data belum dimulai, batas waktu yang sebenarnya akan ditetapkan ke 30 menit.

Jangan menampilkan pesan dan dialog saat memproses (mode diam)

Nilai prasetelnya adalah: **Aktif**.

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.

Coba lagi, jika kesalahan terjadi selama pembuatan snapshot VM

Nilai prasetelnya adalah: **Aktif. 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.

Opsi ini tidak efektif (selalu dinonaktifkan) untuk volume yang diformat dengan sistem file JFS, ReiserFS3, ReiserFS4, ReFS, atau XFS.

Nilai prasetelnya adalah: **Aktif**.

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

Dengan filter file, Anda hanya dapat menyertakan file dan folder spesifik di cadangan, atau mengecualikan file dan folder spesifik dari cadangan.

Filter file tersedia pada pencadangan tingkat disk dan tingkat file, kecuali dinyatakan sebaliknya.

Filter file tidak berlaku jika diterapkan pada disk dinamis (volume LVM atau LDM) dari mesin virtual yang dicadangkan oleh Agen untuk VMware, Agen untuk Hyper-V, atau Agen untuk Scale Computing dalam mode tanpa agen.

Untuk mengaktifkan filter file

1. Di rencana proteksi, perbesar modul **Cadangan**.
2. Dalam **Opsi cadangan**, klik **Ubah**.
3. Pilih **Filter file**.
4. Gunakan opsi mana saja yang dijelaskan di bawah ini.

Sertakan atau kecualikan file yang cocok dengan kriteria spesifik

Ada dua opsi yang berfungsi dengan cara terbalik.

- **Cadangkan hanya file yang cocok dengan kriteria berikut**
  Contoh: Jika Anda memilih untuk mencadangkan keseluruhan mesin dan menentukan **C:\File.exe** pada kriteria filter, hanya file ini yang akan dicadangkan.

Catatan
Filter ini tidak efektif untuk pencadangan tingkat file jika **Versi 11** dipilih pada **Format cadangan** dan tujuan cadangan BUKAN penyimpanan awan.

- **Jangan mencadangkan file yang sesuai dengan kriteria berikut**
  Contoh: Jika Anda memilih untuk mencadangkan keseluruhan mesin dan menentukan **C:\File.exe** pada kriteria filter, hanya file ini yang akan dilewati.

Anda dimungkinkan untuk menggunakan kedua pilihan tersebut secara bersamaan. Opsi terakhir akan mengesampingkan opsi sebelumnya, yaitu jika Anda menentukan **C:\File.exe** di kedua bidang, file akan dilewati selama pencadangan.

Kriteria

- **Jalur lengkap**
  Tentukan jalur lengkap untuk file atau folder, mulai dengan huruf drive (saat mencadangkan Windows) atau direktori root (saat mencadangkan Linux atau MacOS).
  Baik di Windows dan Linux/MacOS, Anda dapat menggunakan garis miring pada jalur file atau folder (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 ada filter penyertaan, pencadangan akan gagal.

  Filter jalur lengkap menyertakan huruf drive (di Windows) atau direktori root (di Linux atau macOS). Misalnya, jalur lengkap file bisa jadi **C:\Temp\File.tmp**. Filter yang menyertakan huruf drive atau direktori root — misalnya **C:\Temp\File.tmp** or **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.

- **Nama**
  Tentukan nama file atau folder, seperti **Document.txt**. Semua file dan folder dengan nama tersebut akan dipilih.

Kriterianya bersifat *tidak* sensitif huruf besar-kecil. Misalnya, dengan menentukan **C:\Temp**, Anda juga akan memilih **C:\TEMP**, **C:\temp**, dan seterusnya.

Anda dapat menggunakan karakter wildcard (*, **, dan ?) pada kriteria. Karakter tersebut dapat digunakan baik pada jalur lengkap dan pada nama file atau folder.

Tanda bintang (*) menggantikan nol atau beberapa karakter pada nama file. Misalnya, kriteria **Doc*.txt** cocok dengan file seperti **Doc.txt** dan **Document.txt**

[Hanya untuk cadangan dalam format **Versi 12**] Tanda bintang ganda (**) menggantikan nol atau beberapa karakter dalam nama file dan jalur, termasuk karakter garis miring. Misalnya, kriteria ****/Docs/**.txt** cocok dengan semua file txt di semua subfolder dari semua folder **Docs**.

Tanda tanya (?) menggantikan satu karakter pada nama file. Misalnya, kriteria **Doc?.txt** cocok dengan file seperti **Doc1.txt** dan **Docs.txt**, namun bukan file **Doc.txt** atau **Doc11.txt**

Kecualikan berkas dan folder tersembunyi

Pilih kotak centang ini untuk melewatkan file dan folder yang memiliki atribut **Tersembunyi** (untuk sistem file yang didukung oleh Windows) atau yang berawalan tanda titik (.) (untuk sistem file di Linux, seperti Ext2 dan Ext3). Jika folder tersembunyi, semua isinya (termasuk file yang tidak tersembunyi) akan dikecualikan.

Kecualikan berkas dan folder sistem

Opsi ini hanya efektif untuk sistem file yang didukung oleh Windows. Pilih kotak centang ini untuk melewatkan file dan folder dengan atribut **Sistem**. Jika sebuah folder memiliki atribut **Sistem**, semuanya isinya (termasuk file yang tidak memiliki atribut **Sistem**) akan dikecualikan.

Catatan
Anda dapat melihat atribut file atau folder pada properti file/folder atau menggunakan perintah attrib. Untuk informasi lebih lanjut, lihat Pusat Bantuan dan Dukungan Windows.

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

Aktivitas berbahaya pada mesin dapat dilakukan oleh virus, malware, dan ransomware. Kasus lain yang mungkin perlu diselidiki adalah mencuri atau mengubah data pada mesin dengan berbagai program. Aktivitas seperti itu mungkin perlu diselidiki tetapi hanya memungkinkan jika Anda menyimpan bukti digital pada mesin untuk diselidiki. Sayangnya, bukti (file, jejak, dan sebagainya) dapat dihapus atau mesin bisa tidak tersedia.

Opsi cadangan yang disebut **Data forensik** memungkinkan Anda mengumpulkan bukti digital yang dapat digunakan dalam penyelidikan forensik. Item berikut dapat digunakan sebagai bukti digital: snapshot dari ruang disk yang tidak digunakan, timbunan memori, dan snapshot dari proses yang berjalan. Fungsionalitas **Data forensik** hanya tersedia untuk seluruh cadangan mesin.

Saat ini, opsi **Data forensik** hanya tersedia untuk mesin Windows dengan versi OS berikut:

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

Catatan
• Setelah rencana proteksi dengan modul Pencadangan diterapkan pada mesin, pengaturan data forensik tidak dapat dimodifikasi. Untuk menggunakan pengaturan data forensik yang berbeda, buat rencana proteksi baru.
• Cadangan dengan pengumpulan data forensik tidak didukung untuk mesin yang tersambung ke jaringan melalui VPN dan tidak memiliki akses langsung ke Internet.

Lokasi yang didukung untuk cadangan dengan data forensik adalah:

- Penyimpanan awan
- Folder lokal

  Catatan
  1. Folder lokal hanya didukung pada hard disk eksternal yang terhubung melalui USB.
  2. Disk dinamis lokal tidak didukung sebagai lokasi untuk cadangan forensik.

- Folder jaringan

Cadangan dengan data forensik secara otomatis dinotariskan. Cadangan forensik memungkinkan penyelidik untuk menganalisis area disk yang biasanya tidak termasuk dalam cadangan disk biasa.

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 web Cyber Protect, buka **Perangkat** > **Semua perangkat**. Rencana proteksi juga dapat dibuat dari tab **Rencana**.
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**.
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. Masuk ke **Dasbor** > **Aktivitas**, verifikasi bahwa cadangan dengan data forensik 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 web Cyber Protect, buka **Penyimpanan cadangan**, pilih lokasi dengan cadangan yang berisi 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 timbunan memori atau file forensik lainnya dan klik **Unduh**.
   - 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 sama persis dengan gambar yang diambil dan tidak disusupi, modul Cadangan menyediakan notaris cadangan dengan data forensik.

Cara kerjanya

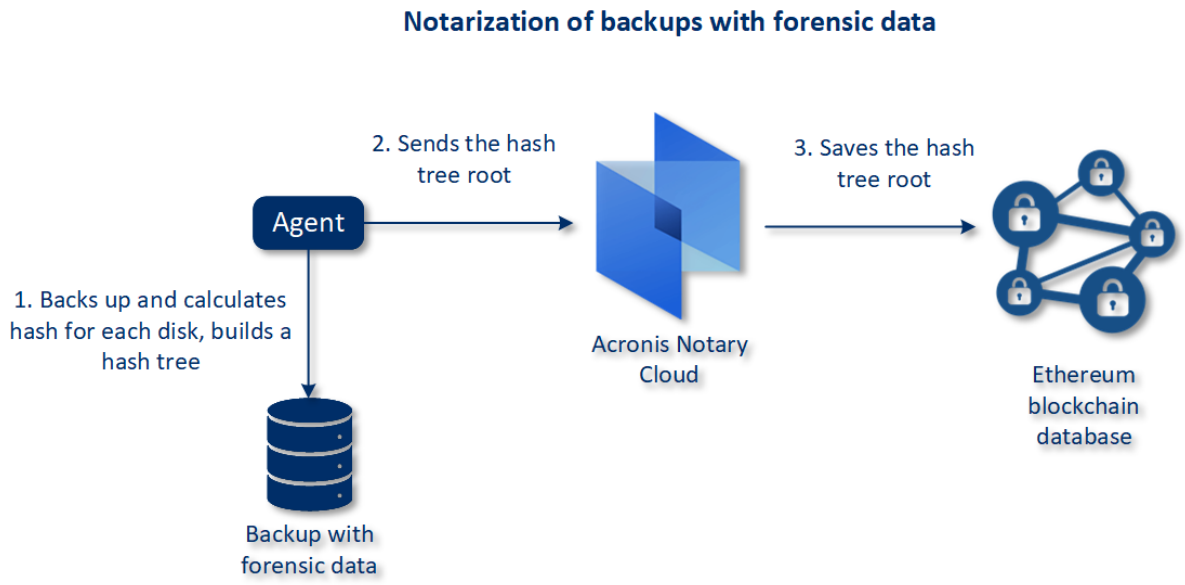
Notarisasi memungkinkan Anda untuk membuktikan bahwa disk dengan data forensik asli dan tidak berubah sejak dicadangkan.

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.

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 Protect 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. Lokasinya berada di: `C:\Program Files\Acronis\BackupAndRecovery`.

Lokasi yang didukung adalah:

- 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:

- daftarkan cadangan
- daftarkan konten
- dapatkan konten
- hitung hash

daftarkan cadangan

Mencantumkan titik pemulihan dalam cadangan.

SINOPSIS:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Opsi

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Output template:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> – GUID cadangan.

<tanggal> – tanggal pembuatan cadangan. Formatnya: DD.MM.YYYY HH24:MM:SS. 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:

```
Disk     Size   Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<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 disk yang ditentukan di titik pemulihan dengan menggunakan algoritma SHA-256 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

```
--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 web. 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 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 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.
--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: **Aktif**.

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).

Nilai prasetelnya adalah: **Oleh perangkat lunak pencadangan**.

- **Oleh perangkat lunak pencadangan**. Data snapshot sebagian besar disimpan dalam RAM. Pencadangan lebih cepat dan ruang tidak teralokasi pada grup volume tidak diperlukan. Dengan

demikian, kami menyarankan Anda untuk mengubah prasetelnya hanya jika Anda mengalami masalah dalam 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.

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**.

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: **Aktif**.
- Jika tidak ada mesin yang dipilih (ini adalah kasus ketika Anda mulai membuat rencana proteksi dari halaman **Rencana** > **Cadangan**): **Aktif**.
- 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 Satu-klik

Pemulihan Satu-klik memungkinkan pengguna untuk memulihkan cadangan disk terbaru dari mesin mereka secara otomatis. Ini dapat berupa cadangan seluruh mesin, atau cadangan disk atau volume tertentu pada mesin ini.

Fitur ini dapat diakses pada mesin pengguna setelah administrator mengaktifkannya, bersamaan dengan Startup Recovery Manager. Administrator dapat melakukan operasi ini hanya melalui antarmuka baris perintah. Untuk mempelajari selengkapnya tentang cara mengaktifkan Startup Recovery Manager dan Pemulihan Satu-klik, lihat Referensi baris perintah.

Pemulihan Satu-klik mendukung penyimpanan cadangan berikut ini:

1. Secure Zone
2. Penyimpanan jaringan
3. Penyimpanan awan

Jika jenis penyimpanan tertentu tidak tersedia atau tidak ada cadangan disk di dalamnya, pengguna diminta untuk menggunakan jenis penyimpanan selanjutnya.

Jika lebih dari satu set cadangan (juga disebut *arsip*) yang berisi cadangan disk tersedia di penyimpanan, pemulihan Satu-klik memilih set cadangan yang diperbarui terakhir. Pengguna tidak dapat memilih set cadangan yang berbeda.

Pemulihan Satu-klik mendukung operasi berikut ini:

- Pemulihan otomatis dari cadangan terbaru
- Pemulihan dari cadangan tertentu (juga disebut *titik pemulihan*) dalam set cadangan yang dipilih secara otomatis

Memulihkan mesin dengan pemulihan Satu-klik

Prasyarat

- Administrator telah mengaktifkan Pemulihan Satu-klik pada mesin yang dipilih.
- Setidaknya ada satu cadangan disk dari mesin yang dipilih.

Untuk memulihkan mesin

1. Nyalakan ulang mesin yang ingin Anda pulihkan.
2. Selama reboot, tekan F11 untuk masuk ke Startup Recovery Manager.
3. Pilih opsi pemulihan Satu-klik yang diinginkan:
   - Untuk memulihkan cadangan terbaru secara otomatis, tekan 1 pada keyboard.
   - Untuk memulihkan cadangan yang berbeda dalam set cadangan yang terakhir diperbarui, tekan 2 pada keyboard.
     - Untuk memilih cadangan yang diinginkan (juga disebut *titik pemulihan*), tekan nomor masing-masing pada keyboard.

Antarmuka pengguna grafis dimulai, dan kemudian menghilang. Prosedur pemulihan berlanjut tanpanya. Saat pemulihan selesai, mesin Anda akan menyala ulang.

Jendela performa dan pencadangan

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.

Opsi ini tidak tersedia untuk pencadangan yang dijalankan oleh agen awan, seperti pencadangan situs web atau pencadangan server yang berada di situs pemulihan awan.

Anda dapat mengonfigurasi opsi ini secara terpisah untuk setiap lokasi yang ditentukan dalam rencana proteksi. Agar dapat mengonfigurasi opsi ini untuk lokasi replikasi, klik ikon roda gigi di sebelah nama lokasi, lalu klik **Jendela performa dan pencadangan**.

Opsi ini hanya efektif untuk proses pencadangan dan replikasi cadangan. Perintah pasca-pencadangan dan operasi lain yang termasuk dalam rencana proteksi (validasi, konversi ke mesin virtual) 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, sesuai dengan **Di bawah normal**).
- Kecepatan output: **Tidak terbatas.**

Ketika opsi ini diaktifkan, pencadangan terjadwal akan diizinkan atau diblokir sesuai dengan parameter performa yang ditentukan untuk jam saat ini. Pada awal jam ketika pencadangan diblokir, proses pencadangan secara otomatis akan dihentikan dan peringatan dibuat.

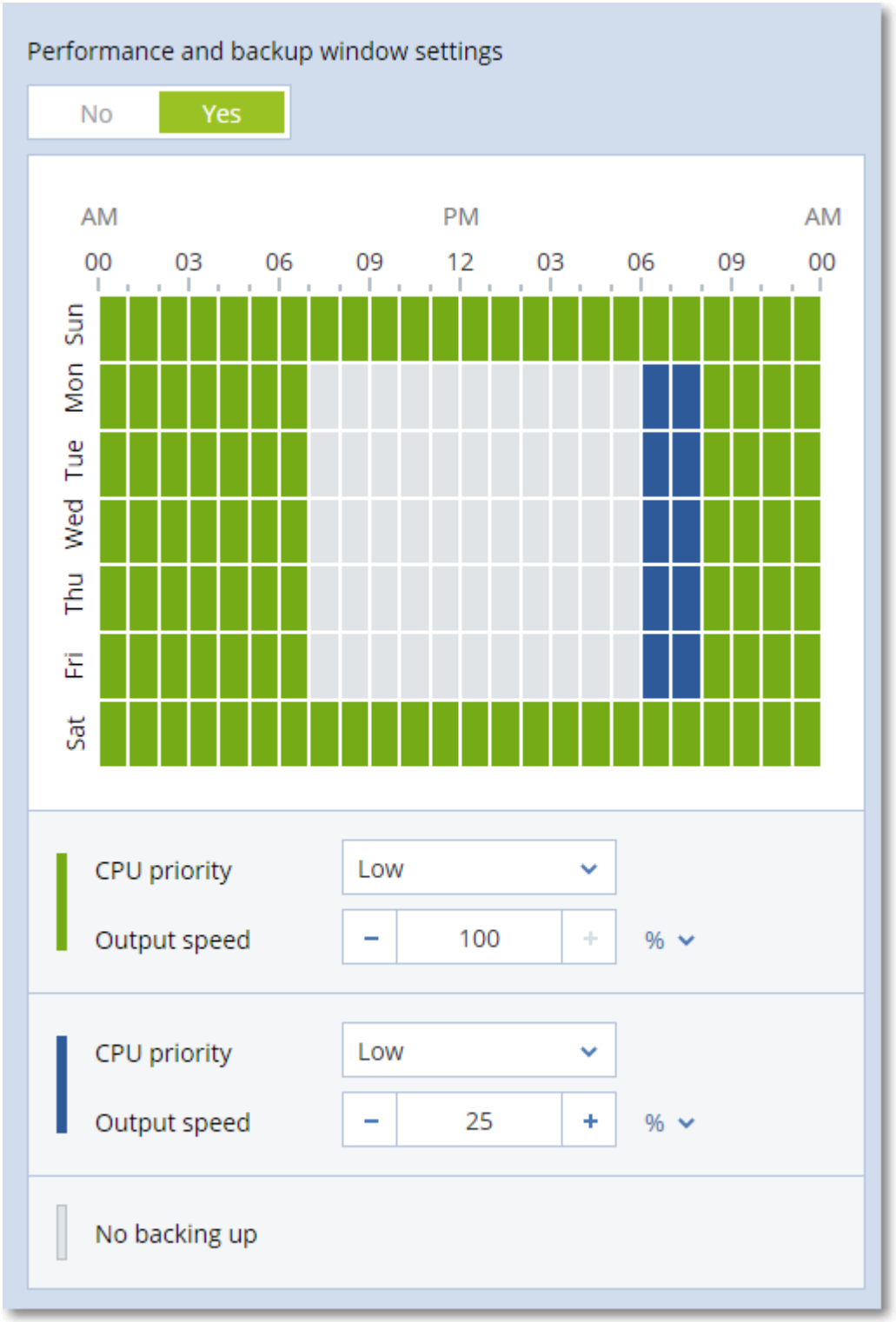
Meskipun pencadangan terjadwal diblokir, pencadangan tetap dapat dimulai secara manual. Pencadangan ini akan menggunakan parameter performa jam terbaru ketika pencadangan diizinkan.

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.



Prioritas CPU

Parameter ini menentukan prioritas proses pencadangan di sistem operasi.

Pengaturan yang tersedia adalah:

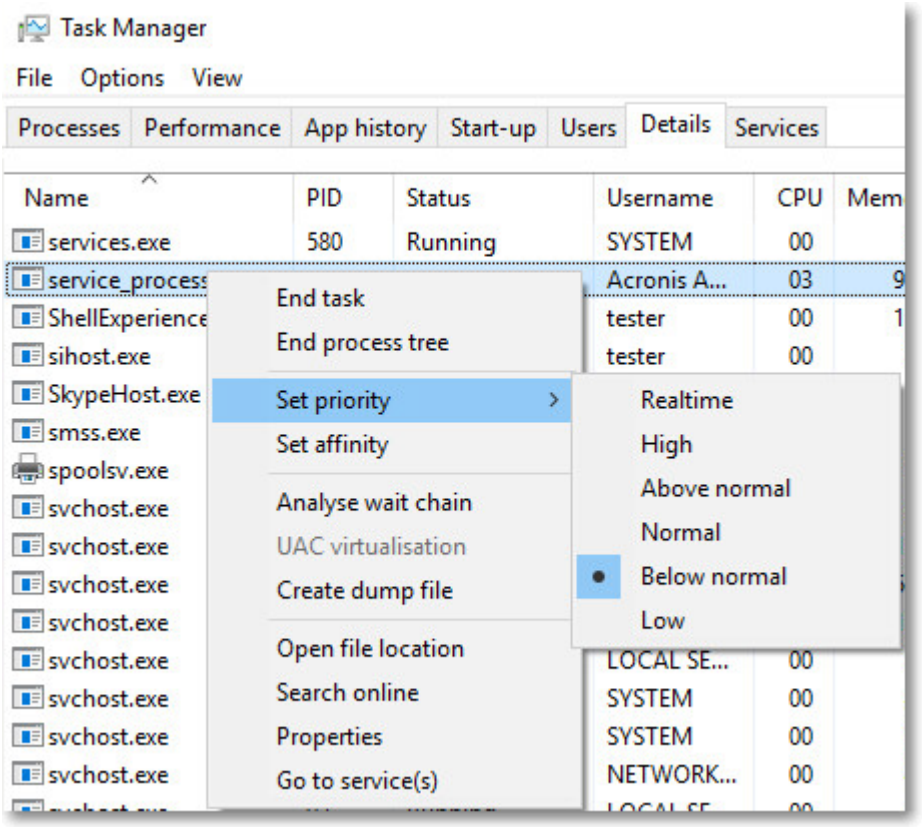
Rendah - di Windows, sesuai dengan **Di bawah normal**.

Normal - di Windows, sesuai dengan **Normal**.

Tinggi - di Windows, sesuai dengan **Tinggi**.

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 OS X.



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 efektif jika tujuan pencadangan adalah penyimpanan awan dan format cadangan 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, dan Agen untuk Hyper-V. Pencadangan yang dibuat pada media yang dapat di-boot tidak didukung.

Opsi ini menentukan apakah cadangan penuh pertama yang dibuat oleh rencana proteksi akan dikirim ke penyimpanan awan pada drive hard disk menggunakan layanan Pengiriman Data Fisik. Pencadangan inkremental berikutnya dapat dilakukan melalui jaringan.

Nilai prasetelnya adalah: **Dinonaktifkan.**

Tentang layanan Pengiriman Data Fisik

Antarmuka web layanan Pengiriman Data Fisik hanya tersedia untuk administrator organisasi pada penyebaran di lokasi dan administrator pada penyebaran awan.

Untuk petunjuk lebih detail 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. Buat rencana proteksi baru. Dalam rencana ini, aktifkan opsi pencadangan **Pengiriman Data Fisik**.

   Anda dapat mencadangkan langsung ke drive atau mencadangkan ke folder lokal atau folder jaringan, lalu salin/pindahkan cadangan ke drive.

   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.

2. Setelah pencadangan pertama selesai, gunakan antarmuka web layanan Pengiriman Data Fisik untuk mengunduh alat pembuatan pesanan dan membuat pesanan.

   Untuk mengakses antarmuka web ini, lakukan salah satu langkah berikut:

   - Pada penyebaran lokal: masuk ke akun Acronis, lalu klik **Buka Konsol Pelacakan** pada **Pengiriman Data Fisik**.
   - Pada penyebaran awan: masuk ke portal manajemen, klik **Ikhtisar** > **Penggunaan**, lalu klik **Kelola layanan** di bawah **Pengiriman Data Fisik**.

3. Kemas drive dan kirim ke pusat data.

   Penting
   Pastikan Anda mengikuti petunjuk pengemasan yang disediakan dalam Panduan Administrator Pengiriman Data Fisik.

4. 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.

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.

Program 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 pencadangan hanya setelah perintah berhasil dieksekusi. Gagalkan pencadangan jika eksekusi perintah gagal.	Lakukan pencadangan setelah perintah dieksekusi, meskipun eksekusi gagal atau berhasil.	N/A	Lakukan pencadangan bersama dengan eksekusi perintah, apa pun hasil eksekusi perintahnya.

* Perintah dianggap gagal jika mengeluarkan kode yang tidak sama dengan nol.

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 dieksekusi 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 dieksekusi.

<table>
<tr><td></td><td colspan="3"><---------- Cadangan ----------></td><td></td></tr>
<tr><td>Perintah pra-pencadangan</td><td>Perintah pengambilan pra-data</td><td>Pengambilan data</td><td>Perintah pengambilan pasca-data</td><td>Perintah pasca-pencadangan</td></tr>
</table>

Jika opsi Layanan Volume Shadow Copy diaktifkan, eksekusi perintah dan tindakan VSS Microsoft akan diurutkan sebagai 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

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.

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
Jangan cadangkan sampai eksekusi perintah	Dipilih	Dipilih	Dihapus	Dihapus

selesai				
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.

Snapshot perangkat keras SAN

Opsi ini efektif untuk pencadangan mesin virtual VMware ESXi.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Opsi ini menentukan apakah akan menggunakan snapshot SAN saat melakukan pencadangan.

Jika opsi ini dinonaktifkan, konten disk virtual akan dibaca dari snapshot VMware. Snapshot akan disimpan selama durasi pencadangan.

Jika opsi ini diaktifkan, konten disk virtual akan dibaca dari snapshot SAN. Snapshot VMware akan dibuat dan disimpan secara singkat, untuk membawa disk virtual ke dalam status konsisten. Jika membaca dari snapshot SAN tidak dimungkinkan, pencadangan akan gagal.

Sebelum mengaktifkan opsi ini, silakan periksa dan jalankan persyaratan yang tercantum di "Menggunakan snapshot perangkat keras SAN".

Penjadwalan

Opsi ini menentukan apakah pencadangan dimulai sesuai jadwal atau dengan penundaan, dan berapa banyak mesin virtual yang dicadangkan secara bersamaan.

Nilai prasetelnya adalah:

- Penyebaran di lokasi: **Mulai semua pencadangan sesuai jadwal.**
- Penyebaran awan: **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**

  Opsi ini hanya tersedia ketika rencana proteksi diterapkan pada beberapa mesin virtual. Opsi ini menentukan berapa banyak mesin virtual yang dapat dicadangkan agen secara bersamaan saat menjalankan rencana proteksi yang ditentukan.

  Jika, berdasarkan rencana proteksi, agen harus mulai mencadangkan beberapa mesin sekaligus, agen akan memilih dua mesin. (Untuk mengoptimalkan performa pencadangan, agen berusaha mencocokkan mesin yang disimpan di penyimpanan yang berbeda.) Setelah salah satu dari dua pencadangan selesai, agen akan memilih mesin ketiga dan seterusnya.

  Anda dapat mengubah jumlah mesin virtual agar agen dapat mencadangkan secara bersamaan. Nilai maksimalnya adalah 10. Namun, jika agen menjalankan beberapa rencana proteksi yang tumpang tindih saat bersamaan, jumlah yang ditentukan dalam opsi mereka akan ditambahkan. Anda dapat membatasi jumlah total mesin virtual dari agen yang dapat mencadangkan secara simultan, berapa pun jumlah rencana proteksi yang sedang berjalan.

  Pencadangan mesin fisik akan dimulai sesuai jadwal.

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 efektif untuk skema pencadangan **Harian penuh**; **Mingguan penuh, Diferensial mingguan, Harian inkremental,**; **Bulanan penuh, Mingguan diferensial, Harian inkremental**

(GFS), dan **Kustom**.

Opsi ini memungkinkan Anda memilih metode pembagian cadangan besar ke file yang lebih kecil.

Nilai prasetelnya adalah: **Otomatis**.

Pengaturan berikut tersedia:

- **Otomatis**
  Cadangan akan dibagi jika melebihi ukuran file maksimum yang didukung oleh sistem file.
- **Ukuran tetap**
  Masukkan ukuran file yang diinginkan atau pilih dari daftar drop-down.

Manajemen pita

Opsi ini efektif ketika tujuan pencadangannya adalah perangkat pita.

Aktifkan pemulihan file dari cadangan disk yang disimpan pada tape

Nilai prasetelnya adalah: **Dinonaktifkan**.

Jika kotak centang ini dipilih, pada setiap pencadangan, perangkat lunak akan membuat file tambahan pada hard disk mesin tempat perangkat pita terpasang. Pemulihan file dari pencadangan disk dimungkinkan selama file tambahan ini masih utuh. File tersebut akan dihapus secara otomatis ketika setiap pita yang menyimpan cadangan dihilangkan, dihapus atau ditimpa.

Lokasi file tambahan adalah sebagai berikut:

- Di Windows XP dan Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**.
- Di Windows 7 dan versi Windows yang lebih baru: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**.
- Di Linux: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**.

Ruang yang diisi oleh file tambahan ini tergantung pada jumlah file di masing-masing pencadangan. Untuk pencadangan penuh disk yang berisi sekitar 20.000 file (pencadangan stasiun kerja disk tipikal), file tambahan akan mengisi sekitar 150 MB. Pencadangan penuh server yang berisi 250.000 file dapat menghasilkan sekitar 700 MB file tambahan. Jadi, jika Anda yakin bahwa Anda tidak perlu memulihkan setiap file, Anda dapat membiarkan kotak centang tidak tercentang untuk menghemat ruang disk.

Jika file tambahan tidak dibuat saat pencadangan, atau telah dihapus, Anda masih dapat membuatnya dengan memindai ulang pita tempat pencadangan disimpan.

Pindahkan tape kembali ke slot setelah setiap cadangan berhasil dari setiap mesin

Nilai prasetelnya adalah: **Aktif**.

Jika Anda menonaktifkan opsi ini, pita akan tetap berada di drive setelah operasi menggunakan pita selesai. Jika tidak, perangkat lunak akan memindahkan pita kembali ke slot di mana pita berada sebelum operasi. Jika, sesuai dengan rencana proteksi, operasi lain dilakukan setelah pencadangan (seperti validasi pencadangan atau replikasi ke lokasi lain), pita akan dikembalikan ke slot setelah operasi ini selesai.

Jika kedua opsi ini dan **Keluarkan pita setelah setiap pencadangan setiap mesin yang berhasil** diaktifkan, pita itu akan dikeluarkan.

Keluarkan tape setelah setiap cadangan berhasil dari setiap mesin

Nilai prasetelnya adalah: **Dinonaktifkan**.

Ketika kotak centang ini dipilih, perangkat lunak akan mengeluarkan pita setelah setiap pencadangan setiap mesin berhasil. Jika, sesuai dengan rencana proteksi, operasi lain dilakukan setelah pencadangan (seperti validasi pencadangan atau replikasi ke lokasi lain), pita akan dikeluarkan setelah operasi ini selesai.

Timpa tape pada drive tape yang berdiri sendiri ketika membuat cadangan penuh

Nilai prasetelnya adalah: **Dinonaktifkan**.

Opsi ini hanya berlaku untuk drive pita yang berdiri sendiri. Ketika opsi ini diaktifkan, pita yang dimasukkan ke drive akan ditimpa setiap kali pencadangan penuh dibuat.

Gunakan alat rekaman dan drive berikut

Opsi ini memungkinkan Anda menentukan alat rekaman dan tape drive yang akan digunakan oleh rencana proteksi.

Pool pita berisi pita dari semua alat rekaman yang terhubung ke mesin, baik simpul penyimpanan maupun mesin tempat agen perlindungan diinstal, atau keduanya. Ketika Anda memilih pool pita sebagai lokasi pencadangan, Anda secara tidak langsung memilih mesin lokasi perangkat pita terpasang. Secara default, pencadangan dapat ditulis ke pita melalui drive pita apa pun pada perangkat pita yang terpasang pada mesin tersebut. Jika beberapa perangkat atau drive hilang atau tidak beroperasi, rencana proteksi akan menggunakan yang tersedia.

Anda dapat mengklik **Hanya perangkat dan drive yang dipilih**, lalu pilih pita drive dan perangkat dari daftar. Dengan memilih seluruh perangkat, Anda akan memilih semua drive-nya. Artinya, semua drive ini dapat digunakan oleh rencana proteksi. Jika perangkat atau drive yang dipilih hilang atau tidak beroperasi, dan tidak ada perangkat lain yang dipilih, pencadangan akan gagal.

Dengan menggunakan opsi ini, Anda dapat mengontrol pencadangan yang dilakukan oleh beberapa agen ke pustaka pita besar dengan beberapa drive. Misalnya, pencadangan server file besar atau berbagi file mungkin tidak dimulai jika beberapa agen mencadangkan mesin mereka selama jendela pencadangan yang sama, karena agen mengisi semua drive. Jika Anda mengizinkan agen untuk

menggunakan, katakanlah, drive 2 dan 3, drive 1 akan disimpan untuk agen yang mencadangkan bagian.

Multistreaming

Nilai prasetelnya adalah: **Dinonaktifkan**.

Multistreaming memungkinkan Anda membagi data dari satu agen menjadi beberapa stream, lalu menulis stream tersebut ke pita yang berbeda dalam waktu bersamaan. Hal ini menghasilkan pencadangan yang lebih cepat dan berguna khususnya ketika agen memiliki throughput yang lebih tinggi daripada tape drive.

Kotak centang **Multistreaming** hanya akan tersedia jika Anda memilih lebih dari satu tape drive pada opsi **Hanya perangkat dan drive yang dipilih**. Jumlah drive yang dipilih sama dengan jumlah streaming dalam waktu bersamaan dari suatu agen. Jika terdapat drive yang tidak tersedia ketika pencadangan dimulai, cadangan ini akan gagal.

Untuk memulihkan pencadangan multistreaming atau multiplexing dan multistreaming, Anda memerlukan minimal jumlah drive yang sama yang digunakan untuk membuat cadangan ini.

Anda tidak dapat mengubah pengaturan multistreaming pada rencana proteksi yang sudah ada. Untuk menggunakan pengaturan lain guna mengubah tape drive yang dipilih, buat rencana proteksi baru.

Multistreaming tersedia baik pada tape drive yang terpasang secara lokal maupun tape drive yang terpasang pada simpul penyimpanan.

Multiplexing

Nilai prasetelnya adalah: **Dinonaktifkan**.

Multiplexing memungkinkan Anda menulis stream data dari beberapa agen ke pita tunggal. Hal ini menghasilkan pemanfaatan yang lebih baik dari tape drive cepat. Secara default, faktor multiplexing—yaitu, jumlah agen yang mengirimkan data ke pita tunggal—diatur ke dua. Anda dapat menambahkannya hingga sepuluh.

Multiplexing berguna untuk lingkungan yang luas dengan banyak operasi pencadangan. Multiplexing tidak meningkatkan performa pencadangan tunggal.

Untuk mencapai pencadagan paling cepat pada lingkungan yang luas, Anda perlu menganalisis throughput agen, jaringan, dan tape drive Anda. Kemudian, atur faktor multiplexing yangs esuai, tanpa multiplexing berlebih. Misalnya, jika agen Anda memberikan data pada 70 Mbit/s, tape drive akan menulis pada 250 Mbit/s, dan tidak ada penyempitan pada jaringan Anda, mengatur faktor multiplexing ke tiga. Faktor multiplexing yang diatur ke empat akan menyebabkan multiplexing berlebih dan mengurangi kinerja pencadangan. Umumnya, faktor multiplexing diatur antara dua dan lima.

Karena strukturnya, pencadangan dengan multiplexing lebih lambat untuk dipulihkan. Makin besar faktor multiplexing, makin lambar pemulihannya. Pemulihan bersamaan dari beberapa pencadangan yang ditulis pada pita multiplexing tunggal tidak didukung.

Anda dapat memilih satu atau beberapa tape drive untuk multiplexing, atau menggunakan opsi multiplexing dengan tape drive yang tersedia. Multiplexing ini tidak tersedia untuk tape drive yang terpasang secara lokal.

Anda tidak dapat mengubah pengaturan multistreaming pada rencana proteksi yang sudah ada. Untuk menggunakan pengaturan yang berbeda, buat rencana proteksi baru.

Pada rencana proteksi, kombinasi multistreaming dan multiplexing berikut dapat diterapkan:

- **Opsi multistreaming dan multiplexing akan dihapus.**
  Setiap agen mengirimkan data ke satu tape drive.
- **Hanya opsi multistreaming yang dipilih.**
  Setiap agen mengirimkan data ke minimal dua tape drive secara bersamaan.
- **Hanya opsi multiplexing yang dipilih.**
  Setiap agen mengirimkan data ke satu tape drive yang menerima stream dari beberapa agen secara bersamaan. Jumlah maksimum stream yang dapat diterima tape drive diatur di rencana proteksi dan tidak dapat diubah selama pengoperasian.
- **Opsi multistreaming dan multiplexing akan dipilih.**
  Setiap agen mengirimkan data ke minimal dua tape drive yang menerima stream dari beberapa agen secara bersamaan.

Tape drive hanya dapat menulis satu jenis cadangan pada satu waktu, baik multiplexing maupun bukan multiplexing, bergantung pada rencana proteksi mana yang dimulai terlebih dahulu.

Gunakan set tape di dalam pool tape yang dipilih untuk cadangan

Nilai prasetelnya adalah: **Dinonaktifkan**.

Pita dalam satu grup dapat dikelompokkan ke dalam **set pita**.

Jika Anda membiarkan opsi ini nonaktif, data akan dicadangkan di semua pita yang dimiliki pool. Jika opsi ini diaktifkan, Anda dapat memisahkan pencadangan sesuai dengan aturan yang telah ditentukan atau kustom.

- **Gunakan set pita terpisah untuk setiap** (pilih aturan: **Jenis pencadangan**, **Jenis perangkat**, **Nama perangkat**, **Hari dalam sebulan**, **Hari dalam seminggu**, **Bulan dalam setahun**, **Tahun**, **Tanggal**)
  Jika varian ini dipilih, Anda dapat mengatur set pita sesuai dengan aturan yang telah ditentukan. Misalnya, Anda dapat memiliki set pita terpisah untuk setiap hari dalam seminggu atau menyimpan pencadangan masing-masing mesin pada set pita terpisah.
- **Tentukan aturan khusus untuk set pita**

Jika varian ini dipilih, tentukan aturan Anda sendiri untuk mengatur set pita. Aturan dapat berisi variabel berikut:

Variabel sintaks	Variabel deskripsi	Nilai yang tersedia
`[Resource Name]`	Cadangan setiap mesin akan disimpan pada set pita terpisah.	Nama mesin yang terdaftar di server manajemen.
`[Backup Type]`	Cadangan penuh, inkremental, dan diferensial akan disimpan pada set pita terpisah.	`full`, `inc`, `diff`
`[Resource Type]`	Cadangan mesin dari setiap jenis akan disimpan pada set pita terpisah.	`Server essentials`, `Server`, `Workstation`, `Physical machine`, `VMware Virtual Machine`, `Virtual-PC Virtual Machine`, `Virtual Server Virtual Machine`, `Hyper-V Virtual Machine`, `Parallels Virtual Machine`, `XEN Virtual Machine`, `KVM Virtual Machine`, `RHEV Virtual Machine`, `Parallels Cloud Virtual Machine`
`[Day]`	Cadangan yang dibuat pada setiap hari dalam sebulan akan disimpan pada set pita terpisah.	`01`, `02`, `03`, ..., `31`
`[Weekday]`	Cadangan yang dibuat pada setiap hari dalam seminggu akan disimpan pada set pita terpisah.	`Sunday`, `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday`
`[Month]`	Cadangan yang dibuat selama setiap bulan dalam setahun akan disimpan pada set pita terpisah.	`January`, `February`, `March`, `April`, `May`, `June`, `July`, `August`, `September`, `October`, `November`, `December`
`[Year]`	Cadangan yang dibuat setiap tahun akan disimpan pada set pita terpisah.	`2017`, `2018`, ...

- Misalnya, jika Anda menetapkan aturan sebagai `[Resource Name]-[Backup Type]`, Anda akan memiliki satu set pita terpisah untuk setiap cadangan penuh, inkremental, dan diferensial dari setiap mesin yang digunakan untuk menerapkan rencana proteksi.

Anda juga dapat menentukan set pita untuk masing-masing pita. Dalam hal ini, perangkat lunak akan terlebih dahulu menulis pencadangan pada pita yang nilai set pitanya sesuai dengan nilai ekspresi yang ditentukan dalam rencana proteksi. Kemudian, jika perlu, pita lain dari pool yang sama akan diambil. Setelah itu, jika pool dapat diisi kembali, pita dari pool **Pita bebas** akan digunakan.

Misalnya, jika Anda menentukan set pita `Monday` untuk Pita 1, `Tuesday` untuk Pita 2, dst. dan menentukan `[Weekday]` dalam opsi pencadangan, pita yang sesuai akan digunakan pada masing-masing hari dalam seminggu.

Penanganan kegagalan tugas

Pilihan ini menentukan perilaku program ketika eksekusi rencana proteksi yang dijadwalkan gagal. 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.

Nilai prasetelnya adalah: **Dinonaktifkan**.

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 syarat ini, lihat "Syarat untuk memulai".

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.

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 Volume Shadow Copy (VSS)

Opsi ini hanya efektif untuk sistem operasi Windows.

Opsi ini menentukan apakah penyedia Layanan Volume Shadow Copy (VSS) harus memberitahukan aplikasi yang mendukung VSS bahwa pencadangan akan segera dimulai. Cara ini akan memastikan

status konsisten 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.

Nilai prasetelnya adalah: **Aktif**. **Memilih penyedia snapshot secara otomatis**.

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 sarankan untuk memilih opsi ini ketika mencadangkan server aplikasi (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint, atau Active Directory).

Nonaktifkan opsi ini jika database Anda tidak kompatibel dengan VSS. Snapshot diambil lebih cepat, namun konsistensi data dari aplikasi yang transaksinya belum selesai pada saat mengambil snapshot tidak dapat dijamin. Anda dapat menggunakan Perintah pengambilan data Pra/Pasca untuk memastikan data yang dicadangkan dalam status konsisten. Misalnya, tentukan perintah pengambilan pra-data yang akan menunda database dan melakukan flush semua cache untuk memastikan semua transaksi selesai; dan tentukan perintah pengambilan pasca-data yang akan melanjutkan operasi database setelah snapshot diambil.

Catatan
Jika opsi ini diaktifkan, 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.

Aktifkan cadangan penuh VSS

Jika opsi ini diaktifkan, log dari Microsoft Exchange Server dan aplikasi yang mendukung VSS lainnya (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.

Mengaktifkan opsi ini tidak mengakibatkan pemotongan log Microsoft SQL Server. Untuk memotong log SQL Server setelah pencadangan, aktifkan opsi pencadangan Pemotongan Log.

Layanan Volume Shadow Copy (VSS) untuk mesin virtual

Opsi ini menentukan apakah snapshot yang didiamkan dari mesin virtual akan diambil. Untuk mengambil snapshot yang didiamkan, perangkat lunak cadangan menerapkan VSS di dalam mesin virtual menggunakan VMware Tools atau Layanan Integrasi Hyper-V.

Nilai prasetelnya adalah: **Aktif**.

Jika opsi ini diaktifkan, transaksi semua aplikasi yang sadar VSS yang berjalan pada mesin virtual diselesaikan sebelum snapshot diambil. Jika snapshot yang didiamkan gagal setelah sejumlah percobaan ulang yang ditentukan dalam opsi "Penanganan eror", dan pencadangan aplikasi dinonaktifkan, snapshot non-didiamkan akan diambil. Jika pencadangan aplikasi diaktifkan, pencadangan akan gagal.

Jika opsi ini dinonaktifkan, snapshot non-didiamkan akan diambil. Mesin virtual akan dicadangkan dalam status konsisten crash. Kami menyarankan agar Anda menyimpan opsi ini yang diaktifkan setiap saat, bahkan untuk mesin virtual yang tidak menjalankan aplikasi sadar VSS. Jika tidak, konsistensi sistem file tidak dapat dijamin di dalam pencadangan yang diambil.

Catatan
Opsi ini tidak memengaruhi mesin virtual Scale Computing HC3. Bagi mereka, pendiaman bergantung pada apakah alat bantu Scale diinstal pada mesin virtual atau tidak.

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.

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.

Apa yang dipulihkan	Metode pemulihan
Mesin fisik (Windows atau Linux)	Menggunakan antarmuka web Menggunakan media yang dapat di-boot
Mesin fisik (Mac)	Menggunakan media yang dapat di-boot
Mesin virtual (VMware, Hyper-V atau Scale Computing HC3)	Menggunakan antarmuka web Menggunakan media yang dapat di-boot
Konfigurasi ESXi	Menggunakan media yang dapat di-boot
File/folder	Menggunakan antarmuka web Mengunduh file dari penyimpanan awan Menggunakan media yang dapat di-boot Mengekstrak file dari pencadangan lokal
Status sistem	Menggunakan antarmuka web
Database SQL	Menggunakan antarmuka web
Basis data Exchange	Menggunakan antarmuka web
Kotak surat Exchange	Menggunakan antarmuka web
Kotak surat Microsoft 365	Menggunakan antarmuka web
Database Oracle	Menggunakan alat Oracle Explorer

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

Gambar yang dicadangkan dari sistem operasi mungkin terinfeksi malware dan dapat menginfeksi ulang mesin tempat ia dipulihkan.

Pemulihan aman memungkinkan Anda untuk mencegah terulangnya infeksi tersebut dengan menggunakan pemindaian antimalware dan penghapusan malware terintegrasi selama proses pemulihan.

Pembatasan:

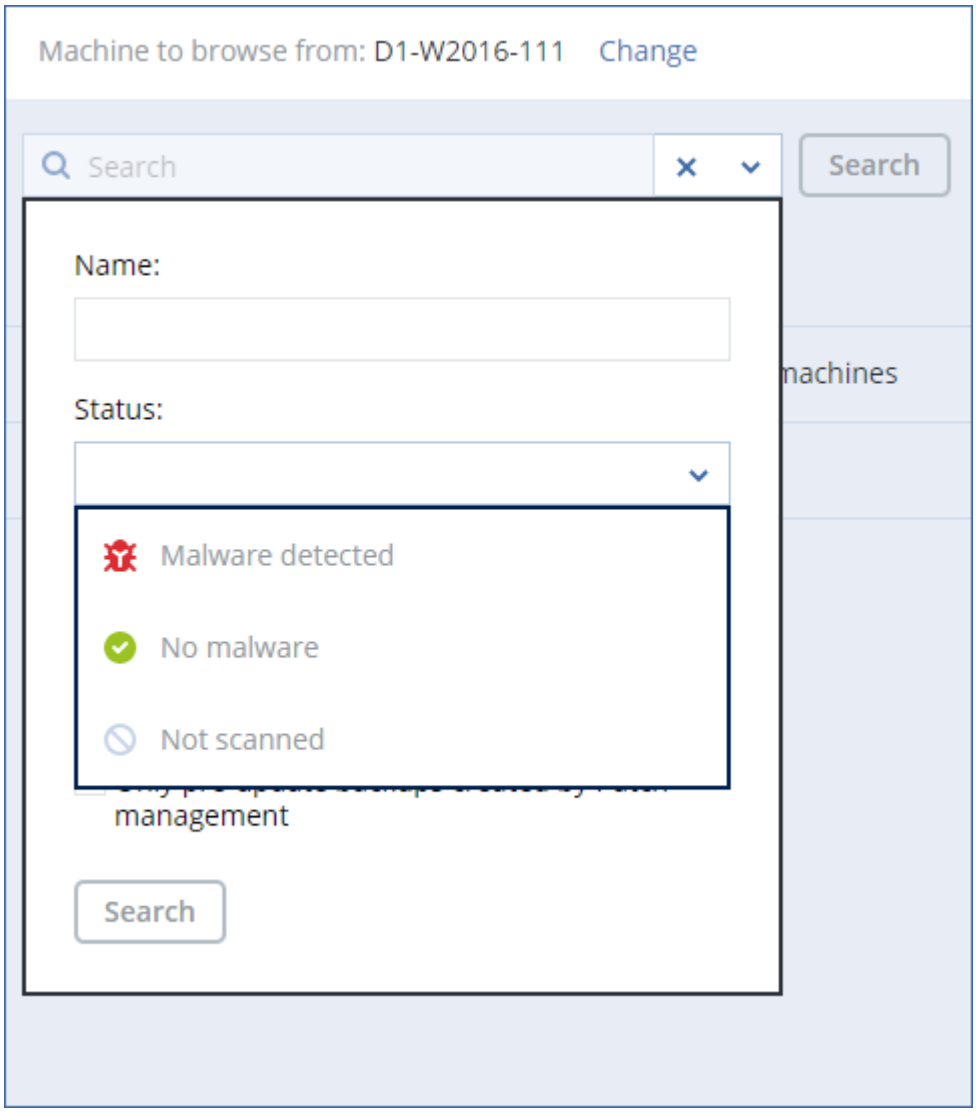
- Pemulihan aman hanya didukung untuk mesin Windows fisik dan virtual dengan Agen untuk Windows diinstal di dalamnya.
- Hanya cadangan jenis **Seluruh mesin** atau **Disk/volume** yang didukung.
- Hanya volume dengan sistem file NTFS yang didukung. Partisi non-NTFS akan dipulihkan tanpa pemindaian malware.
- Pemulihan aman tidak didukung untuk Cadangan perlindungan data berkelanjutan (CDP). Mesin akan dipulihkan berdasarkan cadangan reguler terakhir, tanpa data dalam cadangan CDP. Untuk memulihkan data CDP, jalankan pemulihan **File/folder**.

Cara kerjanya

Jika Anda mengaktifkan opsi Pemulihan aman selama proses pemulihan, sistem akan melakukan hal berikut:

1. Memindai malware pada cadangan profil dan menandai file yang terinfeksi. Salah satu dari status berikut ini ditetapkan ke cadangan:
   - **Tidak ada malware** – Tidak ada malware yang ditemukan di cadangan selama pemindaian.
   - **Malware terdeteksi** – Malware ditemukan di cadangan selama pemindaian.
   - **Tidak dipindai** – Cadangan tidak dipindai untuk menemukan malware.
2. Pulihkan cadangan ke mesin yang dipilih.
3. Hapus malware yang terdeteksi.

Anda dapat memfilter cadangan menggunakan parameter **Status**.



Membuat media yang dapat di-boot

Media yang dapat di-boot adalah CD, DVD, USB flash drive, atau media yang dapat dilepas lainnya yang memungkinkan Anda untuk menjalankan agen tanpa bantuan sistem operasi. Tujuan utama media yang dapat di-boot adalah untuk memulihkan sistem operasi yang tidak dapat memulai.

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.

Untuk membuat media yang dapat di-boot di Windows atau Linux

1. Unduh file ISO media yang dapat diboot. Untuk mengunduh file, klik ikon akun di sudut kanan atas > **Unduhan** > **Media yang dapat di-boot**.
2. Lakukan yang berikut ini:

- Salin CD/DVD menggunakan file ISO.
- Buat USB flash drive yang dapat di-boot menggunakan file ISO dan salah satu alat gratis yang tersedia secara online.

  Gunakan `ISO to USB` atau `RUFUS` jika Anda perlu mem-boot mesin UEFI, `Win32DiskImager` untuk mesin BIOS. Di Linux, Anda dapat menggunakan utilitas `dd`.
- Hubungkan file ISO sebagai drive CD/DVD ke mesin virtual yang ingin Anda pulihkan.

Atau, Anda dapat membuat media yang dapat di-boot menggunakan Pembangun Media yang Dapat Di-boot.

Untuk membuat media 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.

Memulihkan mesin

Memulihkan mesin fisik

Bagian ini menjelaskan cara memulihkan mesin fisik menggunakan konsol web Cyber Protect.

Gunakan media yang dapat di-boot, bukan konsol web Cyber Protect jika Anda perlu memulihkan salah satu dari berikut ini:

- Sistem operasi macOS
- Sistem operasi apa pun pada bare metal atau mesin offline
- Struktur volume logis (volume dibuat oleh Logical Volume Manager di Linux). Media memungkinkan Anda membuat ulang struktur volume logis secara otomatis.

Pemulihan sistem operasi dan pemulihan volume yang terenkripsi dengan BitLocker atau CheckPoint memerlukan mulai ulang. Untuk informasi lebih lanjut, lihat "Pemulihan dengan mulai kembali" (hlm. 314).

Untuk memulihkan mesin fisik

1. Pilih mesin yang dicadangkan.
2. Klik **Pemulihan**.

3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.

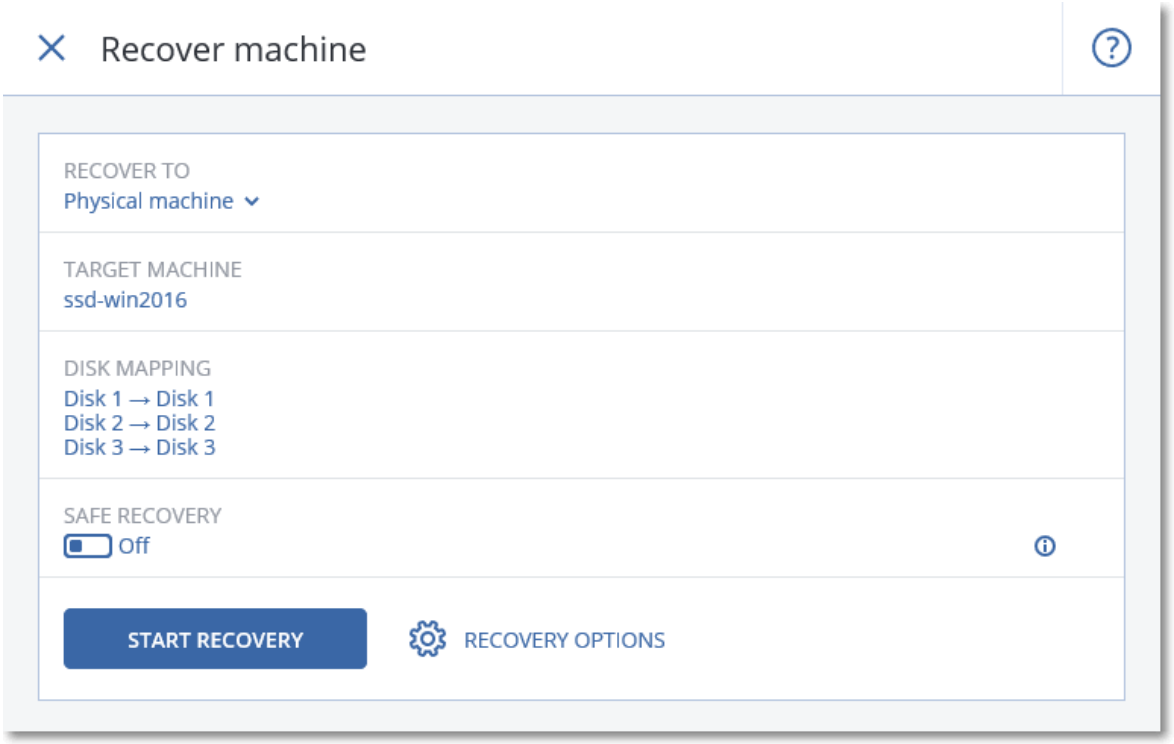
   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Lakukan yang berikut ini:

   - 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**.

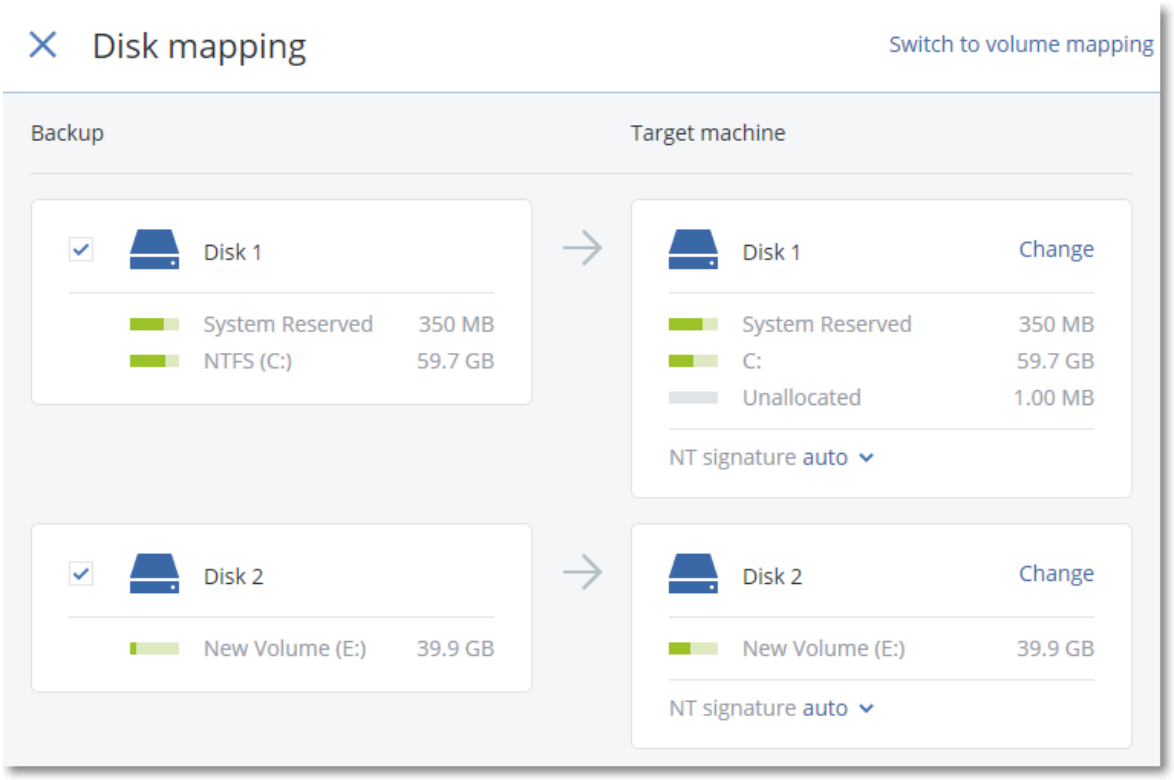
   Perangkat lunak memetakan secara otomatis disk dari cadangan ke disk mesin target.

   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 disk** untuk memetakan ulang disk secara manual.

   Selain itu, di bagian pemetaan, Anda dapat memilih setiap disk atau volume untuk pemulihan. Anda dapat beralih antara memulihkan disk dan volume menggunakan tautan **Alihkan ke...** di sudut kanan atas.



6. [Opsional] Aktifkan switch **Pemulihan aman** guna memindai cadangan terhadap malware. Jika terdeteksi, malware akan ditandai di cadangan dan langsung dihapus setelah proses pemulihan selesai.
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**.

Memulihkan mesin fisik ke mesin virtual

Anda dapat memulihkan cadangan mesin fisik ke mesin virtual.

Memulihkan ke mesin virtual mungkin dilakukan jika setidaknya satu agen untuk hypervisor target yang relevan dipasang di lingkungan Anda dan terdaftar di server manajemen. Misalnya, pemulihan ke VMware ESXi mengharuskan Agen untuk VMware diinstal di lingkungan dan didaftarkan di server manajemen.

Beberapa opsi hanya tersedia dengan penyebaran awan.

Untuk informasi selengkapnya tentang jalur yang didukung untuk migrasi mesin fisik ke virtual (P2V), lihat "Migrasi mesin" (hlm. 498).

Catatan
Anda tidak dapat memulihkan cadangan mesin fisik macOS sebagai mesin virtual.

Untuk memulihkan mesin fisik sebagai mesin virtual

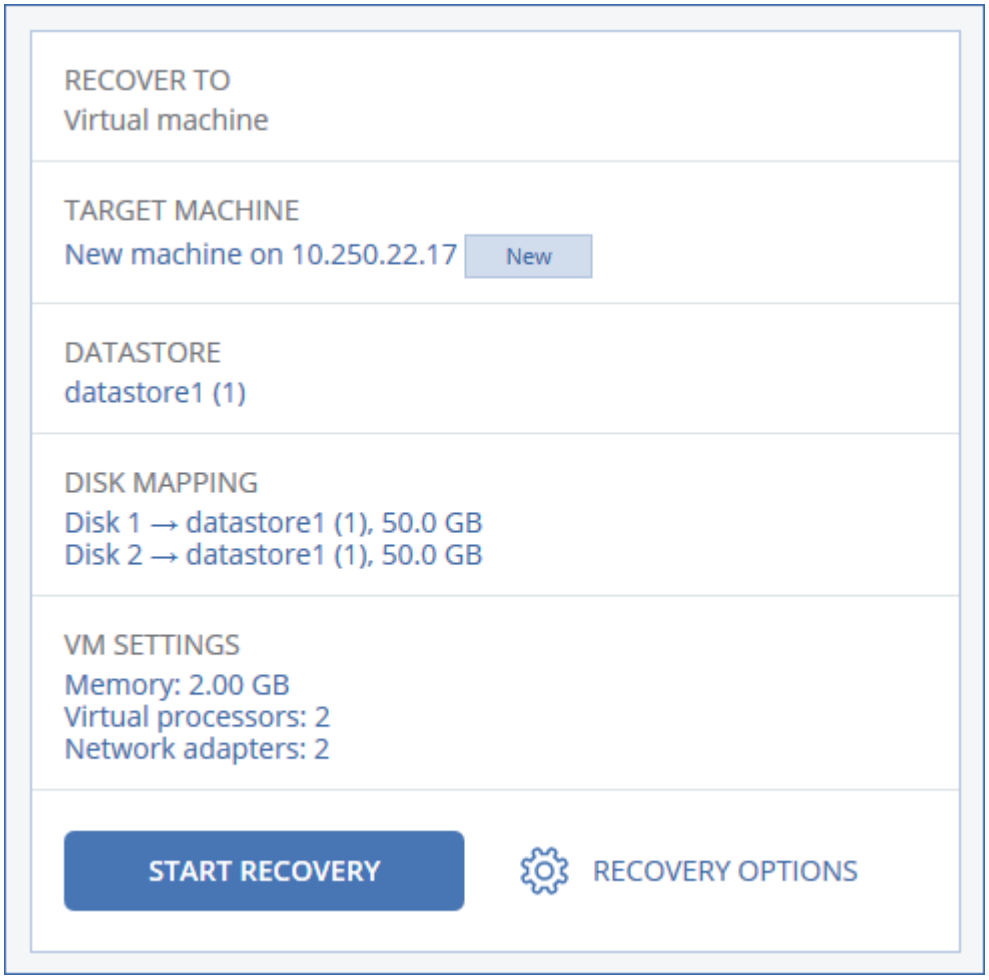
1. Pilih mesin yang dicadangkan.
2. Klik **Pemulihan**.
3. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
   Jika mesin sedang offline, titik pemulihan tidak ditampilkan. Lakukan yang berikut ini:
   - Jika lokasi pencadangan adalah awan atau penyimpanan bersama (artinya, agen lain dapat mengaksesnya), klik **Pilih mesin**, pilih mesin yang online, lalu pilih titik pemulihan.
   - Pilih titik pemulihan pada tab Penyimpanan cadangan.
   - Pulihkan mesin seperti yang dijelaskan di "Memulihkan disk dan volume dengan menggunakan media yang dapat di-boot" (hlm. 315).
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 di lingkungan Anda dan terdaftar di server manajemen.

   b. Pilih apakah akan Anda ingin melakukan pemulihan ke mesin baru atau mesin yang sudah ada. Opsi mesin baru lebih disukai karena tidak mengharuskan konfigurasi disk mesin target sama persis dengan konfigurasi disk di 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**, lalu pilih **Cara**. Sebagai pilihan, Anda dapat mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual.
8. [Opsional] [Saat memulihkan ke mesin baru] Konfigurasikan 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 memilih penyimpanan data (penyimpanan), antarmuka, dan mode provisi untuk setiap disk virtual, klik **Pemetaan disk**. Di bagian pemetaan, Anda dapat memilih setiap disk untuk pemulihan.

Catatan
Anda tidak dapat mengubah pengaturan ini jika 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**.

- [Tersedia untuk VMware ESXi, Hyper-V, Virtuozzo, dan Red Hat Virtualization/oVirt] Untuk mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual, klik **pengaturan VM**.



9. Klik **Mulai pemulihan**.
10. [Ketika memulihkan ke mesin virtual yang ada] Konfirmasi bahwa Anda ingin menimpa disk.

Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

Memulihkan mesin virtual

Anda dapat memulihkan cadangan mesin virtual ke mesin fisik atau ke mesin virtual lainnya.

Memulihkan ke mesin virtual mungkin dilakukan jika setidaknya satu agen untuk hypervisor target yang relevan dipasang di lingkungan Anda dan terdaftar di server manajemen. Misalnya, pemulihan ke VMware ESXi mengharuskan Agen untuk VMware diinstal di lingkungan dan didaftarkan di server manajemen.

Beberapa opsi hanya tersedia dengan penyebaran awan.

Untuk informasi selengkapnya tentang jalur yang didukung untuk migrasi mesin virtual-ke-fisik (V2P) atau virtual-ke-virtual (V2V), lihat "Migrasi mesin" (hlm. 498).

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.

Penting
Mesin virtual harus dihentikan saat Anda memulihkan mesin lain ke dalamnya. 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**).

Untuk memulihkan mesin virtual

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. [Saat memulihkan ke mesin fisik] Di **Pulihkan ke**, pilih **Mesin fisik**.
   Pemulihan ke mesin fisik mungkin dilakukan hanya jika konfigurasi disk mesin target sama persis dengan konfigurasi disk dalam cadangan. Jika hal ini terjadi, lanjutkan ke langkah 4 di "Memulihkan mesin fisik" (hlm. 307). Jika tidak, kami menyarankan Anda melakukan migrasi virtual-ke-fisik (V2P) dengan menggunakan media yang dapat di-boot.
4. [Opsional] Secara default, mesin asli dipilih sebagai mesin target. Untuk memulihkan ke mesin virtual lain, klik **Mesin target**, lalu lakukan hal berikut:
   a. Pilih hypervisor.

      Catatan
      Setidaknya satu agen untuk hypervisor tersebut harus diinstal di lingkungan Anda dan terdaftar di server manajemen.

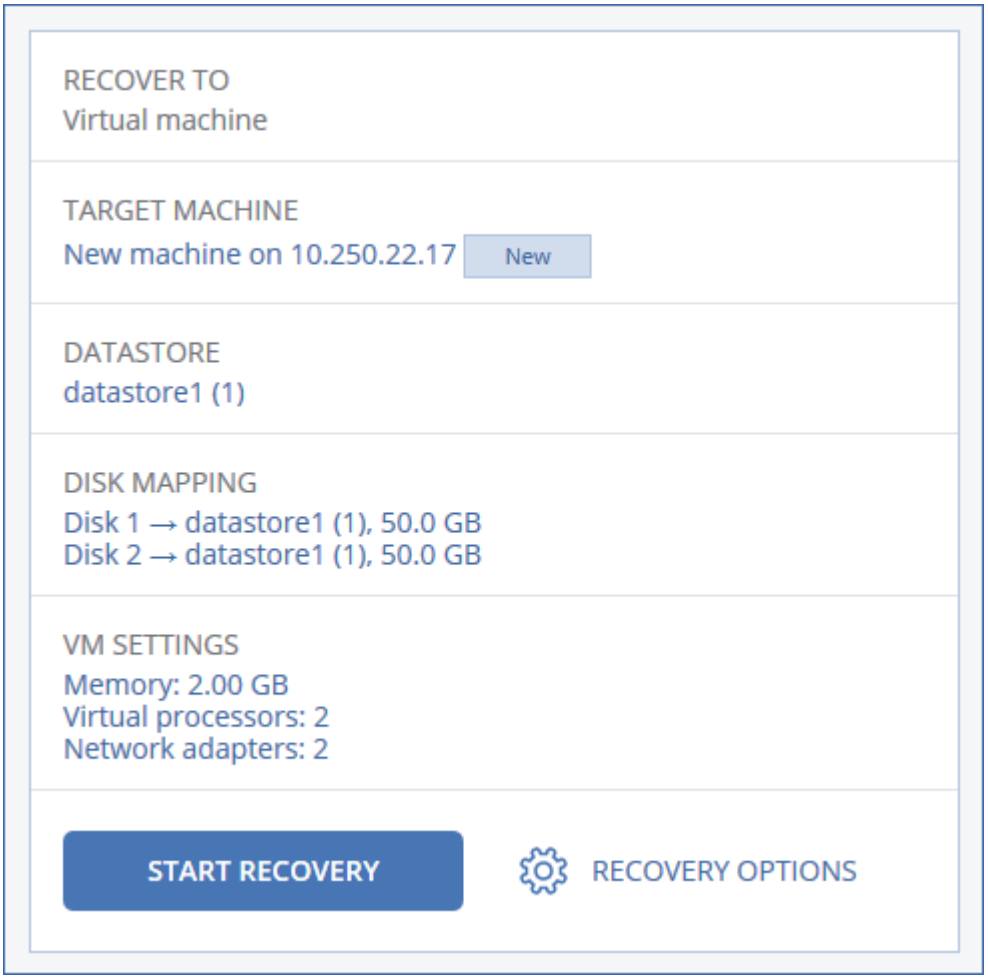
   b. Pilih apakah akan Anda ingin melakukan pemulihan ke mesin baru atau mesin yang sudah ada.
   c. Pilih host, lalu tentukan nama mesin yang baru atau pilih mesin target yang sudah ada.
   d. Klik **OK**.

5. [Untuk Virtuozzo Hybrid Infrastructure] Klik **Pengaturan VM**, lalu pilih **Cara**. Sebagai pilihan, Anda dapat mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual.
6. [Opsional] [Saat memulihkan ke mesin baru] Konfigurasikan 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 memilih penyimpanan data (penyimpanan), antarmuka, dan mode provisi untuk setiap disk virtual, klik **Pemetaan disk**. Di bagian pemetaan, Anda dapat memilih setiap disk untuk pemulihan.

     Catatan
     Anda tidak dapat mengubah pengaturan ini jika 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**.

   - [Tersedia untuk VMware ESXi, Hyper-V, Virtuozzo, dan Red Hat Virtualization/oVirt] Untuk mengubah ukuran memori, jumlah prosesor, dan koneksi jaringan mesin virtual, klik

pengaturan VM.



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**.

Pemulihan dengan mulai kembali

Pengaktifan kembali diperlukan saat Anda memulihkan berikut ini:

- Sistem operasi
- Volume terenkripsi BitLocker atau CheckPoint

Penting
Volume terenkripsi yang dicadangkan dipulihkan menjadi tidak terenkripsi.

Persyaratan

- Pemulihan volume terenkripsi memerlukan adanya volume tidak terenkripsi di mesin yang sama, dan volume ini memiliki setidaknya ruang bebas sebesar 1 GB. Jika tidak, pemulihan akan gagal.

- Pemulihan 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.

Penyelesaian masalah

Jika pemulihan gagal dan mesin Anda dimulai ulang dengan pesan kesalahan `Tidak bisa mendapatkan file dari partisi`, nonaktifkan Boot Aman. Untuk informasi lebih lanjut tentang cara melakukannya, lihat Menonaktifkan Boot Aman di dokumentasi Microsoft.

Memulihkan disk dan volume dengan menggunakan media yang dapat di-boot

Untuk informasi tentang cara membuat media yang dapat di-boot, lihat "Membuat media yang dapat di-boot" (hlm. 306).

Untuk memulihkan disk atau volume dengan menggunakan media yang dapat di-boot

1. Boot mesin target menggunakan media yang dapat di-boot.
2. [Khusus untuk macOS] Jika Anda memulihkan volume berformat APFS ke mesin non-asli atau ke logam, buat kembali konfigurasi disk asli secara manual:
   a. Klik **Utilitas Disk**.
   b. Buat kembali konfigurasi disk asli. Petunjuknya dapat dilihat di https://support.apple.com/guide/disk-utility/welcome.
   c. Klik **Utilitas Disk** > **Keluar dari Utiltas Disk**.

   Catatan
   Mulai dari macOS 11 Big Sur, volume sistem tidak dapat dicadangkan dan dipulihkan. Untuk memulihkan sistem macOS yang dapat di-boot, Anda harus memulihkan Volume data, lalu menginstal macOS pada sistem tersebut.
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 dan port IP. Jika tidak, lewati langkah ini.
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.
   - Untuk memulihkan dari folder lokal atau jaringan, jelajahi folder di dalam **Folder lokal** atau

Folder jaringan.

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 **Cadangan konten**, pilih **Disk** atau **Volume**, lalu pilih item yang ingin Anda pulihkan. Klik **OK** untuk mengonfirmasi pilihan Anda.

   Penting
   Jika mesin yang dicadangkan memiliki disk dinamis atau volume logis (LVM), pilih **Volume**.

10. 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.

11. [Khusus untuk macOS] Untuk memulihkan volume Data dengan format APFS sebagai sistem macOS yang dapat di-boot, pada **bagian Instalasi macOS**, tetap pilih kotak centang **Instal macOS di volume Data macOS**.

    Setelah pemulihan, sistem akan di-boot ulang dan instalasi macOS akan dimulai secara otomatis. Anda memerlukan sambungan internet agar installer mengunduh file yang diperlukan.

    Jika Anda tidak ingin memulihkan volume Data dengan format APFSsebagai sistem yang dapat di-boot, hapus semua tanda pada kotak centang **Instal macOS di volume Data macOS**. Anda nantinya tetap bisa membuat volume ini dapat di-boot dengan menginstal macOS pada sistem secara manual.
12. [Hanya untuk 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.
    c. Konfirmasi pilihan Anda.
13. [Opsional] Klik **Opsi pemulihan** untuk menentukan pengaturan tambahan.
14. Klik **OK** untuk memulai pemulihan.

Menggunakan Pemulihan Universal

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 Pemulihan Universal untuk memperbarui driver dan modul yang sangat penting untuk mulai sistem operasi.

Pemulihan Universal berlaku untuk Windows dan Linux.

Untuk menerapkan Pemulihan Universal

1. Boot mesin dari media yang dapat di-boot.
2. Klik **Terapkan Pemulihan Universal**.
3. Jika ada beberapa sistem operasi pada mesin, pilih salah satu untuk menerapkan Pemulihan Universal.
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.

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 kemudianditransmisikanoleh 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.

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-2.6.16.60-0.21-default
  ```

- Tentukan salinan pada baris **initrd** pada konfigurasi pemuat boot GRUB.

Memulihkan beberapa file

Memulihkan file menggunakan antarmuka web

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 salah satu langkah berikut:

- [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 pencarian untuk mendapatkan daftar file dan folder yang diperlukan.

   Anda dapat menggunakan satu atau lebih karakter wildcard (* dan ?). Untuk detail tentang penggunaan wildcard, lihat "Filter file"

   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.
8. Klik **Pulihkan**.

   Di **Pulihkan ke**, Anda akan melihat salah satu dari pilihan berikut:

   - Mesin yang awalnya berisi file yang ingin Anda pulihkan (jika agen diinstal pada mesin ini).
   - Mesin tempat Agen untuk VMware, Agen untuk Hyper-V, atau Agen untuk Scale Computing HC3 diinstal (jika file berasal dari mesin virtual ESXi, Hyper-V, atau Scale Computing HC3).

   Ini adalah mesin target untuk pemulihan. Anda dapat memilih mesin lain, jika diperlukan.
9. Di **Jalur**, pilih tujuan pemulihan. Anda dapat memilih salah satu dari tindakan berikut:
   - Lokasi asli (ketika memulihkan ke mesin asli)
   - Folder lokal di mesin target

     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

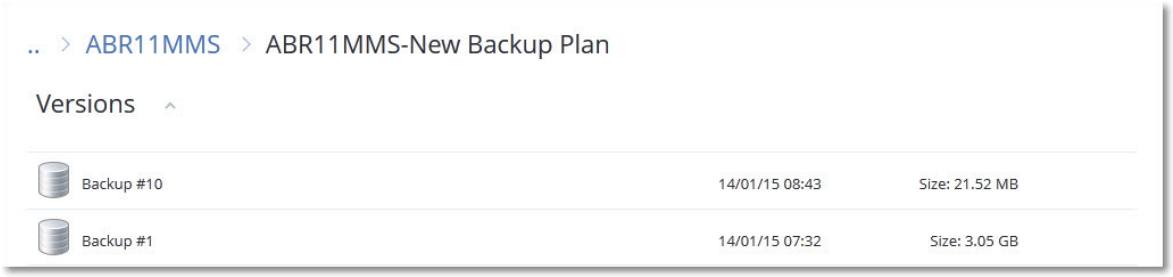
Anda dapat menjelajahi penyimpanan awan, melihat konten pencadangan, dan mengunduh file yang Anda butuhkan.

Pembatasan

- Pencadangan status sistem, database SQL, dan database Exchange tidak dapat diakses.
- Untuk pengalaman mengunduh yang lebih baik, jangan mengunduh lebih dari 100 MB sekaligus. Untuk mengambil data yang besar dari awan dengan cepat, gunakan prosedur pemulihan file.

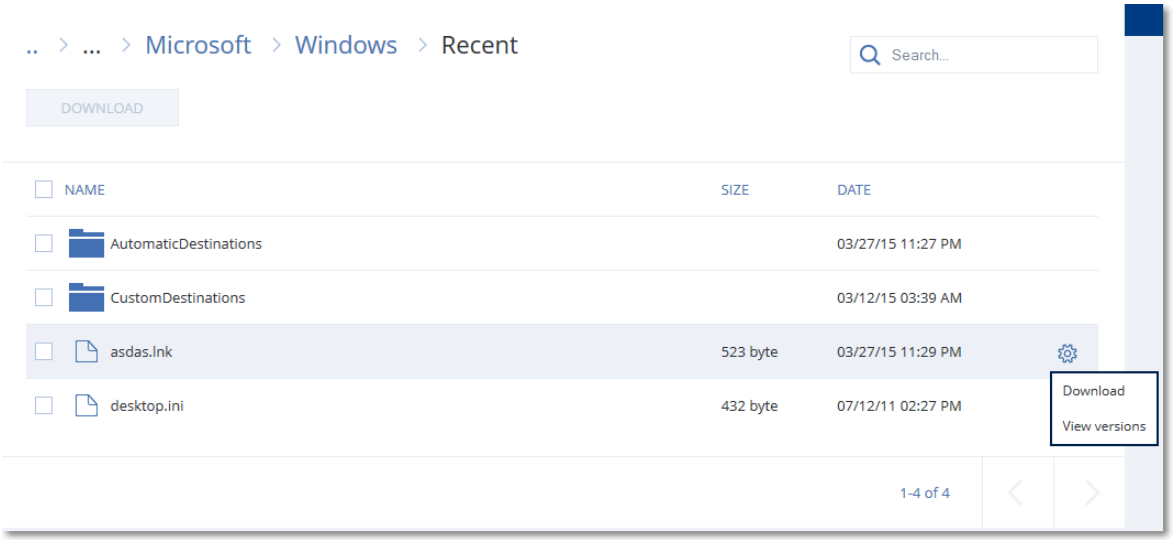
Untuk mengunduh file dari penyimpanan awan

1. Pilih mesin yang dicadangkan.
2. Klik **Pulihkan** > **Cara lain untuk memulihkan...** > **Unduh berkas**.
3. Masukkan kredensial untuk akun yang untuknya mesin yang dicadangkan ditetapkan.
4. [Saat menjelajahi cadangan tingkat disk] Pada **Versi**, klik cadangan yang berisi file yang ingin Anda pulihkan.



[Saat menjelajahi cadangan tingkat file] Anda dapat memilih tanggal dan waktu cadangan pada langkah berikutnya, di bawah ikon roda gigi yang berada di sebelah kanan file yang dipilih. Secara default, file akan dipulihkan dari cadangan terbaru.

5. Jelajahi folder yang diperlukan atau gunakan pencarian untuk mendapatkan daftar file yang diperlukan.



6. Pilih kotak centang untuk item yang perlu Anda pulihkan, lalu klik **Unduh**.

   Jika Anda memilih satu file, file akan diunduh apa adanya. Jika tidak, data yang dipilih akan diarsipkan ke dalam file .zip.
7. Pilih lokasi untuk menyimpan data, lalu klik **Simpan**.

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

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
- 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".
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.

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 dan port IP. Jika tidak, lewati langkah ini.
4. Di layar selamat datang, klik **Pulihkan**.
5. Klik **Pilih data**, lalu klik **Jelajahi**.
6. Tentukan lokasi cadangan:
   - Untuk memulihkan dari penyimpanan awan, pilih **Penyimpanan awan**. Masukkan kredensial untuk akun yang untuknya mesin yang dicadangkan ditetapkan.
   - Untuk memulihkan dari folder lokal atau jaringan, jelajahi folder di dalam **Folder lokal** atau **Folder jaringan**.

   Klik **OK** untuk mengonfirmasi pilihan Anda.
7. Pilih cadangan yang berisi data yang ingin Anda pulihkan. Jika diminta, ketik kata sandi untuk cadangan.
8. Di **Konten pencadangan**, pilih **Folder/file**.
9. Pilih data yang ingin Anda pulihkan. Klik **OK** untuk mengonfirmasi pilihan Anda.
10. Pada **Lokasi pemulihan**, tentukan foldernya. Secara opsional, Anda dapat melarang penimpaan versi file yang lebih baru atau mengecualikan beberapa file dari pemulihan.
11. [Opsional] Klik **Opsi pemulihan** untuk menentukan pengaturan tambahan.
12. Klik **OK** untuk memulai pemulihan.

Catatan
Lokasi Pita membutuhkan banyak ruang dan mungkin tidak sesuai dengan RAM saat Anda memindai ulang dan memulihkan dengan media yang dapat di-boot Linux dan media yang dapat di-boot WinPE. Untuk Linux, Anda harus menetapkan lokasi lain untuk menyimpan data pada disk atau membagikannya. Lihat Acronis Cyber Backup Lanjutan: Mengubah Folder TapeLocation (KB 27445). Untuk Windows PE, belum ada solusi untuk saat ini.

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.
- Agen perlindungan harus diinstal pada mesin tempat Anda menjelajahi cadangan.
- Sistem file yang dicadangkan harus berupa salah satu dari sistem berikut: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS, or HFS+.
- 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.

Memulihkan status sistem

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 yang dapat di-boot".

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.

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.

	Disk			**File**				**Mesin virtual**	**SQL dan Exchange**
	Windows	Linux	Media	Windows	Linux	macOS	Media	ESXi, Hyper-	Windows

			yang dapat di-boot				yang dapat di-boot	V, Scale Computing HC3	
Validasi cadangan	+	+	+	+	+	+	+	+	+
Mode boot	+	-	-	-	-	-	-	+	-
Tanggal dan waktu untuk file	-	-	-	+	+	+	+	-	-
Penanganan eror	+	+	+	+	+	+	+	+	+
Pengecualian file	-	-	-	+	+	+	+	-	-
Flashback	+	+	+	-	-	-	-	+	-
Pemulihan jalur lengkap	-	-	-	+	+	+	+	-	-
Titik mount	-	-	-	+	-	-	-	-	-
Performa	+	+	-	+	+	+	-	+	+
Perintah pra/pasca	+	+	-	+	+	+	-	+	+
Mengubah SID	+	-	-	-	-	-	-	-	-
Manajemen daya VM	-	-	-	-	-	-	-	+	-
"Manajemen pita" (hlm. 334) > Gunakan cache disk	-	-	-	+	+	+	-	-	-

untuk memperc epat pemuliha n									
Log event Windows	+	-	-	+	-	-	-	Hanya Hyper-V	+
Nyalakan setelah pemuliha n	-	-	-	-	-	-	+	-	-

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**.

Validasi akan menghitung checksum untuk tiap blok data yang tersimpan di cadangan. Satu-satunya pengecualian adalah validasi cadangan tingkat file yang terletak di penyimpanan awan. Cadangan ini divalidasi dengan cara memeriksa konsistensi informasi meta yang tersimpan dalam cadangan.

Validasi adalah proses yang membutuhkan waktu cukup lama, bahkan untuk sebuah cadangan inkremental atau diferensial, yang ukurannya lebih kecil. Hal ini dikarenakan operasi bukan hanya memvalidasi data yang hanya ditampung secara fisik di dalam cadangan, namun semua data yang dapat dipulihkan dengan memilih cadangan. Proses ini membutuhkan akses ke cadangan yang sebelumnya telah dibuat.

Catatan
Validasi tersedia untuk penyimpanan awan yang terletak di pusat data Acronis dan disediakan oleh mitra Acronis.

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.

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: **Aktif**.

Penanganan eror

Opsi ini memungkinkan Anda untuk menentukan cara menangani eror yang mungkin terjadi selama pemulihan.

Coba lagi, jika eror terjadi

Nilai prasetelnya adalah: **Aktif. 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.

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: **Aktif**.

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.

Jika opsi ini diaktifkan, hanya perbedaan antara data dalam cadangan dan disk target yang akan dipulihkan. Opsi mempercepat pemulihan data ke disk yang sama seperti yang dicadangkan, terutama jika tata letak volume disk tidak berubah. Data dibandingkan pada tingkat blok.

Untuk mesin fisik, membandingkan data pada level blok adalah operasi yang memakan waktu. Jika koneksi ke penyimpanan cadangan cepat, waktu yang diperlukan untuk memulihkan seluruh disk akan lebih sedikit dibandingkan dengan menghitung perbedaan data. Karena itu, kami sarankan Anda untuk mengaktifkan opsi ini hanya jika koneksi ke penyimpanan pencadangan lambat (misalnya, jika pencadangan disimpan dalam penyimpanan awan atau pada folder jaringan jarak jauh).

Saat memulihkan mesin fisik, prasetel akan bergantung pada lokasi pencadangan:

- Jika lokasi pencadangan adalah penyimpanan awan, prasetelnya adalah: **Aktif**.
- Untuk lokasi pencadangan lainnya, prasetelnya adalah: **Dinonaktifkan**.

Saat memulihkan mesin virtual, nilai prasetelnya adalah: **Aktif**.

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.

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				
	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.

Manajemen pita

Anda dapat menggunakan opsi pemulihan manajemen pita berikut.

Gunakan cache disk untuk mempercepat pemulihan

Nilai prasetelnya adalah: **Dinonaktifkan**.

Kami sangat menyarankan agar Anda menggunakan **Gunakan cache disk untuk mempercepat opsi pemulihan** saat Anda memulihkan file dari arsip citra. Atau, pemulihan operasi dapat memerlukan waktu lama. Dengan opsi ini, pembacaan pita dijalankan secara berurutan, tanpa gangguan dan pemutaran balik.

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, atau Agen untuk Scale Computing HC3.

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.

Manajemen daya VM

Opsi ini efektif ketika pemulihan ke mesin virtual dilakukan oleh Agen untuk VMware, Agen untuk Hyper-V, atau Agen untuk Scale Computing HC3.

Matikan daya mesin virtual ketika memulai pemulihan

Nilai prasetelnya adalah: **Aktif**.

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**.

Nyalakan setelah pemulihan

Opsi ini berlaku jika operasi dilakukan dengan media yang dapat di-boot.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Opsi ini memungkinkan booting mesin ke sistem operasi yang dipulihkan tanpa interaksi pengguna.

Pemulihan bencana

Fitur ini hanya tersedia di penyebaran awan Acronis Cyber Protect. Untuk deskripsi detail mengenai fungsi ini, silakan lihat https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html.

Operasi dengan pencadangan

Tab Penyimpanan cadangan

Tab **Penyimpanan cadangan** menunjukkan cadangan dari semua mesin yang pernah terdaftar pada server manajemen. Termasuk mesin offline dan mesin yang tidak lagi terdaftar.

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. Pada penyebaran awan, administrator dapat melihat pencadangan atas nama akun apa pun yang termasuk dalam grup yang sama dan grup turunannya. Akun ini secara tidak langsung dipilih di **Mesin untuk dijelajahi**. Tab **Penyimpanan cadangan** menampilkan cadangan semua mesin yang pernah didaftarkan dalam akun yang sama saat mesin ini didaftarkan.

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.

Peringatan!
Jangan mencoba mengedit file cadangan secara manual karena ini dapat mengakibatkan kerusakan file dan membuat cadangan tidak dapat digunakan. Selain itu, sebaiknya Anda mengekspor cadangan atau menggunakan replikasi cadangan daripada memindahkan file cadangan secara manual.

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 dijelajahi**, 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 dijelajahi** 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 dijelajahi**.

4. Klik **Tampilkan cadangan**.
5. Pilih titik pemulihan.

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 akan membuat cadangan inkremental berisi perubahan yang Anda buat pada konten pencadangan. Perlu diketahui 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. Secara default, 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.

5. Klik kanan volume yang akan di-mount, lalu klik salah satu pilihan berikut:
   - **Mount**

     Catatan
     Hanya cadangan terakhir dalam arsip (rantai cadangan) yang dapat dipasang dalam mode baca-tulis.

   - **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. 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

Validasi adalah operasi untuk memeriksa kemungkinan pemulihan data dari cadangan. Untuk informasi lebih lanjut tentang operasi ini, lihat "Validasi" (hlm. 346).

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. 337).
4. Klik ikon roda gigi, lalu klik **Validasi**.
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. Ekspor memungkinkan Anda untuk memisahkan pencadangan spesifik dari rantai pencadangan inkremental dan diferensial untuk pemulihan cepat, menulis ke media yang dapat dilepas atau dicopot, maupun tujuan lain.

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.

Nama file cadangan dari cadangan yang diekspor bergantung pada nilai opsi format cadangan:

- Untuk format **Versi 12** dengan skema pencadangan apa pun, nama file cadangan akan sama dengan yang ada pada cadangan asli, kecuali nomor urut. 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.
- Untuk format **Versi 11** dengan skema pencadangan **Selalu inkremental (file tunggal)**, nama file cadangan akan sama persis dengan nama file cadangan dari cadangan asli. Jika beberapa cadangan dari rantai cadangan yang sama diekspor ke lokasi yang sama, setiap operasi ekspor akan menimpa cadangan yang diekspor sebelumnya.
- Untuk format **Versi 11** dengan skema pencadangan lain, nama file cadangan akan sama dengan yang ada pada cadangan asli, kecuali untuk stempel waktu. Stempel waktu dari cadangan yang diekspor sesuai dengan waktu ketika ekspor dilakukan.

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 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.
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.
7. Tentukan tujuan ekspor.
8. Klik **Mulai**.

Menghapus beberapa cadangan

Peringatan!
Ketika cadangan dihapus, semua datanya akan hilang secara permanen. Data yang dihapus tidak dapat dipulihkan.

Untuk menghapus cadangan mesin yang sedang online dan ada di dalam konsol web Cyber Protect

1. Pada tab **Semua perangkat**, pilih mesin yang cadangannya ingin Anda hapus.
2. Klik **Pemulihan**.
3. Pilih lokasi dari cadangan yang akan dihapus.
4. Lakukan salah satu langkah berikut:
   - Untuk menghapus cadangan tunggal, pilih cadangan yang akan dihapus, klik ikon roda gigi, lalu klik **Hapus**.
   - Untuk menghapus semua cadangan di lokasi yang dipilih, klik **Hapus semua**.
5. Konfirmasi keputusan Anda.

Untuk menghapus cadangan dari semua mesin

1. Pada tab **Penyimpanan cadangan**, pilih lokasi di mana Anda ingin menghapus 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.
3. Lakukan salah satu langkah berikut:

- Untuk menghapus cadangan tunggal, klik **Tampilkan cadangan**, pilih cadangan yang akan dihapus, klik ikon roda gigi, lalu klik **Hapus**.
- Untuk menghapus grup yang dipilih, klik **Hapus**.

4. Konfirmasi keputusan Anda.

Untuk menghapus pencadangan langsung dari penyimpanan awan

1. Masuk ke penyimpanan awan, seperti yang dijelaskan dalam "Mengunduh file dari penyimpanan awan".
2. Klik nama mesin yang cadangannya ingin Anda hapus.
   Perangkat lunak ini menampilkan satu atau beberapa grup cadangan.
3. Klik ikon roda gigi yang terkait dengan grup cadangan yang ingin Anda hapus.
4. Klik **Hapus**.
5. Konfirmasi operasi.

Tab Rencana

Dengan lisensi Lanjutan, Anda dapat mengelola rencana proteksi dan rencana lain menggunakan tab **Rencana**.

Setiap bagian dari tab **Rencana** berisi semua rencana jenis tertentu. Bagian berikut tersedia:

- **Perlindungan**
- **Pemindaian cadangan**
- **Replikasi cadangan**
- **Validasi**
- **Pembersihan**
- **Konversi ke VM**
- **Replikasi VM**
- **Media yang dapat di-boot**. Bagian ini menampilkan rencana proteksi yang dibuat untuk mesin yang di-boot dari media yang dapat di-boot dan hanya dapat diterapkan pada mesin tersebut.

Di setiap bagian, Anda dapat membuat, mengedit, menonaktifkan, mengaktifkan, menghapus, memulai, dan memantau eksekusi suatu rencana.

Kloning dan penghentian hanya tersedia untuk rencana proteksi. Tidak seperti menghentikan pencadangan dari tab **Perangkat**, penghentian rencana proteksi akan menghentikan pencadangan di semua perangkat yang menerapkan rencana ini. Jika waktu mulai pencadangan untuk semua perangkat didistribusikan dalam jendela waktu, menghentikan rencana proteksi akan menghentikan pencadangan yang berjalan atau mencegah dimulainya pencadangan.

Anda juga dapat mengekspor rencana ke file dan mengimpor rencana yang diekspor sebelumnya.

Pemrosesan data off-host

Sebagian besar tindakan yang merupakan bagian dari rencana proteksi, seperti replikasi, validasi, dan penerapan aturan retensi, dilakukan oleh agen yang melakukan pencadangan. Ini akan menempatkan beban kerja tambahan pada mesin tempat agen berjalan, bahkan setelah proses pencadangan selesai.

Memisahkan rencana pemindaian anti-malware, replikasi, validasi, pembersihan, dan konversi dari rencana proteksi akan memberi Anda fleksibilitas:

- Untuk memilih agen lain yang akan melakukan operasi ini
- Untuk menjadwalkan operasi ini selama jam-jam tidak sibuk untuk meminimalkan konsumsi bandwidth jaringan
- Untuk menggeser operasi ini di luar jam kerja, jika penyiapan agen khusus tidak ada dalam rencana Anda

Jika Anda menggunakan simpul penyimpanan, menginstal agen khusus pada mesin yang sama adalah tindakan yang wajar.

Berbeda dengan cadangan dan rencana replikasi VM yang menggunakan pengaturan waktu mesin yang menjalankan agen, rencana pemrosesan data off-host berjalan sesuai dengan pengaturan waktu mesin server manajemen.

Rencana pemindaian cadangan

Lokasi yang didukung

Anda dapat memindai cadangan untuk malware di lokasi berikut: **Penyimpanan awan**, **Folder lokal**, dan **Folder jaringan**. Hanya agen yang terinstal pada mesin terpindai yang dapat mengakses lokasi **Folder lokal**.

Untuk keterangan lebih lanjut tentang pemindaian cadangan dan batasannya, lihat "Pemindaian antimalware untuk cadangan".

Untuk membuat rencana pemindaian cadangan

1. Di konsol web Cyber Protect, klik **Rencana** > **Pemindaian cadangan**.
2. Klik **Buat rencana**.
3. [Opsional] Untuk mengubah nama rencana, klik ikon pensil di samping nama default.
4. Pilih agen pemindaian.
5. Pilih lokasi cadangan atau cadangan individual untuk dipindai.
   Anda dapat memilih beberapa lokasi cadangan sekaligus. Untuk menyertakan beberapa cadangan individual dalam satu rencana, Anda perlu menambahkan cadangan satu per satu.
6. [Jika **Penyimpanan awan** atau **Folder jaringan** dipilih] Jika diminta, berikan kredensial untuk mengakses penyimpanan cadangan.
7. [Jika cadangan terenkripsi dipilih] Berikan kata sandi untuk mengakses cadangan. Jika kubah atau beberapa cadangan dipilih, Anda dapat menetapkan kata sandi tunggal. Jika kata sandi tidak tepat untuk cadangan spesifik, peringatan akan ditampilkan. Hanya cadangan dengan kata sandi yang tepat yang akan dipindai.
8. Konfigurasi jadwal untuk pemindaian.
9. Ketika sudah siap, klik **Buat**.

Hasilnya, rencana pemindaian cadangan dibuat.

Replikasi cadangan

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	+	+
Folder NFS	–	–
Secure Zone	–	–
Server SFTP	–	–
Lokasi yang dikelola*	+	+
Perangkat pita	–	+

* Periksa batasan yang dijelaskan dalam topik "Pertimbangan untuk pengguna dengan lisensi Lanjutan" (hlm. 254).

Untuk membuat rencana replikasi cadangan

1. Klik **Rencana** > **Replikasi cadangan**.
2. Klik **Buat rencana**.
   Perangkat lunak menampilkan templat rencana baru.
3. [Opsional] Untuk mengubah nama rencana, klik nama default.
4. Klik **Agen**, lalu pilih agen yang akan melakukan replikasi.
   Anda dapat memilih agen apa pun yang memiliki akses ke sumber dan menargetkan lokasi pencadangan.
5. Klik **Item untuk direplikasi**, lalu pilih cadangan yang akan direplikasi oleh rencana 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.
6. Klik **Tujuan**, lalu tentukan lokasi target.
7. [Opsional] Di **Bagaimana cara mereplikasi**, pilih cadangan mana yang akan direplikasi. Anda dapat memilih salah satu dari tindakan berikut:
   - **Semua cadangan** (default)
   - **Hanya cadangan penuh**
   - **Hanya cadangan terakhir**
8. [Opsional] Klik **Jadwal**, lalu ubah jadwal.
9. [Opsional] Klik **Aturan retensi**, lalu tentukan aturan retensi untuk lokasi target, seperti yang dijelaskan dalam "Aturan retensi".

10. Jika cadangan yang dipilih dalam **Item untuk direplikasi** dienkripsi, aktifkan switch **Kata sandi cadangan**, lalu berikan kata sandi enkripsi. Jika tidak, lewati langkah ini.
11. [Opsional] Untuk mengubah opsi rencana, klik ikon roda gigi.
12. Klik **Buat**.

Validasi

Validasi adalah operasi untuk memeriksa kemungkinan pemulihan data dari cadangan.

Validasi lokasi pencadangan akan memvalidasi semua cadangan yang disimpan di lokasi.

Cara kerjanya

Rencana validasi menawarkan dua metode validasi. Jika Anda memilih kedua metode, operasi akan dilakukan secara berurutan.

- **Menghitung checksum untuk setiap blok data yang disimpan dalam cadangan**
  Untuk informasi lebih lanjut tentang validasi dengan menghitung checksum, lihat "Validasi cadangan".
- **Menjalankan mesin virtual dari cadangan**
  Metode ini hanya berfungsi untuk pencadangan level disk yang berisi sistem operasi. Untuk menggunakan metode ini, Anda memerlukan host ESXi atau Hyper-V dan agen perlindungan (Agen untuk VMware atau Agen untuk Hyper-V) yang mengelola host ini.
  Agen menjalankan mesin virtual dari cadangan, lalu terhubung ke VMware Tools atau Hyper-V Heartbeat Service 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.

Jika validasi gagal, Anda dapat menelusuri ke detail pada bagian **Aktivitas** dari tab **Ikhtisar**.

Lokasi yang didukung

Tabel berikut merangkum lokasi pencadangan yang didukung oleh rencana validasi.

Lokasi cadangan	Menghitung checksum	Menjalankan VM
Penyimpanan awan	+	+
Folder lokal	+	+
Folder jaringan	+	+
Folder NFS	–	–

Secure Zone	–	–
Server SFTP	–	–
Lokasi yang dikelola	+	+
Perangkat pita	+	–

Untuk membuat rencana validasi baru

1. Klik **Rencana** > **Validasi**.
2. Klik **Buat rencana**.
   Perangkat lunak menampilkan templat rencana baru.
3. [Opsional] Untuk mengubah nama rencana, klik nama default.
4. Klik **Agen**, lalu pilih agen yang akan melakukan validasi.
   Jika Anda ingin melakukan validasi dengan menjalankan mesin virtual dari cadangan, pilih Agen untuk VMware atau Agen untuk Hyper-V. Jika tidak, pilih agen apa pun yang terdaftar di server manajemen dan memiliki akses ke lokasi pencadangan.
5. Klik **Item untuk divalidasi**, lalu pilih cadangan yang akan divalidasi oleh rencana 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.
6. [Opsional] Di **Apa yang akan divalidasi**, pilih cadangan mana yang akan divalidasi. Anda dapat memilih salah satu dari tindakan berikut:
   - **Semua cadangan**
   - **Hanya cadangan terakhir**
7. [Opsional] Klik **Bagaimana cara memvalidasi**, lalu pilih salah satu metode berikut:
   - **Verifikasi checksum**
     Perangkat lunak akan menghitung checksum untuk setiap blok data yang disimpan dalam cadangan
   - **Jalankan sebagai mesin virtual**
     Perangkat lunak ini akan menjalankan mesin virtual dari setiap cadangan.
8. Jika Anda memilih **Jalankan sebagai mesin virtual**:
   a. Klik **Mesin target**, lalu pilih jenis mesin virtual (ESXi atau Hyper-V), host dan templat nama mesin.
      Nama default adalah **[Nama Mesin]_validate**.
   b. Klik **Penyimpanan data** untuk ESXi atau **Jalur** untuk Hyper-V, lalu pilih penyimpanan data untuk mesin virtual.
   c. [Opsional] Ubah mode provisi disk.

Pengaturan default adalah **Tipis** untuk VMware ESXi dan **Memperluas secara dinamis** untuk Hyper-V.

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.

Catatan
Pengalih **VM heartbeat** selalu diaktifkan untuk memvalidasi status heartbeat mesin virtual yang dilaporkan oleh alat hypervisor di sistem operasi tamu (VMware Tool atau Hyper-V Integration Service), dengan menjalankan mesin virtual dari cadangan. Sakelar ini dirancang untuk rilis mendatang, jadi Anda tidak dapat berinteraksi dengannya.

9. [Opsional] Klik **Jadwal**, lalu ubah jadwal.
10. Jika cadangan yang dipilih dalam **Item untuk divalidasi** dienkripsi, aktifkan switch **Kata sandi cadangan**, lalu berikan kata sandi enkripsi. Jika tidak, lewati langkah ini.
11. [Opsional] Untuk mengubah opsi rencana, klik ikon roda gigi.
12. Klik **Buat**.

Pembersihan

Pembersihan adalah operasi yang menghapus cadangan usang sesuai dengan aturan retensi.

Lokasi yang didukung

Rencana pembersihan mendukung semua lokasi pencadangan, kecuali untuk folder NFS, server SFTP, dan Secure Zone.

Untuk membuat rencana pembersihan baru

1. Klik **Rencana** > **Pembersihan**.
2. Klik **Buat rencana**.
   Perangkat lunak menampilkan templat rencana baru.
3. [Opsional] Untuk mengubah nama rencana, klik nama default.
4. Klik **Agen**, lalu pilih agen yang akan melakukan pemberisihan.
   Anda dapat memilih agen apa pun yang memiliki akses ke lokasi pencadangan.
5. Klik **Item untuk dibersihkan**, lalu pilih cadangan yang akan dibersihkan oleh rencana 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.
6. [Opsional] Klik **Jadwal**, lalu ubah jadwal.

7. [Opsional] Klik **Aturan retensi**, lalu tentukan aturan retensi, seperti yang dijelaskan dalam "Aturan retensi".
8. Jika pencadangan yang dipilih dalam **Item untuk dibersihkan** dienkripsi, aktifkan switch **Kata sandi cadangan**, lalu berikan kata sandi enkripsi. Jika tidak, lewati langkah ini.
9. [Opsional] Untuk mengubah opsi rencana, klik ikon roda gigi.
10. Klik **Buat**.

Konversi ke mesin virtual

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, silakan lihat "Yang perlu Anda ketahui tentang konversi".

Untuk membuat rencana konversi ke mesin virtual

1. Klik **Rencana** > **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 tindakan berikut:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **File VHDX**

   Catatan
   Untuk menghemat ruang penyimpanan, setiap konversi ke file VHDX menimpa file VHDX di lokasi target yang dibuat selama konversi sebelumnya.
5. Lakukan salah satu langkah berikut:
   - [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**.

Media yang dapat di-boot

Penting
Beberapa fitur yang dijelaskan dalam bagian ini hanya tersedia untuk penyebaran lokal.

Media yang dapat di-boot

Media yang dapat di-boot adalah media fisik (CD, DVD, drive flash USB, atau media yang dapat dilepas lainnya yang didukung oleh BIOS mesin sebagai perangkat boot) yang memungkinkan Anda untuk menjalankan agen perlindungan baik di lingkungan berbasis Linux atau Windows Preinstallation Environment (WinPE), tanpa bantuan sistem operasi.

Media yang dapat di-boot paling sering digunakan untuk:

- Memulihkan sistem operasi yang tidak dapat memulai
- Mengakses dan mencadangkan data yang masih berfungsi dalam sistem rusak
- Menyebarkan sistem operasi pada logam
- Membuat volume dasar atau dinamis pada logam
- Mencadangkan sektor demi sektor disk dengan sistem file yang tidak didukung
- Mencadangkan secara offline data apa pun yang tidak dapat dicadangkan secara online, misalnya karena data dikunci oleh aplikasi yang berjalan atau karena aksesnya dibatasi.

Mesin juga dapat di-boot menggunakan boot jaringan dari Server PXE Acronis, Windows Deployment Services (WDS), atau Remote Installation Services (RIS). Server dengan komponen yang dapat di-boot yang diunggah ini juga dapat dianggap sebagai media yang dapat di-boot. Anda dapat membuat media yang dapat di-boot atau mengonfigurasi server PXE atau WDS/RIS dengan menggunakan wizard yang sama.

Membuat media yang dapat di-boot atau unduh yang siap pakai?

Dengan 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. Untuk media yang dapat di-boot dengan fitur lengkap, Anda perlu menentukan kunci lisensi Acronis Cyber Protect. Tanpa kunci ini, media yang dapat di-boot hanya akan mampu menjalankan operasi pemulihan.

Catatan
Media yang dapat di-boot tidak mendukung drive hybrid.

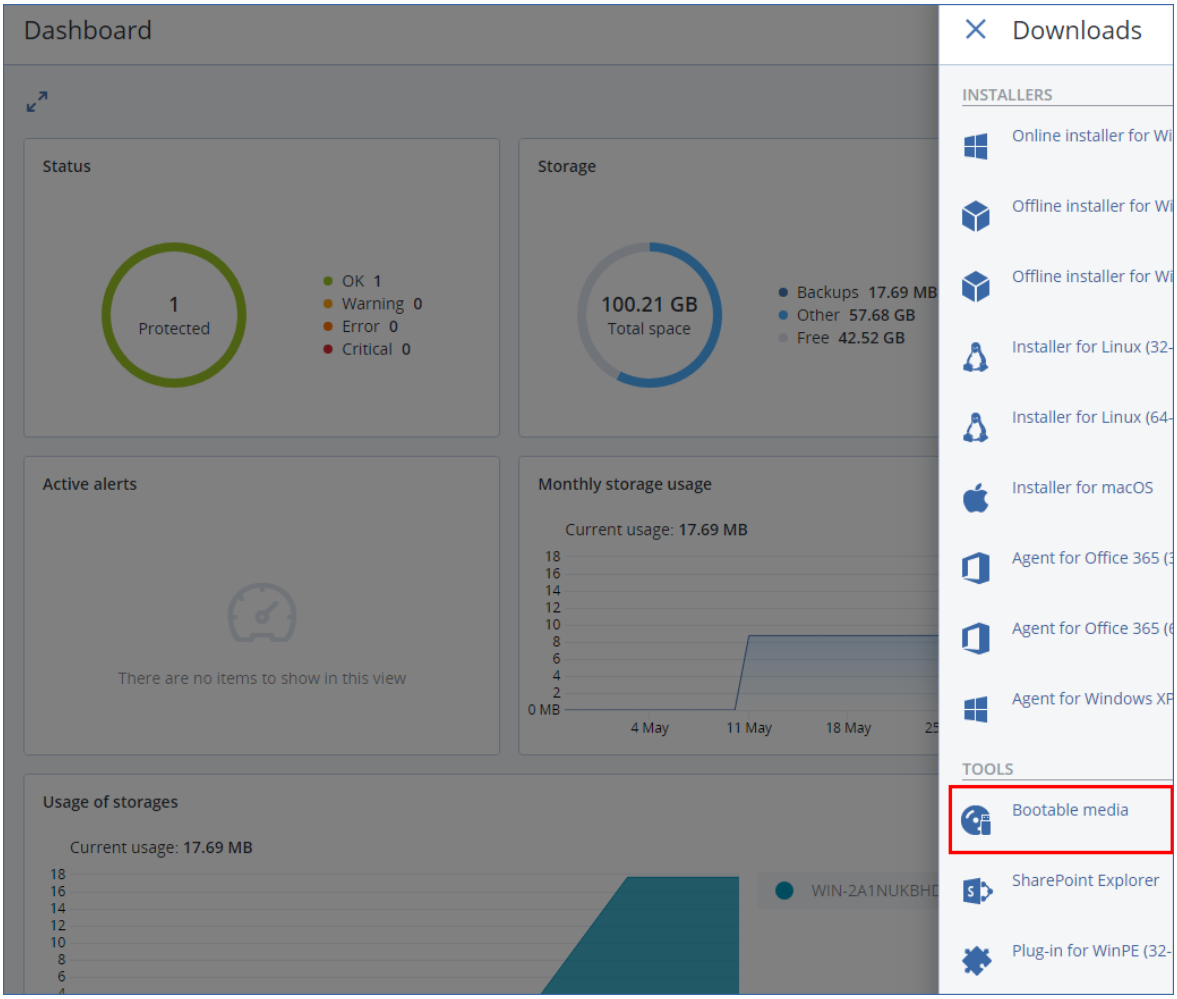
Anda juga dapat mengunduh media yang dapat di-boot yang siap pakai (hanya berbasis Linux). Anda hanya dapat menggunakan unduhan media yang dapat di-boot untuk operasi pemulihan dan

akses ke Acronis Universal Restore. Anda tidak dapat mencadangkan data, memvalidasi atau mengekspor cadangan, mengelola disk, atau menggunakannya dengan skrip. Unduhan media yang dapat di-boot tidak sesuai untuk komputer macOS.

Catatan
Media yang dapat di-boot siap pakai tidak mendukung simpul penyimpanan, lokasi pita, dan lokasi SFTP. Jika Anda ingin menggunakan lokasi penyimpanan ini di penyebaran di lokasi, Anda harus membuat sendiri media yang dapat di-boot dengan menggunakan Pembangun Media Yang Dapat Di-Boot. Lihat https://kb.acronis.com/content/61566.

Untuk mengunduh media yang dapat di-boot siap pakai

1. Di konsol web Cyber Protect, klik ikon akun di pojok kanan atas, lalu klik **Unduhan**.
2. Pilih **Media yang dapat di-boot**.



Anda dapat menyalin file ISO yang telah diunduh ke CD/DVD atau membuat drive flash USB yang dapat di-boot menggunakan salah satu alat bantu gratis yang tersedia secara online. Gunakan `ISO to USB` atau `RUFUS` jika Anda perlu mem-boot mesin UEFI, atau `Win32DiskImager` untuk mesin BIOS. Di Linux, Anda dapat menggunakan utilitas `dd`.

Jika konsol web Cyber Protect tidak dapat diakses, Anda dapat mengunduh media yang dapat di-boot siap pakai dari akun Anda di Portal Pelanggan Acronis:

1. Buka https://account.acronis.com.
2. Temukan Acronis Cyber Protect, lalu klik **Unduhan**.
3. Pada halaman yang terbuka, temukan **Unduhan tambahan**, lalu klik **ISO Media yang Dapat Di-Boot (untuk Windows dan Linux)**.

Media yang dapat di-boot berbasis Linux atau WinPE?

Berbasis Linux

Media yang dapat di-boot berbasis Linux berisi agen perlindungan 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. Operasi dapat dikonfigurasikan dan dikontrol secara lokal maupun jarak jauh, di konsol web Cyber Protect.

Daftar perangkat keras yang didukung oleh media berbasis Linux tersedia di: http://kb.acronis.com/content/55310.

Berbasis WinPE

Media yang dapat di-boot berbasis WinPE berisi sistem Windows minimal yang disebut Windows Preinstallation Environment (WinPE) dan Plugin Acronis untuk WinPE, yaitu modifikasi dari agen perlindungan yang dapat dijalankan di lingkungan prapenginstalan.

WinPE terbukti menjadi solusi bootable yang paling mudah di lingkungan besar dengan perangkat keras yang beragam.

Kelebihan:

- Menggunakan Acronis Cyber Protect 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 perlindungan, 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 lebih baru memungkinkan pemuatan dinamis dari 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).
- Ketika mesin di-boot dengan media yang dapat di-boot berbasis PE, Anda tidak dapat memilih media optik seperti CD, DVD, atau Blu-ray Disc (BD) sebagai tujuan cadangan.

Pembangun Media Yang Dapat Di-Boot

Pembangun Media yang Dapat Di-boot adalah alat khusus untuk membuat media yang dapat di-boot. Hanya tersedia untuk penyebaran di lokasi.

Pembangun Media yang Dapat Di-boot diinstal secara default saat Anda menginstal server manajemen. Anda dapat menginstal pembangun media secara terpisah di mesin apa pun yang menjalankan Windows atau Linux. Sistem operasi yang didukung sama dengan sistem untuk agen yang terkait.

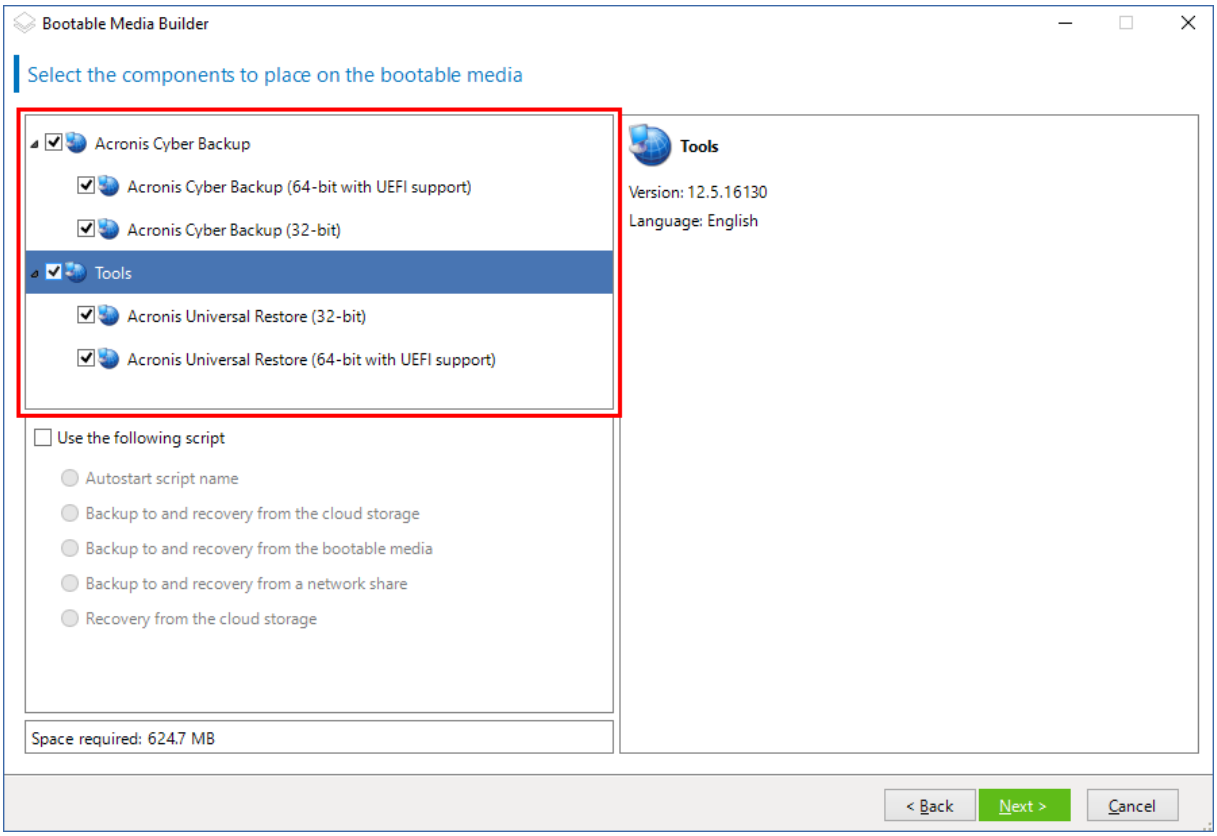
Mengapa menggunakan pembangun media?

Media yang dapat di-boot yang tersedia untuk diunduh di konsol web Cyber Protect hanya dapat digunakan untuk pemulihan. Media ini didasarkan pada kernel Linux. Tidak seperti Windows PE, media tersebut tidak memungkinkan penyuntikan driver kustom selama proses.

- Pembuat media memungkinkan Anda untuk membuat media yang dapat di-boot berbasis Linux dan berbasis WinPE kustom, berfitur lengkap dengan fungsionalitas cadangan.
- Selain membuat media fisik yang dapat di-boot, Anda dapat mengunggah komponen media ke Windows Deployment Services (WDS) dan menggunakan boot jaringan.
- Media yang dapat di-boot siap pakai tidak mendukung simpul penyimpanan, lokasi pita, dan lokasi SFTP. Jika Anda ingin menggunakan lokasi penyimpanan ini pada penyebaran di lokasi lokal, Anda harus membuat sendiri media yang dapat di-boot dengan menggunakan Pembangun Media Yang Dapat Di-Boot. Lihat https://kb.acronis.com/content/61566.

32- atau 64-bit?

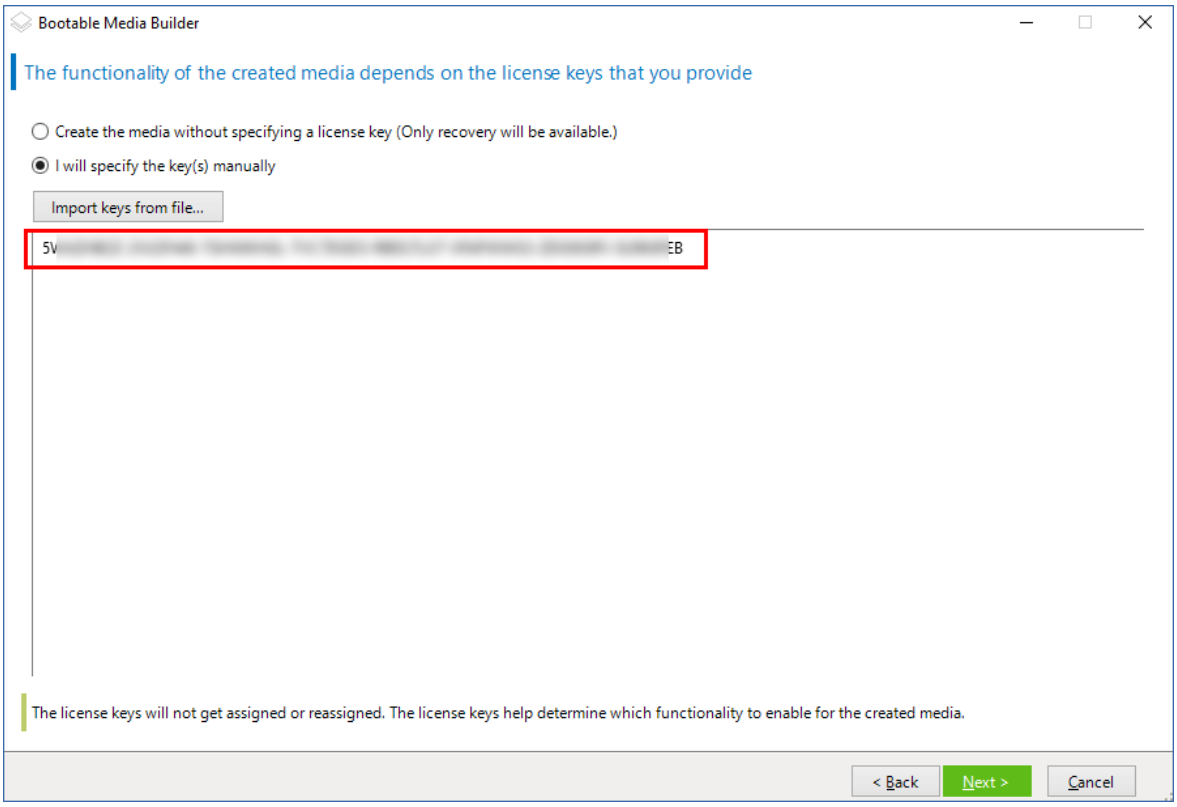
Pembangun Media Yang Dapat Di-Boot membuat media dengan komponen 32-bit dan 64-bit. Dalam sebagian besar kasus, Anda membutuhkan media 64-bit untuk mem-boot mesin yang menggunakan Unified Extensible Firmware Interface (UEFI).



Media yang dapat di-boot berbasis Linux

Untuk membuat media bootable berbasis Linux

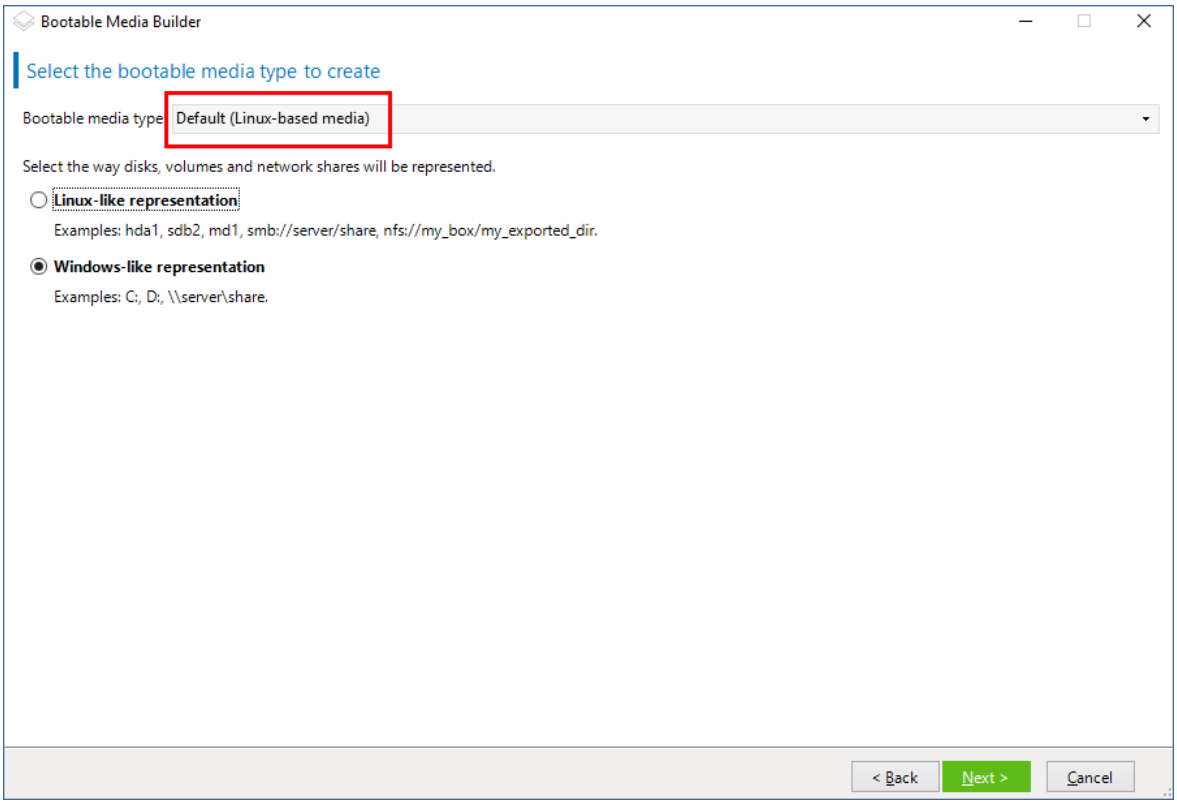
1. Mulai **Pembangun Media Yang Dapat Di-Boot**.
2. Untuk membuat media yang dapat di-boot dengan fitur lengkap, tentukan kunci lisensi Acronis Cyber Protect. Kunci ini digunakan untuk menentukan fitur yang akan disertakan dalam media yang dapat di-boot. Tidak ada lisensi yang akan dibatalkan dari mesin mana pun.
   Jika Anda tidak menentukan kunci lisensi, media yang dapat di-boot yang dihasilkan hanya dapat digunakan untuk operasi pemulihan.



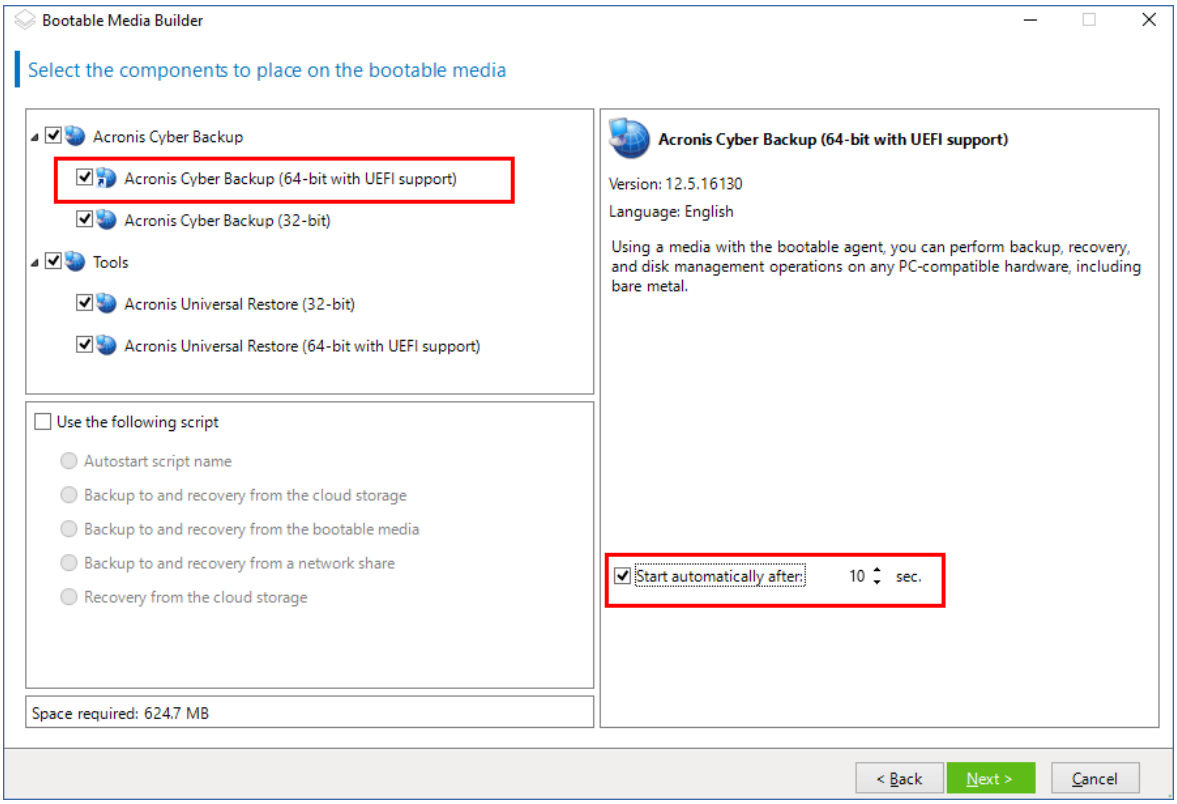
3. Pilih **Tipe media yang dapat di-boot: Default (media berbasis Linux)**.

   Pilih cara volume dan sumber daya jaringan akan direpresentasikan:

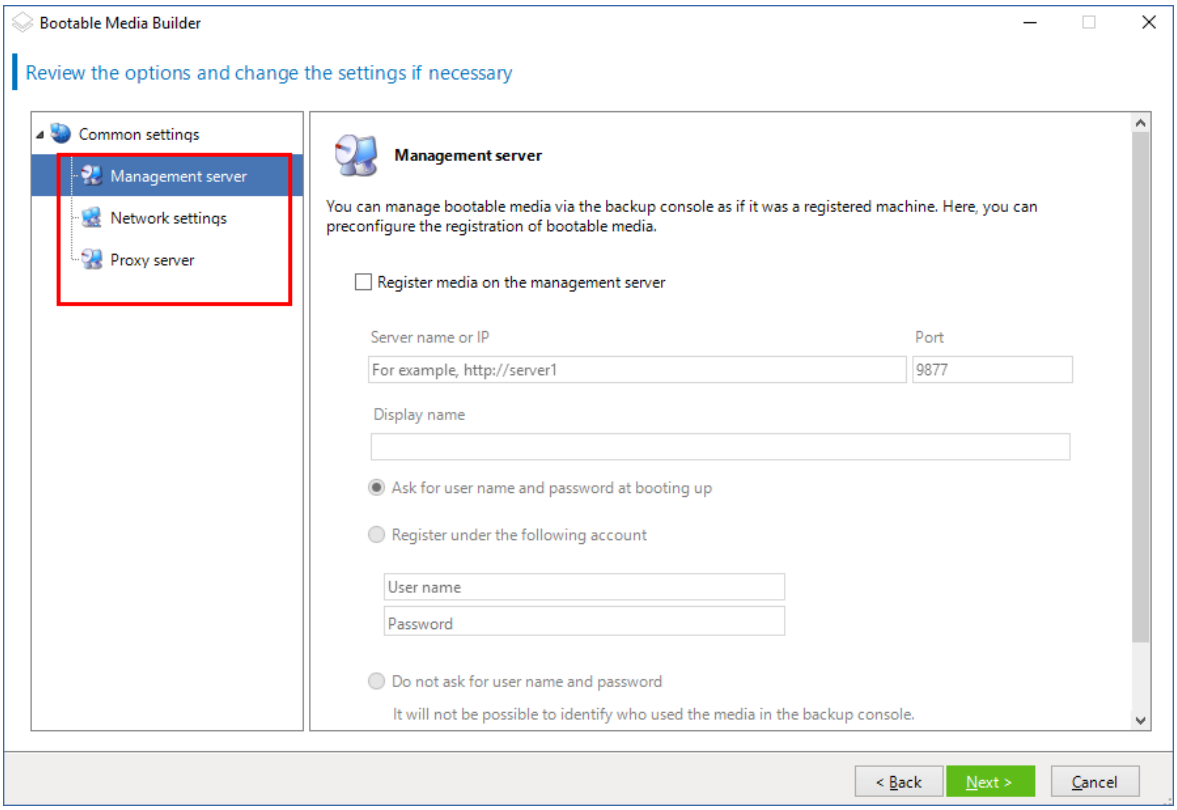
   - Media dengan representasi volume seperti Linux akan menampilkan volume sebagai, misalnya, hda1 dan sdb2. Media tersebut mencoba merekonstruksi perangkat MD dan volume logis (LVM) sebelum memulai pemulihan.
   - Media dengan representasi volume seperti Windows akan menampilkan volume sebagai, misalnya, 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.
5. [Opsional] Pilih bahasa yang akan digunakan dalam media yang dapat di-boot.
6. Pilih komponen yang akan ditempatkan pada media: agen Acronis Cyber Protect yang dapat di-boot, dan/atau Universal Restore jika Anda berencana untuk memulihkan sistem pada perangkat keras yang berbeda.
   Dengan agen yang dapat di-boot, Anda dapat melakukan operasi pencadangan, pemulihan, dan manajemen disk pada perangkat keras yang kompatibel dengan PC, termasuk logam.
   Universal Restore memungkinkan Anda mem-boot sistem operasi yang dipulihkan ke perangkat keras yang berbeda atau ke mesin virtual. Alat bantu ini menemukan dan menginstal driver untuk perangkat yang penting untuk memulai sistem operasi, seperti pengontrol penyimpanan, motherboard, atau chipset.
7. [Opsional] Tentukan interval batas waktu untuk menu boot, bersama dengan komponen yang akan secara otomatis dimulai saat batas waktu habis. Untuk melakukannya, klik komponen yang diinginkan di panel kiri atas, lalu atur intervalnya. Pengaturan ini memungkinkan operasi di lokasi tanpa pengawasan saat booting dari WDS/RIS.
   Jika pengaturan ini tidak dikonfigurasi, pemuat akan menunggu Anda memilih apakah akan mem-boot sistem operasi (jika ada) atau komponen.



8. [Opsional] Jika Anda ingin mengotomatiskan operasi agen yang dapat di-boot, pilih kotak centang **Gunakan skrip berikut**. Kemudian, pilih salah satu skrip dan tentukan parameter skrip.
9. [Opsional] Pilih cara mendaftarkan media pada server manajemen saat booting. Untuk informasi lebih lanjut tentang pengaturan pendaftaran, lihat Server manajemen.



10. [Opsional] Tentukan pengaturan jaringan: Pengaturan TCP/IP yang akan ditetapkan ke adaptor jaringan mesin. Untuk informasi lebih lanjut, lihat "Pengaturan jaringan" (hlm. 370).
11. [Opsional] Tentukan port jaringan: Port TCP yang didengarkan agen yang dapat di-boot untuk koneksi masuk.
12. [Opsional] Jika server proksi diaktifkan di jaringan Anda, tentukan nama host/alamat dan port IP-nya.
13. Pilih jenis media. Anda dapat:
    - Membuat profil ISO. Kemudian Anda dapat menyalinnya ke CD/DVD; menggunakannya untuk membuat drive flash USB yang dapat di-boot; atau menghubungkannya ke mesin virtual.
    - Membuat file ZIP.
    - Unggah komponen yang dipilih ke Server PXE Acronis.
    - Unggah komponen yang dipilih ke WDS/RIS.
14. [Opsional] Tambahkan ke sistem Windows driver untuk digunakan oleh Universal Restore. Jendela ini muncul jika Universal Restore ditambahkan ke media dan media selain WDS/RIS dipilih.
15. Jika diminta, tentukan nama host/alamat IP dan kredensial untuk WDS/RIS, atau jalur ke file ISO media.
16. Periksa pengaturan Anda di layar ringkasan, lalu klik **Lanjutkan**.

Parameter Kernel:

Jendela ini memungkinkan Anda menentukan satu atau beberapa parameter kernel Linux. Parameter tersebut akan diterapkan secara otomatis ketika media yang dapat di-boot dimulai.

Parameter ini biasanya digunakan ketika terdapat 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 lain pada mesin yang berbeda. Kami menyarankan penggunaan parameter **vga=ask** terlebih dahulu guna memilih nilai untuk *mode_number*.

quiet

Menonaktifkan tampilan pesan startup saat kernel Linux memuat, dan memulai konsol manajemen setelah kernel dimuat.

Parameter ini ditentukan secara implisit saat membuat media yang dapat di-boot, tetapi Anda dapat menghapus parameter ini saat berada di menu boot.

Tanpa parameter ini, semua pesan startup 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

Nonaktifkan 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**

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 di bawah 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 ditentukan, Anda dapat menentukan skrip saat membuat media dalam Pembangun Media yang Dapat Di-boot. Setiap kali melakukan boot, media akan menjalankan skrip ini, bukan menampilkan antarmuka pengguna.

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:

- Cadangkan ke dan pulihkan dari penyimpanan awan (**entire_pc_cloud**)
- Cadangkan ke dan pulihkan dari media yang dapat di-boot (**entire_pc_local**)
- Cadangkan ke dan pulihkan dari jaringan bersama (**entire_pc_share**)
- Pemulihan dari penyimpanan awan (**golden_image**)

Skrip dapat ditemukan di mesin tempat Pembangun Media yang Dapat Di-boot diinstal, di direktori berikut:

- Di Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Di Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Cadangkan ke dan pulihkan dari penyimpanan awan

Skrip ini akan mencadangkan mesin ke penyimpanan awan atau memulihkan mesin dari pencadangan terbarunya yang dibuat di penyimpanan awan oleh skrip ini. Pada saat memulai, skrip akan meminta pengguna untuk memilih antara cadangan, pemulihan, dan memulai antarmuka pengguna.

Di Pembangun Media yang Dapat Di-boot, tentukan parameter skrip berikut:

1. Nama pengguna dan kata sandi untuk penyimpanan awan.
2. [Opsional] Kata sandi yang akan digunakan oleh skrip untuk mengenkripsi atau mengakses cadangan.

Cadangkan ke dan pulihkan dari media yang dapat di-boot

Skrip ini akan mencadangkan mesin ke media yang dapat di-boot atau memulihkan mesin dari cadangan terbarunya yang dibuat oleh skrip ini di media yang sama. Pada saat memulai, skrip akan

meminta pengguna untuk memilih antara cadangan, pemulihan, dan memulai antarmuka pengguna.

Di Pembangun Media yang Dapat Di-boot, Anda dapat menentukan kata sandi yang akan digunakan oleh skrip untuk mengenkripsi atau mengakses cadangan.

Cadangkan ke dan pulihkan dari jaringan bersama

Skrip ini akan mencadangkan mesin ke jaringan bersama atau memulihkan mesin dari cadangan terbarunya yang berada di jaringan bersama. Pada saat memulai, skrip akan meminta pengguna untuk memilih antara cadangan, pemulihan, dan memulai antarmuka pengguna.

Di Pembangun Media yang Dapat Di-boot, tentukan parameter skrip berikut:

1. Jalur jaringan bersama.
2. Nama pengguna dan kata sandi untuk jaringan bersama.
3. [Opsional] Nama file cadangan. Nilai standarnya adalah **AutoBackup**. Jika Anda menginginkan skrip untuk menambahkan cadangan ke cadangan yang sudah ada, atau memulihkan dari cadangan dengan nama non-default, ubah nilai default ke nama file cadangan ini.

   Untuk mengetahui nama file cadangan

   a. Di konsol web 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**.
4. [Opsional] Kata sandi yang akan digunakan oleh skrip untuk mengenkripsi atau mengakses cadangan.

Pemulihan dari penyimpanan awan

Script ini akan memulihkan mesin dari pencadangan terbaru yang berada di penyimpanan awan. Di awal, skrip akan meminta pengguna untuk menentukan:

1. Nama pengguna dan kata sandi untuk penyimpanan awan.
2. Kata sandi jika pencadangan dienkripsi.

Kami menyarankan agar Anda menyimpan cadangan hanya untuk satu mesin di bawah akun penyimpanan awan ini. Selain itu, jika pencadangan mesin lain lebih baru dari pencadangan mesin saat ini, skrip akan memilih pencadangan mesin tersebut.

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:

  ```
  #!/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`	nomor	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**.
`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`	nomor (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`)	nomor	Tidak	Nilai minimum kontrol putaran dalam kotak putaran. Jika pasangan tidak ditentukan, nilainya akan `0`.
`max` (khusus untuk `spinner`)	nomor	Tidak	Nilai maksimum kontrol putaran dalam kotak putaran. Jika pasangan tidak ditentukan, nilainya akan `100`.
`step` (khusus untuk `spinner`)	nomor	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` (untuk `string`, `multiString`, `password`, dan `enum`)	nomor	Tidak	Menentukan apakah nilai kontrol dapat kosong (`0`) atau tidak (`1`). Jika pasangan tidak ditentukan, nilai kontrol dapat kosong.

Jenis kontrol

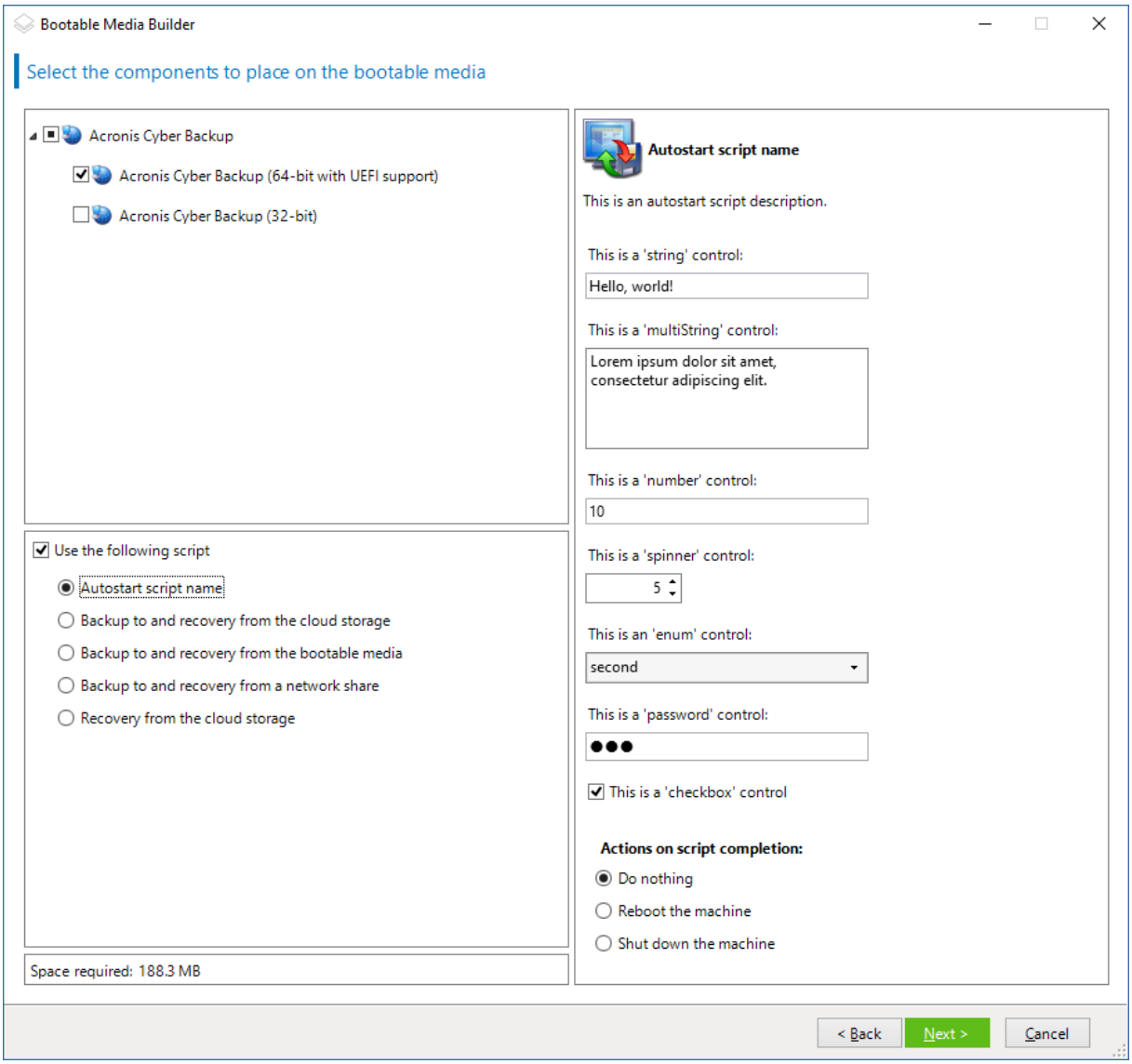
Nama	Deskripsi
`string`	Kotak teks baris tunggal yang tidak dibatasi digunakan untuk memasukkan atau mengedit string pendek.
`multiString`	Kotak teks multi-baris yang tidak dibatasi digunakan untuk memasukkan atau mengedit string panjang.
`password`	Kotak teks baris tunggal yang tidak dibatasi digunakan 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.
`checkbox`	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,
                        "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
            }
        }
}
```

Ini adalah tampilannya di Pembangun Media yang Dapat Di-boot.



Server manajemen

Saat membuat media yang dapat di-boot, Anda memiliki opsi untuk melakukan pra-konfigurasi pendaftaran media di server manajemen.

Mendaftarkan media akan memungkinkan Anda mengelola media melalui konsol web Cyber Protect seolah-olah media tersebut adalah mesin terdaftar. Selain kemudahan akses jarak jauh, cara ini juga memberi administrator kemampuan untuk melacak semua operasi yang dilakukan di bawah media yang dapat di-boot. Operasi ini masuk dalam **Aktivitas**, sehingga Anda dimungkinkan untuk melihat kapan dan siapa yang memulai operasi.

Jika pendaftaran tidak dipra-konfigurasi, Anda masih dapat mendaftarkan media setelah mem-boot mesin darinya.

Untuk melakukan pra-konfigurasi pendaftaran di server manajemen

1. Pilih kotak centang **Daftarkan media di server manajemen**.
2. Pada **Nama atau IP server**, tentukan nama host atau alamat IP mesin tempat server manajemen diinstal. Anda dapat memilih salah satu dari format berikut:
   - `http://<server>`. Misalnya, `http://10.250.10.10` atau `http://server1`
   - `<alamat IP>`. Misalnya, `10.250.10.10`
   - `<nama host>`. Misalnya, `server1` atau `server1.example.com`
3. Pada **Port**, tentukan port yang akan digunakan untuk mengakses server manajemen. Nilai default adalah 9877.
4. Pada **Nama tampilan**, tentukan nama yang akan ditampilkan untuk mesin ini di konsol web Cyber Protect. Jika Anda membiarkan bidang ini kosong, nama tampilan akan ditetapkan ke salah satu dari pilihan berikut:
   - Jika mesin sebelumnya terdaftar di server manajemen, nama mesin akan sama.
   - Jika tidak, nama domain yang memenuhi syarat (FQDN) atau alamat IP mesin akan digunakan.
5. Pilih akun mana yang akan digunakan untuk mendaftarkan media di server manajemen. Opsi berikut tersedia:
   - **Minta nama pengguna dan kata sandi saat boot**

     Kredensial harus diberikan setiap kali mesin di-boot dari media.

     Agar registrasi berhasil, akun harus ada di dalam daftar administrator server manajemen (**Pengaturan** > **Akun**). Di konsol web Cyber Protect, media akan tersedia pada organisasi atau unit spesifik, sesuai dengan izin yang diberikan ke akun yang ditentukan.

     Di antarmuka media yang dapat di-boot, Anda dapat mengubah nama pengguna dan kata sandi dengan mengklik **Alat** > **Daftarkan media di server manajemen**.
   - **Daftar berdasarkan akun berikut**

     Mesin akan didaftarkan secara otomatis setiap kali di-boot dari media.

     Akun yang Anda tentukan harus ada dalam daftar administrator server manajemen (**Pengaturan** > **Akun**). Di konsol web Cyber Protect, media akan tersedia pada organisasi atau unit spesifik, sesuai dengan izin yang diberikan ke akun yang ditentukan.

     Pada antarmuka media yang dapat di-boot, *tidak* dimungkinkan untuk mengubah parameter pendaftaran.

Pengaturan jaringan

Saat membuat media yang dapat di-boot, Anda memiliki opsi untuk melakukan pra-konfigurasi koneksi jaringan yang akan digunakan oleh agen yang dapat di-boot. Parameter berikut dapat dipra-konfigurasi:

- 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 pra-konfigurasi, agen akan menggunakan konfigurasi otomatis DHCP. Anda juga memiliki kemampuan untuk mengonfigurasi pengaturan jaringan secara manual ketika agen yang dapat di-boot berjalan pada mesin.

Pra-konfigurasi beberapa koneksi jaringan

Anda dapat melakukan pra-konfigurasi pengaturan TCP/IP hingga sepuluh kartu antarmuka jaringan. 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 untuk menghemat media. Alamat MAC dari setiap NIC yang ada juga disimpan di media.

Anda dapat mengubah pengaturan, kecuali untuk alamat MAC; atau mengonfigurasi pengaturan untuk NIC yang tidak ada, jika perlu.

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 di atas.

Agen yang dapat di-boot menetapkan pengaturan yang sesuai pada setiap NIC yang dikenal, yang mengidentifikasi NIC dengan alamat MAC mereka. Setelah NIC dengan alamat MAC yang dikenal dikonfigurasi, pengaturan yang telah Anda buat untuk NIC yang tidak ada akan ditetapkan ke NIC yang tersisa, dimulai dari NIC yang tidak ditetapkan.

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 yang dikenal dan akan mengkonfigurasi NIC dalam urutan yang sama seperti yang Anda lakukan.

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 dalam jaringan cadangan khusus melalui pengaturan TCP/IP statis.

Port jaringan

Saat membuat media yang dapat di-boot, Anda memiliki opsi untuk melakukan pra-konfigurasi port jaringan yang didengarkan agen yang dapat di-boot untuk koneksi masuk dari utilitas `acrocmd`. Pilihan yang tersedia di antaranya:

- port default
- port yang sedang digunakan
- port baru (masukkan nomor port)

Jika port belum dipra-konfigurasi, agen akan menggunakan port 9876.

Driver untuk Universal Restore

Saat membuat media yang dapat di-boot, Anda memiliki opsi untuk menambahkan driver Windows ke media. Driver akan digunakan oleh Universal Restore untuk mem-boot Windows yang dimigrasikan ke perangkat keras yang berbeda.

Anda akan dapat mengonfigurasi Universal Restore:

- guna mencari media untuk driver yang paling sesuai dengan perangkat keras target
- guna mendapatkan driver penyimpanan massal yang Anda tentukan secara eksplisit dari media. Ini diperlukan ketika perangkat keras target memiliki pengontrol penyimpanan massal tertentu (seperti SCSI, RAID, atau adaptor Fibre Channel) untuk hard disk.

Driver akan ditempatkan di folder Drivers yang dapat dilihat di media yang dapat di-boot. Driver tidak dimuat ke dalam RAM mesin target, oleh karena itu, media harus tetap dimasukkan atau dihubungkan selama operasi Universal Restore.

Menambahkan driver ke media yang dapat di-boot tersedia saat Anda membuat media yang dapat dilepas maupun ISO atau media yang dapat dicopot, seperti flash drive. Driver tidak dapat diunggah di WDS/RIS.

Driver hanya dapat ditambahkan ke daftar dalam grup, dengan menambahkan file INF atau folder yang berisi file tersebut. Memilih driver individual dari file INF tidak dimungkinkan, tetapi pembangun media menunjukkan konten file untuk informasi Anda.

Untuk menambahkan driver:

1. Klik **Tambah** dan jelajahi ke file INF atau folder yang berisi file INF.
2. Pilih file atau folder INF.
3. Klik **OK**.

Driver hanya dapat dihapus dari daftar dalam grup, dengan menghapus file INF.

Untuk menghapus driver:

1. Pilih file INF.
2. Klik **Hapus**.

Media yang dapat di-boot berbasis WinPE

Pembangun Media Yang Dapat Di-Boot menyediakan dua metode untuk mengintegrasikan Acronis Cyber Protect dengan WinPE:

- Membuat PE ISO dengan plug-in dari awal.
- Menambahkan Plug-in Acronis ke file WIM untuk tujuan apa pun pada waktu mendatang (pembuatan ISO manual, yang menambahkan alat lain ke citra dan sebagainya).

Anda dapat membuat citra PE berbasis WinRE tanpa persiapan tambahan, atau membuat citra PE setelah menginstal Windows Automated Installation Kit (AIK) atau Windows Assessment and Deployment Kit (ADK).

Citra PE berbasis WinRE

Pembuatan citra berbasis WinRE didukung untuk sistem operasi berikut:

- Windows 7 (64-bit)
- Windows 8, 8.1, 10 (32-bit dan 64-bit)
- Windows Server 2012, 2016, 2019 (64-bit)

Citra PE

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 untuk Windows 10)

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).

Citra PE berbasis WinPE 4 dan yang lebih baru membutuhkan sekitar 1 GB RAM agar dapat bekerja.

Catatan
Fungsionalitas manajemen disk tidak tersedia untuk media yang dapat di-boot berbasis Windows PE 4.0 dan versi yang lebih baru. Jadi, manajemen disk didukung untuk Windows 7 dan sistem operasi versi sebelumnya. Untuk menjalankan operasi manajemen di Windows 8 dan versi setelahnya, Anda harus menginstal Acronis Disk Director. Untuk informasi lebih lanjut, lihat artikel KB ini: https://kb.acronis.com/content/47031.

Persiapan: WinPE 2.x dan 3.x

Agar dapat membuat atau memodifikasi citra PE 2.x atau 3.x, instal Pembangun Media yang Dapat Di-boot pada mesin tempat Windows Automated Installation Kit (AIK) diinstal. Jika Anda tidak memiliki mesin dengan AIK, persiapkan dengan langkah berikut.

Untuk menyiapkan mesin dengan AIK

1. Unduh dan instal Windows Automated Installation Kit.

   Automated Installation Kit (AIK) untuk Windows Vista (PE 2.0):
   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en

   Automated Installation Kit (AIK) untuk Windows Vista SP1 dan Windows Server 2008 (PE 2.1):
   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=en

   Automated Installation Kit (AIK) untuk Windows 7 (PE 3.0):
   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en

   Automated Installation Kit (AIK) Supplement untuk Windows 7 SP1 (PE 3.1):
   http://www.microsoft.com/download/en/details.aspx?id=5188

   Anda dapat menemukan persyaratan sistem untuk instalasi dengan mengikuti tautan di atas.
2. [Optional] Bakar WAIK ke DVD atau salin ke flash drive.
3. Instal Microsoft .NET Framework dari kit ini (NETFXx86 atau NETFXx64, tergantung pada perangkat keras Anda).
4. Instal Microsoft Core XML (MSXML) 5.0 atau 6.0 Parser dari kit ini.
5. Instal Windows AIK dari kit ini.
6. Instal Pembangun Media yang Dapat Di-boot di mesin yang sama.

Disarankan agar Anda memahami dokumentasi bantuan yang disertakan dengan Windows AIK. Untuk mengakses dokumentasi, pilih **Microsoft Windows AIK -> Documentation** (Dokumentasi) dari menu start.

Persiapan: WinPE 4.0 ke atas

Agar dapat membuat atau memodifikasi image PE 4 atau yang lebih baru, instal Pembangun Media yang Dapat Di-boot pada mesin di mana Windows Assessment and Deployment Kit (ADK) diinstal. Jika Anda tidak memiliki mesin dengan ADK, persiapkan dengan lengkah berikut.

Untuk menyiapkan mesin dengan ADK

1. Unduh program pengaturan Assessment and Deployment Kit.

   Assessment and Deployment Kit (ADK) untuk Windows 8 (PE 4.0): http://www.microsoft.com/en-us/download/details.aspx?id=30652.

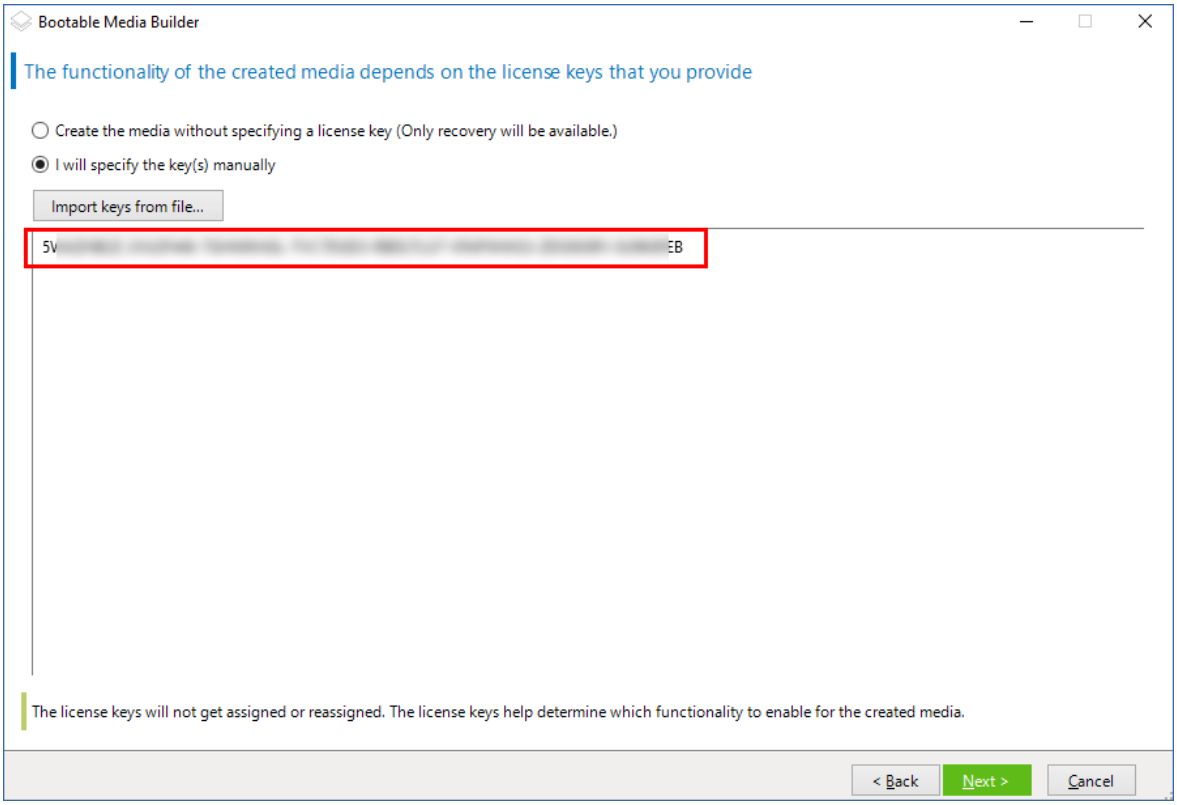
Assessment and Deployment Kit (ADK) untuk Windows 8.1 (PE 5.0):
http://www.microsoft.com/en-US/download/details.aspx?id=39982.
Assessment and Deployment Kit (ADK) untuk Windows 10 (PE untuk Windows 10):
https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx.
Anda dapat menemukan persyaratan sistem untuk instalasi dengan mengikuti tautan di atas.

2. Instal Assessment and Deployment Kit pada mesin.
3. Instal Pembangun Media yang Dapat Di-boot di mesin yang sama.

Menambahkan Plug-in Acronis ke WinPE

Untuk menambahkan Plug-in Acronis ke WinPE:

1. Mulai Pembangun Media Yang Dapat Di-Boot.
2. Untuk membuat media yang dapat di-boot dengan fitur lengkap, tentukan kunci lisensi Acronis Cyber Protect. Kunci ini digunakan untuk menentukan fitur yang akan disertakan dalam media yang dapat di-boot. Tidak ada lisensi yang akan dibatalkan dari mesin mana pun.
   Jika Anda tidak menentukan kunci lisensi, media yang dapat di-boot yang dihasilkan hanya dapat digunakan untuk operasi pemulihan.



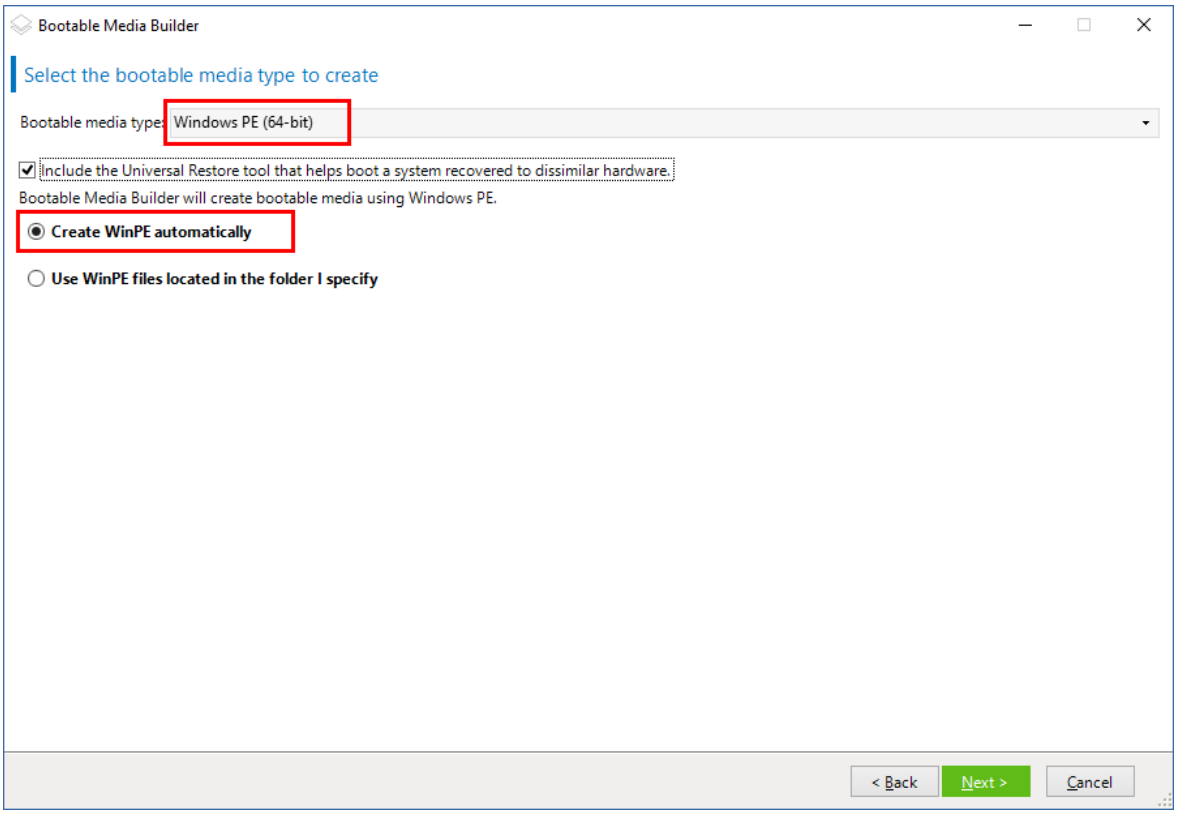
3. Pilih **Tipe media yang dapat di-boot: Windows PE** atau **Tipe media yang dapat di-boot: Windows PE (64-bit)**. Media 64-bit diperlukan untuk mem-boot mesin yang menggunakan Unified Extensible Firmware Interface (UEFI).
   Jika Anda memilih **Tipe media yang dapat di-boot: Windows PE**, lakukan langkah berikut terlebih dahulu:

- Klik **Unduh Plug-in untuk WinPE (32-bit)**.
- Simpan plug-in ke **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**.

Jika Anda berencana untuk memulihkan sistem operasi ke perangkat keras yang berbeda atau ke mesin virtual dan ingin memastikan kemampuan boot sistem, pilih kotak centang **Sertakan alat Universal Restore...**.

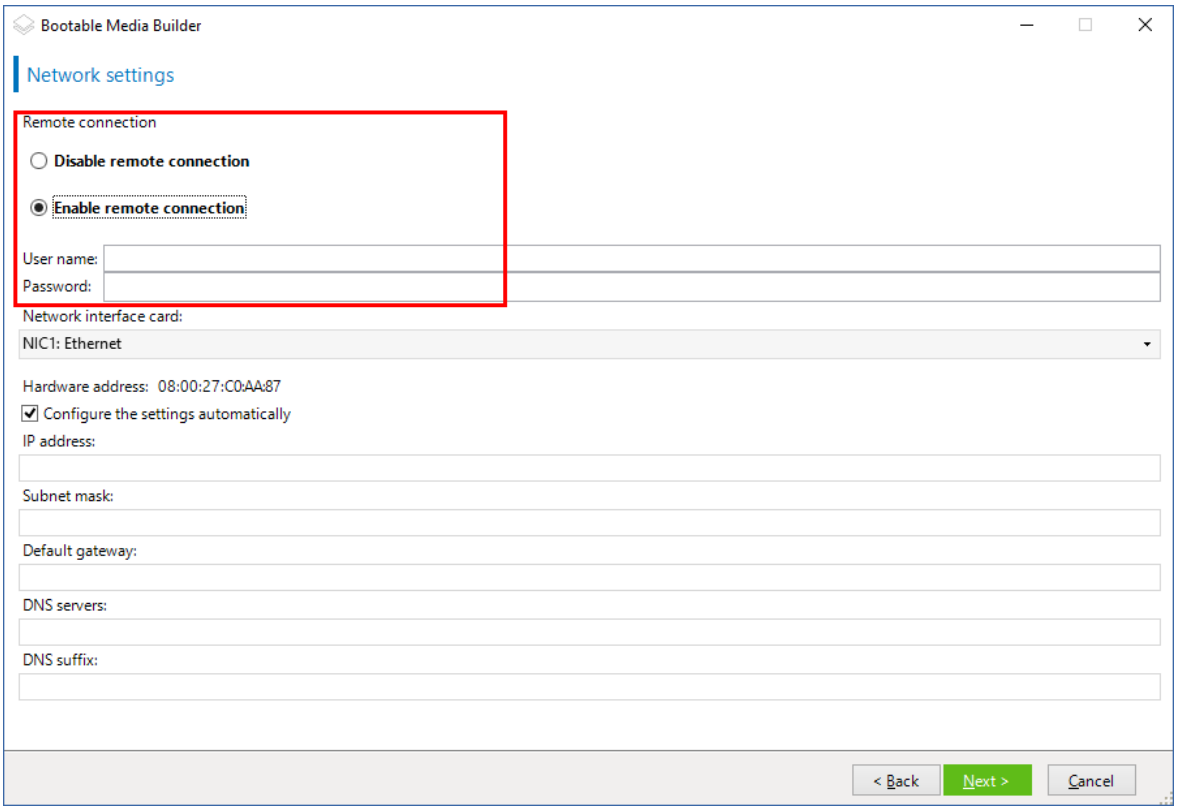
4. Pilih **Buat WinPE secara otomatis**.

   Perangkat lunak menjalankan skrip yang sesuai dan melanjutkan ke jendela berikutnya.



5. Pilih bahasa yang akan digunakan dalam media yang dapat di-boot.
6. Pilih apakah akan mengaktifkan atau menonaktifkan koneksi jarak jauh ke mesin yang di-boot dari media. Jika diaktifkan, masukkan nama pengguna dan kata sandi yang akan ditentukan dalam baris perintah jika utilitas `acrocmd` berjalan di mesin lain. Anda juga dapat membiarkan kotak ini kosong, dan koneksi jarak jauh melalui antarmuka baris perintah pun dapat dilakukan tanpa kredensial.

   Kredensial ini juga diperlukan ketika Anda mendaftarkan media di server manajemen dari konsol web Cyber Protect.



7. Tentukan pengaturan jaringan untuk adaptor jaringan mesin atau pilih konfigurasi otomatis DHCP.

Catatan
Pengaturan jaringan hanya tersedia dengan lisensi Acronis Cyber Protect 15 Tingkat lanjut dan Acronis Cyber Protect 15 Cadangan Tingkat Lanjut. Untuk perbandingan fitur terperinci, lihat artikel basis pengetahuan ini.

8. [Opsional] Pilih cara mendaftarkan media pada server manajemen saat booting. Untuk informasi lebih lanjut tentang pengaturan pendaftaran, lihat Server manajemen.
9. [Opsional] Tentukan driver Windows yang akan ditambahkan ke Windows PE.

   Setelah Anda mem-boot mesin ke Windows PE, driver dapat membantu Anda mengakses perangkat tempat cadangan berada. Tambahkan driver 32-bit jika Anda menggunakan distribusi WinPE 32-bit atau driver 64-bit jika Anda menggunakan distribusi WinPE 64-bit.

   Selain itu, Anda akan dapat menunjuk ke driver yang ditambahkan saat mengonfigurasi Universal Restore untuk Windows. Untuk Universal Restore, tambahkan driver 32 bit atau 64 bit tergantung pada apakah Anda berencana memulihkan sistem operasi Windows 32 bit atau 64 bit.

   Untuk menambahkan driver:

   - Klik **Tambahkan** dan tentukan jalur ke file .inf yang diperlukan untuk SCSI, RAID, pengontrol SATA, adaptor jaringan, tape drive, atau perangkat lain yang sesuai.
   - Ulangi prosedur ini untuk setiap driver yang ingin Anda sertakan dalam media WinPE yang dihasilkan.

10. Pilih apakah Anda ingin membuat image ISO atau WIM atau mengunggah media di server (WDS atau RIS).
11. Tentukan jalur penuh ke file image yang dihasilkan termasuk nama file, atau tentukan server dan berikan nama pengguna dan kata sandi untuk mengaksesnya.
12. Periksa pengaturan Anda di layar ringkasan, lalu klik **Lanjutkan**.
13. Salin .ISO ke CD atau DVD menggunakan alat bantu pihak ketiga atau siapkan flash drive yang dapat di-boot.

Setelah mesin melakukan boot ke WinPE, agen akan dimulai secara otomatis.

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:

```
copy c:\AcronisMedia.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.

Untuk informasi lebih lanjut tentang cara menyesuaikan Windows PE 2.x dan 3.x, lihat Panduan Pengguna Lingkungan Pra-Instalasi Windows (Winpe.chm). Informasi tentang cara menyesuaikan Windows PE 4.0 dan yang lebih baru tersedia di Microsoft TechNet Library.

Menghubungkan ke mesin yang di-boot dari media

Setelah mesin melakukan boot dari media yang dapat di-boot, terminal mesin akan menampilkan jendela startup dengan alamat IP yang diperoleh dari DHCP atau diatur sesuai dengan nilai yang telah dikonfigurasi sebelumnya.

Mengonfigurasi pengaturan jaringan

Untuk mengubah pengaturan jaringan untuk sesi saat ini, klik **Konfigurasi jaringan** di jendela startup. 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**.

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.

Koneksi jarak jauh

Untuk terhubung ke media dari jarak jauh, daftarkan di server manajemen, seperti yang dijelaskan dalam "Mendaftarkan media di server manajemen".

Mendaftarkan media di server manajemen

Mendaftarkan media yang dapat di-boot memungkinkan Anda mengelola media melalui konsol web Cyber Protect seolah-olah media tersebut adalah mesin terdaftar. Hal ini berlaku untuk semua media yang dapat di-boot, apa pun metode boot-nya (media fisik, Startup Recovery Manager, Server PXE Acronis, WDS, atau RIS). Namun, tidak dimungkinkan untuk mendaftarkan media yang dapat di-boot yang dibuat di macOS.

Mendaftarkan media hanya dimungkinkan jika minimal satu lisensi Lanjutan Acronis Cyber Protect ditambahkan ke server manajemen.

Anda dapat mendaftarkan media dari UI media.

Parameter pendaftaran dapat dipra-konfigurasi di opsi Server manajemen dari Pembangun Media yang Dapat Di-boot. Jika semua parameter registrasi sudah dikonfigurasi sejak awal, media akan muncul di konsol web Cyber Protect secara otomatis. Jika beberapa parameter sudah dipra-konfigurasi, beberapa langkah dalam prosedur berikut ini mungkin tidak tersedia.

Mendaftarkan media dari UI media

Media dapat diunduh atau dibuat menggunakan Pembangun Media yang Dapat Di-boot.

Untuk mendaftarkan media dari UI media

1. Boot mesin dari media.
2. Lakukan salah satu langkah berikut:
   - Di jendela startup, pada **Server manajemen**, klik **Edit**.
   - Di antarmuka media yang dapat di-boot, klik **Alat** > **Daftarkan media di server manajemen**.
3. Pada **Daftar di**, tentukan nama host atau alamat IP dari mesin tempat server manajemen diinstal. Anda dapat memilih salah satu dari format berikut:
   - `http://<server>`. Misalnya, `http://10.250.10.10` atau `http://server`
   - `<alamat IP>`. Misalnya, `10.250.10.10`
   - `<nama host>`. Misalnya, `server` atau `server.example.com`
4. Di **Nama pengguna** dan **Kata Sandi**, berikan kredensial akun yang ada dalam daftar administrator server manajemen (**Pengaturan** > **Akun**). Di konsol web Cyber Protect, media akan tersedia pada organisasi atau unit spesifik, sesuai dengan izin yang diberikan ke akun yang ditentukan.
5. Pada **Nama tampilan**, tentukan nama yang akan ditampilkan untuk mesin ini di konsol web Cyber Protect. Jika Anda membiarkan bidang ini kosong, nama tampilan akan ditetapkan ke salah satu dari pilihan berikut:
   - Jika mesin sebelumnya terdaftar di server manajemen, nama mesin akan sama.
   - Jika tidak, nama domain yang memenuhi syarat (FQDN) atau alamat IP mesin akan digunakan.
6. Klik **OK**.

Operasi lokal dengan media yang dapat di-boot

Operasi dengan media yang dapat di-boot mirip dengan operasi pencadangan dan 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
   Kami menyarankan Anda untuk 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. Cadangan yang dibuat menggunakan media yang dapat di-boot memiliki nama file yang disederhanakan. Nama standar ditetapkan ke cadangan hanya jika ditambahkan ke arsip yang ada dengan penamaan file standar atau jika tujuan tidak mendukung nama file yang disederhanakan.
4. Media yang dapat di-boot dengan representasi volume serupa Linux tidak dapat menulis cadangan ke volume berformat NTFS. Ganti ke media dengan representasi volume seperti Windows jika perlu. Untuk berganti representasi volume media yang dapat di-boot, klik **Alat bantu** > **Ubah representasi volume**.
5. Tugas tidak dapat dijadwalkan. Jika Anda perlu mengulangi operasi, konfigurasikan dari awal.
6. Masa aktif log terbatas pada sesi saat ini. Anda dapat menyimpan entri seluruh isi log atau log terfilter ke file.
7. Kubah terpusat tidak ditampilkan di pohon folder dari jendela **Arsip**.
   Untuk mengakses kubah yang dikelola, ketik string berikut ini di bidang **Path**:
   bsp://node_address/vault_name/
   Untuk mengakses kubah terpusat yang tidak dapat dikelola, ketik path lengkap ke folder kubah.
   Setelah memasukkan kredensial akses, Anda akan melihat daftar arsip yang berada di kubah.

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 berikut ini: **vga=ask**, kemudian lanjutkan dengan booting.
3. Dari daftar mode video yang didukung, pilih yang sesuai dengan mengetikkan nomornya (misalnya, **318**), lalu tekan **Enter**.

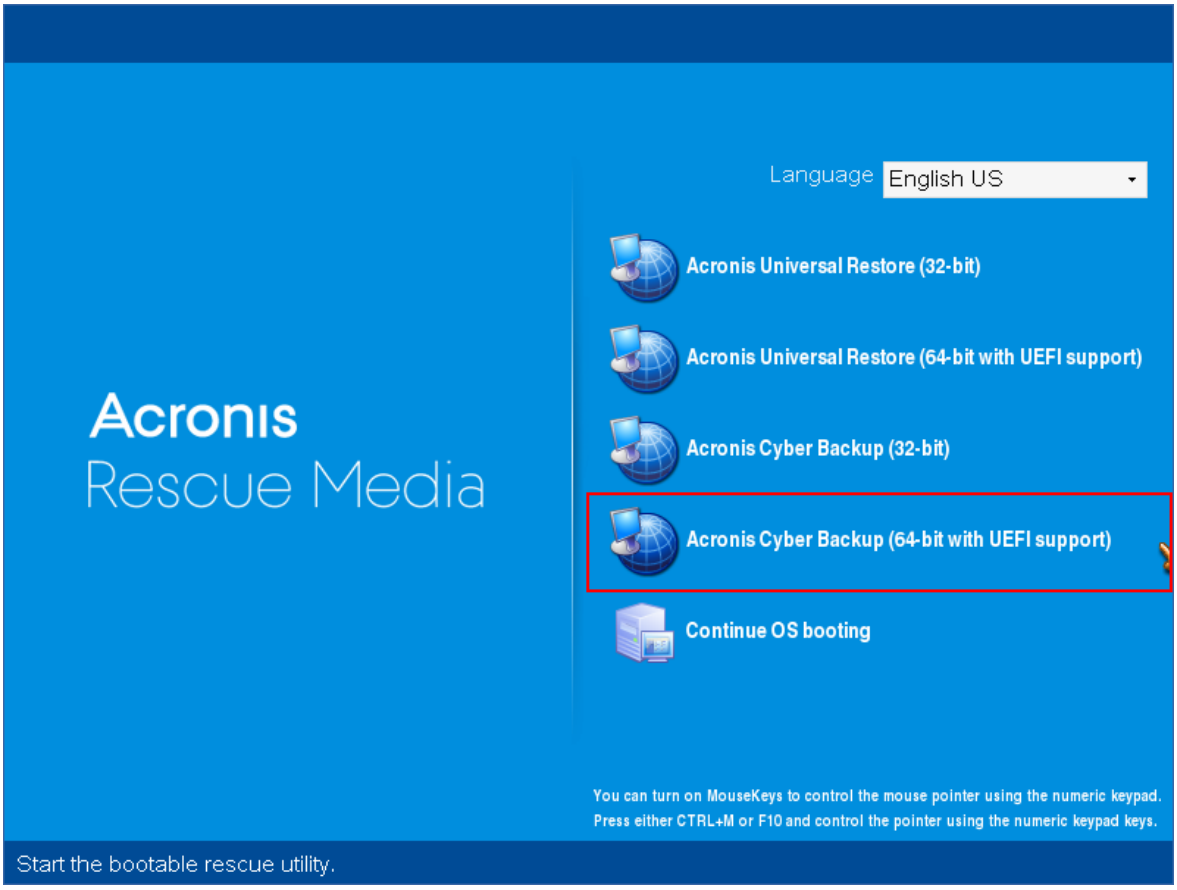
Jika tidak ingin mengikuti prosedur ini setiap kali Anda mem-boot konfigurasi perangkat keras tertentu, buat ulang media yang dapat di-boot dengan nomor mode yang sesuai (dalam contoh di atas, **vga = 0x318**) yang diketik di jendela **Parameter kernel**.

Cadangan dengan media yang dapat di-boot secara lokal

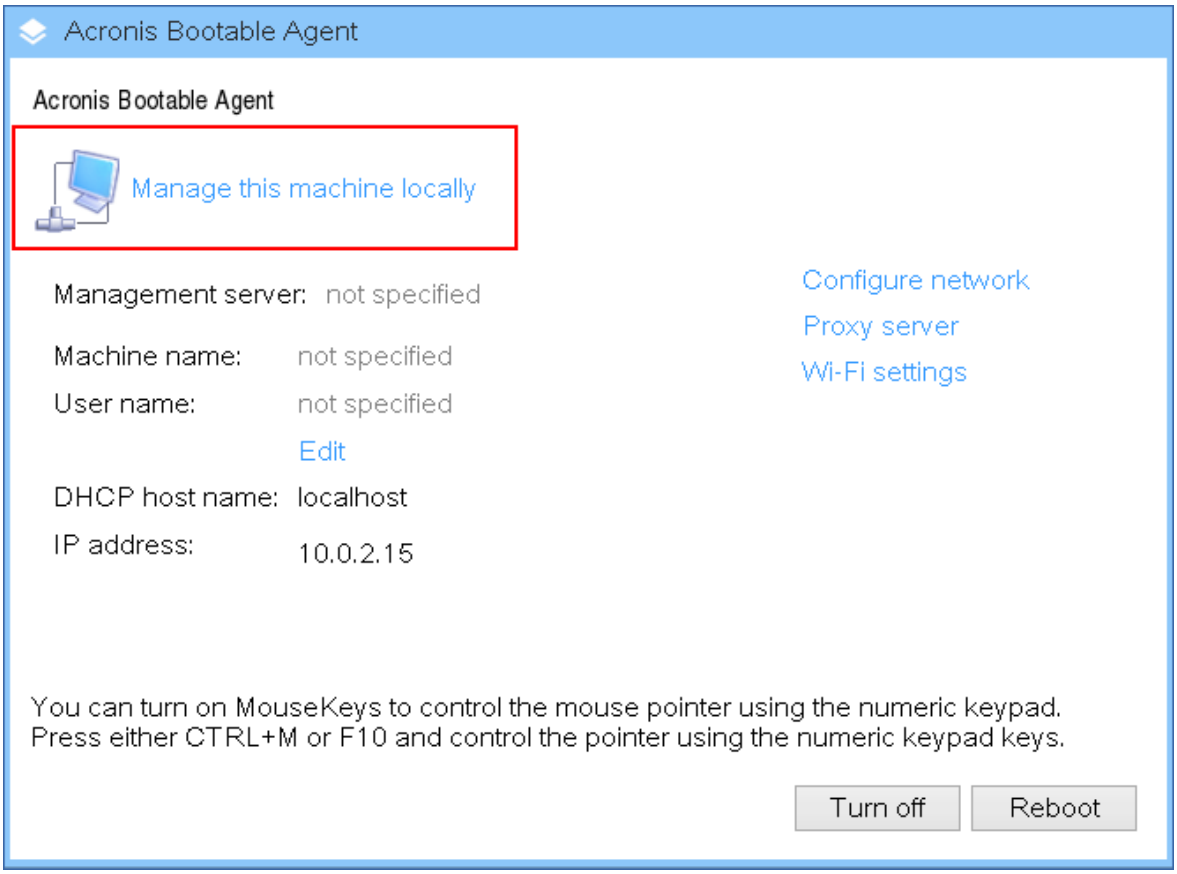
Anda hanya dapat mencadangkan data dengan media yang dapat di-boot yang sudah dibuat dengan Pembangun Media Yang Dapat Di-Boot, dan kunci lisensi Acronis Cyber Protect. Untuk informasi selengkapnya tentang cara membuat media yang dapat di-boot, lihat media yang dapat di-boot berbasis Linux atau media yang dapat di-boot berbasis Windows-PE.

Untuk mencadangkan data di bawah media yang dapat di-boot

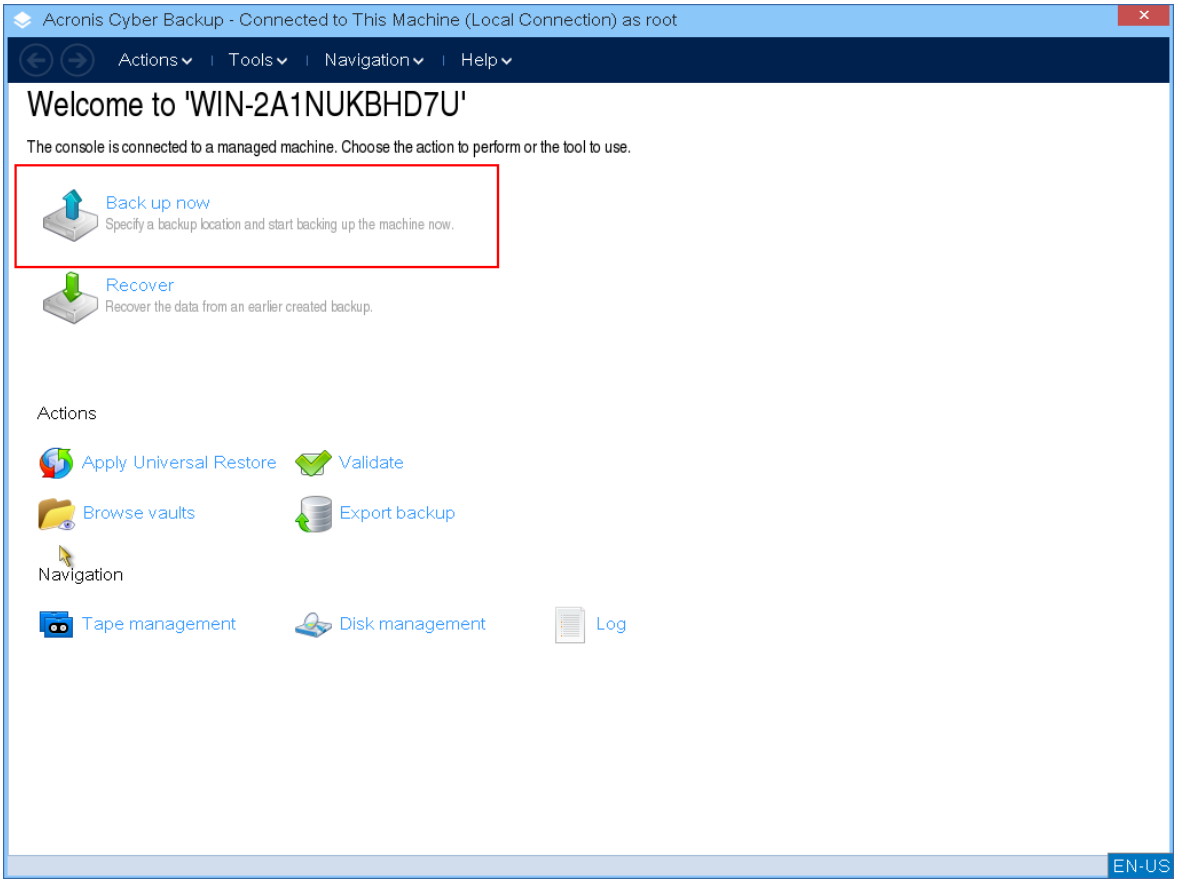
1. Booting dari media cadangan yang dapat di-boot Acronis.



2. Untuk mencadangkan mesin lokal, klik **Kelola mesin ini secara lokal**. Untuk koneksi jarak jauh, lihat Mendaftarkan media di server manajemen.



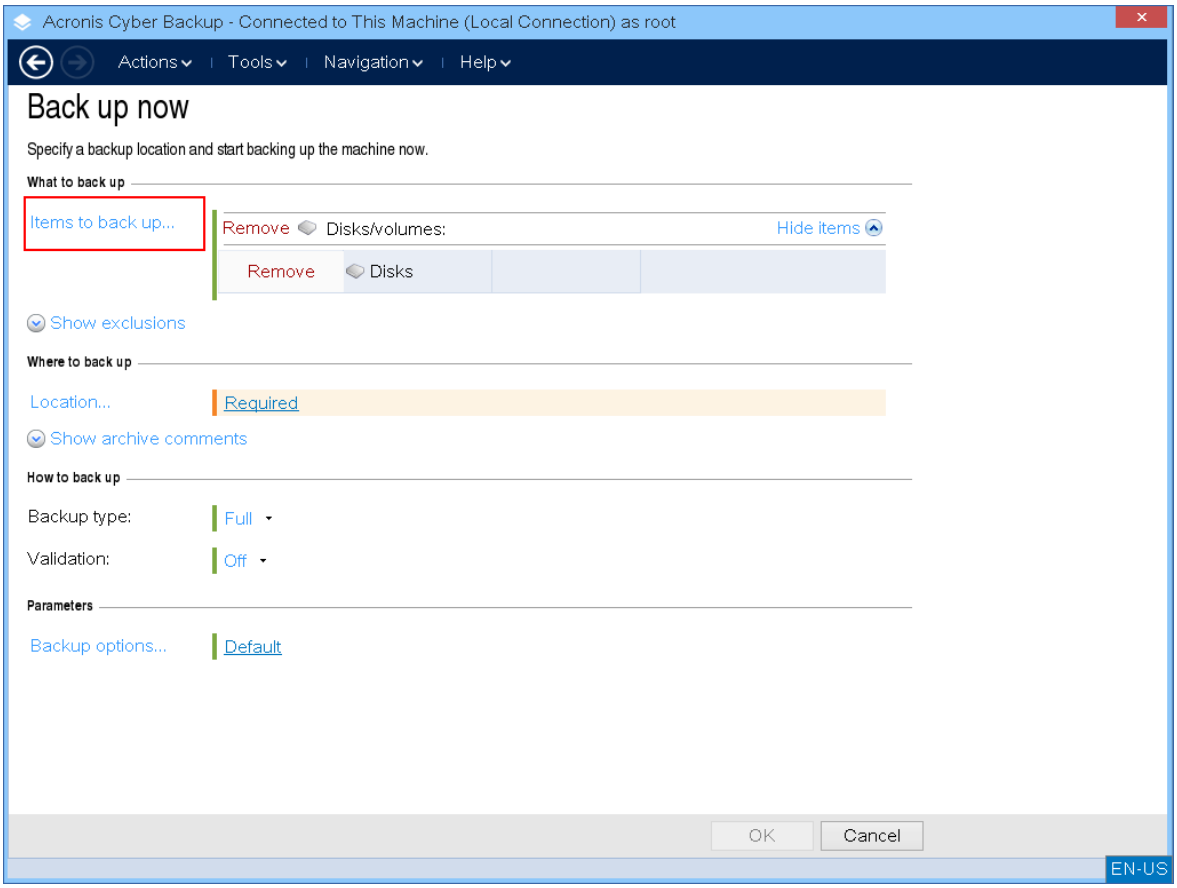
3. Klik **Cadangkan sekarang**.



4. Semua disk yang tidak dapat dipindah dari mesin secara otomatis dipilih untuk cadangan. Untuk mengubah data yang akan dicadangkan, klik **Item yang akan dicadangkan**, lalu pilih disk atau volume yang diinginkan.

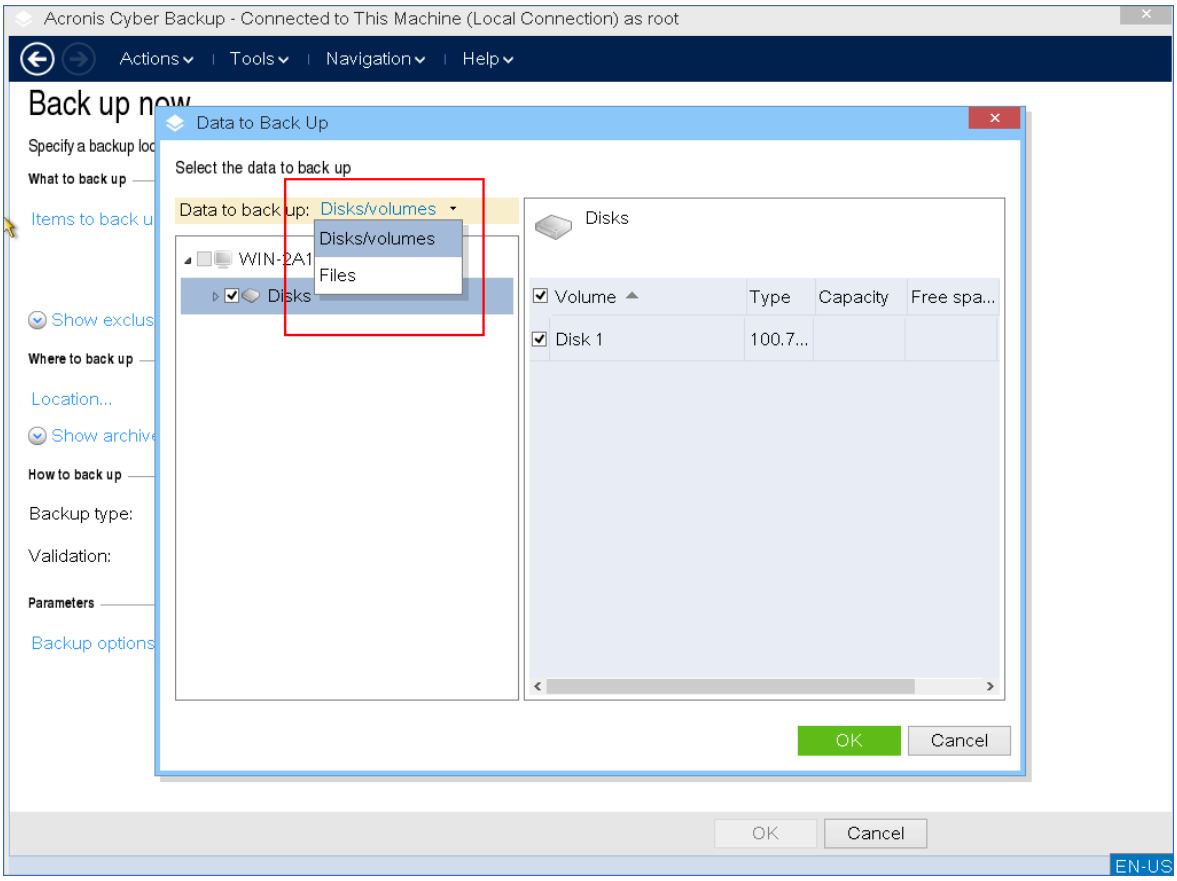
   Saat memilih data yang akan dicadangkan, Anda mungkin melihat pesan berikut ini: "*Mesin ini tidak dapat dipilih secara langsung. Versi agen sebelumnya terinstal pada mesin. Gunakan aturan kebijakan untuk memilih mesin ini untuk pencadangan.*" Ini adalah masalah GUI yang dapat diabaikan. Lanjutkan dengan memilih disk individual atau volume yang ingin Anda cadangkan.

   Catatan
   Dengan media yang dapat di-boot berbasis Linux, Anda mungkin melihat huruf drive yang berbeda dari yang ada di Windows. Cobalah mengidentifikasi drive atau partisi yang Anda butuhkan dari ukuran atau labelnya.

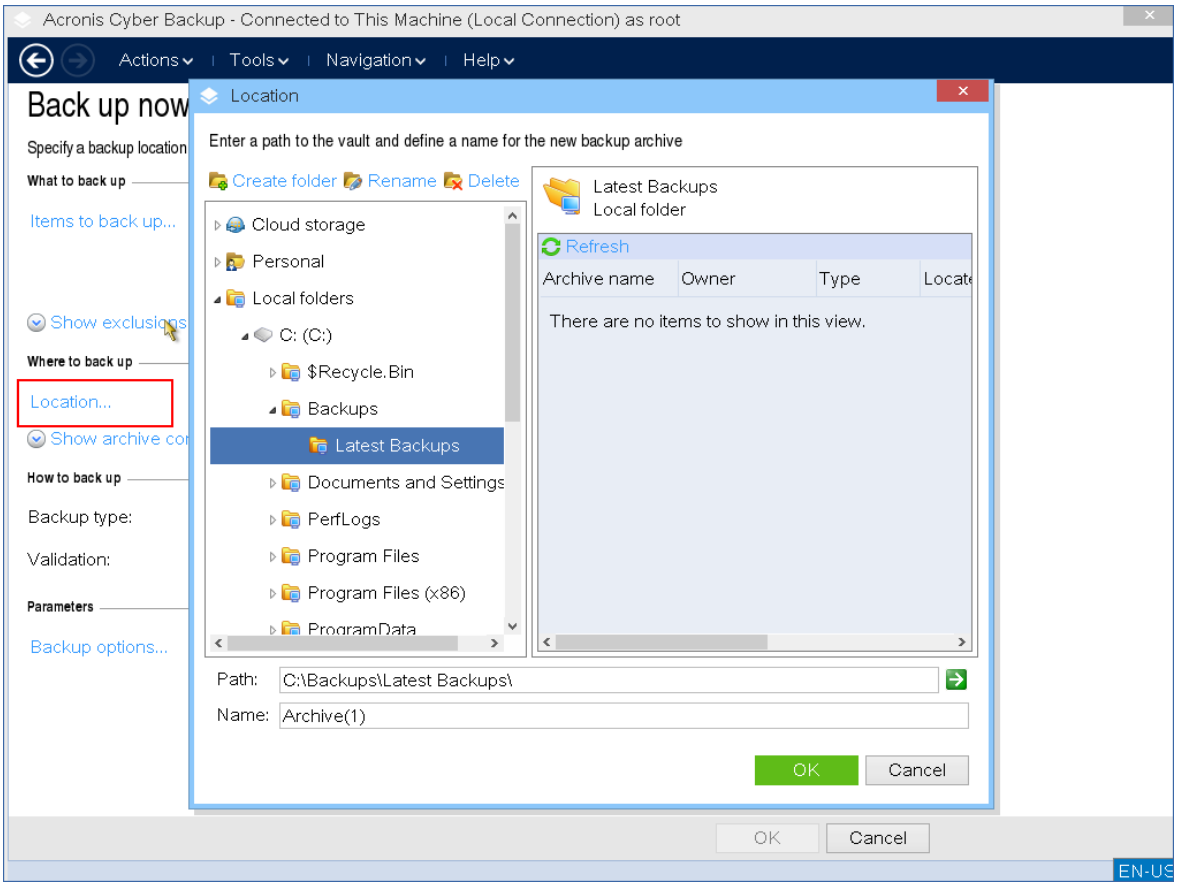


5. Jika Anda perlu mencadangkan file atau folder, bukan disk, beralihlah ke **File** di **Data yang akan dicadangkan**.

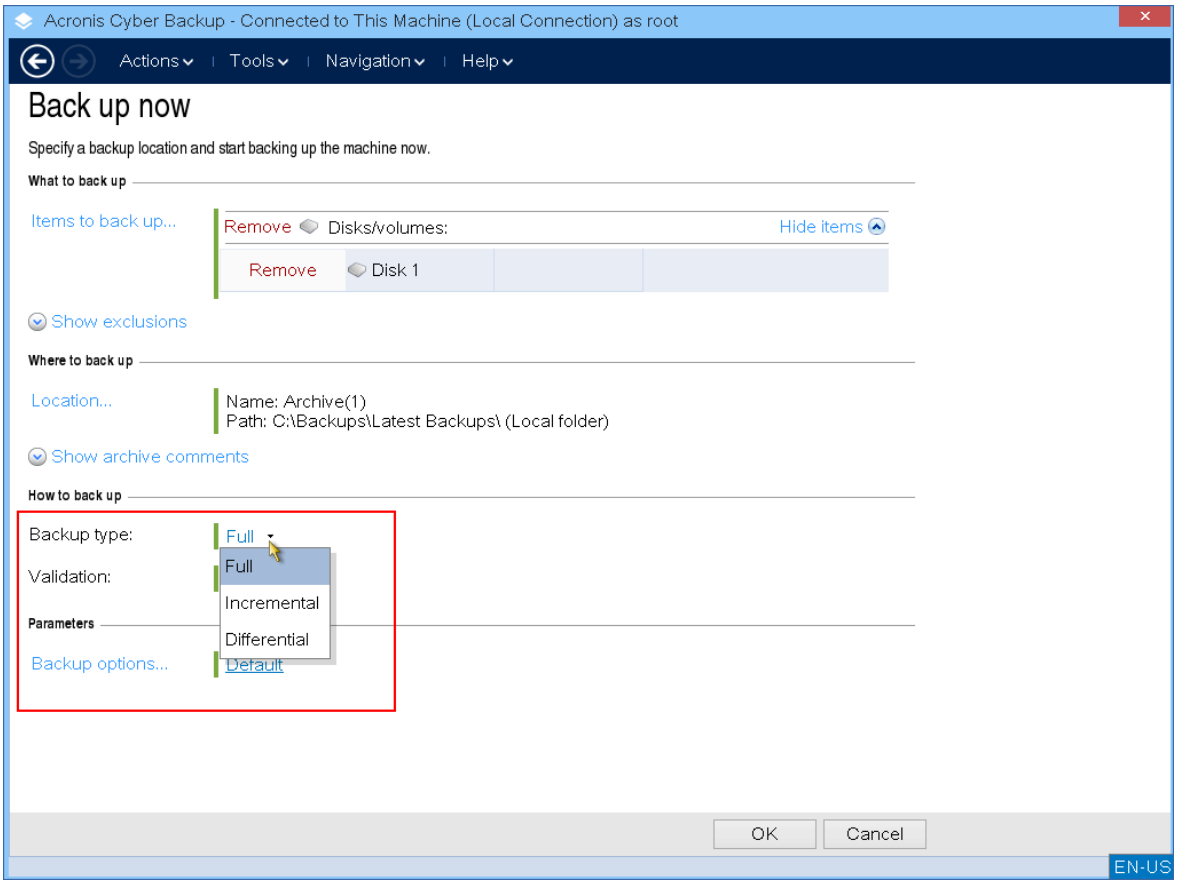
   Hanya cadangan disk/partisi dan file/folder yang ada di bawah media yang dapat di-boot. Jenis-jenis lain cadangan, seperti cadangan database, hanya tersedia di bawah sistem operasi yang berjalan.



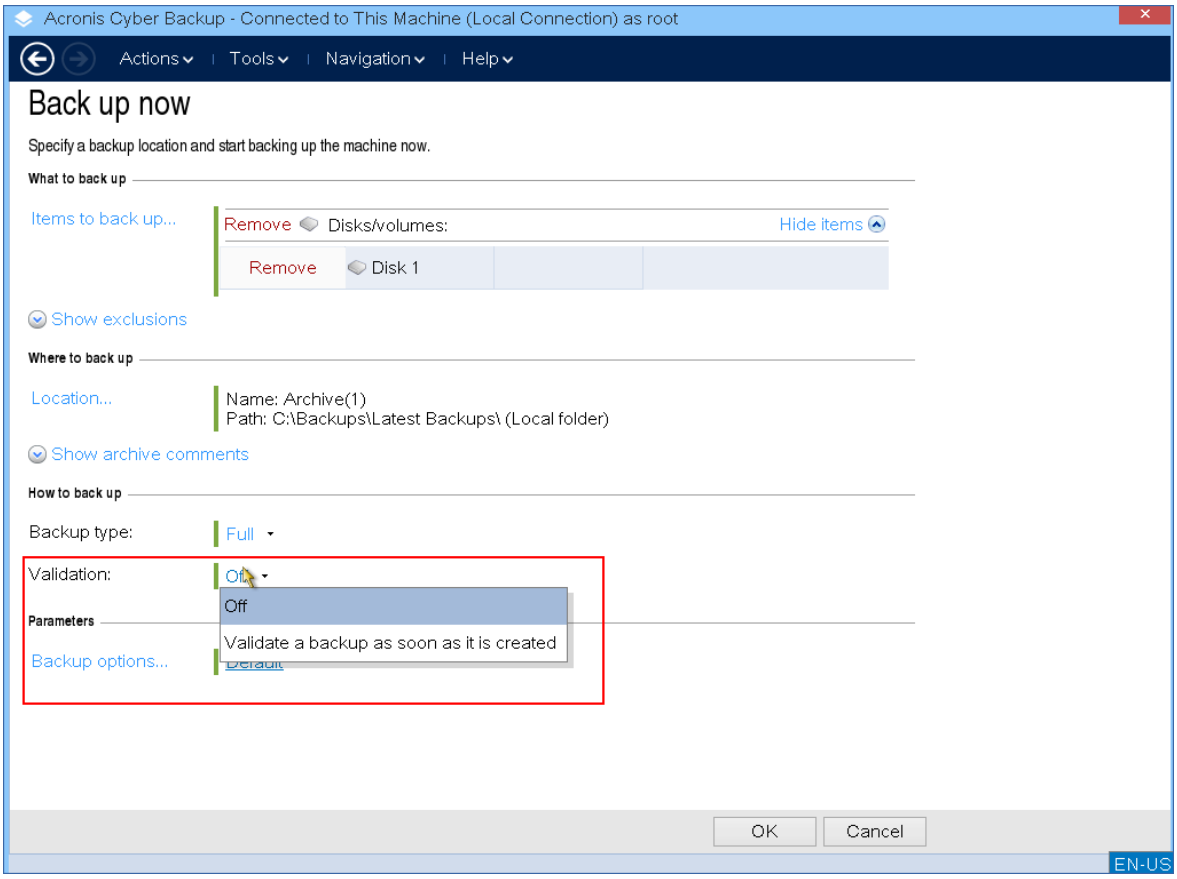
6. Klik **Lokasi** untuk memilih di mana cadangan akan disimpan.



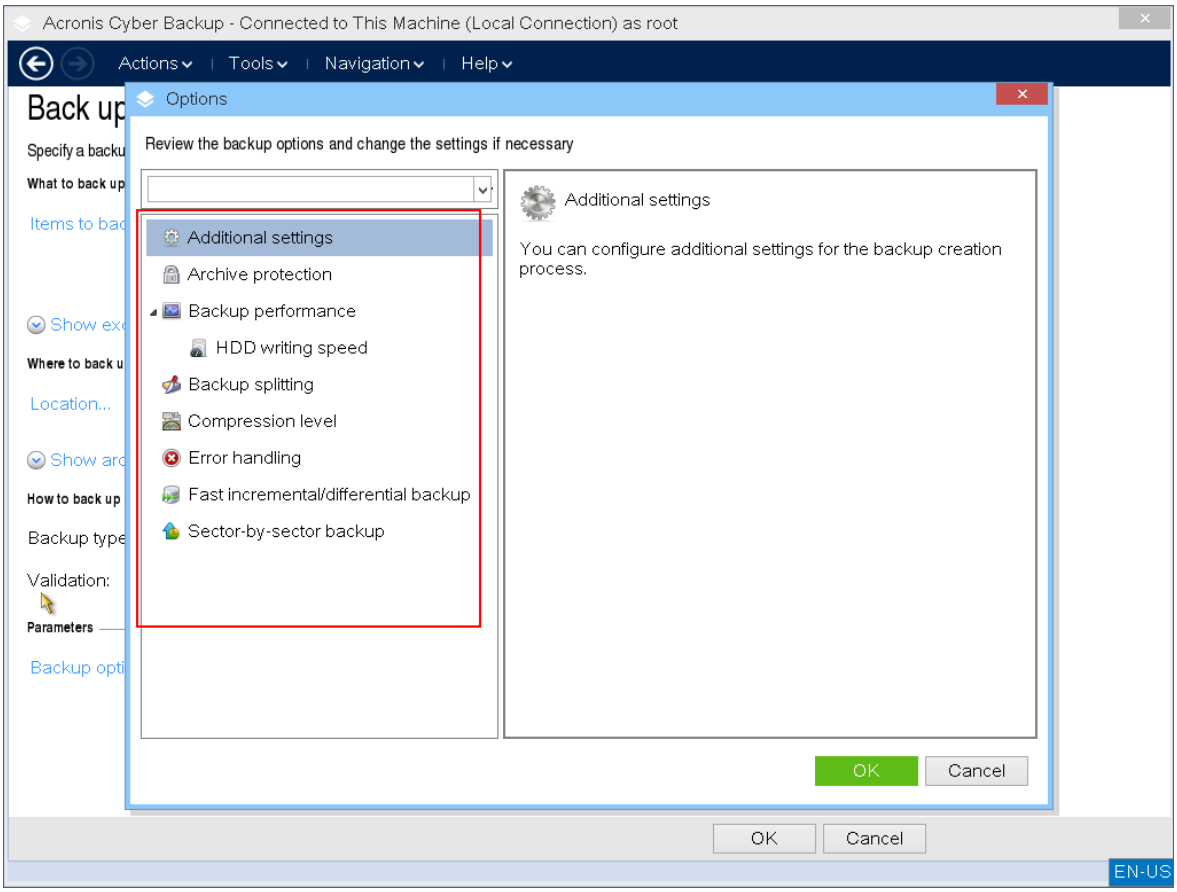
7. Tentukan lokasi dan nama untuk cadangan Anda.
8. Tentukan jenis cadangan. Jika ini adalah cadangan pertama di lokasi ini, cadangan penuh akan dibuat. Jika melanjutkan rangkaian pencadangan, Anda dapat memilih **Inkremental** atau **Diferensial** untuk menghemat ruang. Untuk informasi lebih lanjut tentang jenis cadangan, lihat https://kb.acronis.com/content/1536.



9. [Opsional] Jika Anda ingin memvalidasi cadangan file, pilih **Memvalidasi cadangan setelah dibuat**.

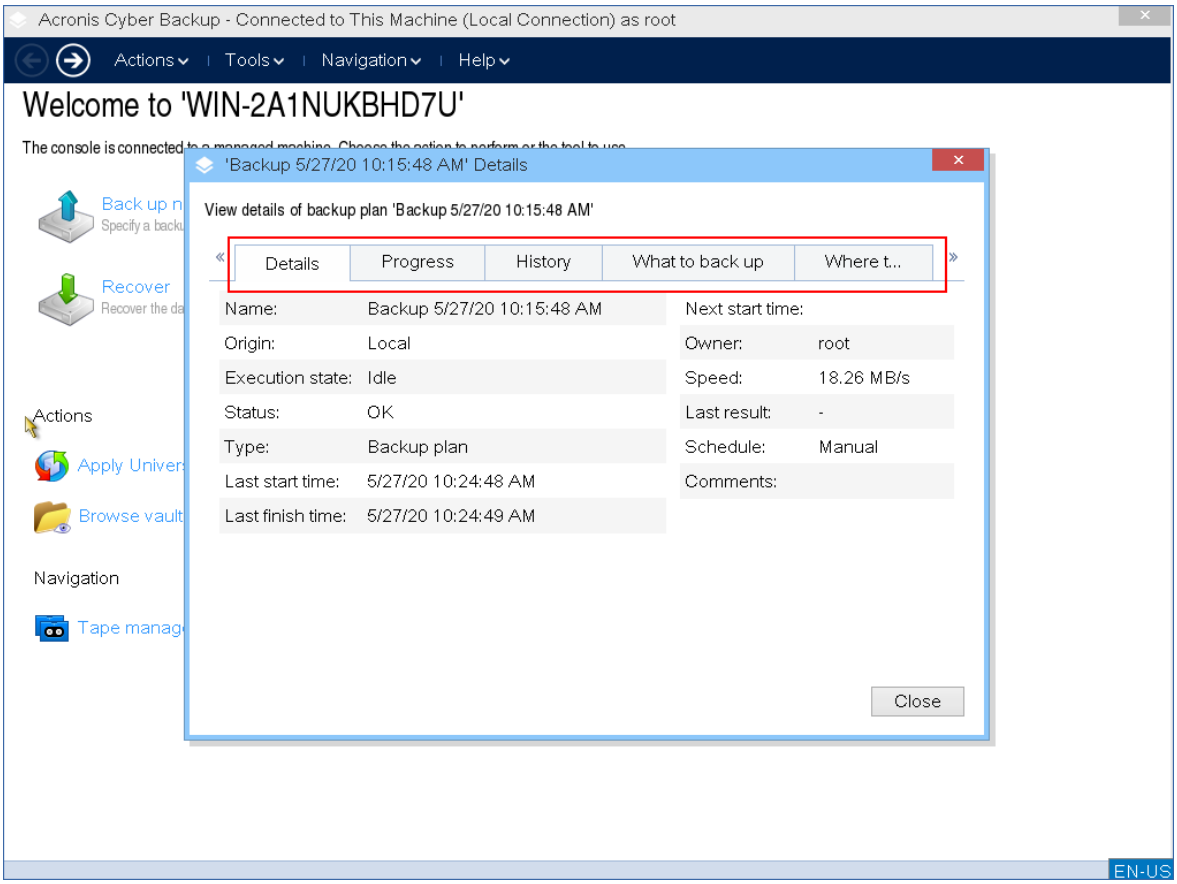


10. [Opsional] Tentukan opsi pencadangan yang mungkin Anda perlukan, seperti kata sandi untuk file cadangan, pemisahan cadangan, atau penanganan kesalahan.



11. Klik **OK** untuk memulai cadangan.

    Media yang dapat di-boot membaca data dari disk, mengompresnya menjadi file .tib, lalu menulis file ini ke lokasi yang dipilih. Ini tidak membuat snapshot disk karena tidak ada aplikasi yang berjalan.
12. Anda dapat memeriksa status tugas pencadangan dan informasi tambahan tentang pencadangan di jendela yang muncul.

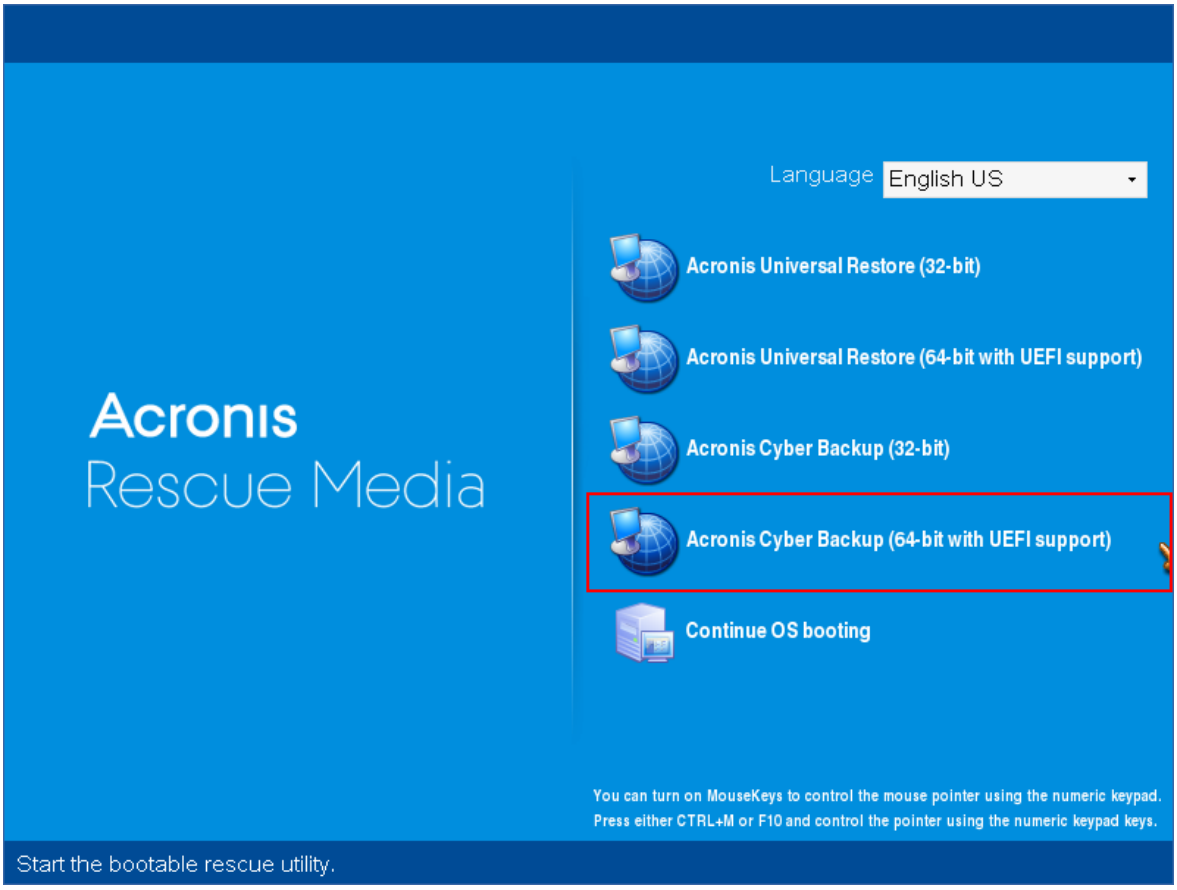


Pemulihan dengan media yang dapat di-boot secara lokal

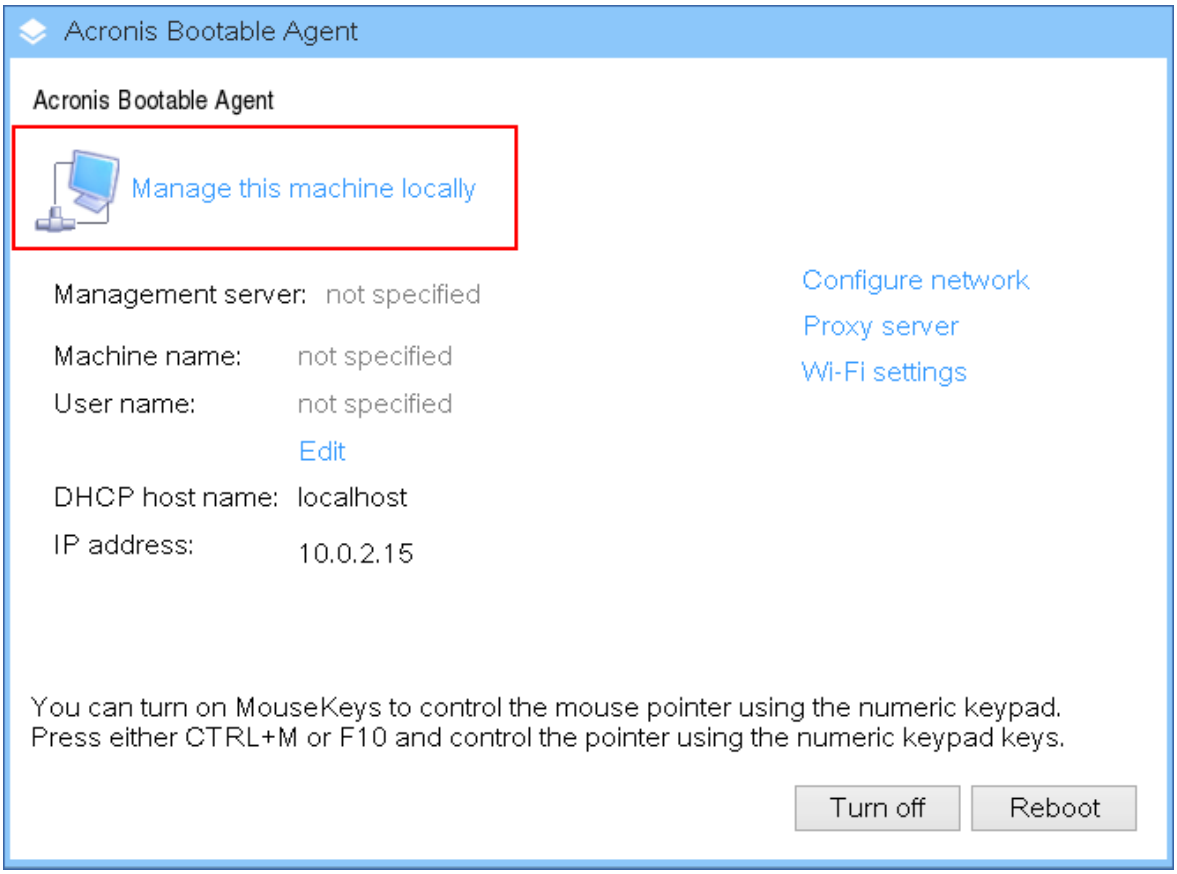
Operasi Pemulihan tersedia di media yang dapat di-boot yang dibuat dengan Pembangun Media Yang Dapat Di-Boot serta media siap pakai yang dapat di-boot yang diunduh.

Untuk memulihkan data di bawah media yang dapat di-boot

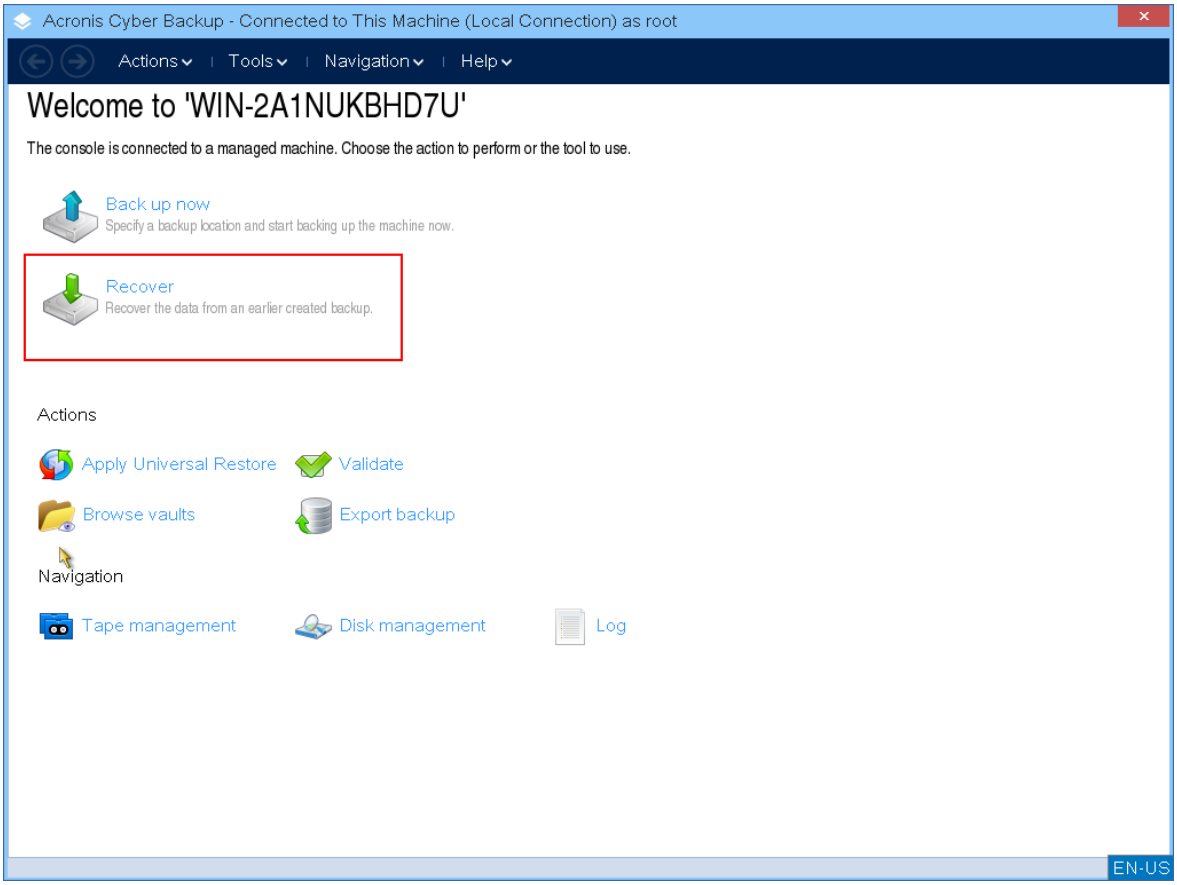
1. Booting dari media cadangan yang dapat di-boot Acronis.



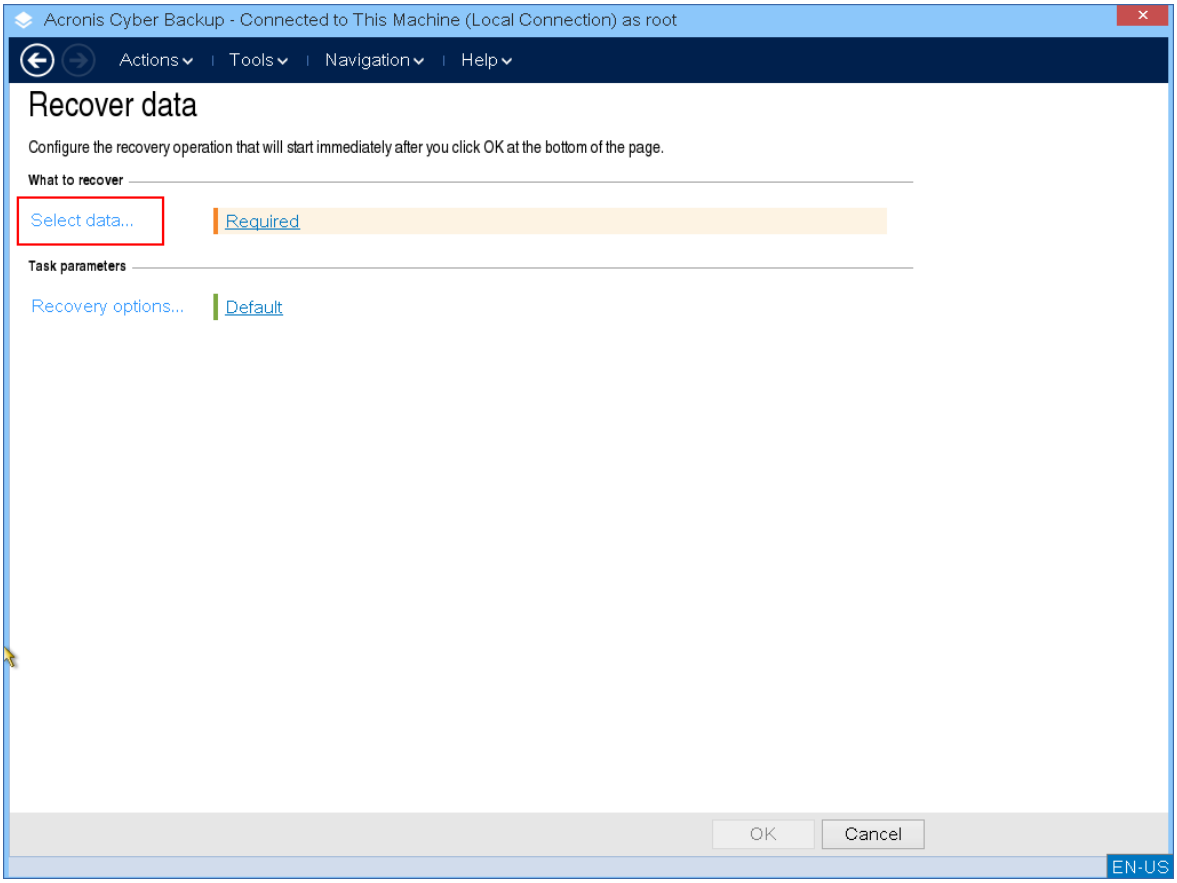
2. Untuk memulihkan data ke mesin lokal, klik **Kelola mesin ini secara lokal**. Untuk koneksi jarak jauh, lihat Mendaftarkan media di server manajemen.



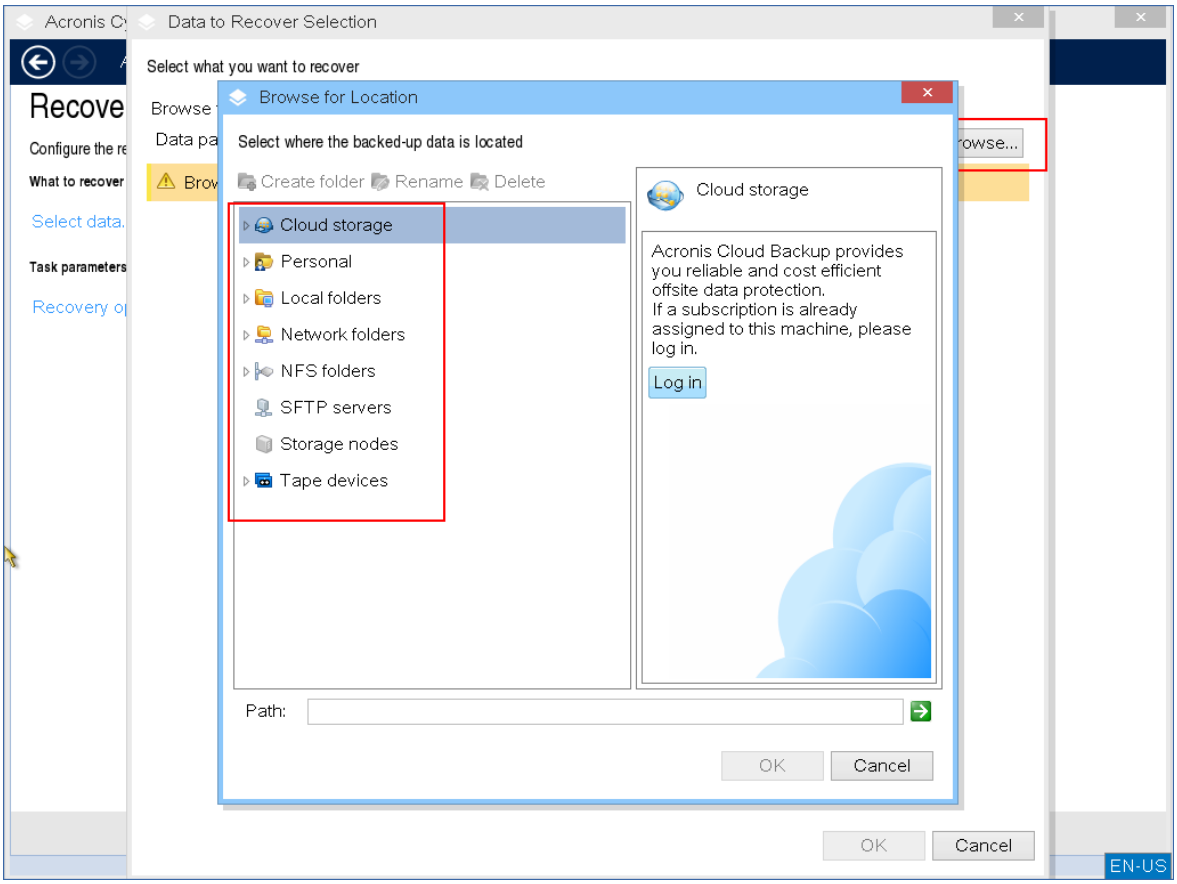
3. Klik **Pulihkan**.



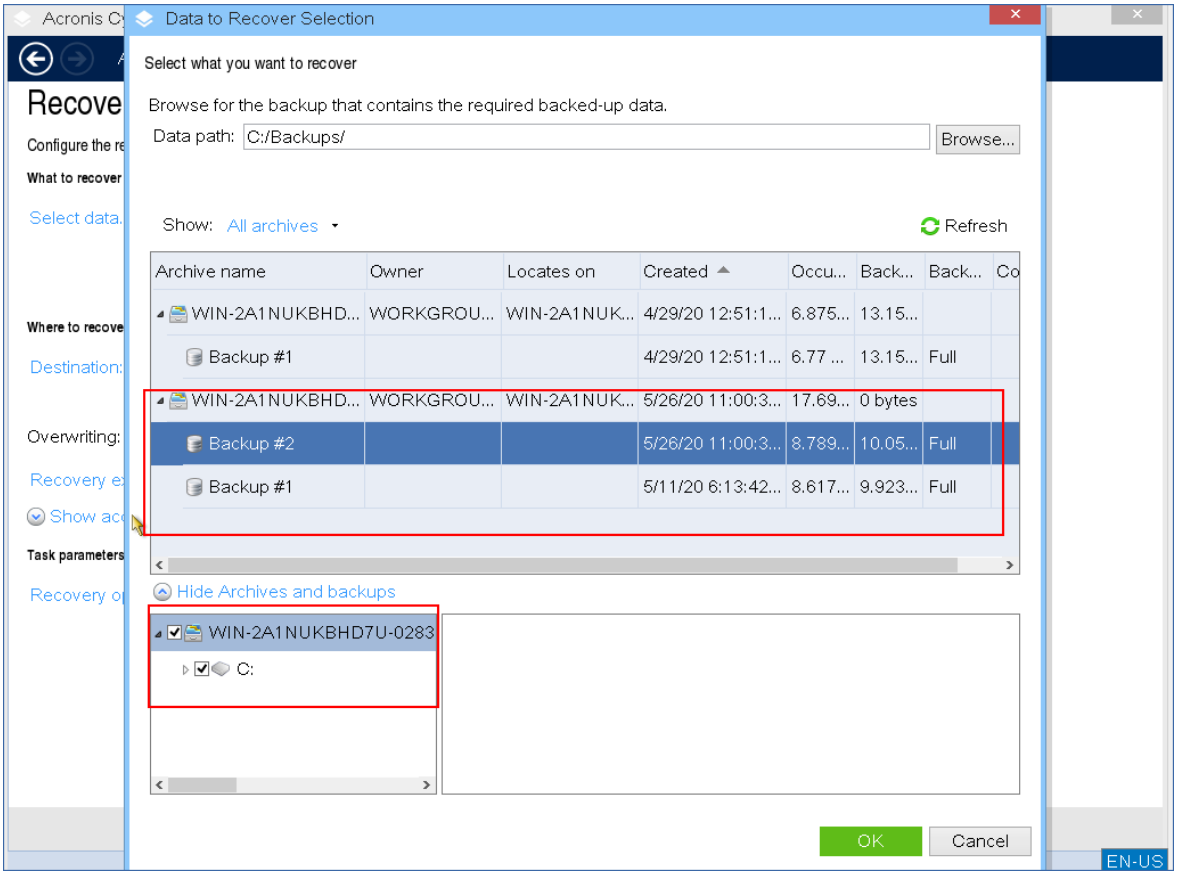
4. Di **Apa yang akan dipulihkan**, klik **Pilih data**.



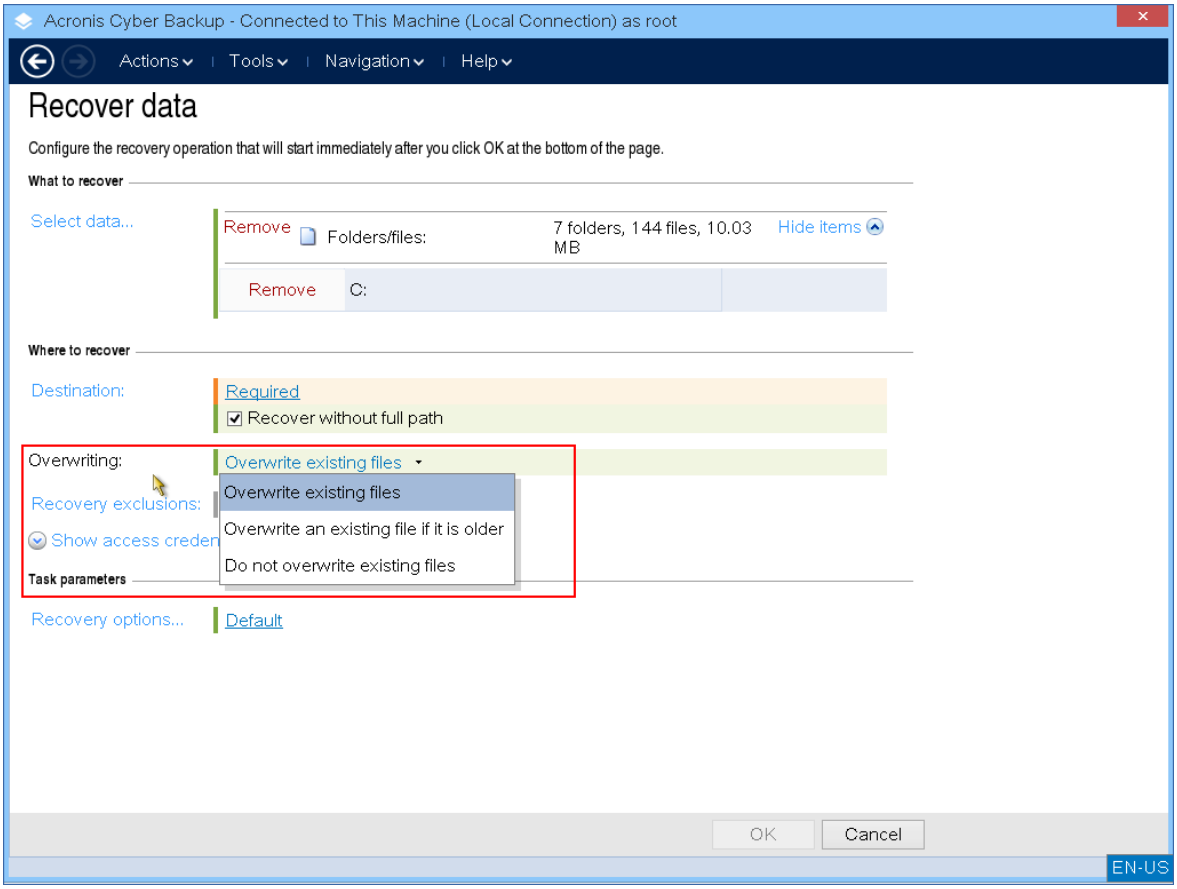
5. Klik **Jelajahi** dan pilih cadangan lokasi.



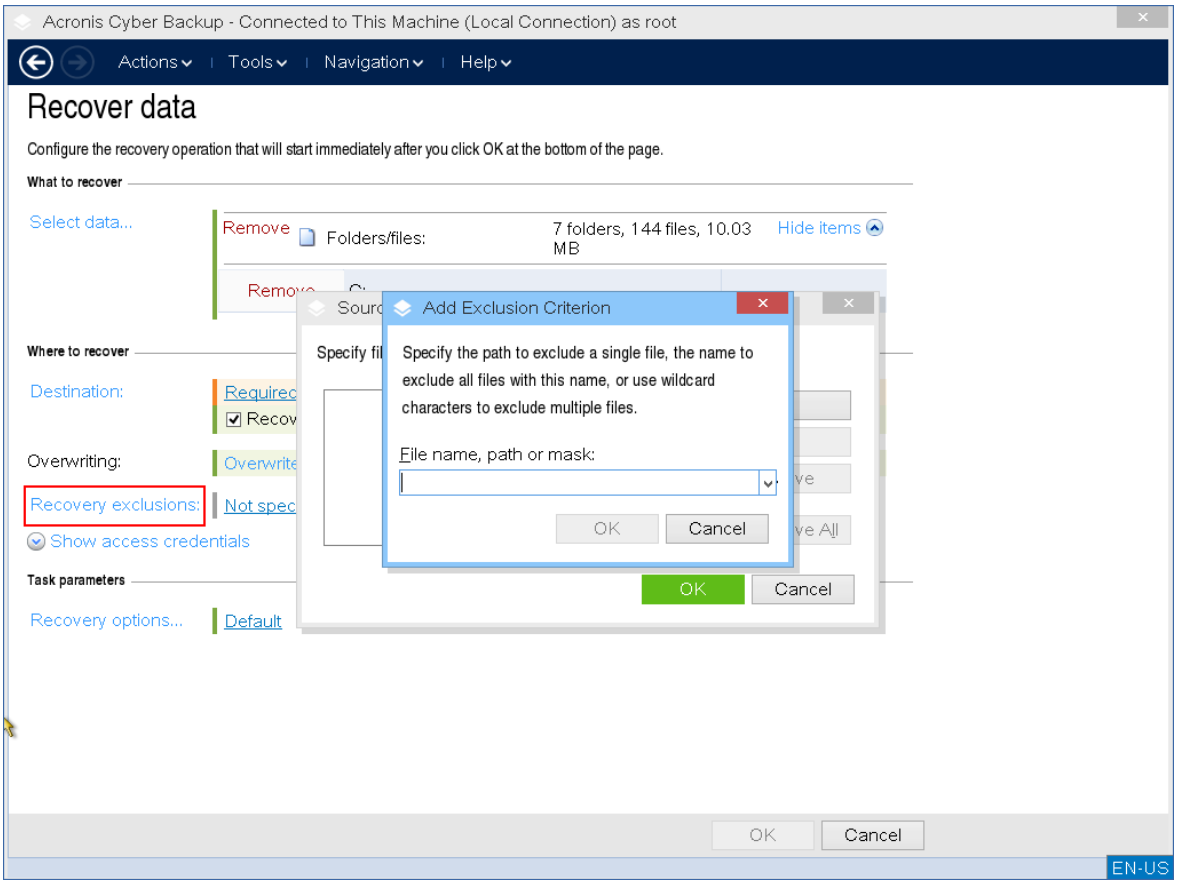
6. Pilih file cadangan yang ingin Anda pulihkan.



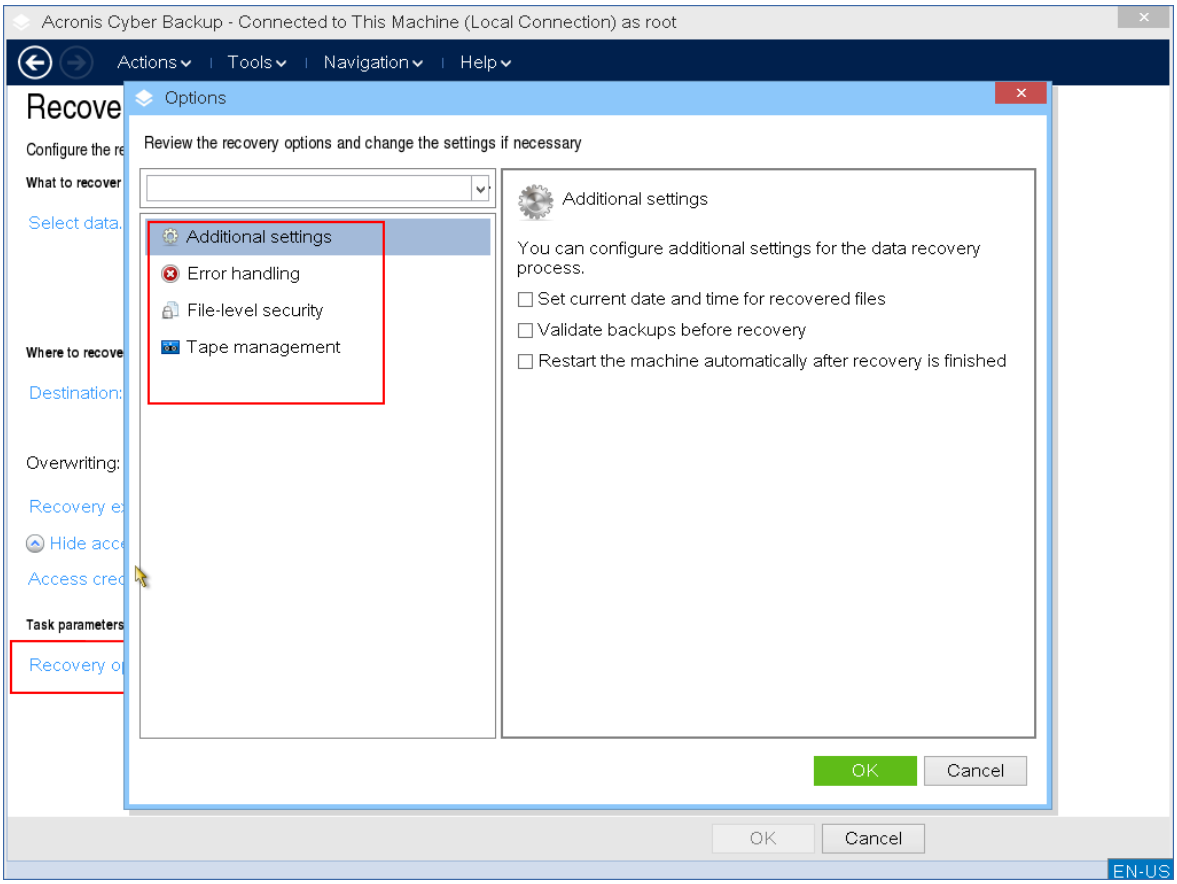
7. Di panel kiri bawah, pilih drive/volume (atau file/folder) yang ingin Anda pulihkan, lalu klik **OK**.
8. [Opsional] Konfigurasi aturan penimpaan.



9. [Opsional] Konfigurasi pengecualian pemulihan.



10. [Opsional] Konfigurasi opsi pemulihan.



11. Pastikan bahwa pengaturan Anda benar, dan kemudian klik **OK**.

Catatan
Untuk memulihkan data ke perangkat keras yang berbeda, Anda harus menggunakan Acronis Universal Restore.
Acronis Universal Restore tidak akan tersedia jika cadangan berada di Acronis Secure Zone.

Manajemen disk dengan media yang dapat di-boot

Dengan media yang dapat di-boot dari Acronis, Anda dapat menyiapkan konfigurasi disk/volume untuk memulihkan citra volume yang dicadangkan dengan Acronis Cyber Protect.

Terkadang, setelah volume dicadangkan dan citranya dipindahkan ke penyimpanan yang aman, konfigurasi disk mesin dapat berubah karena penggantian HDD atau hilangnya perangkat keras. Dalam kasus seperti ini, Anda dapat membuat ulang konfigurasi disk yang diperlukan sehingga citra volume dapat dipulihkan "seperti sebelumnya" atau dengan beberapa perubahan disk atau struktur volume yang mungkin Anda anggap perlu.

Untuk menghindari kemungkinan kehilangan data, lakukan semua tindakan pencegahan yang diperlukan.

Penting

Semua operasi pada disk dan volume memiliki risiko kerusakan data tertentu. Operasi pada volume sistem, yang dapat di-boot, atau data harus dilakukan dengan sangat hati-hati untuk menghindari kemungkinan masalah dengan proses booting atau penyimpanan data hard disk.
Operasi dengan hard disk dan volume memerlukan waktu beberapa lama, dan apabila listrik mati, mesin dimatikan secara tidak sengaja, atau tombol Reset ditekan secara tidak sengaja selama prosedur ini, kerusakan volume dan kehilangan data dapat terjadi.

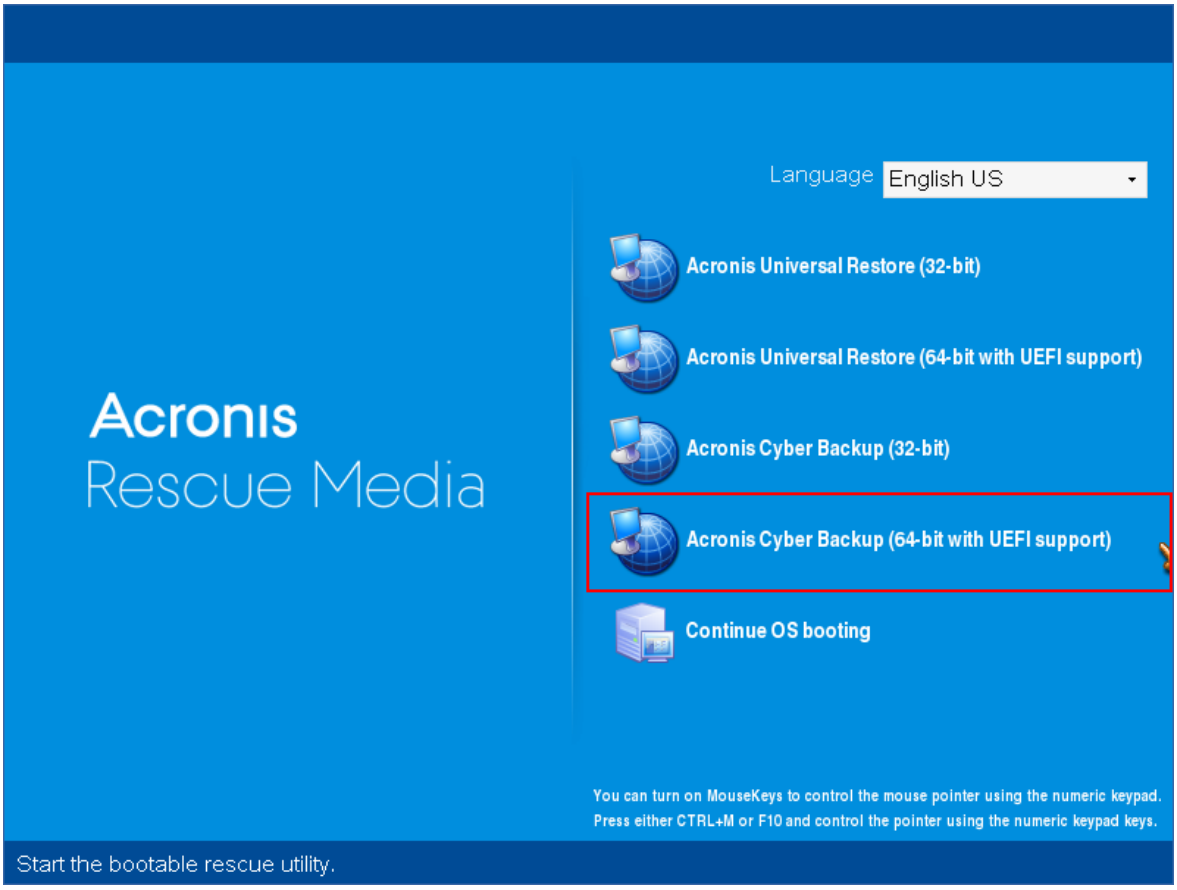
Anda dapat melakukan operasi manajemen disk pada logam, pada mesin yang tidak dapat melakukan booting, atau pada mesin non-Windows. Anda memerlukan media yang dapat di-boot yang sudah dibuat dengan Pembangun Media Yang Dapat Di-Boot, dan kunci lisensi Acronis Cyber Protect. Untuk informasi selengkapnya tentang cara membuat media yang dapat di-boot, lihat media yang dapat di-boot berbasis Linux atau media yang dapat di-boot berbasis Windows-PE.

Catatan

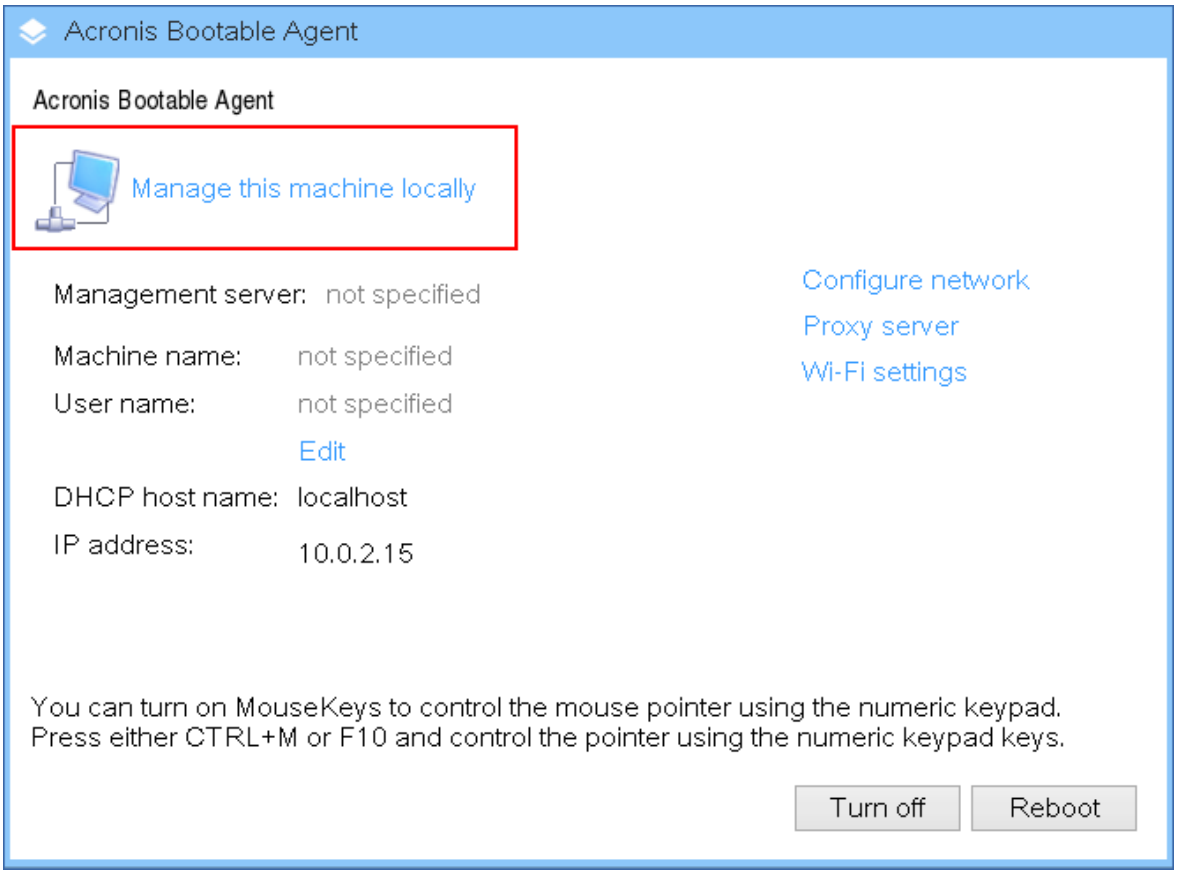
Fungsionalitas manajemen disk tidak tersedia untuk media yang dapat di-boot berbasis Windows PE 4.0 dan versi yang lebih baru. Jadi, manajemen disk didukung untuk Windows 7 dan sistem operasi versi sebelumnya. Untuk menjalankan operasi manajemen di Windows 8 dan versi setelahnya, Anda harus menginstal Acronis Disk Director. Untuk informasi lebih lanjut, lihat artikel KB ini: https://kb.acronis.com/content/47031.

Untuk melakukan operasi manajemen disk

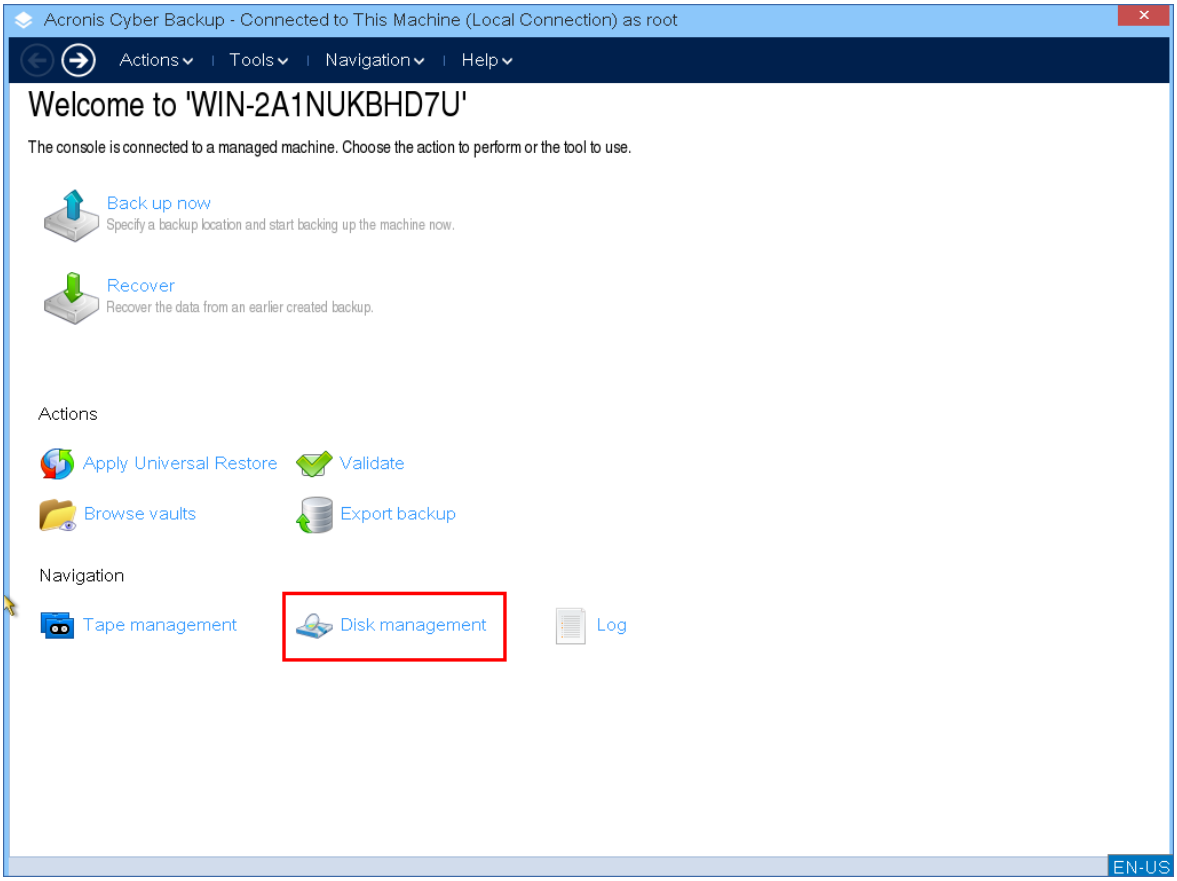
1. Booting dari media cadangan yang dapat di-boot Acronis.



2. Untuk bekerja pada mesin lokal, klik **Kelola mesin ini secara lokal**. Untuk koneksi jarak jauh, lihat Mendaftarkan media di server manajemen.



3. Klik **Manajemen disk**.



Catatan
Operasi manajemen disk pada media yang dapat di-boot mungkin bekerja secara tidak tepat jika ruang penyimpanan dikonfigurasi pada mesin.

Sistem file yang didukung

Media yang dapat di-boot mendukung manajemen disk dengan sistem file berikut:

- FAT 16/32
- NTFS

Jika Anda perlu melakukan operasi pada volume dengan sistem file yang berbeda, gunakan Acronis Disk Director. Layanan ini menyediakan lebih banyak alat bantu dan utilitas untuk mengelola disk dan volume dengan sistem file berikut:

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Linux SWAP

Tindakan pencegahan dasar

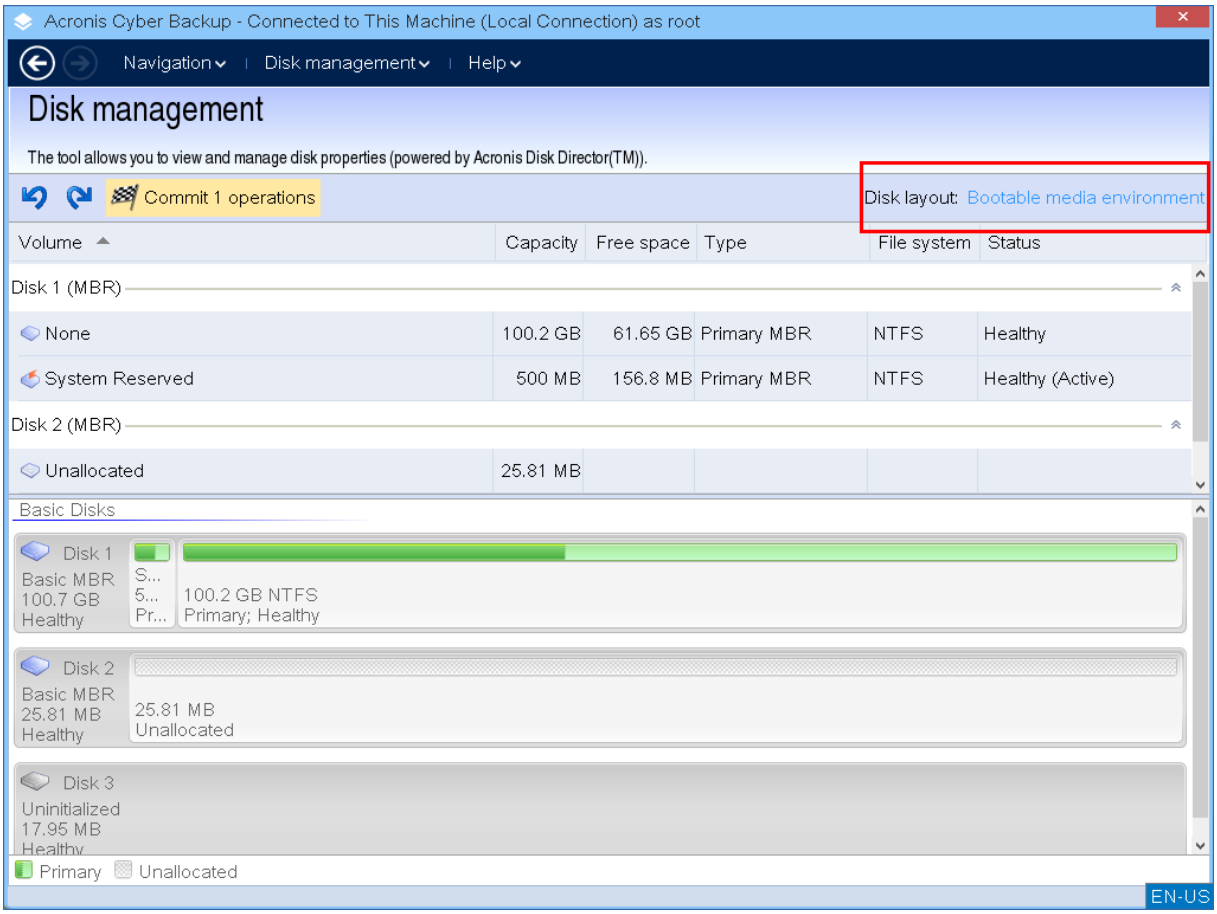
Untuk menghindari kemungkinan kerusakan disk dan struktur volume atau kehilangan data, lakukan semua tindakan pencegahan yang diperlukan dan ikuti pedoman berikut:

1. Cadangkan disk tempat volume akan dibuat atau dikelola. Mencadangkan data penting ke hard disk lain, berbagi jaringan, atau media yang dapat dilepas memungkinkan Anda menangani volume disk tanpa masalah karena data akan tetap aman.
2. Lakukan pengujian untuk memastikan disk berfungsi sepenuhnya dan tidak memiliki sektor buruk atau kesalahan sistem file.
3. Jangan lakukan operasi disk/volume apa pun selagi menjalankan perangkat lunak lain yang memiliki akses disk tingkat rendah.

Memilih sistem operasi untuk manajemen disk

Pada mesin yang memiliki dua atau lebih sistem operasi, tampilan disk dan volume bergantung pada sistem operasi yang sedang berjalan. Volume yang sama mungkin memiliki huruf yang berbeda pada sistem operasi yang berbeda.

Ketika menjalankan operasi manajemen disk, Anda harus menentukan tata letak disk untuk sistem operasi mana yang akan ditampilkan. Untuk melakukannya, klik nama sistem operasi di samping label **Tata letak disk**, lalu pilih sistem operasi yang diinginkan di jendela yang terbuka.



Operasi disk

Dengan media yang dapat di-boot, Anda dapat melakukan operasi manajemen disk berikut:

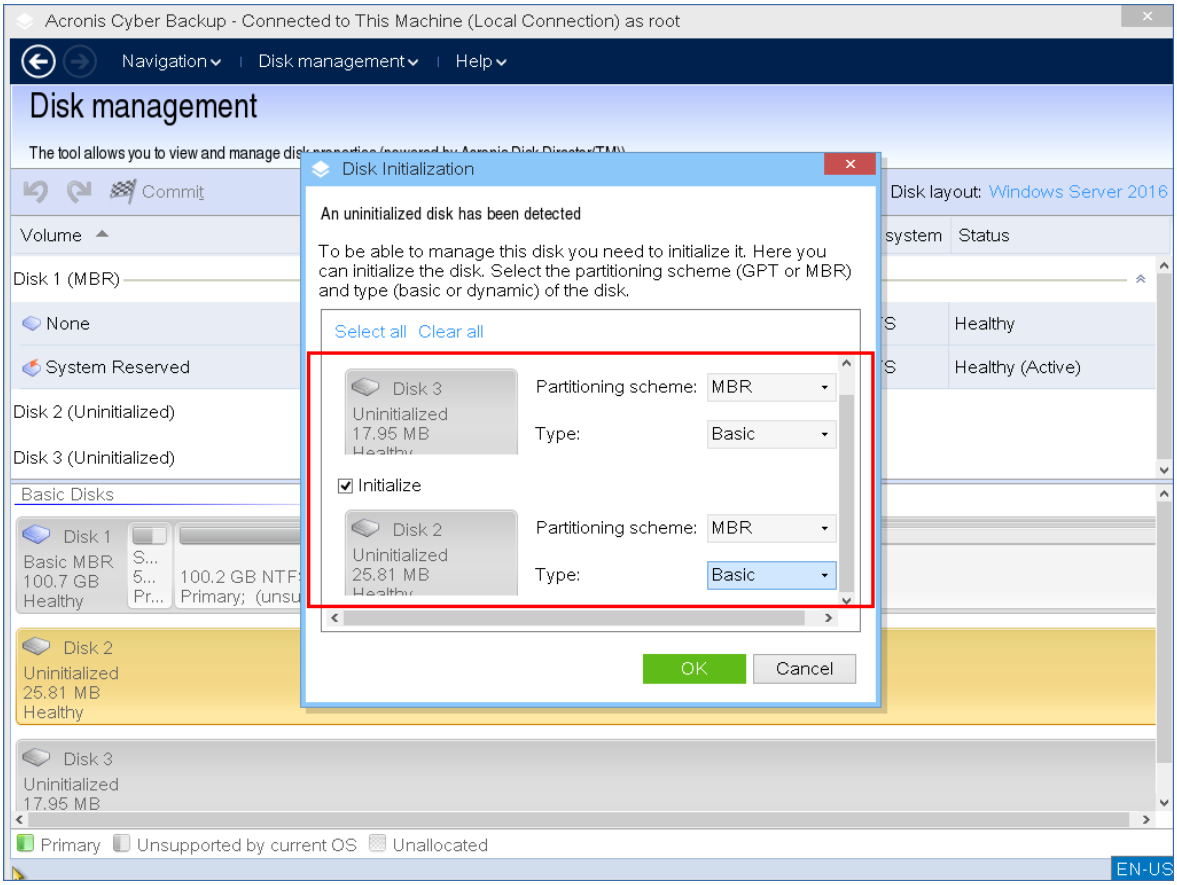
- Inisialisasi Disk - Menginisialisasi perangkat keras baru yang ditambahkan ke sistem
- Kloning disk standar - Mentransfer data lengkap dari disk MBR standar sumber ke disk target
- Konversi disk: MBR ke GPT - Mengubah tabel partisi MBR menjadi GPT
- Konversi disk: GPT ke MBR - Mengubah tabel partisi GPT menjadi MBR
- Konversi disk: Standar ke Dinamis - Mengubah disk standar menjadi dinamis
- Konversi disk: Dinamis ke Standar - Mengubah disk dinamis menjadi standar

Inisialisasi disk

Media yang dapat di-boot menunjukkan disk yang tidak diinisialisasi sebagai blok abu-abu dengan ikon abu-abu, menunjukkan bahwa disk tidak dapat digunakan oleh sistem.

Untuk menginisialisasi disk

1. Klik kanan disk yang diinginkan, lalu klik **Inisialisasi**.
2. Di jendela **Inisialisasi Disk**, atur skema pembuatan partisi disk (MBR atau GPT) dan jenis disk (standar atau dinamis).
3. Dengan mengklik **OK**, Anda akan menambahkan operasi inisialisasi disk yang tertunda.
4. Untuk menyelesaikan operasi yang ditambahkan, lakukan. Menutup program tanpa melakukan operasi akan membatalkannya.
5. Setelah inisialisasi, ruang disk tetap belum dialokasikan. Agar dapat menggunakannya, Anda harus membuat volume padanya.



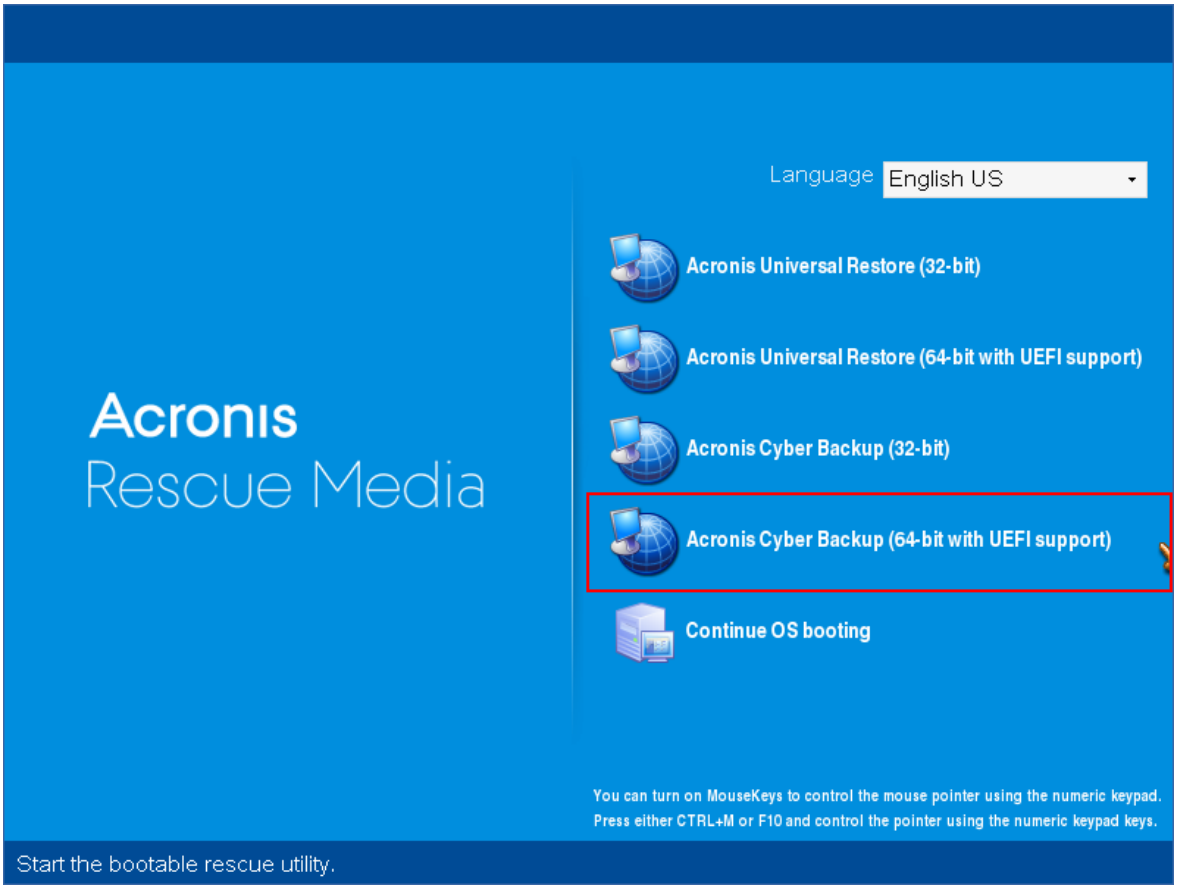
Kloning disk standar

Dengan media yang dapat di-boot berbasis Linux berfitur lengkap, Anda dapat mengkloning disk MBR standar. Kloning disk tidak tersedia di media siap pakai yang dapat di-boot yang dapat Anda unduh atau di media yang dapat di-boot yang dibuat tanpa kunci lisensi.

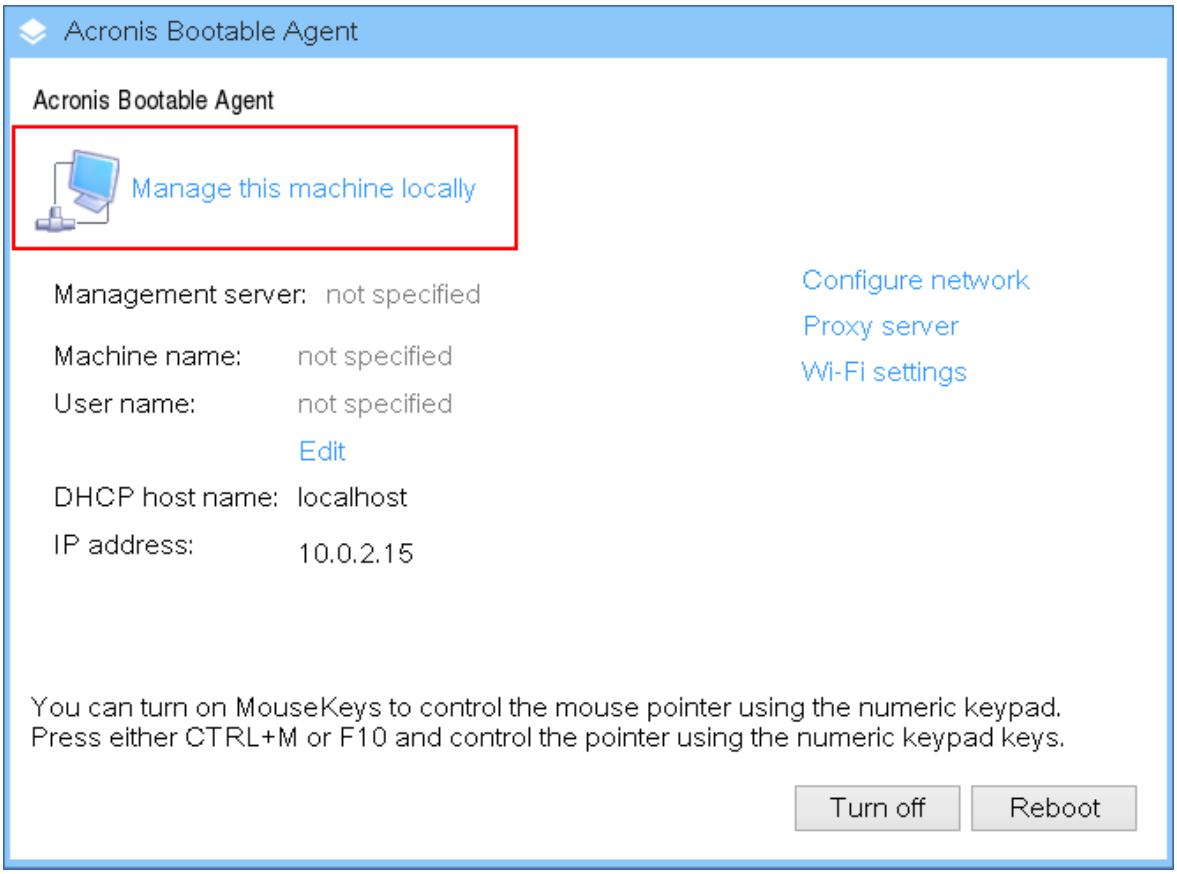
Catatan
Anda juga dapat membuat klona disk menggunakan Utilitas baris perintah Acronis Cyber Protect.

Untuk mengkloning disk standar di bawah media yang dapat di-boot

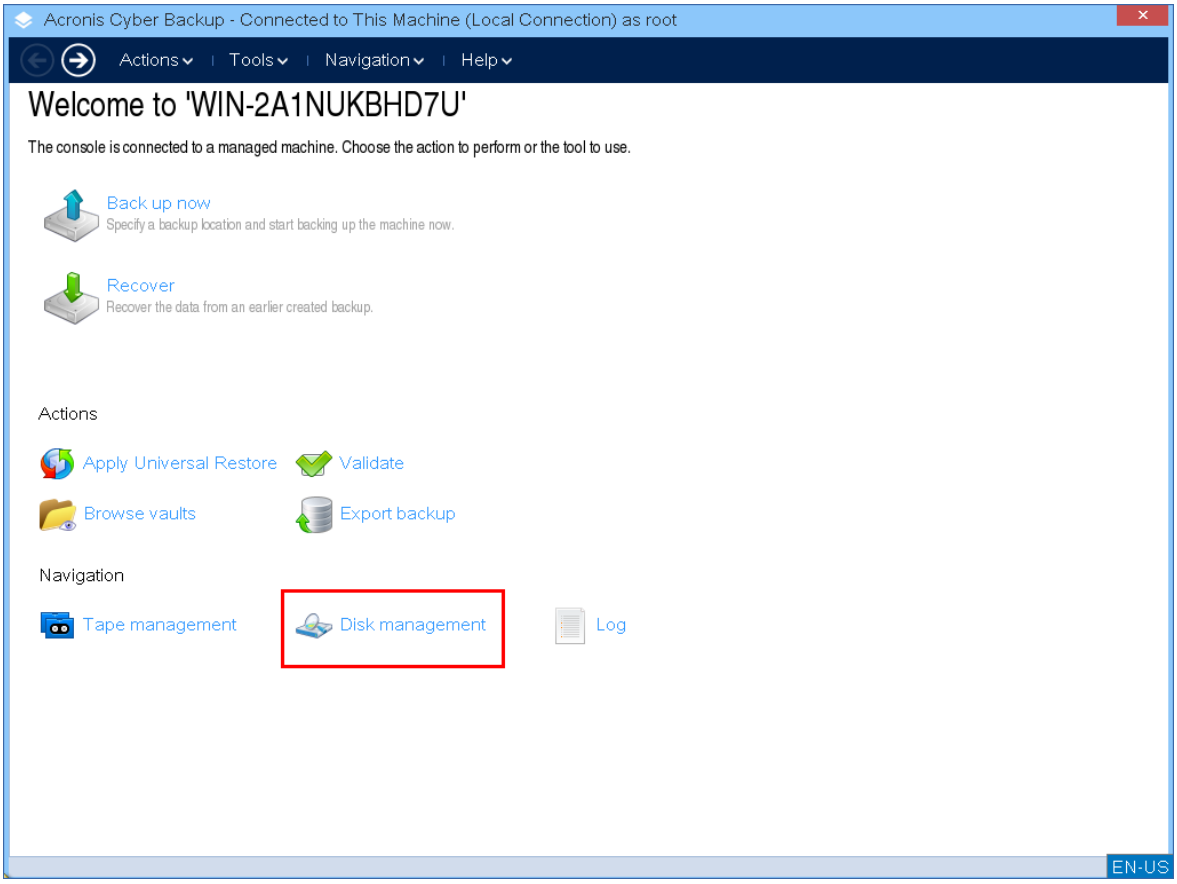
1. Booting dari media cadangan yang dapat di-boot Acronis.



2. Untuk mengkloning disk mesin lokal, klik **Kelola mesin ini secara lokal**. Untuk koneksi jarak jauh, lihat Mendaftarkan media di server manajemen.

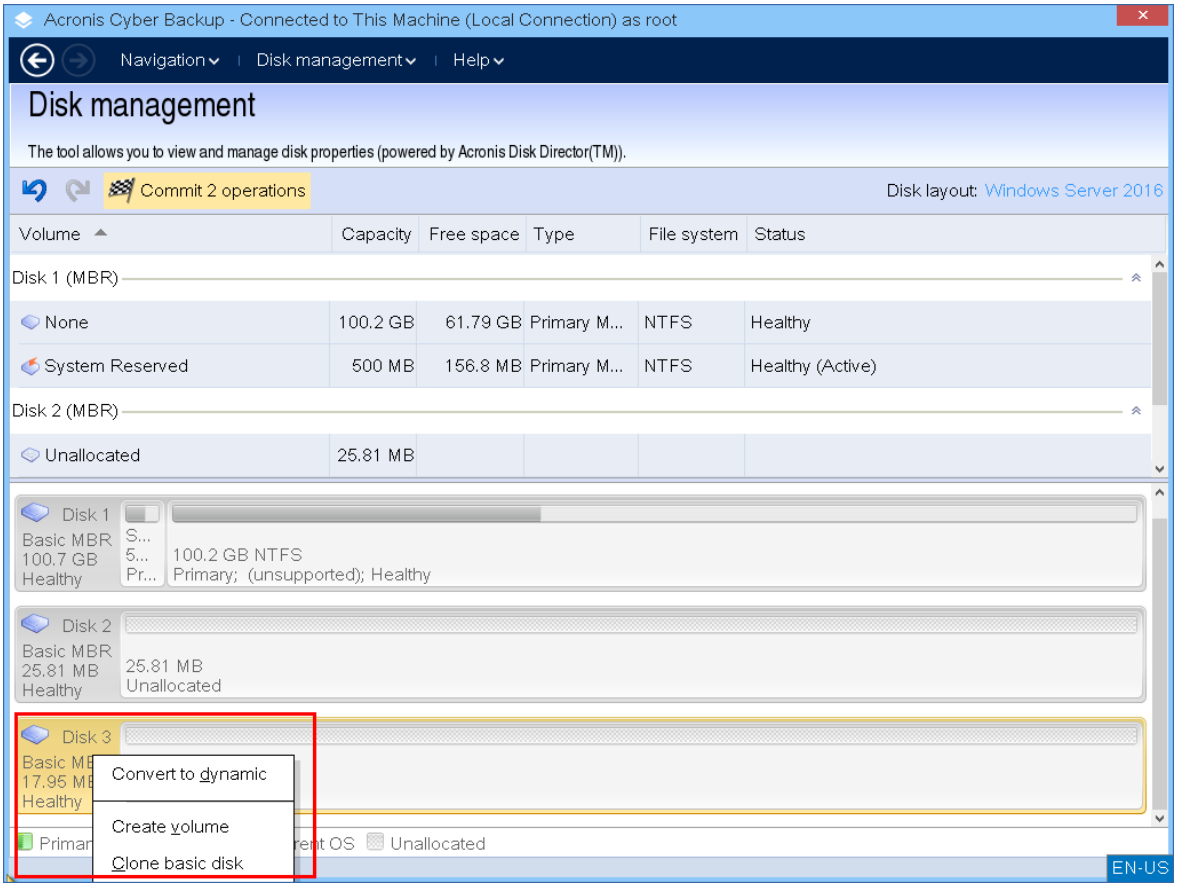


3. Klik **Manajemen disk**.

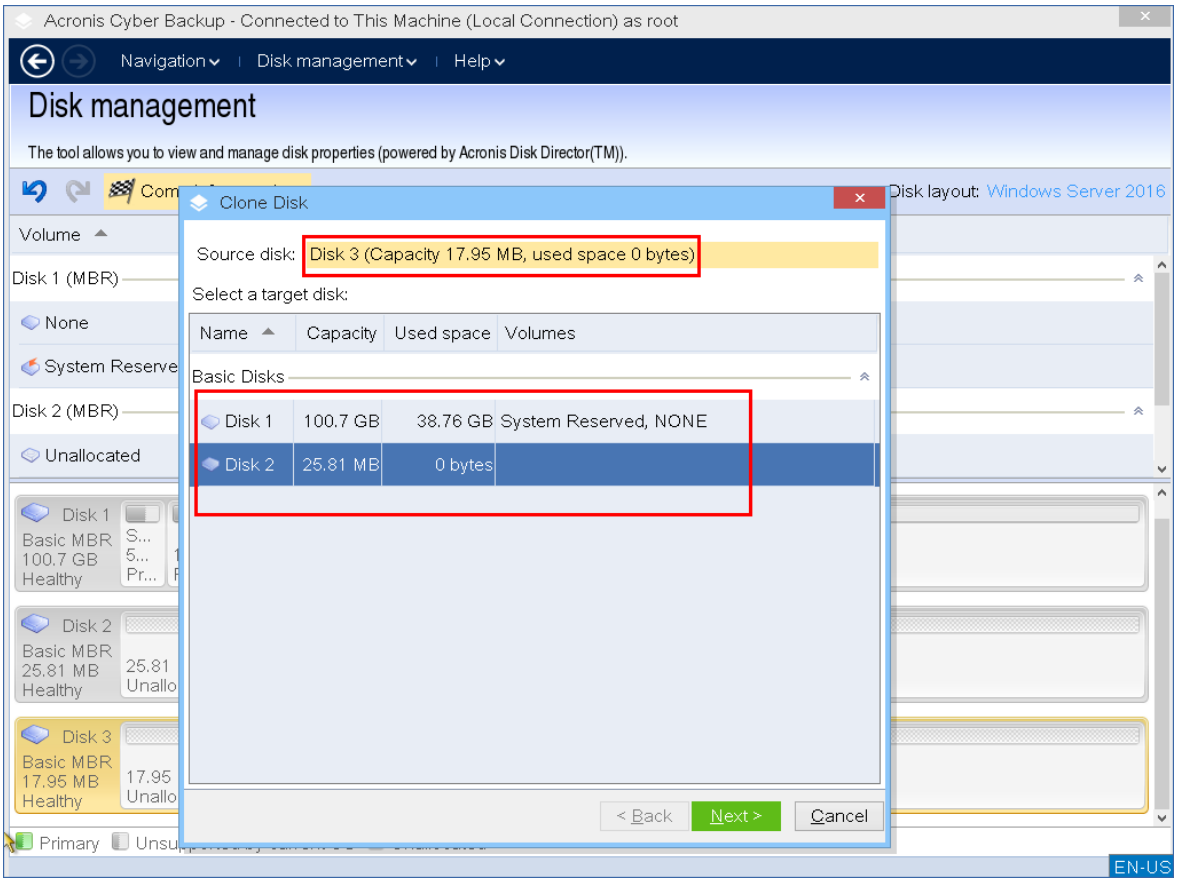


4. Disk yang tersedia ditampilkan. Klik kanan disk yang ingin Anda buat klonanya, lalu klik **Buat klona disk standar**.

Catatan
Anda hanya dapat membuat klona untuk seluruh isi disk. Kloning partisi tidak tersedia.



5. Daftar kemungkinan disk target ditampilkan. Program memungkinkan Anda memilih disk target jika cukup besar untuk menampung semua data dari disk sumber tanpa kehilangan apa pun. Pilih disk target, kemudian Klik **Berikutnya**.

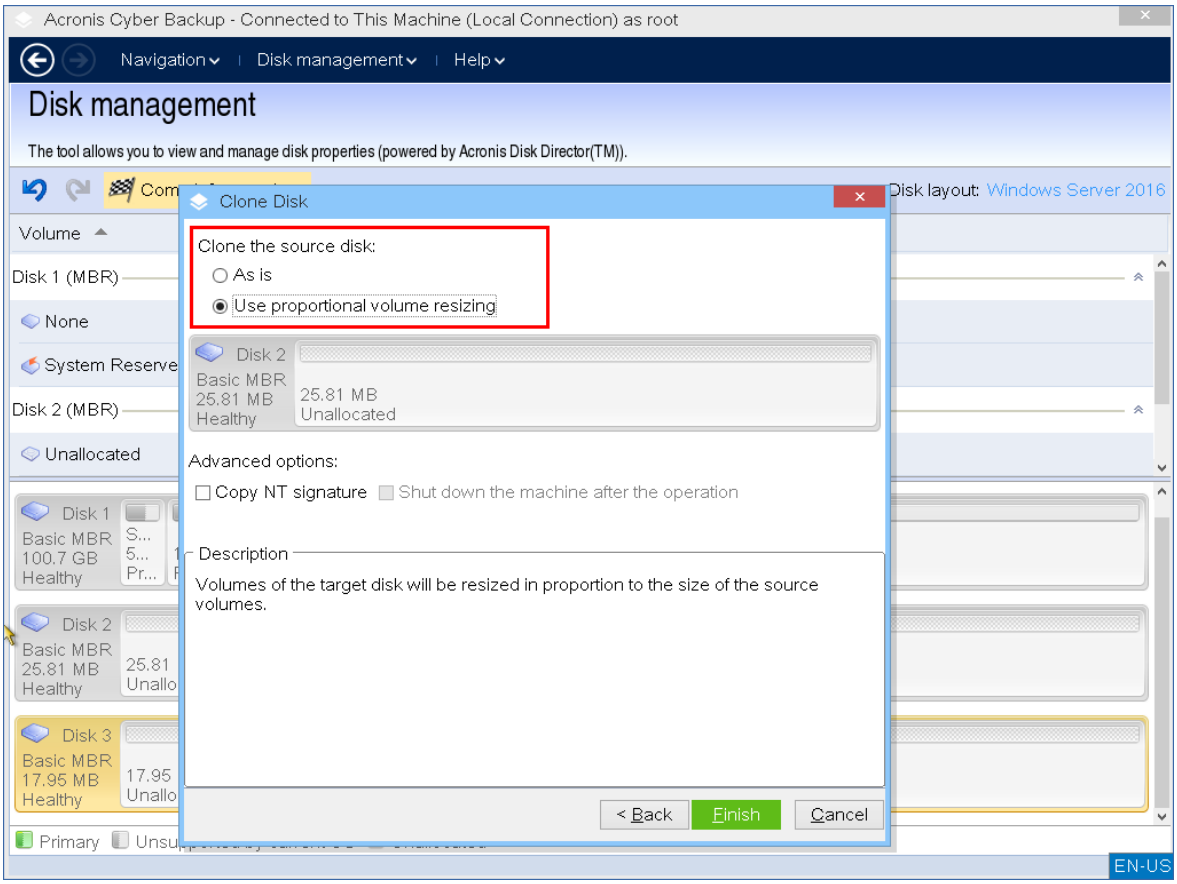


Jika disk target berukuran lebih besar, Anda dapat membuat klona disk apa adanya atau mengubah ukuran volume disk sumber secara proporsional (opsi default) agar tidak ada ruang tidak teralokasi pada disk target.

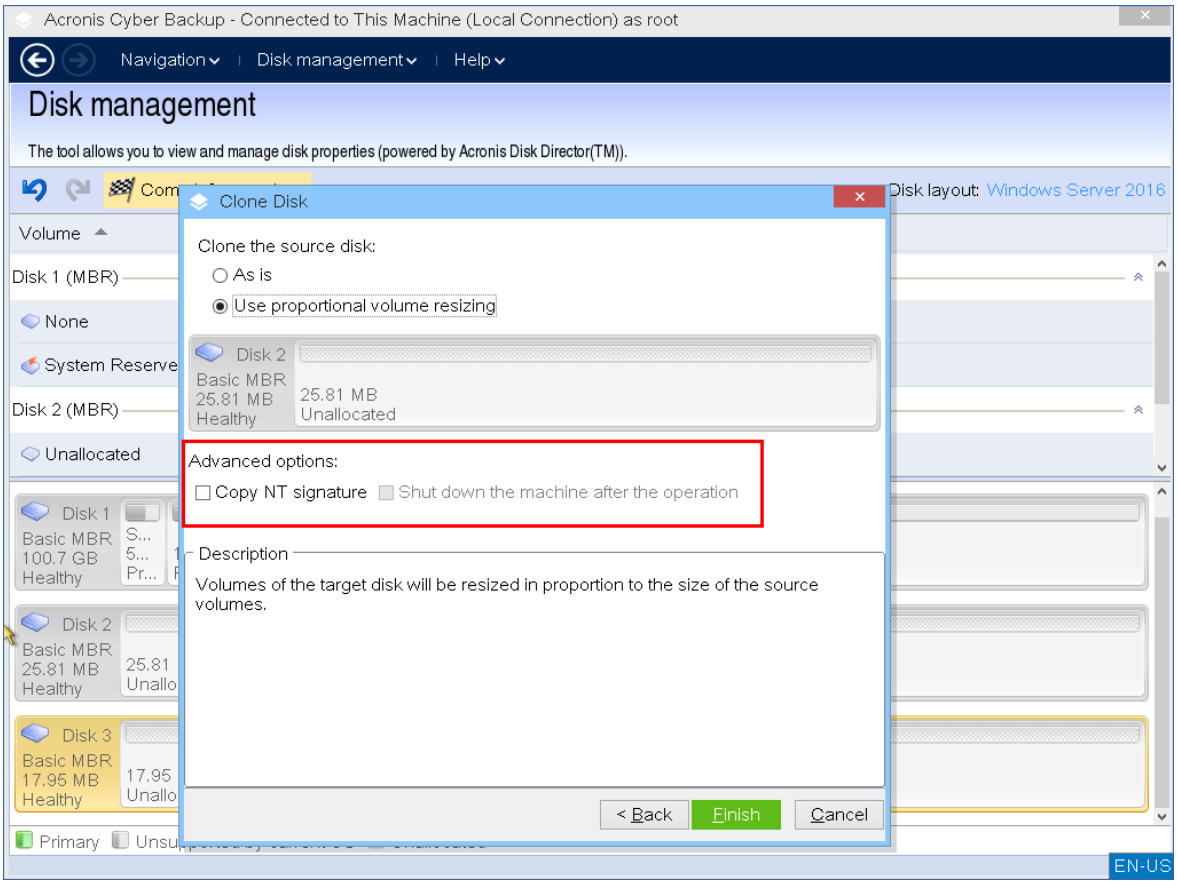
Jika disk target lebih kecil, hanya pengubahan ukuran proporsional yang tersedia. Jika kloning aman tidak mungkin dilakukan meskipun dengan pengubahan ukuran proporsional, Anda tidak akan dapat melanjutkan operasi.

Penting

Jika ada data di disk target, Anda akan melihat peringatan: "*Disk target yang dipilih tidak kosong. Data pada volumenya akan ditimpa.*" Jika Anda melanjutkan, semua data yang saat ini ada di disk target akan hilang dan tidak dapat dibatalkan.



6. Pilih untuk menyalin tanda tangan NT.



Jika Anda mengkloning disk yang terdiri dari volume sistem, Anda harus mempertahankan bootabilitas sistem operasi pada volume disk target. Artinya, sistem operasi harus memiliki informasi volume sistem (misalnya, huruf volume) yang cocok dengan tanda tangan NT disk, yang disimpan dalam rekaman disk MBR. Namun, dua disk dengan tanda tangan NT yang sama tidak dapat bekerja dengan semestinya di bawah satu sistem operasi.

Jika ada dua disk bertanda tangan NT yang sama yang terdiri dari volume sistem pada satu mesin, sistem operasi akan berjalan dari disk pertama pada saat penyalaan, menemukan tanda tangan yang sama pada disk kedua, lalu otomatis membuat tanda tangan NT unik baru dan menetapkannya ke disk kedua. Akibatnya, semua volume pada disk kedua akan kehilangan hurufnya, semua jalur tidak valid lagi, dan program tidak akan menemukan filenya. Sistem operasi pada disk itu tidak akan bisa di-boot.

Untuk memelihara bootabilitas sistem pada disk target volume, Anda dapat:

a. **Salin tanda tangan NT** – memberikan pada disk target tanda tangan NT disk sumber yang cocok dengan kunci registri yang juga akan disalin pada disk target.

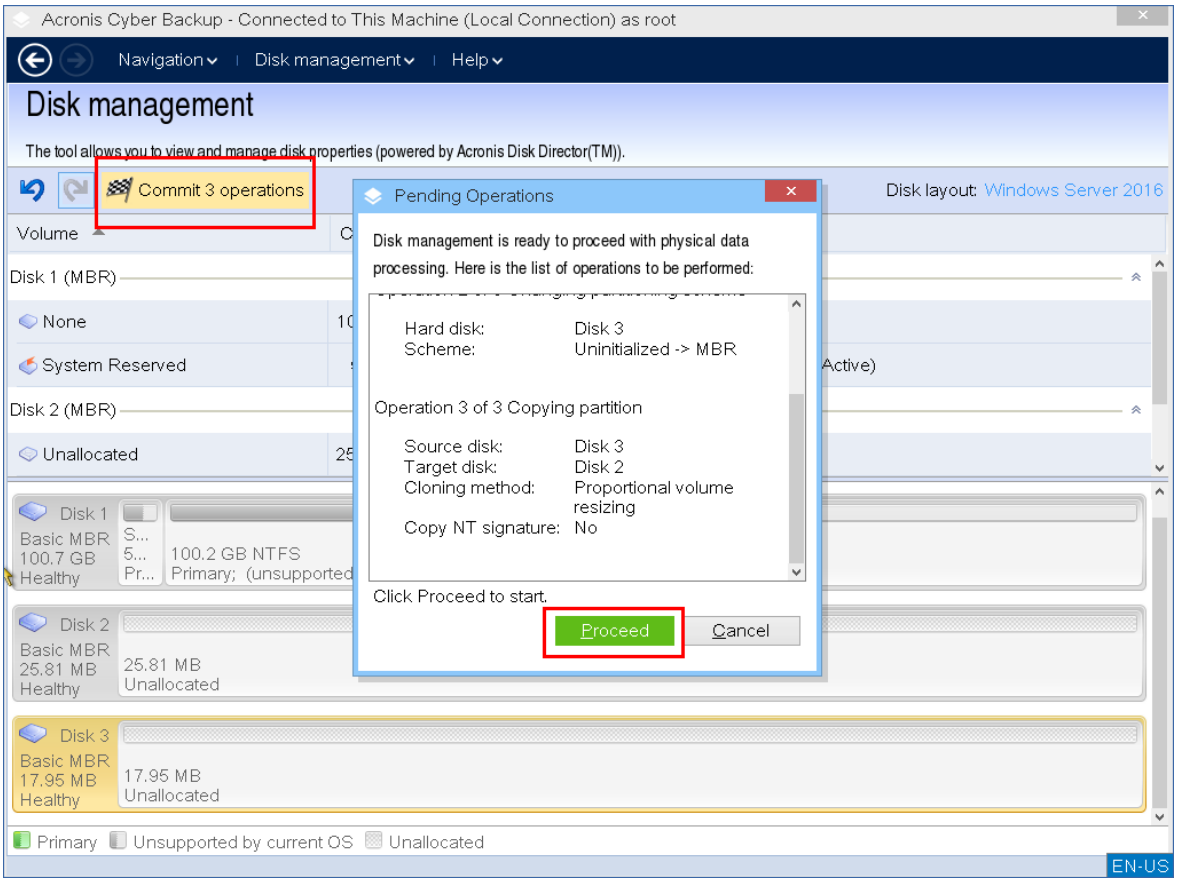
   Untuk melakukannya, pilih kotak centang **Salin tanda tangan NT**.
   Anda akan menerima peringatan: *"Jika ada sistem operasi pada hard disk, hapus instalan drive hard disk sumber atau target dari mesin Anda sebelum memulai mesin lagi. Jika tidak, OS akan dimulai dari yang pertama dari keduanya, dan OS pada disk kedua menjadi tidak dapat di-boot."*
   Kotak centang **Matikan mesin setelah operasi** dipilih dan dinonaktifkan secara otomatis.

b. **Biarkan tanda tangan NT** – pertahankan tanda tangan disk target lama dan perbarui sistem operasi sesuai dengan tanda tangannya.

Untuk melakukannya, klik untuk menghapus kotak centang **Salin tanda tangan NT**, jika perlu.

Kotak centang **Matikan mesin setelah operasi** akan dihapus secara otomatis.

7. Klik **Selesai** untuk menambahkan operasi kloning disk yang tertunda.
8. Klik **Lakukan**, lalu klik **Lanjutkan** di jendela **Operasi Tertunda**. Menutup program tanpa melakukan operasi akan membatalkannya.



9. Jika Anda memilih untuk menyalin tanda tangan NT, tunggu hingga operasi selesai dan komputer dimatikan, kemudian putuskan sambungan drive hard disk sumber atau target dari mesin.

Konversi disk: MBR ke GPT

Anda mungkin perlu mengonversi disk standar MBR menjadi disk dasar GPT jika memerlukan:

- Lebih dari 4 volume utama pada satu disk.
- Keandalan disk yang lebih tinggi terhadap kemungkinan kerusakan data.

Penting

Disk MBR standar yang berisi volume boot dengan sistem operasi yang sedang berjalan tidak dapat dikonversi menjadi GPT.

Untuk mengonversi disk MBR standar menjadi disk GPT standar

1. Klik kanan disk yang ingin Anda kloning, lalu klik **Konversikan ke GPT**.
2. Dengan mengeklik **OK**, Anda akan menambahkan operasi konversi disk MBR ke GPT yang tertunda.
3. Untuk menyelesaikan operasi yang ditambahkan, lakukan. Menutup program tanpa melakukan operasi akan membatalkannya.

Catatan
Disk yang dipartisi GPT mencadangkan ruang di akhir area partisi yang diperlukan untuk area cadangan, yang menyimpan salinan header GPT dan tabel partisi. Jika disk penuh dan ukuran volume tidak dapat dikecilkan secara otomatis, operasi konversi disk MBR ke GPT akan gagal. Operasi ini tidak dapat dibatalkan. Jika terdapat volume utama milik disk MBR dan Anda mengonversi disk terlebih dahulu ke GPT lalu kembali ke MBR, volume tersebut akan menjadi logis dan tidak dapat digunakan sebagai volume sistem.

Konversi disk dinamis: MBR ke GPT

Media yang dapat di-boot tidak mendukung konversi langsung MBR ke GPT untuk disk dinamis. Namun, Anda dapat menjalankan konversi berikut untuk melakukannya:

1. Konversi disk MBR: dinamis ke standar menggunakan operasi **Konversikan ke standar**.
2. Konversi disk standar: MBR ke GPT menggunakan operasi **Konversikan ke GPT**.
3. Konversi disk GPT: standar ke dinamis menggunakan operasi **Konversikan ke dinamis**.

Konversi disk: GPT ke MBR

Jika Anda berencana menginstal OS yang tidak mendukung disk GPT, konversi disk GPT ke MBR dapat dilakukan.

Penting
Disk GPT standar yang berisi volume boot dengan sistem operasi yang sedang berjalan tidak dapat dikonversi menjadi MBR.

Untuk mengonversi disk GPT menjadi MBR

1. Klik kanan disk yang ingin Anda buat kloningnya, lalu klik **Konversikan ke MBR**.
2. Dengan mengklik **OK**, Anda akan menambahkan operasi konversi disk GPT ke MBR yang tertunda.
3. Untuk menyelesaikan operasi yang ditambahkan, lakukan. Menutup program tanpa melakukan operasi akan membatalkannya.

Catatan
Setelah operasi, volume pada disk ini akan menjadi logis. Perubahan ini tidak dapat dibatalkan.

Konversi disk: standar ke dinamis

Anda mungkin perlu mengonversi disk standar menjadi dinamis jika:

- Berencana menggunakan disk sebagai bagian dari grup disk dinamis
- Ingin meningkatkan keandalan disk untuk penyimpanan data

Ingin mengonversi disk standar menjadi dinamis

1. Klik kanan disk yang ingin Anda konversikan, lalu klik **Konversikan ke dinamis**.
2. Klik **OK**.

Konversi akan dilakukan saat itu juga dan mesin akan di-boot ulang, jika perlu.

Catatan
Disk dinamis menggunakan megabyte terakhir disk fisik untuk menyimpan database, termasuk deskripsi empat tingkat (Volume-Komponen-Partisi-Disk) untuk setiap volume dinamis. Jika saat konversi ke dinamis disk standar sudah penuh dan ukuran volumenya tidak dapat dikurangi secara otomatis, operasi akan gagal.
Konversi disk yang terdiri dari volume sistem memerlukan beberapa waktu, dan apabila listrik mati, mesin mati secara tidak sengaja, atau tombol Reset ditekan secara tidak sengaja selama prosedur ini, bootabilitas dapat hilang.

Berbeda dengan Windows Disk Manager, program ini memastikan bootabilitas **sistem operasi offline** pada disk setelah operasi.

Konversi disk: dinamis ke standar

Anda mungkin perlu mengonversi disk dinamis kembali ke disk standar, misalnya, jika ingin menggunakan sistem operasi yang tidak mendukung disk dinamis.

Untuk mengonversi disk dinamis menjadi standar:

1. Klik kanan disk yang ingin Anda konversikan, lalu klik **Konversikan ke standar**.
2. Klik **OK**.

Konversi akan dilakukan saat itu juga dan mesin akan di-boot ulang, jika perlu.

Catatan
Operasi ini tidak tersedia untuk disk dinamis yang berisi volume Spanned, Striped, atau RAID-5.

Setelah konversi, 8 Mb terakhir ruang disk akan dicadangkan untuk konversi disk dari standar ke dinamis di masa mendatang. Dalam beberapa kasus, kemungkinan ruang tidak teralokasi dan ukuran volume maksimum yang diusulkan mungkin berbeda (misalnya, ketika ukuran satu duplikat menentukan ukuran duplikat lainnya, atau 8 Mb terakhir ruang disk dicadangkan untuk konversi disk dari standar ke dinamis di masa mendatang).

Catatan
Konversi disk yang terdiri dari volume sistem memerlukan waktu agak lama, dan apabila listrik mati, mesin mati secara tidak sengaja, atau tombol Reset ditekan secara tidak sengaja selama prosedur ini, bootabilitas dapat hilang.

Berbeda dengan Windows Disk Manager, program ini memastikan:

- Konversi disk dinamis ke standar yang aman jika berisi volume **dengan data** untuk volume sederhana dan duplikat
- Dalam sistem multiboot, bootabilitas sistem yang **offline** selama operasi

Operasi volume

Dengan media yang dapat di-boot, Anda dapat melakukan operasi berikut pada volume:

- Buat Volume - Membuat volume baru
- Hapus Volume - Menghapus volume yang dipilih
- Setel Aktif - Mengaktifkan volume yang dipilih sehingga mesin dapat melakukan booting dengan OS yang diinstal di volume tersebut
- Ubah Huruf - Mengubah huruf volume yang dipilih
- Ubah Label - Mengubah label volume yang dipilih
- Format Volume - Memformat volume baru dengan sistem file

Jenis volume dinamis

Volume Sederhana

Volume yang dibuat dari ruang bebas di disk fisik tunggal. Volume ini dapat terdiri dari satu wilayah di disk atau beberapa wilayah, yang secara virtual disatukan oleh Logical Disk Manager (LDM). Volume ini tidak memberikan keandalan tambahan atau peningkatan kecepatan, juga ukuran ekstra.

Volume Rentang

Volume yang dibuat dari ruang bebas disk yang secara virtual ditautkan oleh LDM dari beberapa disk fisik. Maksimal 32 disk dapat dimasukkan ke dalam satu volume sehingga mengatasi batasan ukuran perangkat keras. Namun, jika satu disk rusak, semua data akan hilang. Selain itu, tidak ada bagian dari volume rentang yang dapat dihapus tanpa merusak seluruh volume. Maka, volume rentang tidak memberikan keandalan tambahan atau kecepatan I/O yang lebih baik.

Volume Bergaris

Volume, disebut juga RAID 0, terdiri dari garis-garis data berukuran sama, yang ditulis di setiap disk dalam volume. Karena itu, untuk membuat volume bergaris, Anda membutuhkan dua

disk dinamis atau lebih. Disk dalam volume bergaris tidak harus identik, tetapi harus ada ruang tidak terpakai yang tersedia di setiap disk yang ingin Anda sertakan dalam volume. Ukuran volume akan bergantung pada ukuran ruang terkecil. Akses ke data pada volume bergaris biasanya lebih cepat daripada akses ke data yang sama pada satu disk fisik, karena I/O tersebar di lebih dari satu disk.

Volume bergaris dibuat untuk meningkatkan kinerja, bukan untuk keandalannya yang lebih baik – volume tersebut tidak berisi informasi yang berlebihan.

Volume Duplikat

Volume yang toleran terhadap kesalahan, disebut juga RAID 1, yang datanya digandakan pada dua disk fisik yang identik. Semua data di satu disk disalin ke disk lain untuk memberikan redundansi data. Hampir semua volume dapat dijadikan duplikat, termasuk volume sistem dan boot, dan jika salah satu disk rusak, data masih dapat diakses dari disk yang tersisa. Sayangnya, batasan perangkat keras pada ukuran dan kinerja bahkan lebih berat dengan penggunaan volume duplikat.

Volume Bergaris-Duplikat

Volume yang toleran terhadap kesalahan, terkadang juga disebut RAID 1+0, yang menggabungkan keunggulan kecepatan I/O tinggi dari tata letak bergaris dan redundansi jenis duplikat. Kerugiannya tetap melekat pada arsitektur duplikat – rasio ukuran disk-ke-volume yang rendah.

RAID-5

Volume yang toleran terhadap kesalahan yang datanya ada di seluruh susunan tiga disk atau lebih. Disk tidak harus identik, tetapi harus ada blok ruang tidak teralokasi berukuran sama yang tersedia di setiap disk dalam volume. Paritas (nilai terhitung yang dapat digunakan untuk merekonstruksi data jika terjadi kegagalan) juga ada di seluruh susunan disk dan selalu disimpan di disk yang berbeda dari data itu sendiri. Jika disk fisik rusak, porsi volume RAID-5 yang berada di disk yang rusak tersebut dapat dibuat ulang dari data yang tersisa dan paritas. Volume RAID-5 memberikan keandalan dan dapat mengatasi batasan ukuran disk fisik dengan rasio ukuran yang lebih tinggi daripada disk duplikat-ke-volume.

Membuat volume

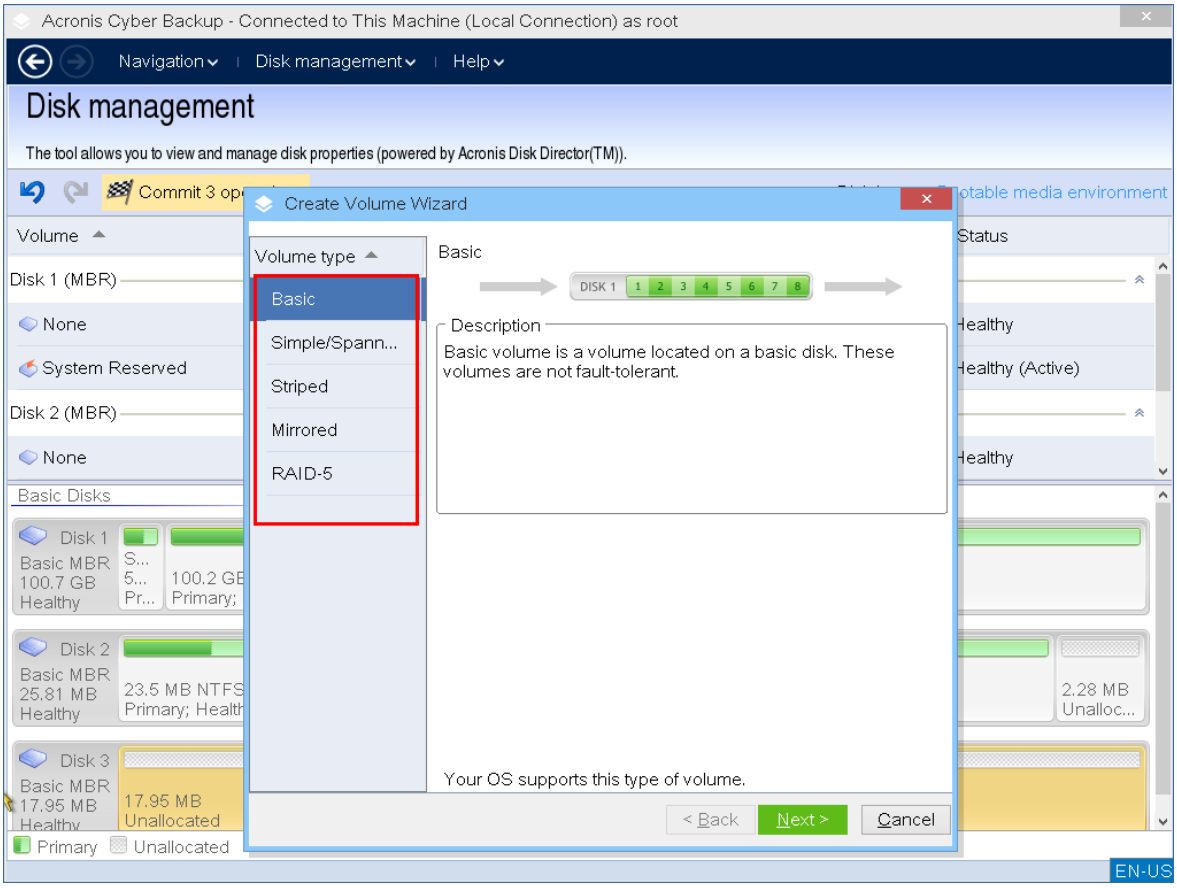
Anda mungkin membutuhkan volume baru untuk:

- Memulihkan salinan cadangan yang disimpan sebelumnya dalam konfigurasi "persis seperti sebelumnya"
- Menyimpan koleksi file serupa secara terpisah — misalnya, koleksi MP3 atau file video pada volume terpisah
- Simpan cadangan (citra) dari volume/disk lain pada volume khusus

- Menginstal sistem operasi baru (atau swap file) pada volume baru
- Menambahkan perangkat keras baru ke mesin

Untuk membuat volume

1. Klik kanan ruang tidak teralokasi dalam disk, kemudian klik **Buat volume**. Wizard **Buat volume** terbuka.



2. Pilih jenis volume. Opsi berikut tersedia:
   - Dasar
   - Sederhana/Rentang
   - Bergaris
   - Duplikat
   - RAID-5

   Jika sistem operasi saat ini tidak mendukung jenis volume yang dipilih, Anda akan menerima peringatan dan tombol **Berikutnya** akan dinonaktifkan. Anda harus memilih jenis volume lain untuk melanjutkan.
3. Tentukan ruang tidak teralokasi atau pilih disk tujuan.
   - Untuk volume standar, tentukan ruang tidak teralokasi pada disk yang ditentukan.
   - Untuk volume sederhana/rentang, pilih satu disk tujuan atau lebih banyak.
   - Untuk volume duplikat, pilih dua disk tujuan.

- Untuk volume bergaris, pilih dua disk tujuan atau lebih.
- Untuk volume RAID-5, pilih tiga disk tujuan

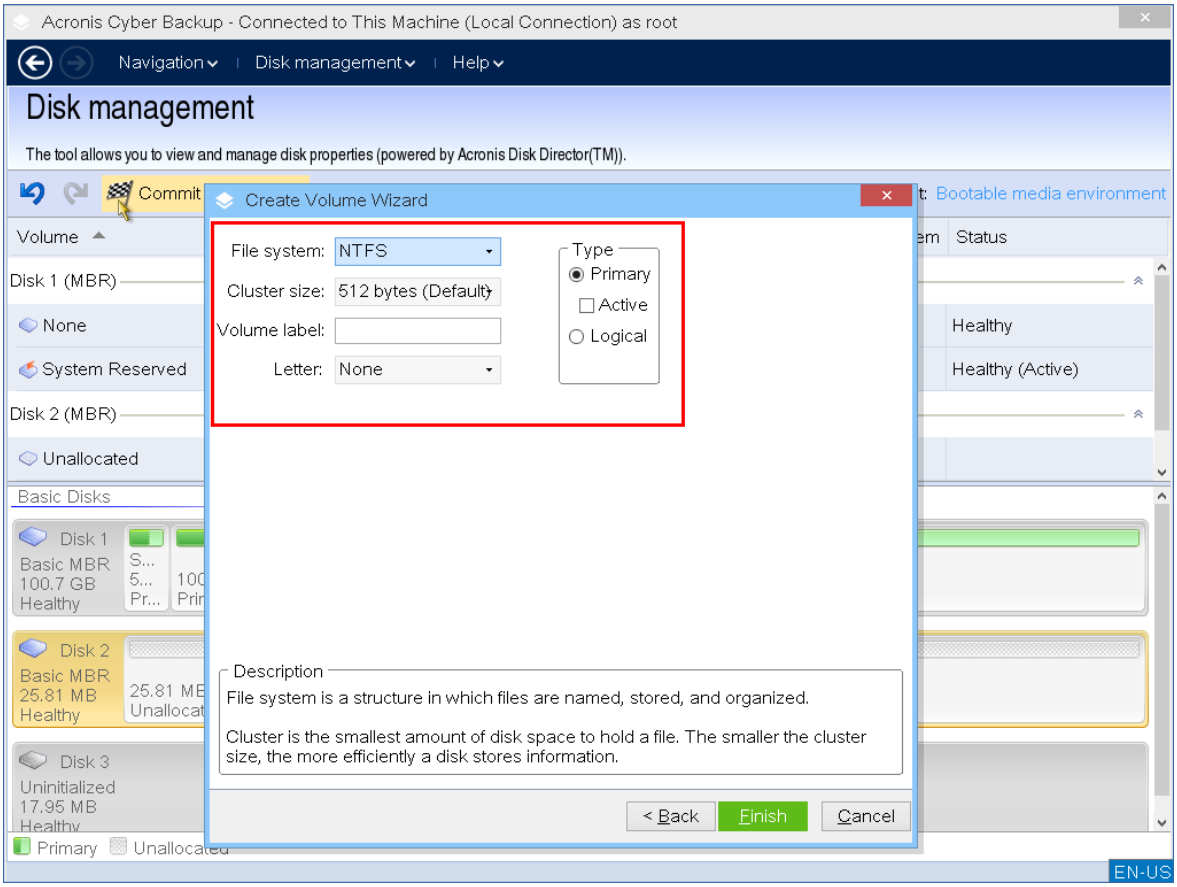
Jika Anda membuat volume **dinamis** dan memilih satu atau beberapa disk **standar** sebagai tujuannya, Anda akan menerima peringatan bahwa disk yang dipilih akan diubah menjadi dinamis secara otomatis.

4. Mengatur ukuran volume.

   Nilai maksimal biasanya mencerminkan kemungkinan ruang tidak teralokasi maksimum. Dalam beberapa kasus, nilai maksimum yang diusulkan mungkin berbeda – misalnya, ketika ukuran satu duplikat menentukan ukuran duplikat lainnya, atau 8 MB terakhir ruang disk dicadangkan untuk konversi disk dari standar ke dinamis di masa mendatang.

   Anda dapat memilih posisi volume dasar baru pada disk, jika ruang tidak teralokasi pada disk tersebut lebih besar daripada volume.

5. Mengatur opsi volume.



Anda dapat menetapkan **Huruf** volume (secara default – tiga huruf bebas pertama dari alfabet) dan secara opsional – **Label** (secara default – tidak ada). Anda juga harus menentukan **Sistem file** dan **Ukuran klaster**.

Opsi sistem file yang memungkinkan adalah:

- FAT16 (dinonaktifkan jika ukuran volume telah diatur lebih dari 2 GB)
- FAT32 (dinonaktifkan jika ukuran volume telah diatur lebih dari 2 TB)

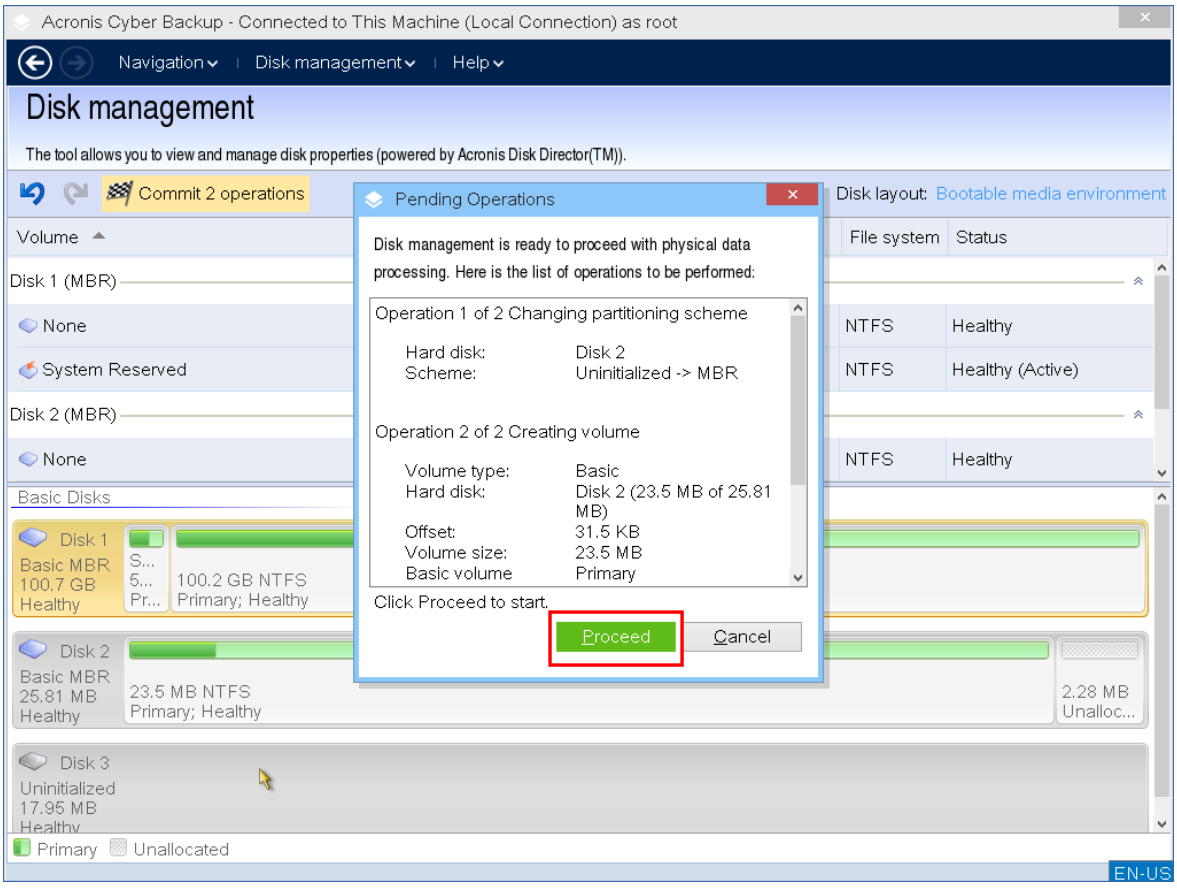
- NTFS
- Tinggalkan volume tanpa diformat.

  Saat mengatur ukuran klaster, Anda dapat memilih berapa saja dalam jumlah standar untuk setiap sistem file. Ukuran klaster yang disarankan secara default paling sesuai dengan volume dengan sistem file yang dipilih. Jika Anda menetapkan ukuran klaster 64K untuk FAT16/FAT32 atau ukuran klaster 8KB-64KB untuk NTFS, Windows dapat memasang volume, tetapi beberapa program (misalnya, program penyiapan) mungkin menghitung ruang disk-nya secara tidak benar.

  Jika Anda membuat volume dasar, yang dapat dijadikan volume sistem, Anda juga dapat memilih jenis volume — **Utama** (**Utama Aktif**) atau **Logis**. Khususnya, **Utama** dipilih saat Anda ingin menginstal sistem operasi ke volume. Pilih nilai **Aktif** (default) jika Anda ingin menginstal sistem operasi pada volume ini untuk booting saat mesin dinyalakan. Jika tombol **Utama** tidak dipilih, opsi **Aktif** akan menjadi tidak aktif. Jika volume tidak ditujukan untuk penyimpanan data, pilih **Logis**.

  Catatan
  Disk standar dapat berisi hingga empat volume utama. Jika sudah ada, disk harus diubah menjadi dinamis, jika tidak opsi **Aktif** dan **Utama** akan dinonaktifkan dan Anda hanya akan dapat memilih jenis volume **Logis**.

6. Klik **Lakukan**, lalu klik **Lanjutkan** di jendela **Operasi Tertunda**. Menutup program tanpa melakukan operasi akan membatalkannya.



Menghapus volume

Untuk menghapus volume

1. Klik kanan volume yang ingin Anda hapus.
2. Klik **Hapus volume** .

> **Catatan**
> Semua informasi di volume ini akan hilang dan tidak dapat dipulihkan kembali.

3. Dengan mengklik **OK**, Anda akan menambahkan operasi penghapusan volume yang tertunda.
4. Untuk menyelesaikan operasi yang ditambahkan, lakukan. Menutup program tanpa melakukan operasi akan membatalkannya.

Setelah volume dihapus, ruangnya ditambahkan ke ruang disk yang tidak teralokasi. Anda dapat menggunakannya untuk membuat volume baru atau untuk mengubah jenis volume lain.

Mengatur volume aktif

Jika Anda memiliki beberapa volume utama, Anda harus menentukan satu untuk menjadi volume boot. Untuk ini, Anda dapat mengatur volume menjadi aktif. Disk hanya dapat memiliki satu volume aktif.

Untuk mengatur volume menjadi aktif:

1. Klik kanan pada volume utama yang diinginkan di MBR standar, kemudian klik **Tandai sebagai aktif**.

   Jika tidak ada volume aktif lainnya dalam sistem, operasi pengaturan volume aktif yang tertunda akan ditambahkan. Jika volume aktif lain ada di sistem, Anda akan menerima peringatan bahwa volume aktif sebelumnya harus disetel pasif terlebih dahulu.

   Catatan
   Karena pengaturan volume aktif baru, huruf volume aktif sebelumnya mungkin berubah dan beberapa program yang diinstal mungkin berhenti berjalan.

2. Dengan mengklik **OK**, Anda akan menambahkan operasi pengaturan volume aktif yang tertunda.

   Catatan
   Meskipun Anda memiliki sistem operasi pada volume aktif yang baru, dalam beberapa kasus mesin tidak akan dapat melakukan boot dari volume tersebut. Anda harus mengonfirmasi keputusan Anda untuk mengatur volume baru sebagai aktif.

3. Untuk menyelesaikan operasi yang ditambahkan, lakukan. Menutup program tanpa melakukan operasi akan membatalkannya.

Mengubah huruf volume

Sistem operasi Windows menetapkan huruf (C:, D:, dll) untuk volume hard disk saat startup. Huruf-huruf ini digunakan oleh aplikasi dan sistem operasi untuk mencari file dan folder dalam volume. Menghubungkan disk tambahan, serta membuat atau menghapus volume pada disk yang ada, dapat mengubah konfigurasi sistem Anda. Akibatnya, beberapa aplikasi mungkin berhenti bekerja secara normal atau file pengguna mungkin tidak ditemukan dan dibuka secara otomatis. Untuk mencegah hal ini, Anda dapat secara manual mengubah huruf yang secara otomatis ditetapkan ke volume oleh sistem operasi.

Untuk mengubah huruf yang ditetapkan ke volume oleh sistem operasi

1. Klik kanan volume yang diinginkan, kemudian klik **Ubah huruf**.
2. Di jendela **Ubah Huruf**, pilih huruf baru.
3. Dengan mengklik **OK**, Anda akan menambahkan operasi penetapan huruf volume yang tertunda.
4. Untuk menyelesaikan operasi yang ditambahkan, lakukan. Menutup program tanpa melakukan operasi akan membatalkannya.

Mengubah label volume

Label volume adalah atribut opsional. Label adalah nama yang ditetapkan ke volume agar lebih mudah dikenali.

Untuk mengubah label volume

1. Klik kanan volume yang diinginkan, kemudian klik **Ubah label**.
2. Masukkan label baru di bidang teks jendela **Ubah label**.
3. Dengan mengklik **OK**, Anda akan menambahkan operasi perubahan label volume yang tertunda.
4. Untuk menyelesaikan operasi yang ditambahkan, lakukan. Menutup program tanpa melakukan operasi akan membatalkannya.

Memformat volume

Anda mungkin ingin memformat volume jika ingin mengganti sistem file-nya:

- Untuk menghemat ruang tambahan yang hilang karena ukuran klaster pada sistem file FAT16 atau FAT32
- Sebagai cara yang cepat dan kurang lebih dapat diandalkan untuk menghancurkan data, yang berada di volume ini

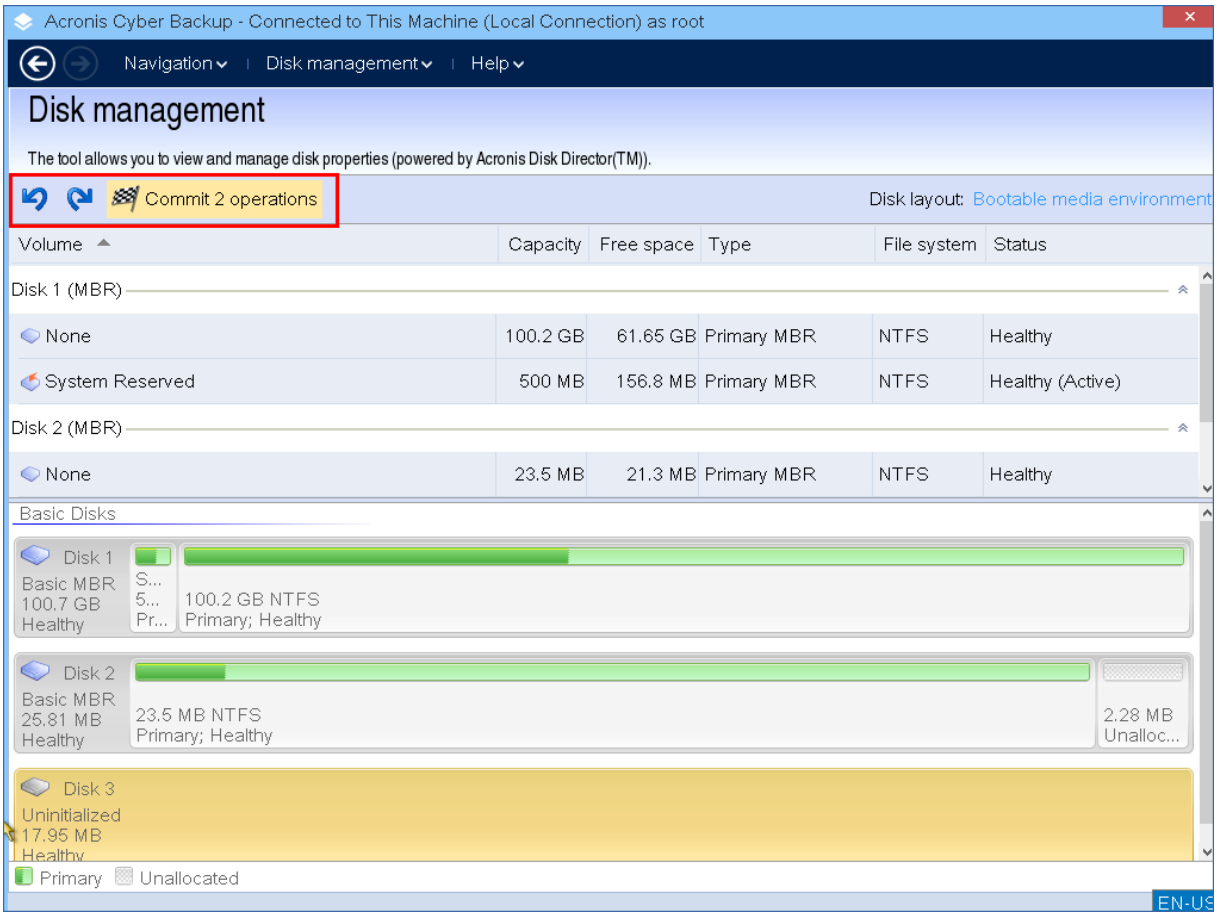
Untuk memformat volume:

1. Klik kanan volume yang diinginkan, kemudian klik **Format**.
2. Pilih ukuran klaster dan sistem file. Opsi sistem file yang memungkinkan adalah:
   - FAT16 (dinonaktifkan jika ukuran volume telah diatur lebih dari 2 GB)
   - FAT32 (dinonaktifkan jika ukuran volume telah diatur lebih dari 2 TB)
   - NTFS
3. Dengan mengklik **OK**, Anda akan menambahkan operasi pemformatan volume yang tertunda.
4. Untuk menyelesaikan operasi yang ditambahkan, lakukan. Menutup program tanpa melakukan operasi akan membatalkannya.

Operasi tertunda

Semua operasi dianggap tertunda hingga Anda melakukan dan mengonfirmasi perintah **Lakukan**. Dengan demikian, Anda dapat mengendalikan semua operasi yang direncanakan, memeriksa ulang perubahan yang diinginkan, dan membatalkan operasi apa pun sebelum dijalankan, jika perlu.

Tampilan **Manajemen disk** berisi toolbar dengan ikon untuk **Urungkan**, **Ulangi**, dan **Lakukan** tindakan yang ditujukan untuk operasi tertunda. Tindakan ini mungkin juga dimulai dari menu **Manajemen disk**.



Semua operasi yang direncanakan ditambahkan ke daftar operasi tertunda.

Tindakan **Urungkan** mengizinkan Anda mengurungkan operasi terakhir dalam daftar. Meskipun daftar tidak kosong, tindakan ini tersedia.

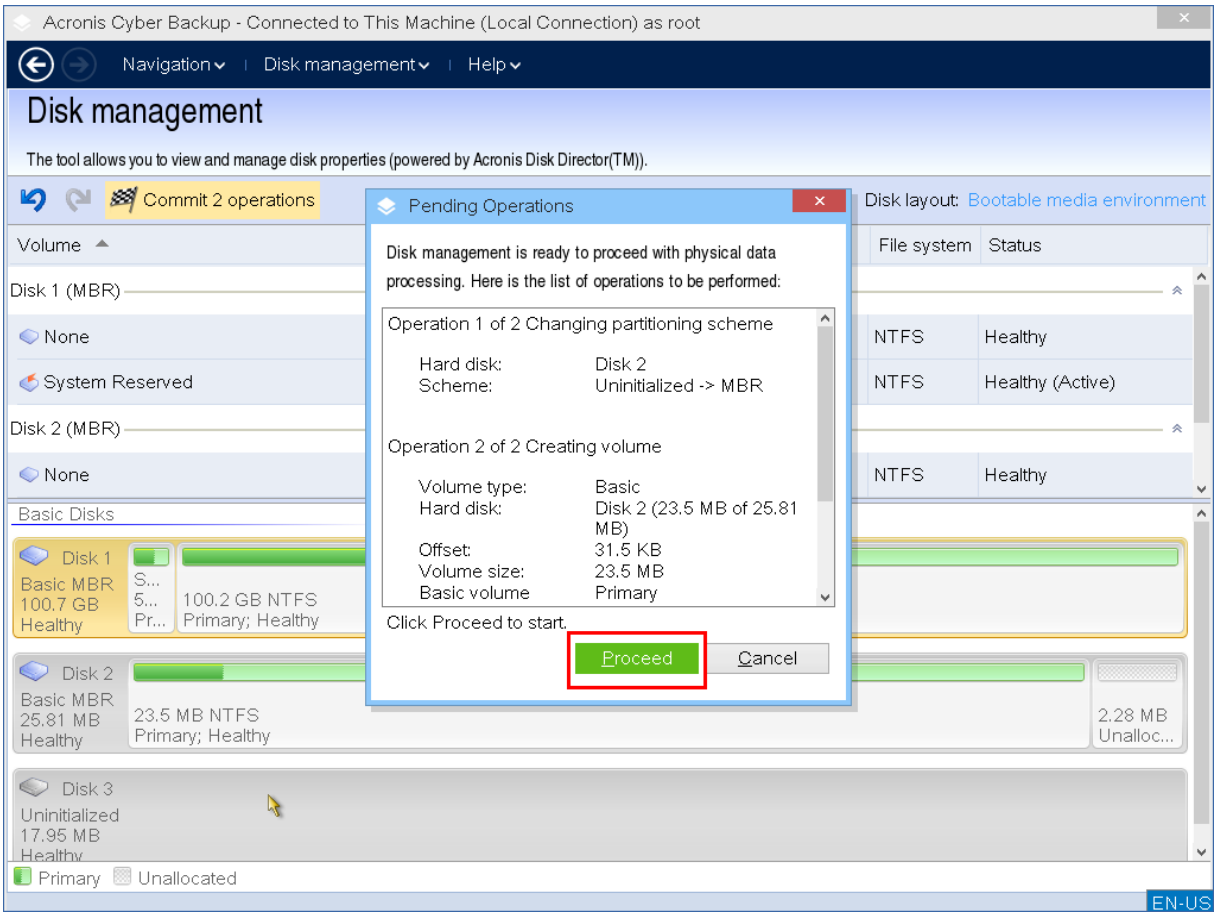
Tindakan **Ulangi** mengizinkan Anda memulihkan operasi tertunda terakhir yang diurungkan.

Tindakan **Lakukan** meneruskan Anda ke jendela **Operasi Tertunda**, di mana Anda akan dapat melihat daftar operasi yang tertunda.

Untuk memulai eksekusi, klik **Lanjutkan**.

Catatan
Anda tidak akan bisa membatalkan tindakan atau operasi apa pun setelah Anda memilih operasi **Lanjutkan**!

Jika Anda tidak ingin melanjutkan operasi, klik **Batalkan**. Maka, tidak ada perubahan yang akan dilakukan pada daftar operasi yang tertunda. Menutup program tanpa melakukan operasi yang tertunda juga akan langsung membatalkannya.



Operasi jarak jauh dengan media yang dapat di-boot

Untuk melihat media yang dapat di-boot di konsol Cyber Protect, pertama-tama Anda harus mendaftarkannya seperti yang dijelaskan di "Mendaftarkan media di server manajemen" (hlm. 379).

Setelah Anda mendaftarkan media di konsol Cyber Protect, media tersebut akan muncul di **Perangkat** > **Media yang dapat di-boot**.

Dengan menggunakan antarmuka web, Anda dapat mengelola media dari jarak jauh. Misalnya, Anda dapat memulihkan data, memulai ulang atau mematikan mesin yang di-boot dengan media, atau melihat informasi, aktivitas, dan peringatan tentang media.

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.

   Anda dapat menggunakan satu atau lebih karakter wildcard (* dan ?). Untuk detail lebih lanjut tentang penggunaan wildcard, lihat "Filter file" (hlm. 271).
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. 326).
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 fisik" (hlm. 307).
5. Untuk konfigurasi pemulihan lanjutan, klik **Opsi pemulihan**. Untuk informasi lebih lanjut, lihat "Opsi pemulihan" (hlm. 326).
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.

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.

Mengonfigurasi perangkat iSCSI

Bagian ini menjelaskan cara mengonfigurasi perangkat Internet Small Computer System Interface (iSCSI) saat bekerja dengan media yang dapat di-boot. Setelah melakukan langkah-langkah di bawah ini, Anda akan dapat menggunakan perangkat ini seolah-olah perangkat tersebut terpasang secara lokal pada mesin yang di-boot menggunakan media yang dapat di-boot.

Server target iSCSI (atau **portal target**) adalah server yang meng-host perangkat iSCSI. **Target iSCSI** adalah komponen pada server target; komponen ini membagikan perangkat dan mencantumkan iSCSI Initiator yang diizinkan untuk mengakses perangkat. **Inisiator iSCSI** adalah komponen pada mesin; komponen ini menyediakan interaksi antara mesin dan target iSCSI. Saat mengkonfigurasi akses ke perangkat iSCSI pada mesin yang di-boot menggunakan media yang dapat di-boot, Anda harus menentukan portal target iSCSI perangkat dan salah satu iSCSI Initiator yang tercantum dalam target. Jika target berbagi beberapa perangkat, Anda akan mendapatkan akses ke semua perangkat tersebut.

Untuk menambahkan perangkat iSCSI di media yang dapat di-boot berbasis Linux

1. Klik **Alat** > **Konfigurasikan perangkat iSCSI/NDAS**.
2. Klik **Tambah host**.
3. Tentukan alamat IP dan port portal target iSCSI, serta nama iSCSI Initiator apa pun yang diizinkan untuk mengakses perangkat.
4. Jika host memerlukan autentikasi, tentukan nama pengguna dan kata sandi untuknya.
5. Klik **OK**.
6. Pilih target iSCSI dari daftar, lalu klik **Hubungkan**.

7. Jika autentikasi CHAP diaktifkan di pengaturan target iSCSI, Anda akan diminta memasukkan kredensial untuk mengakses target iSCSI. Tentukan nama pengguna dan rahasia target yang sama seperti pada pengaturan target iSCSI. Klik **OK**.
8. Klik **Tutup** untuk menutup jendela.

Untuk menambahkan perangkat iSCSI dalam media yang dapat di-boot berbasis-PE

1. Klik **Alat** > **Jalankan Pengaturan iSCSI**.
2. Klik tab **Penemuan**.
3. Pada **Portal Target**, klik **Tambah**, lalu tentukan alamat IP dan port portal target iSCSI. Klik **OK**.
4. Klik tab **Umum**, klik **Ubah**, lalu tentukan nama iSCSI Initiator yang diizinkan untuk mengakses perangkat.
5. Klik tab **Target**, klik **Segarkan**, pilih target iSCSI dari daftar, lalu klik **Hubungkan**. Klik **OK** untuk terhubung ke target iSCSI
6. Jika autentikasi CHAP diaktifkan di pengaturan target iSCSI, Anda akan melihat kesalahan **Kegagalan Autentikasi**. Pada kasus ini, klik **Hubungkan**, klik **Lanjutan**, pilih kotak centang **Aktifkan masuk CHAP**, lalu tentukan nama pengguna dan target rahasia yang sama seperti pada pengaturan target iSCSI. Klik **OK** untuk menutup jendela, lalu klik **OK** untuk terhubung ke target iSCSI.
7. Klik **OK** untuk menutup jendela.

Startup Recovery Manager

Startup Recovery Manager adalah komponen yang dapat di-booting yang bertempat di hard drive Anda. Dengan Startup Recovery Manager, Anda dapat memulai utilitas penyelamat yang dapat di-booting tanpa menggunakan media yang dapat di-booting lainnya.

Startup Recovery Manager sangat berguna untuk pengguna yang bepergian. Jika terjadi kegagalan, boot ulang mesin, tunggu perintah **Tekan F11 untuk Acronis Startup Recovery Manager...** muncul, lalu tekan F11. Program akan memulai dan Anda dapat melakukan pemulihan. Di mesin yang menginstal pemuat boot GRUB, pilih Startup Recovery Manager dari menu boot, bukan menekan F11 selama boot ulang.

Anda juga dapat mencadangkan menggunakan Startup Recovery Manager, saat bepergian.

Untuk menggunakan Startup Recovery Manager, Anda harus mengaktifkannya. Oleh karena itu, Anda mengaktifkan anjuran waktu-boot **Tekan F11 untuk Acronis Startup Recovery Manager** (atau tambahkan item **Startup Recovery Manager** ke menu GRUB jika Anda memiliki pemuat boot GRUB).

Catatan
Untuk mengaktifkan Startup Recovery Manager di mesin dengan sistem volume tidak terenkripsi, mesin harus memiliki setidaknya ruang bebas sebesar 100 MB di mesin ini. Operasi pemulihan yang mengharuskan mesin dimulai kembali memerlukan tambahan 100 MB.

Anda dapat mengaktifkan Startup Recovery Manager di mesin dengan volume yang dienkripsi BitLocker jika mesin tersebut setidaknya memiliki satu volume lain yang tidak dienkripsi. Volume tidak terenkripsi harus memiliki setidaknya ruang bebas 500 MB. Untuk operasi pemulihan yang mengharuskan mesin dimulai ulang, mesinnya harus memiliki ruang bebas tambahan sebanyak 500 MB.

Penting
Jika Startup Recovery Manager tidak dapat diaktifkan, operasi pencadangan yang membuat cadangan pemulihan Sekali klik akan gagal.

Kecuali jika Anda menggunakan pemuat boot GRUB dan diinstal di Master Boot Record (MBR), aktivasi Startup Recovery Manager akan menimpa MBR dengan kode boot-nya sendiri. Maka, Anda mungkin perlu mengaktifkan kembali pemuat boot pihak ketiga jika pemuat boot tersebut diinstal.

Di Linux, ketika menggunakan pemuat boot selain GRUB (misalnya LILO), pertimbangkan untuk menginstalnya ke catatan boot partisi root (atau boot) Linux, bukan MBR, sebelum mengaktifkan Startup Recovery Manager. Jika tidak, konfigurasikan ulang boot loader secara manual setelah aktivasi.

Mengaktifkan Startup Recovery Manager

Di mesin yang menjalankan Agen untuk Windows atau Agen untuk Linux, Anda dapat mengaktifkan Startup Recovery Manager di konsol web Cyber Protect.

Untuk mengaktifkan Startup Recovery Manager di konsol web Cyber Protect

1. Pilih mesin tempat Anda ingin mengaktifkan Startup Recovery Manager.
2. Klik **Detail**.
3. Aktifkan switch **Startup Recovery Manager** .
4. Tunggu sementara perangkat lunak mengaktifkan Startup Recovery Manager.

Untuk mengaktifkan Startup Recovery Manager pada mesin tanpa agen

1. Boot mesin dari media yang dapat di-boot.
2. Klik **Alat** > **Aktifkan Startup Recovery Manager** .
3. Tunggu sementara perangkat lunak mengaktifkan Startup Recovery Manager.

Menonaktifkan Startup Recovery Manager

Untuk deaktivasi Startup Recovery Manager, ulangi prosedur aktivasi dan pilih tindakan yang berlawanan. Deaktivasi akan menonaktifkan anjuran waktu-boot **Tekan F11 untuk Acronis Startup Recovery Manager** (atau item menu di GRUB).

Jika Startup Recovery Manager tidak diaktifkan, Anda akan memerlukan salah satu dari hal berikut untuk memulihkan sistem ketika gagal boot:

- boot mesin dari media yang dapat di-boot terpisah
- gunakan boot jaringan dari server PXE atau Microsoft Remote Installation Services (RIS)

Acronis Server PXE

Server PXE Acronis memungkinkan booting mesin untuk komponen Acronis yang dapat di-boot melalui jaringan.

Boot jaringan:

- mengeliminasi kebutuhan akan teknisi di lokasi untuk menginstal media yang dapat di-boot ke dalam sistem yang harus di-boot
- selama operasi grup, mengurangi waktu yang diperlukan untuk melakukan booting beberapa mesin dibandingkan dengan menggunakan media yang dapat di-boot secara fisik.

Komponen yang dapat di-boot diunggah ke Server PXE Acronis menggunakan Pembangun Media yang Dapat Di-Boot Acronis. Untuk mengunggah komponen yang dapat di-boot, mulai Pembangun Media yang Dapat Di-boot, lalu ikuti petunjuk langkah demi langkah yang dijelaskan dalam "Media yang dapat di-boot berbasis Linux".

Melakukan booting beberapa mesin dari Server PXE Acronis dapat dilakukan jika terdapat server Dynamic Host Control Protocol (DHCP) di jaringan Anda. Antarmuka jaringan dari mesin yang dibooting kemudian akan secara otomatis mendapatkan alamat IP.

Pembatasan:

Server PXE Acronis tidak mendukung pemuat boot UEFI.

Menginstal Server PXE Acronis

Untuk menginstal Server PXE Acronis

1. Masuk sebagai administrator dan mulai program penyiapan Acronis Cyber Protect.
2. [Opsional] Untuk mengubah bahasa program penyiapan, klik **Pengaturan bahasa**.
3. Terima persyaratan perjanjian lisensi dan pernyataan privasi, lalu klik **Lanjutkan**.
4. Klik **Sesuaikan pengaturan instalasi**.
5. Di sebelah **Apa yang diinstal**, klik **Ubah**.

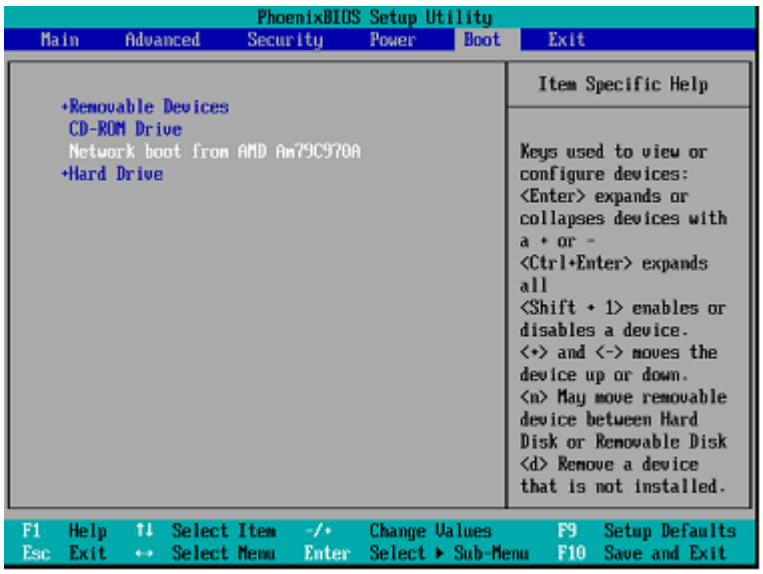
6. Pilih kotak centang **PXE Server**. Jika Anda tidak ingin menginstal komponen lain pada mesin ini, kosongkan kotak centang yang sesuai. Klik **Selesai** untuk melanjutkan.
7. [Opsional] Ubah pengaturan instalasi lainnya.
8. Klik **Instal** untuk melanjutkan instalasi.
9. Setelah instalasi selesai, klik **Tutup**.

Server PXE Acronis akan segera berjalan sebagai layanan setelah instalasi. Berikutnya akan secara otomatis diluncurkan pada setiap sistem memulai ulang. Anda dapat menghentikan dan memulai Server PXE Acronis dengan cara yang sama seperti layanan Windows lainnya.

Menyiapkan mesin untuk boot dari PXE

Untuk bare metal, cukup bahwa BIOS mesin mendukung boot jaringan.

Pada mesin yang memiliki sistem operasi pada hard disk, BIOS harus dikonfigurasikan agar kartu antarmuka jaringan dapat menjadi perangkat boot pertama, atau setidaknya sebelum perangkat Hard Drive. Contoh di bawah ini menunjukkan salah satu konfigurasi BIOS yang dapat diterima. Jika Anda tidak memasukkan media yang dapat di-boot, mesin akan melakukan boot dari jaringan.



Di beberapa versi BIOS, Anda harus menyimpan perubahan pada BIOS setelah mengaktifkan kartu antarmuka jaringan sehingga kartu tersebut muncul dalam daftar perangkat boot.

Jika perangkat keras memiliki beberapa kartu antarmuka jaringan, pastikan kartu yang didukung oleh BIOS memiliki kabel jaringan yang terhubung.

Bekerja lintas subnet

Untuk mengaktifkan Server PXE Acronis agar bekerja di subnet lain (lintas switch), konfigurasikan switch untuk merelai lalu lintas PXE. Alamat IP server PXE dikonfigurasikan pada basis per antarmuka menggunakan fungsi IP helper dengan cara yang sama seperti alamat server DHCP.

Untuk informasi lebih lanjut, lihat: https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/boot-from-pxe-server.

Melindungi perangkat seluler

Aplikasi pencadangan memungkinkan untuk mencadangkan data seluler Anda ke penyimpanan Cloud, lalu pulihkan apabila hilang atau rusak. Perhatikan bahwa pencadangan ke penyimpanan awan memerlukan akun dan langganan Cloud.

Perangkat seluler yang didukung

Anda dapat menginstal aplikasi pencadangan di perangkat seluler yang menjalankan sistem operasi berikut:

- iOS 10.3 dan di atasnya (iPhone, iPod, dan iPad)
- Android 5.0 dan ke atas

Apa yang dapat Anda cadangkan

- Kontak
- Foto
- 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:
  - Untuk Android 7.0 atau versi di atasnya, aplikasi pencadangan mendeteksi data baru selama perjalanan secara otomatis dan mengunggahnya ke Cloud.
  - Untuk Android 5 dan 6, ini akan memeriksa perubahan setiap tiga jam. Anda dapat menonaktifkan pencadangan kontinu dalam pengaturan aplikasi.
- Opsi **Hanya gunakan Wi-Fi** diaktifkan secara standar di pengaturan aplikasi. Jika pengaturan ini diaktifkan, aplikasi pencadangan 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.
- Anda memiliki dua cara untuk menghemat energi:
  - Fungsi **Cadangkan selama mengisi daya** dinonaktifkan secara standar. Jika pengaturan ini diaktifkan, aplikasi pencadangan 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 pencadangan akan mencadangkan data Anda hanya saat baterai perangkat tidak lemah. Jika baterai perangkat melemah, pencadangan kontinu akan dijeda. Pilihan ini tersedia untuk Android 8 dan yang di atasnya.
- 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 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 setiap perangkat menggunakan konsol web 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 pencadangan, Anda hanya dapat memulihkan data terakhir. Jika Anda perlu memulihkan dari versi cadangan tertentu, gunakan konsol web Cyber Protect di tablet atau komputer.
- [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 pencadangan

1. Di perangkat seluler, buka browser lalu buka https://backup.acronis.com/.
2. Masuk dengan akun Anda.
3. Klik **Semua perangkat** > **Tambah**.
4. Di dalam **Perangkat seluler**, pilih jenis perangkat.
   Tergantung jenis perangkat, Anda akan dialihkan ke App Store atau Google Play Store.
5. [Hanya di perangkat iOS] Klik **Dapatkan**.
6. Klik **Instal** untuk menginstal aplikasi pencadangan.

Cara memulai pencadangan data Anda

1. Buka aplikasi.
2. Masuk dengan akun Anda.

Sentuh **Atur** untuk membuat cadangan pertama Anda.

1. Pilih kategori data yang ingin Anda cadangkan. Secara default, semua kategori dipilih.
2. [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**.

3. Ketuk **Cadangkan**.
4. Izinkan akses aplikasi ke data pribadi Anda. Jika Anda menolak akses ke beberapa kategori data, data tidak akan dicadangkan.

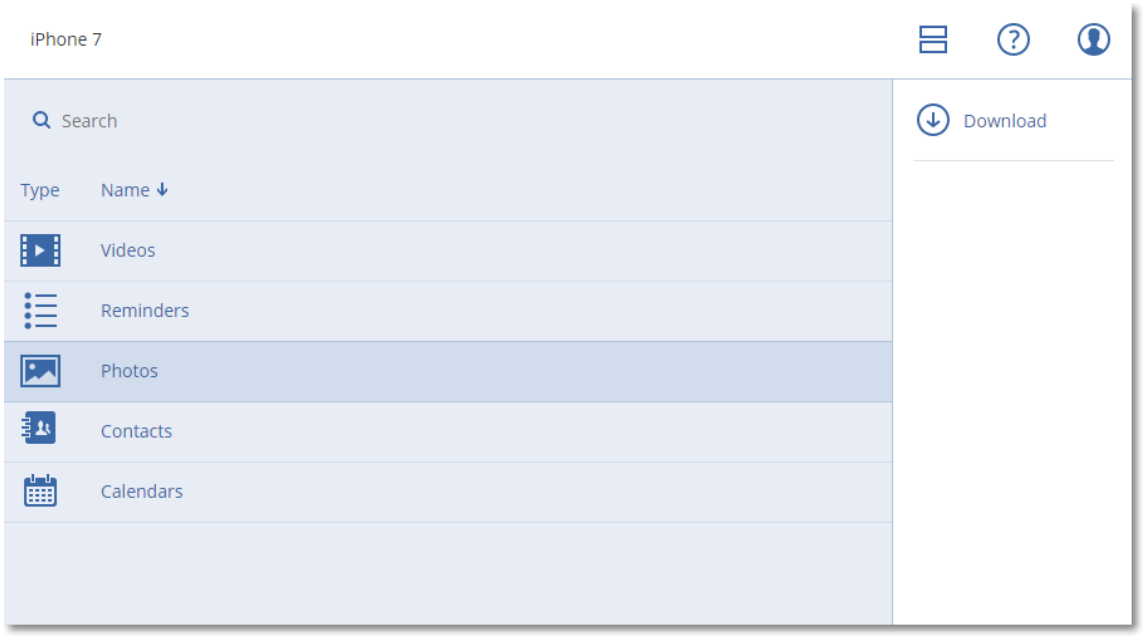
Mulai mencadangkan.

Cara memulihkan data ke perangkat seluler

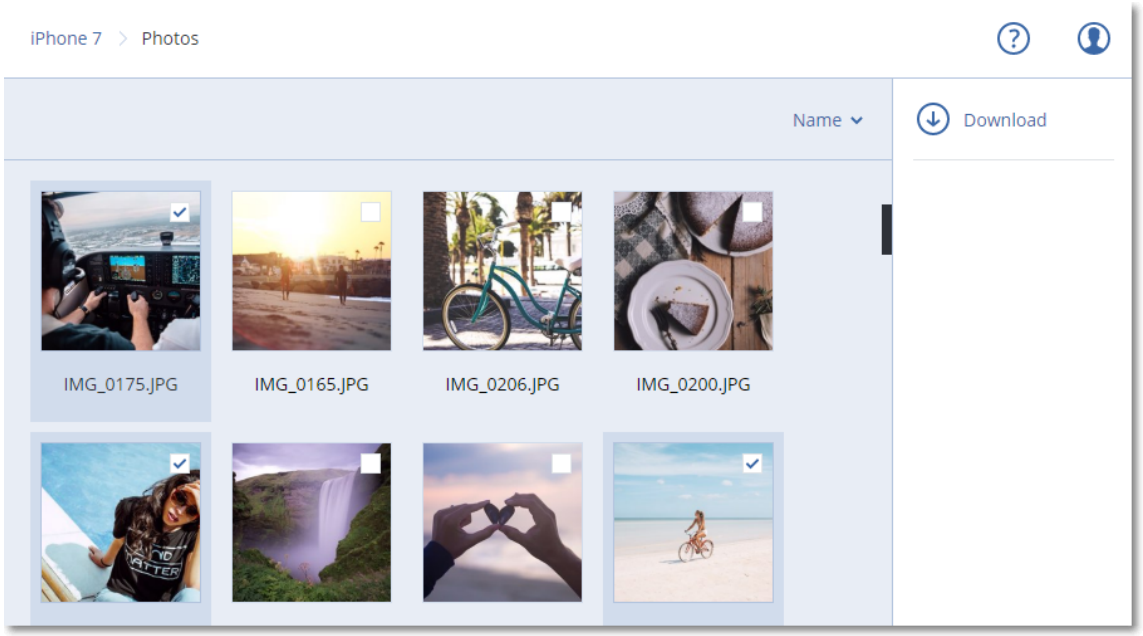
1. Buka aplikasi pencadangan.
2. Sentuh **Jelajahi**.
3. Ketuk nama perangkat.
4. Lakukan salah satu langkah berikut:
   - Untuk memulihkan semua data yang dicadangkan, ketuk **Pulihkan semua**. Tidak diperlukan tindakan lainnya.
   - Untuk memulihkan satu atau beberapa kategori data, ketuk **Pilih**, 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 web Cyber Protect

1. Di komputer, buka browser dan ketik URL konsol web Cyber Protect.
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**.



- 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 aplikasi Microsoft

Penting
Beberapa fitur yang dijelaskan dalam bagian ini hanya tersedia untuk penyebaran lokal.

Melindungi Microsoft SQL Server dan Microsoft Exchange Server

Ada dua metode untuk melindungi aplikasi ini:

- **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 Exchange Web Services. 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.

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
Microsoft Exchange Server	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	-

* Pemulihan granular juga tersedia dari pencadangan kotak surat.

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 di: https://kb.acronis.com/content/40040..

Pada pengontrol domain, pastikan:

- Active Directory writer untuk VSS dihidupkan.

Saat membuat rencana proteksi, pastikan bahwa:

- Untuk mesin fisik, opsi pencadangan Layanan Volume Shadow Copy (VSS) diaktifkan.
- Untuk mesin virtual, opsi pencadangan Layanan Volume Shadow Copy (VSS) untuk mesin virtual diaktifkan.

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 built-in (DOMAIN\Administrator) ketika mengaktifkan pencadangan aplikasi.

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 built-in (DOMAIN\Administrator) ketika mengaktifkan pencadangan aplikasi.
- 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 Volume Shadow Copy (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.
   - 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", kotak pesan 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 Availability Groups (DAG)".
   - 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", Anda dapat memilih kotak surat untuk pencadangan.
4. Jika diminta, berikan kredensial untuk mengakses data.
5. Klik **Lindungi**.

Melindungi Always On Availability Group (AAG)

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.

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.

   Catatan
   Setelah Anda menginstal agen di salah satu simpul, perangkat lunak akan menampilkan AAG dan simpulnya pada **Perangkat** > **Microsoft SQL** > **Database**. Untuk menginstal Agen untuk SQL di seluruh simpul, pilih AAG, klik **Detail**, lalu klik **Instal agen** di sebelah setiap simpul.

2. Pilih AAG atau database yang diatur untuk dicadangkan seperti yang dijelaskan di "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 pencadangan 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.

Melindungi Database Availability Group (DAG)

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.

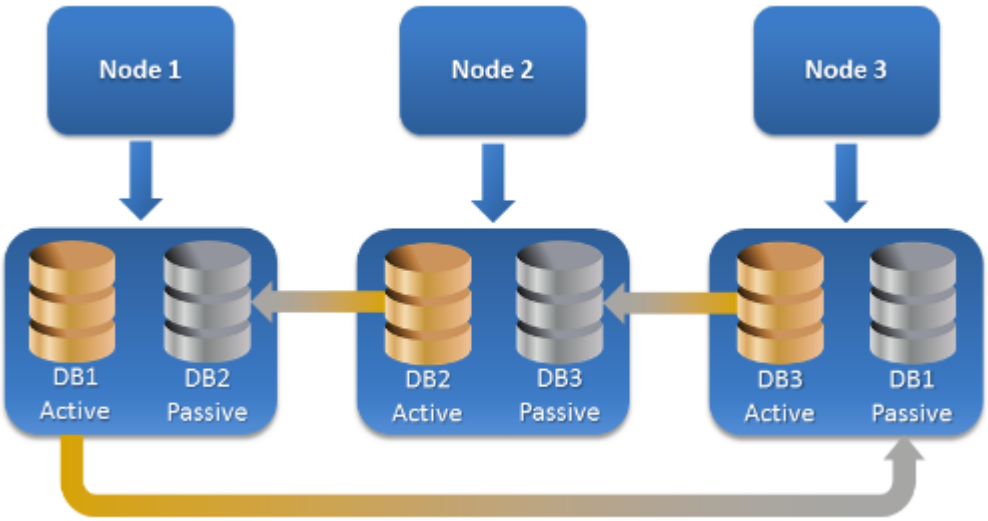
Pencadangan keberadaan klaster

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.



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 simpul, konsol web Cyber Protect akan menampilkan DAG dan simpulnya pada **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".
2. Konfigurasikan opsi pencadangan "Mode pencadangan klaster".
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 pencadangan klaster** akan diabaikan.

Memulihkan data klaster Exchange

1. Pilih titik pemulihan untuk database yang ingin Anda pulihkan. Memilih seluruh klaster untuk pemulihan tidak dimungkinkan.

   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", 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

Cadangan tingkat disk keberadaan aplikasi tersedia untuk mesin fisik dan, 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:

1. Aplikasi dicadangkan dalam status konsisten, sehingga aplikasi dapat segera tersedia setelah mesin dipulihkan.
2. Anda dapat memulihkan database SQL dan Exchange, kotak surat, dan item kotak surat tanpa memulihkan keseluruhan mesin.
3. 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.
4. 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.

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 yang menjalankan Windows Server 2022, cadangan keberadaan aplikasi tidak didukung dalam mode tanpa agen, yaitu saat pencadangan dilakukan oleh Agen untuk Hyper-V. Untuk melindungi berbagai aplikasi Microsoft dalam mesin-mesin ini, instal Agen untuk Windows di dalam sistem operasi tamu.

Agen untuk VMware (Virtual Appliance) dan Agen untuk VMware (Linux) dapat membuat cadangan keberadaan aplikasi, tetapi tidak dapat memulihkan data aplikasi darinya. Untuk memulihkan data aplikasi dari pencadangan yang dibuat oleh agen-agen tersebut, Anda memerlukan 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 lainnya tercantum dalam "Prasyarat" (hlm. 436) dan "Hak pengguna yang diperlukan untuk pencadangan berbasis aplikasi" (hlm. 444).

Hak pengguna yang diperlukan untuk pencadangan berbasis 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:

  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.
- 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**.
- 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 built-in (DOMAIN\Administrator) ketika mengaktifkan pencadangan aplikasi.

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 Anda tidak ingin menonaktifkan kebijakan UAC, Anda harus memberikan kredensial administrator domain bawaan (DOMAIN\Administrator) saat mengonfigurasi pencadangan terinformasi untuk aplikasi.

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**.

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.
2. Klik **Kotak Surat**, lalu pilih kotak surat yang ingin Anda buat cadangannya.
3. Klik **Cadangkan**.

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

Bagian ini menjelaskan pemulihan dari pencadangan database dan pencadangan keberadaan aplikasi.

Anda dapat memulihkan database SQL ke instance SQL Server jika Agen untuk SQL diinstal pada mesin yang menjalankan instans.

Jika Anda menggunakan autentikasi Windows, Anda perlu memberikan kredensial untuk akun yang merupakan anggota grup **Operator Pencadangan** atau **Administrator** pada mesin dan anggota peran **sysadmin** pada instans target. Jika Anda menggunakan autentikasi SQL Server, Anda perlu memberikan kredensial untuk akun yang merupakan anggota peran **sysadmin** pada instans target.

Selain itu, Anda juga dapat memulihkan database sebagai file. Cara ini dapat berguna jika Anda perlu mengekstrak data untuk penggalian data, audit, atau pemrosesan lebih lanjut dari alat pihak ketiga. Anda dapat memasang file database SQL ke instans SQL Server, seperti yang dijelaskan dalam "Memasang database SQL Server".

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.

Database sistem pada dasarnya dipulihkan dengan cara yang sama seperti database pengguna. Penjelasan tentang pemulihan database sistem dijelaskan dalam "Memulihkan database sistem".

Untuk memulihkan database SQL ke instans SQL Server

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 SQL**, 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 SQL, 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 database SQL.
4. Lakukan salah satu langkah berikut:
   - Saat memulihkan dari cadangan keberadaan aplikasi, klik **Pulihkan** > **Database SQL**, pilih database yang ingin Anda pulihkan, lalu klik **Pulihkan**.
   - Saat memulihkan dari cadangan database, klik **Pulihkan** > **Database ke instans**.
5. Secara default, database dipulihkan ke yang asli. Jika database asli tidak ada, database akan dibuat kembali. Anda dapat memilih instans SQL Server lain (yang berjalan di mesin yang sama) untuk memulihkan database.

   Untuk memulihkan database sebagai jenis yang lain dengan instans yang sama:

   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. [Opsional] [Tidak tersedia untuk database yang dipulihkan ke instans aslinya sebagai database baru] Untuk mengubah status database setelah pemulihan, klik nama database, lalu pilih salah satu status berikut:
   - **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

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.

7. Klik **Mulai pemulihan**.

Progres pemulihan akan ditampilkan pada tab **Aktivitas**.

Untuk memulihkan database SQL 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 SQL**, 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 SQL 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 database SQL.
4. Lakukan salah satu langkah berikut:
   - Saat memulihkan dari cadangan keberadaan aplikasi, klik **Pulihkan** > **Database SQL**, 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**.

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.
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

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:
   - [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

Bagian ini menjelaskan cara memulihkan kotak surat Exchange dan item kotak surat dari cadangan database, cadangan keberadaan aplikasi, dan cadangan kotak surat. Kotak surat atau item kotak surat dapat dipulihkan ke Exchange Server langsung atau ke Microsoft 365.

Item berikut dapat dipulihkan:

- Kotak surat (kecuali untuk kotak surat arsip)
- Folder publik

  Catatan
  Tersedia hanya dari cadangan database. Lihat "Memilih data Exchange Server" (hlm. 438)

- Item folder publik
- Folder Email
- Pesan email
- Acara kalender
- Tugas
- Kontak
- Entri jurnal
- Catatan

Anda dapat menggunakan pencarian untuk menemukan item.

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.

Jika beberapa kotak surat dilewati, pemulihan akan berhasil namun disertai peringatan. Jika semua kotak surat dilewati, pemulihan akan gagal.

Pemulihan ke Microsoft 365

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 kotak surat Microsoft 365" (hlm. 461).

Memulihkan kotak surat

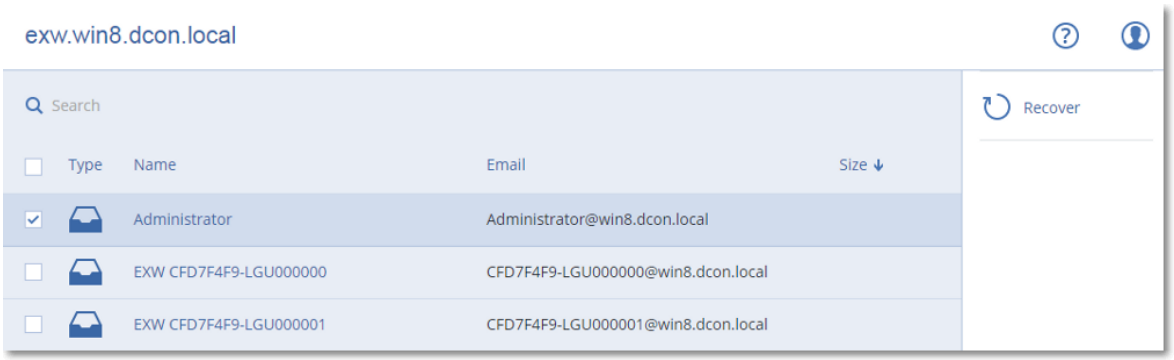
Untuk memulihkan kotak surat dari cadangan keberadaan aplikasi atau cadangan database

1. [Hanya ketika memulihkan dari cadangan database ke Microsoft 365] Jika Agen untuk Office 365 tidak diinstal pada mesin yang menjalankan Exchange Server yang dicadangkan, lakukan salah satu langkah berikut:
   - Jika tidak ada Agen untuk Office 365 di organisasi Anda, instal Agen untuk Office 365 pada mesin yang dicadangkan (atau pada mesin lain dengan versi Microsoft Exchange Server yang sama).
   - Jika Anda sudah memiliki Agen untuk Office 365 di organisasi, salin pustaka dari mesin yang dicadangkan (atau dari mesin lain dengan versi Microsoft Exchange Server yang sama) ke mesin dengan Agen untuk Office 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**.
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 Office 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.

9. 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.

   Jika diminta, berikan kredensial akun yang akan digunakan untuk mengakses mesin. Persyaratan untuk akun ini tercantum di "Hak pengguna yang diperlukan" (hlm. 447).

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

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 Office 365 tidak diinstal pada mesin yang menjalankan Exchange Server yang dicadangkan, lakukan salah satu langkah berikut:
   - Jika tidak ada Agen untuk Office 365 di organisasi Anda, instal Agen untuk Office 365 pada mesin yang dicadangkan (atau pada mesin lain dengan versi Microsoft Exchange Server yang sama).
   - Jika Anda sudah memiliki Agen untuk Office 365 di organisasi, salin pustaka dari mesin yang dicadangkan (atau dari mesin lain dengan versi Microsoft Exchange Server yang sama) ke

mesin dengan Agen untuk Office 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.

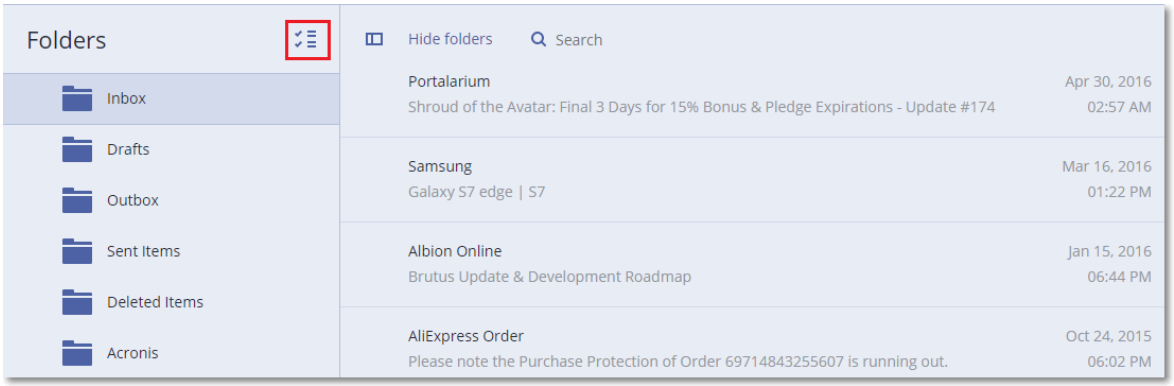
   Mesin yang dipilih untuk menjelajahi dalam tindakan di atas akan melakukan pemulihan, bukan dalam mesin asli yang sedang offline.
5. Klik **Pulihkan** > **Kotak surat Exchange**.
6. Klik kotak surat yang awalnya berisi item yang ingin Anda pulihkan.
7. Pilih item yang ingin Anda pulihkan.

   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 Office 365** di **Pulihkan ke**.

   Untuk memulihkan ke Exchange Server, pertahankan nilai default **Microsoft Exchange** di **Pulihkan ke**.
10. [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.

    Jika diminta, berikan kredensial akun yang akan digunakan untuk mengakses mesin. Persyaratan untuk akun ini tercantum di "Hak pengguna yang diperlukan" (hlm. 447).
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.
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 Office 365.

Salin file berikut, sesuai dengan versi Microsoft Exchange Server yang didukung.

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 kotak surat Microsoft 365

Penting
Bagian ini valid untuk penyebaran lokal Acronis Cyber Protect. Jika Anda menggunakan penyebaran awan, silakan lihat https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-microsoft-365-data.html.

Untuk informasi lebih lanjut tentang opsi pelisensian, lihat Acronis Cyber Backup untuk Pelisensian Microsoft 365.

Mengapa perlu mencadangkan kotak surat Microsoft 365?

Meskipun Microsoft 365 adalah layanan awan, pencadangan reguler dapat menyediakan lapisan perlindungan tambahan dari kesalahan pengguna dan tindakan berbahaya yang disengaja. Anda dapat memulihkan item yang dihapus dari cadangan bahkan setelah periode penyimpanan Microsoft 365 berakhir. Selain itu, Anda juga dapat menyimpan salinan lokal kotak surat Microsoft 365 jika diperlukan untuk memenuhi kepatuhan terhadap peraturan.

Pemulihan

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.

Pemulihan dapat dilakukan ke Microsoft 365 atau ke Exchange Server langsung.

Ketika kotak surat dipulihkan ke kotak surat Microsoft 365 yang ada, item yang ada dengan ID yang sama akan ditimpa. Ketika kotak surat dipulihkan ke kotak surat Exchange Server yang ada, item yang sudah ada akan tetap utuh. Item yang dipulihkan akan ditempatkan di sebelahnya.

Pemulihan item kotak surat tidak menimpa apa pun. Sebaliknya, jalur lengkap ke item kotak surat dibuat kembali di folder target.

Pembatasan

- Menerapkan rencana proteksi ke lebih dari 500 kotak surat dapat menyebabkan penurunan kinerja pencadangan. Untuk melindungi banyak kotak surat, buat beberapa rencana proteksi dan jadwalkan agar berjalan pada waktu yang berbeda.
- Kotak surat arsip (**Arsip Di Tempat**) tidak dapat dicadangkan.
- 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.
- Pemulihan ke kotak surat Microsoft 365 baru tidak dapat dilakukan. Anda harus terlebih dahulu membuat pengguna Microsoft 365 baru secara manual, lalu memulihkan item ke kotak surat pengguna ini.
- Pemulihan ke organisasi Microsoft 365 yang berbeda tidak didukung.
- Beberapa jenis atau properti item yang didukung oleh Microsoft 365 mungkin tidak didukung oleh Exchange Server. Item tersebut akan dilewati selama pemulihan ke Exchange Server.

Menambahkan organisasi Microsoft 365

Untuk menambahkan organisasi Microsoft, Anda perlu mengetahui ID aplikasi, rahasia aplikasi, dan ID penyewa Microsoft 365 Anda. Untuk informasi lebih lanjut tentang cara mendapatkannya, lihat Cara mendapatkan ID dan rahasia aplikasi.

Untuk menambahkan organisasi Microsoft 365

1. Instal Agen untuk Office 365 pada mesin Windows yang terhubung ke Internet. Hanya diperbolehkan satu Agen untuk Office 365 di satu organisasi.
2. Di konsol web Cyber Protect, klik **Microsoft Office 365**.
3. Di jendela yang terbuka, masukkan ID aplikasi, rahasia aplikasi, dan ID penyewa Microsoft 365 Anda.
4. Klik **Masuk**.

Hasilnya, item data organisasi Anda akan muncul pada konsol web Cyber Protect, di tab **Microsoft Office 365**.

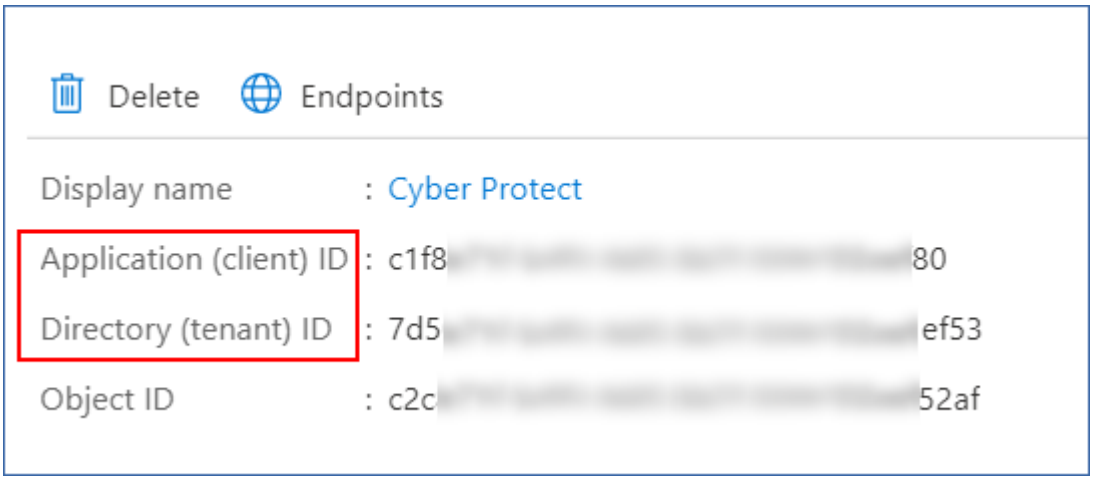
Mendapatkan ID aplikasi dan rahasia aplikasi

Untuk menggunakan autentikasi modern untuk Microsoft 365, Anda perlu membuat aplikasi kustom di Azure Active Directory dan memberinya izin API khusus. Dengan begitu, Anda akan mendapatkan **ID aplikasi**, **rahasia aplikasi**, dan **ID direktori (penyewa)** yang Anda perlukan untuk masuk di konsol web Cyber Protect.

Untuk membuat aplikasi di Azure Active Directory

1. Masuk ke portal Azure sebagai administrator.
2. Navigasi ke **Azure Active Directory** > **Registrasi apl**, kemudian klik **Registrasi baru**.
3. Tentukan nama untuk aplikasi kustom Anda, misalnya, Cyber Protect.
4. Dalam **jenis Dukungan Akun**, pilih **Akun di direktori organisasi ini saja**.
5. Klik **Daftar**.

Aplikasi Anda selesai dibuat. Di portal Azure, navigasi ke halaman **Ikhtisar** aplikasi dan periksa ID aplikasi (klien) dan direktori (ID penyewa).



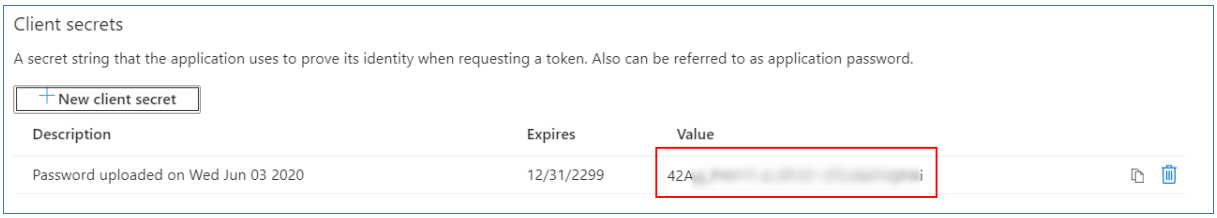
Untuk informasi lebih lanjut mengenai cara membuat aplikasi di portal Azure, lihat dokumentasi Microsoft.

Untuk memberi aplikasi Anda izin API yang dibutuhkan

1. Di portal Azure, 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 **Ya**.

Untuk membuat rahasia aplikasi

1. Di portal Azure, navigasi ke **Sertifikat & rahasia** > **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.



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. Di konsol web Cyber Protect buka **Perangkat** > **Microsoft Office 365**.
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 mendapatkannya, lihat Cara mendapatkan ID dan rahasia aplikasi.
5. Klik **Masuk**.

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

1. Di konsol web Cyber Protect buka **Perangkat** > **Microsoft Office 365**.
2. Pilih kotak surat yang ingin Anda cadangkan.
3. Klik **Cadangkan**.

Memulihkan kotak surat dan item kotak surat

Memulihkan kotak surat

1. [Hanya ketika memulihkan ke Exchange Server] Pastikan ada pengguna Exchange dengan nama masuk yang sama dengan nama pengguna yang kotak suratnya sedang dipulihkan. Jika tidak, buat pengguna. Lihat daftar lengkap persyaratan untuk pengguna ini di "Persyaratan pada akun pengguna" (hlm. 454).
2. Di konsol web Cyber Protect buka **Perangkat** > **Microsoft Office 365**.
3. 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**.

4. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
5. Klik **Pulihkan** > **Kotak surat**.
6. Untuk memulihkan ke Exchange Server, di **Pulihkan ke**, pilih **Microsoft Exchange**. Lanjutkan pemulihan seperti dijelaskan dalam "Memulihkan kotak surat" (hlm. 454), mulai dari langkah 9. Langkah lebih lanjut dari prosedur ini tidak diperlukan.

   Untuk memulihkan ke Microsoft 365, di **Pulihkan ke**, pertahankan nilai **Microsoft Office 365** default.
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**.

Memulihkan item kotak surat

1. [Hanya ketika memulihkan ke Exchange Server] Pastikan ada pengguna Exchange dengan nama masuk yang sama dengan nama pengguna yang kotak suratnya sedang dipulihkan. Jika tidak, buat pengguna. Lihat daftar lengkap persyaratan untuk pengguna ini di "Persyaratan pada akun pengguna" (hlm. 454).
2. Di konsol web Cyber Protect buka **Perangkat** > **Microsoft Office 365**.
3. 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**.
4. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
5. Klik **Pulihkan** > **Pesan Email**.
6. 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": 

7. Klik **Pulihkan**.
8. Untuk memulihkan ke Exchange Server, di **Pulihkan ke**, pilih **Microsoft Exchange**.
   Untuk memulihkan ke Microsoft 365, di **Pulihkan ke**, pertahankan nilai **Microsoft Office 365** default.
9. [Hanya ketika memulihkan ke Exchange Server] Untuk memilih atau mengubah mesin target, klik **Mesin target dengan Microsoft Exchange Server**. 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** Microsoft Exchange Server diaktifkan. Mesin harus dimiliki oleh forest Active Directory yang sama dengan mesin yang melakukan pemulihan.
   Jika diminta, berikan kredensial akun yang akan digunakan untuk mengakses mesin. Persyaratan untuk akun ini tercantum di "Hak pengguna yang diperlukan" (hlm. 447).
10. 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.
11. [Hanya ketika memulihkan pesan email] Di **Folder target**, lihat atau ubah folder target di kotak surat target. Secara default, folder **Pulihkan item** dipilih.
12. Klik **Mulai pemulihan**.

Melindungi data Google Workspace

Fitur ini hanya tersedia di penyebaran awan Acronis Cyber Protect. Untuk deskripsi detail mengenai fungsi ini, silakan lihat https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.html.

Melindungi Database Oracle

Perlindungan Oracle Database dijelaskan dalam dokumen terpisah yang tersedia di https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_OracleBackup_whitepaper.pdf.

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 untuk menjalankan mesin virtual sementara hingga selama 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.

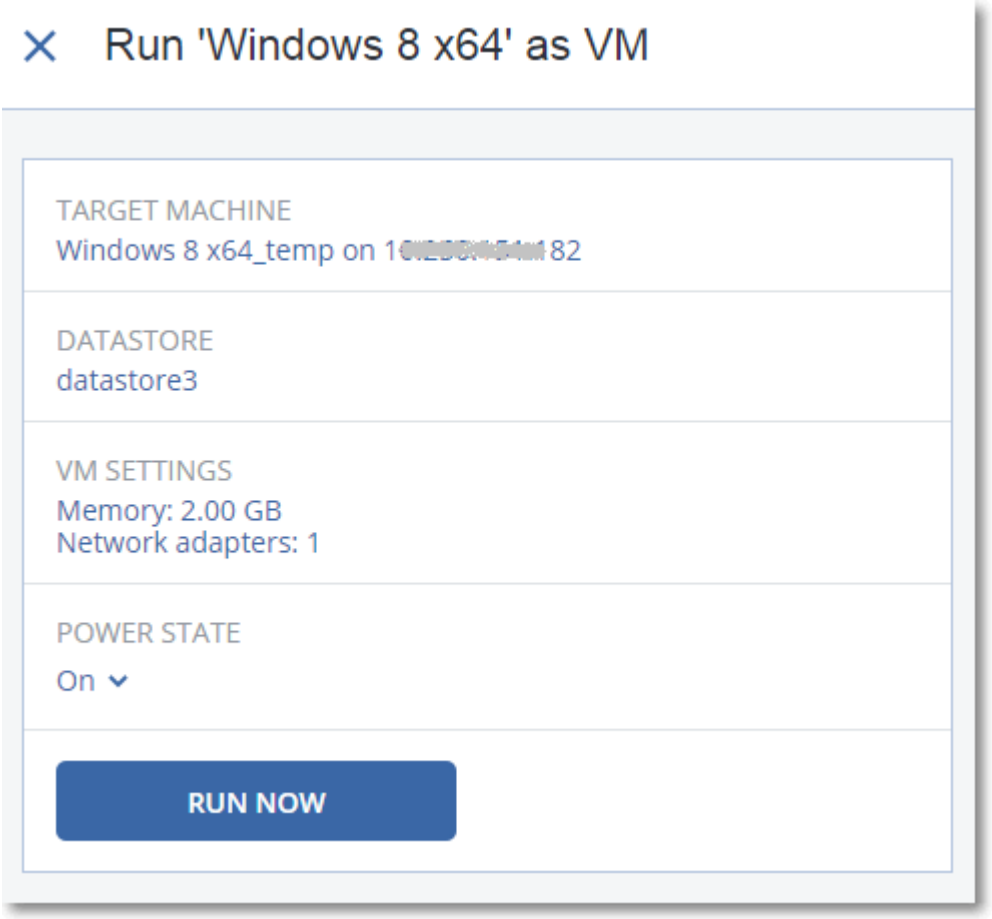
Prasyarat

- Setidaknya satu Agen untuk VMware atau Agen untuk Hyper-V harus terdaftar di layanan Perlindungan Cyber.
- Cadangan dapat disimpan dalam folder jaringan, pada simpul penyimpanan, atau dalam 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. Mesin virtual tidak dapat dijalankan dari cadangan yang disimpan di server SFTP, perangkat pita, atau di Secure Zone.
- 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.

- 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.

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.

Menghapus mesin

Kami tidak menyarankan untuk menghapus mesin virtual sementara secara langsung di vSphere/Hyper-V. Tindakan ini dapat 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 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. Sebaiknya jalankan mesin virtual dari cadangan lokal jika Anda berencana menjalankan finalisasi dan memiliki pilihan untuk itu.

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.

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.

Batasan

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.

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.
      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.

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**.
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".

Perintah pra/pasca

Opsi ini mirip dengan opsi pencadangan "Perintah pra/pasca".

Layanan Volume Shadow Copy VSS untuk mesin virtual

Opsi ini mirip dengan opsi pencadangan "Layanan Volume Shadow Copy 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.
   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.

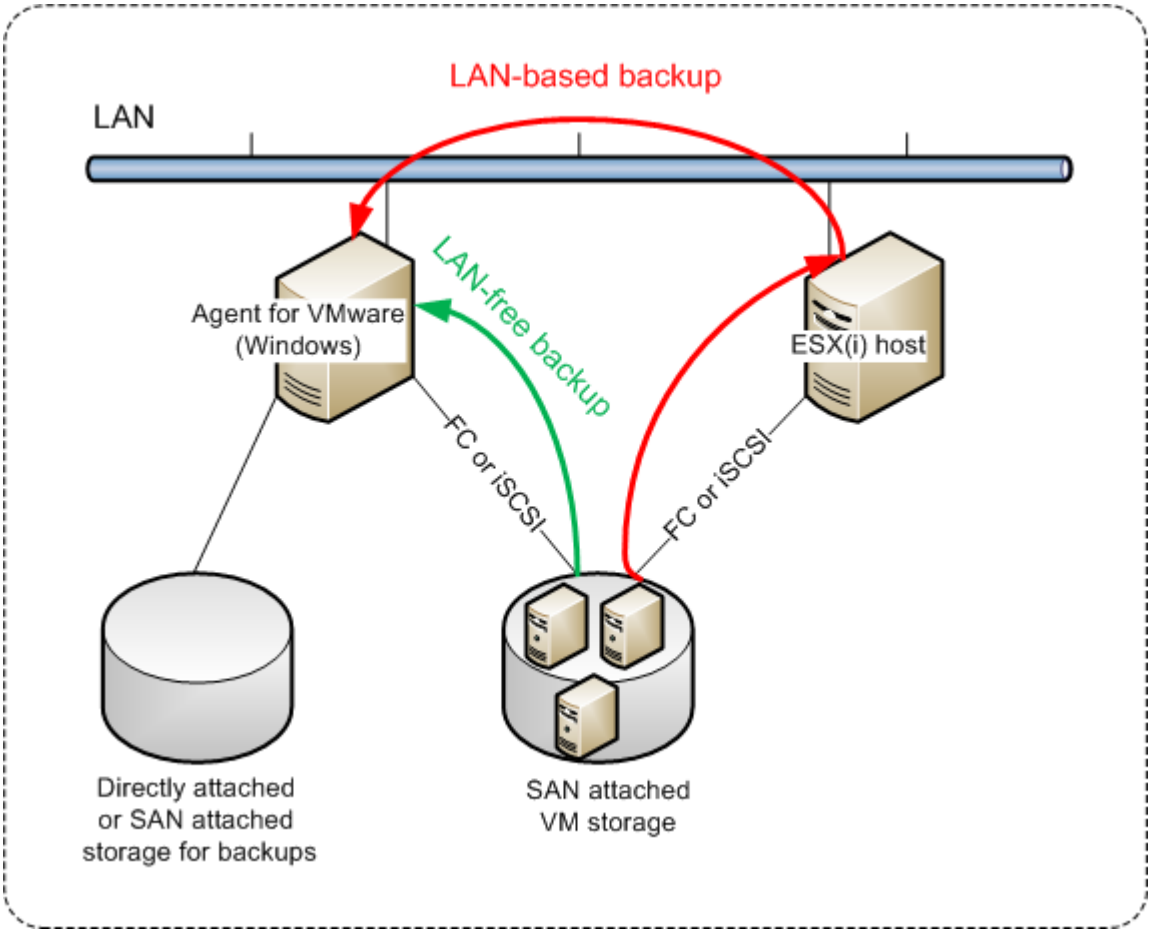
Hasilnya, perangkat lunak akan melanjutkan memperbarui replika. Semua replikasi akan bertambah secara bertahap.

Pencadangan bebas LAN

Jika host ESXi produksi Anda terlalu banyak muatan sehingga menjalankan alat virtual tidak diinginkan, pertimbangkan untuk menginstal Agen untuk VMware (Windows) pada mesin fisik di luar infrastruktur ESXi.

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.



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.

     Untuk menghindari inisialisasi LUN, **Kebijakan SAN** secara otomatis diatur ke **Offline Semua** selama instalasi Agen untuk VMware (Windows).

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 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.

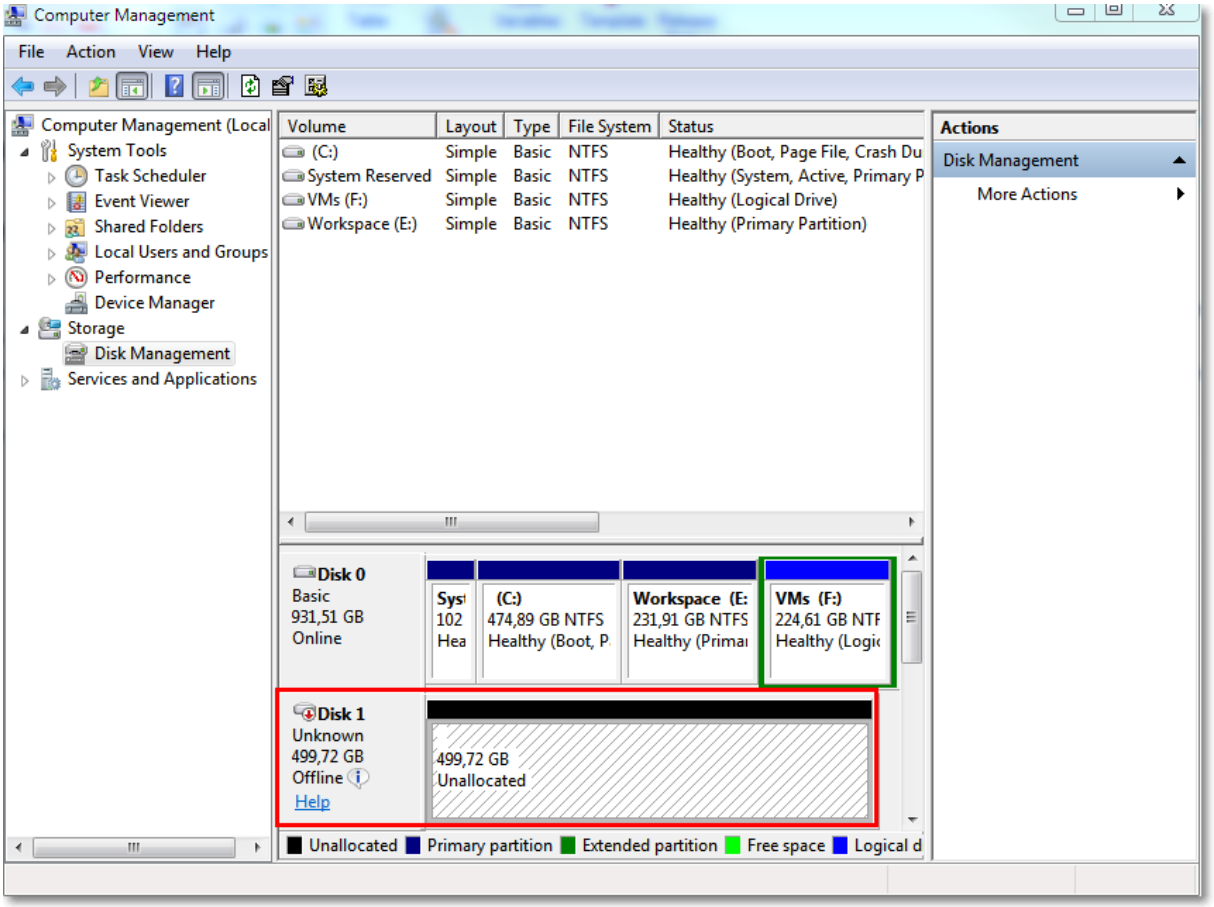
Untuk mengonfigurasi iSCSI initiator

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.



Menggunakan snapshot perangkat keras SAN

Jika VMware vSphere Anda menggunakan sistem penyimpanan jaringan area penyimpanan (SAN) sebagai penyimpanan data, Anda dapat mengaktifkan Agen untuk VMware (Windows) guna menggunakan snapshot perangkat keras SAN saat melakukan pencadangan.

Penting
Hanya mendukung penyimpanan NetApp SAN.

Mengapa perlu menggunakan snapshot perangkat keras SAN?

Agen untuk VMware memerlukan snapshot mesin virtual untuk membuat cadangan yang konsisten. Karena agen membaca konten disk virtual dari snapshot, snapshot harus disimpan selama seluruh proses backup.

Secara default, agen menggunakan snapshot VMware asli yang dibuat oleh host ESXi. Ketika snapshot disimpan, file disk virtual akan berada dalam status hanya-baca, dan host menulis semua perubahan yang dilakukan pada disk untuk memisahkan file delta. Setelah proses pencadangan selesai, host akan menghapus snapshot, yaitu menggabungkan file delta dengan file disk virtual.

Mempertahankan maupun menghapus snapshot dapat memengaruhi performa mesin virtual. Dengan disk virtual besar dan perubahan data yang cepat, operasi ini membutuhkan waktu yang lama selama performa dapat menurun. Dalam kasus yang ekstrem, ketika beberapa mesin didukung secara bersamaan, file delta yang bertambah hampir dapat memenuhi penyimpanan data dan menyebabkan semua mesin virtual mati.

Anda dapat mengurangi pemanfaatan sumber daya hypervisor dengan melepas snapshot ke SAN. Dalam kasus ini, urutan operasinya adalah sebagai berikut:

1. ESXi mengambil snapshot VMware di awal proses pencadangan, untuk membawa disk virtual ke status yang konsisten.
2. SAN membuat snapshot perangkat keras volume atau LUN yang berisi mesin virtual dan snapshot VMware-nya. Operasi ini biasanya memerlukan waktu beberapa detik.
3. ESXi menghapus snapshot VMware. Agen untuk VMware membaca konten disk virtual dari snapshot perangkat keras SAN.

Karena snapshot VMware hanya dipertahankan selama beberapa detik, penurunan performa mesin virtual diminimalkan.

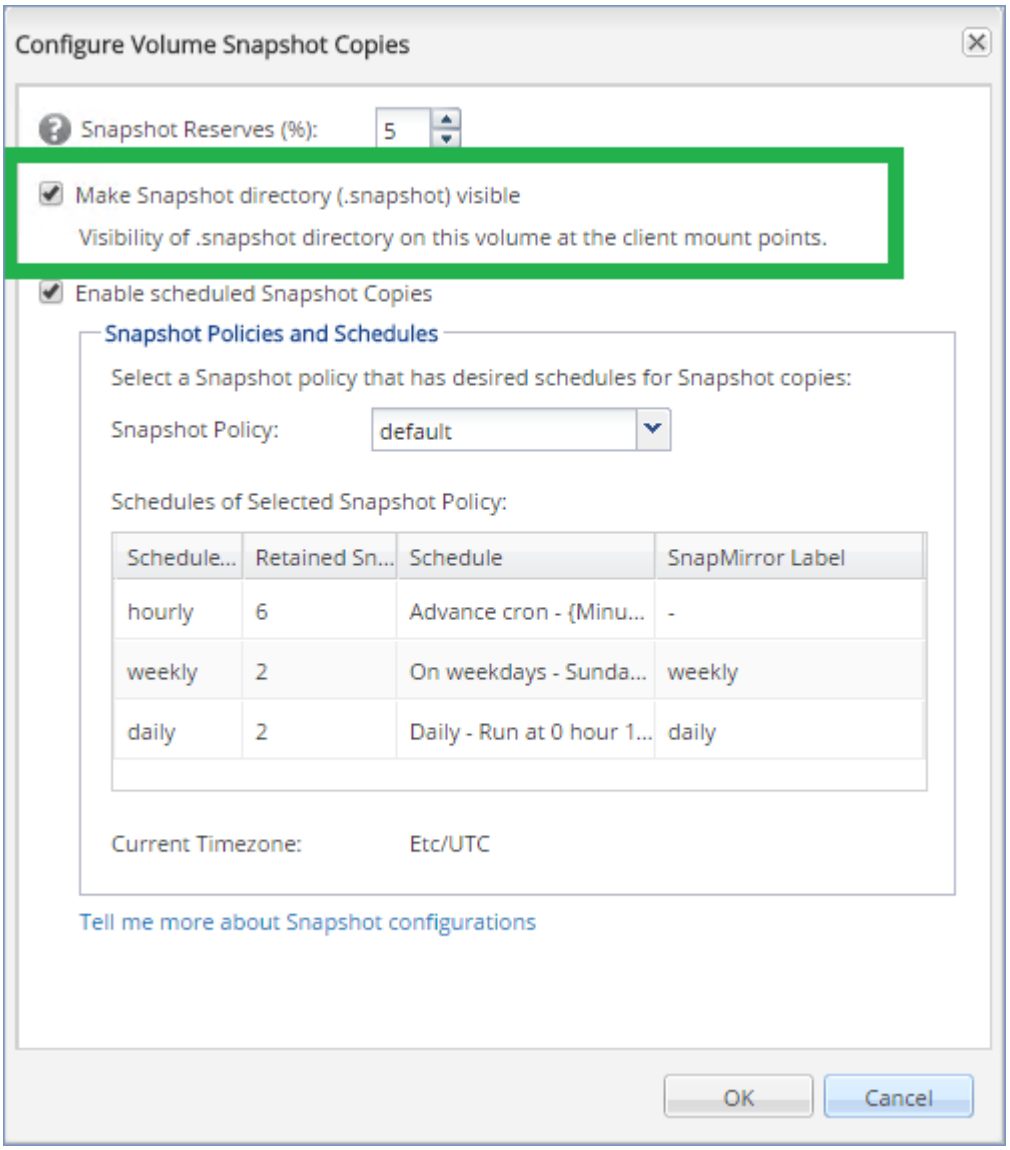
Apa yang saya perlukan untuk menggunakan snapshot perangkat keras SAN?

Jika Anda ingin menggunakan snapshot perangkat keras SAN saat mencadangkan mesin virtual, pastikan semua hal berikut benar:

- Penyimpanan NetApp SAN memenuhi persyaratan yang dijelaskan dalam "Persyaratan penyimpanan NetApp SAN".
- Mesin yang menjalankan Agen untuk VMware (Windows) dikonfigurasi seperti yang dijelaskan dalam "Mengonfigurasi mesin yang menjalankan Agen untuk VMware".
- Penyimpanan SAN terdaftar di server manajemen.
- [Jika ada Agen untuk VMware yang tidak ikut serta dalam pendaftaran di atas] Mesin virtual yang berada di penyimpanan SAN akan ditetapkan ke agen yang diaktifkan SAN, seperti dijelaskan dalam "Pengikatan mesin virtual".
- Opsi pencadangan "Snapshot perangkat keras SAN" diaktifkan dalam opsi rencana proteksi.

Persyaratan penyimpanan NetApp SAN

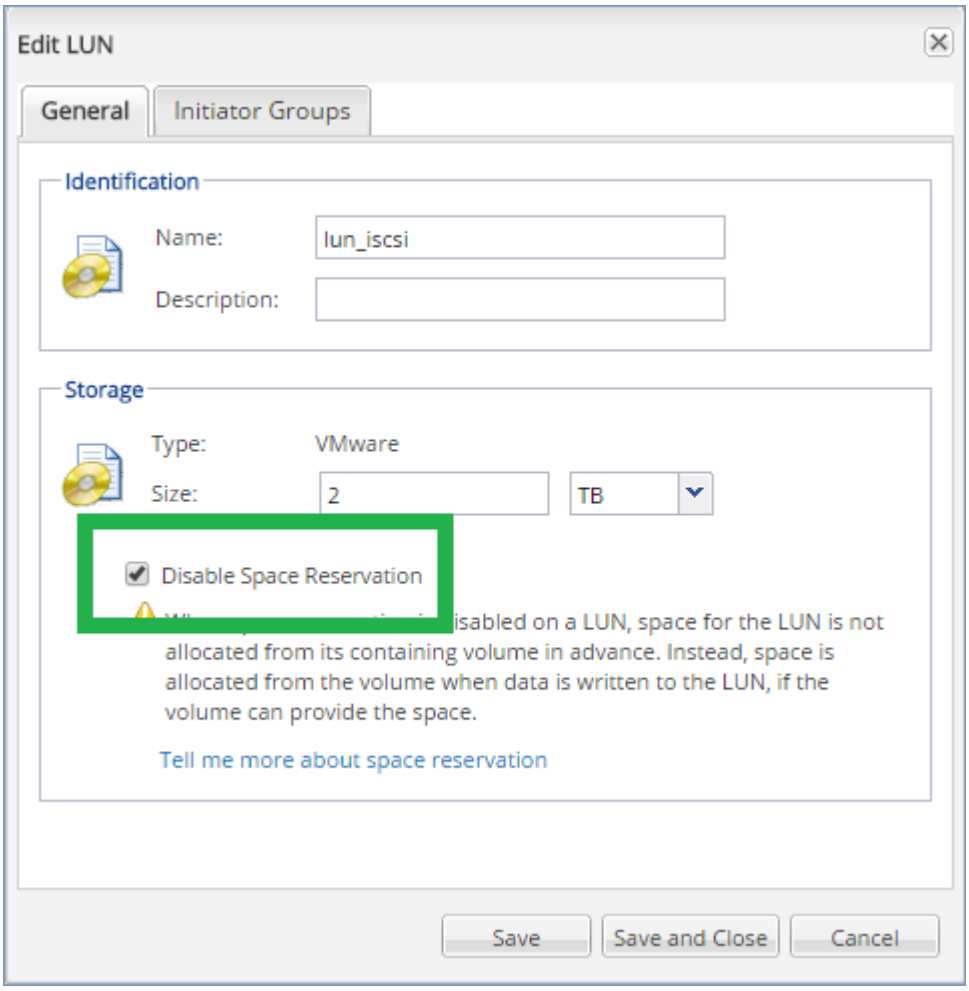
- Penyimpanan SAN harus digunakan sebagai penyimpanan data NFS atau iSCSI.
- SAN harus menjalankan Data ONTAP 8.1 atau yang lebih baru di mode **Clustered Data ONTAP (cDOT)**. Mode **7-mode** tidak didukung.
- Di NetApp OnCommand System Manager, kotak centang **Snapshot copies** > **Configure** > **Make Snapshot directory (.snapshot) visible** harus dipilih untuk volume tempat penyimpanan data berada.



- [Untuk penyimpanan data NFS] Akses ke NFS bersama dari klien Windows NFSv3 harus diaktifkan pada Storage Virtual Machine (SVM) yang ditentukan saat membuat penyimpanan data. Akses dapat diaktifkan dengan perintah berikut:

  ```
  vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
  ```

  Untuk informasi lebih lanjut, lihat dokumentasi Praktik Terbaik NetApp: https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices
- [Untuk penyimpanan data iSCSI] Di NetApp OnCommand System Manager, kotak centang **Disable Space Reservation** harus dipilih untuk LUN iSCSI tempat penyimpanan data berada.



Mengonfigurasi mesin yang menjalankan Agen untuk VMware

Tergantung apakah penyimpanan SAN digunakan sebagai penyimpanan data NFS atau iSCSI, lihat bagian terkait di bawah ini.

Mengonfigurasi iSCSI Initiator

Pastikan semua hal berikut ini benar:

- Microsoft iSCSI Initiator diinstal.
- Jenis startup Microsoft iSCSI Initiator Service diatur ke **Otomatis** atau **Manual**. Hal tersebut dapat dilakukan di snap-in **Layanan**.
- iSCSI initiator dikonfigurasikan seperti yang dijelaskan pada bagian contoh "Pencadangan bebas LAN".

Mengonfigurasi Klien NFS

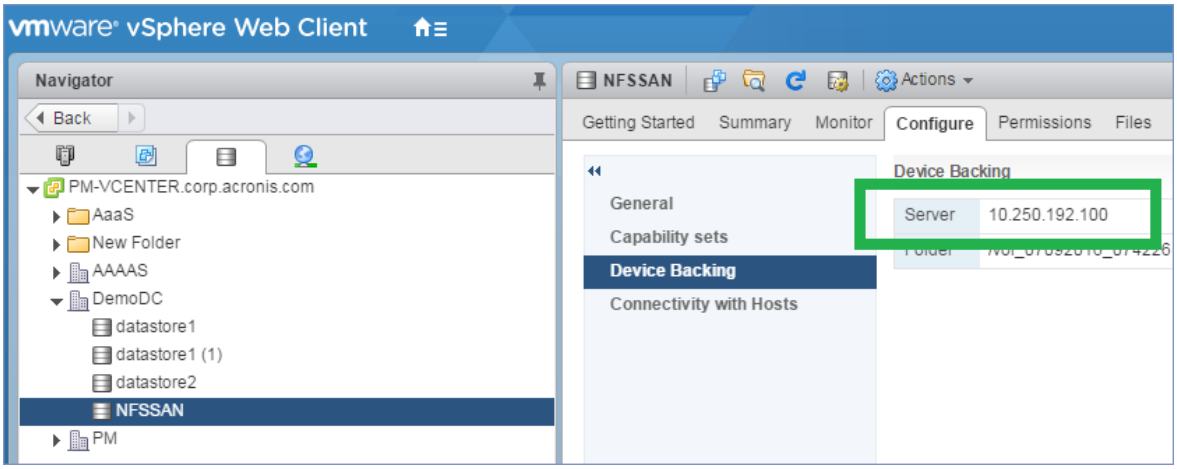
Pastikan semua hal berikut ini benar:

- Microsoft **Services for NFS** (di Windows Server 2008) atau **Client for NFS** (di Windows Server 2012 ke atas) diinstal.

- Klien NFS dikonfigurasi untuk akses anonim. Hal tersebut dapat dilakukan dengan langkah berikut:
  a. Buka Registry Editor.
  b. Temukan kunci registri berikut: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default**
  c. Dalam kunci ini, buat nilai **DWORD** baru bernama **AnonymousUID** dan atur nilai data ke 0.
  d. Dalam kunci yang sama, buat nilai **DWORD** baru bernama **AnonymousGID** dan atur nilai data ke 0.
  e. Mulai ulang mesin.

Mendaftarkan penyimpanan SAN di server manajemen

1. Klik **Pengaturan** > **Penyimpanan SAN**.
2. Klik **Tambah penyimpanan**.
3. [Opsional] Pada **Nama**, ubah nama penyimpanan.
   Nama ini akan ditampilkan pada tab **penyimpanan SAN**.
4. Pada **Nama host atau alamat IP**, tentukan Mesin Virtual Penyimpanan NetApp (SVM, disebut juga filer) yang ditentukan saat membuat penyimpanan data.
   Untuk menemukan informasi yang diperlukan di VMware vSphere Web Client, pilih penyimpanan data, lalu klik **Konfigurasi** > **Dukungan perangkat**. Nama host atau alamat IP ditampilkan di bidang **Server**.



5. Pada **Nama pengguna** dan **Kata sandi**, tentukan kredensial administrator SVM.

Penting
Akun yang ditentukan harus merupakan administrator lokal di SVM, bukan administrator manajemen sistem NetApp.

Anda dapat menentukan pengguna yang sudah ada atau membuat yang baru. Untuk membuat pengguna baru, di NetApp OnCommand System Manager, navigasikan ke **Konfigurasi** > **Keamanan** > **Pengguna**, lalu buat pengguna baru.

6. Pilih satu atau beberapa Agen untuk VMware (Windows) yang akan diberikan izin baca untuk perangkat SAN.
7. Klik **Tambah**.

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.

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 **Refresh**.
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:**.

Pengikatan mesin virtual

Bagian ini memberi Anda gambaran tentang bagaimana server manajemen 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.

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, server manajemen akan meredistribusikan mesin menggunakan algoritma yang sama.

Misalnya, Anda menyadari bahwa Anda membutuhkan lebih banyak agen untuk membantu dengan throughput dan 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 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

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.
- Pengikatan manual diperlukan jika Anda menggunakan snapshot perangkat keras SAN. Lakukan pengikatan Agen untuk VMware (Windows) yang untuknya snapshot perangkat keras SAN dikonfigurasikan dengan mesin yang berada di penyimpanan data SAN.
- 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.

Dukungan untuk migrasi VM

Bagian ini menginformasikan kepada Anda tentang hal-hal yang diharapkan jika mesin virtual bermigrasi dalam lingkungan vSphere, termasuk migrasi antara host ESXi yang merupakan bagian dari klaster vSphere.

vMotion

vMotion memindahkan status mesin virtual dan konfigurasinya ke host lain selama disk mesin tetap di lokasi yang sama di penyimpanan yang dibagi.

- vMotion Agen untuk VMware (Alat Virtual) tidak didukung.
- vMotion mesin virtual dinonaktifkan selama pencadangan. Pencadangan akan berlanjut setelah migrasi selesai.

VMotion penyimpanan

vMotion penyimpanan memindahkan disk mesin virtual dari satu datastore ke yang lainnya.

- vMotion penyimpanan Agen untuk VMware (Alat Virtual) tidak didukung dan dinonaktifkan.
- vMotion penyimpanan mesin virtual dinonaktifkan selama pencadangan. Pencadangan akan berlanjut setelah migrasi.

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

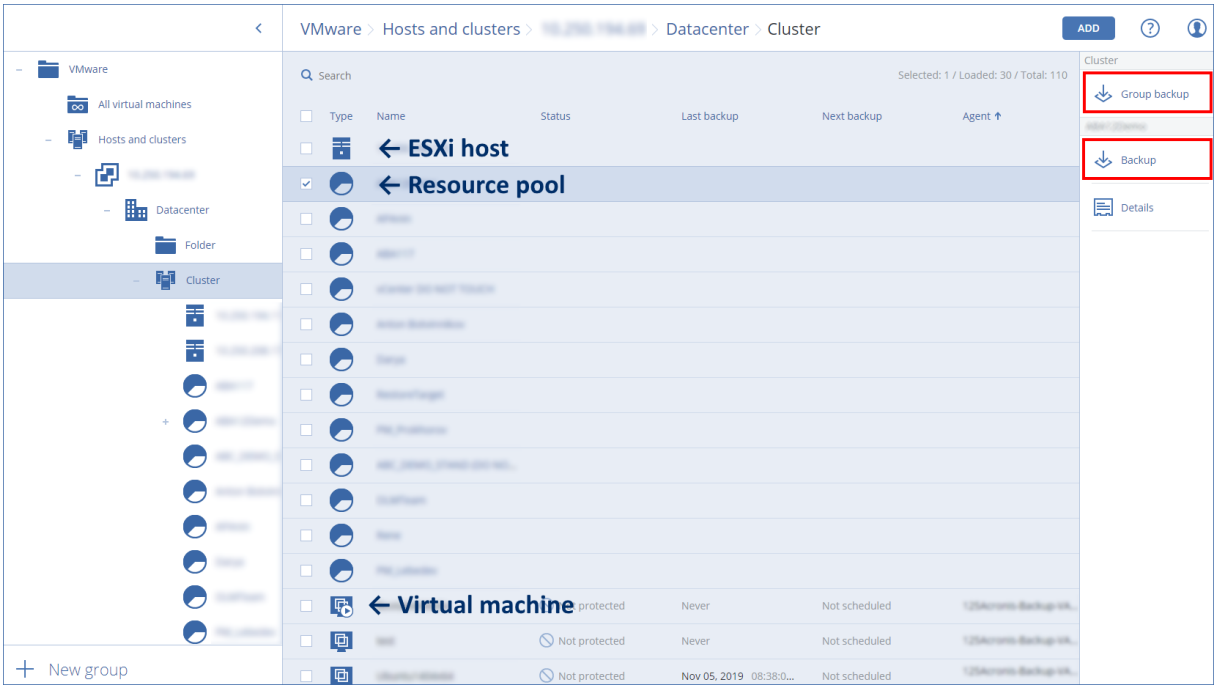
pada **Perangkat**.

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 mengeklik **Cadangkan**, atau mesin grup induk di mana grup yang dipilih termasuk dengan mengeklik **Pencadangan grup**.

Misalnya, Anda telah memilih klaster dan kemudian memilih kumpulan sumber daya di dalamnya. Jika Anda mengeklik **Cadangkan**, semua mesin virtual yang termasuk dalam kumpulan sumber daya terpilih akan dicadangkan. Jika Anda mengeklik **Pencadangan grup**, semua mesin virtual yang termasuk di dalam klaster akan dicadangkan.



Anda dapat mengubah kredensial akses untuk Server vCenter 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**

Agen untuk VMware – hak istimewa yang diperlukan

Bagian ini menjelaskan tentang privilese yang diperlukan untuk operasi dengan mesin virtual ESXi dan, untuk penyebaran alat virtual.

Catatan
API vStorage harus diinstal pada host ESXi untuk mengaktifkan cadangan mesin virtual. Lihat https://kb.acronis.com/content/14931.

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.

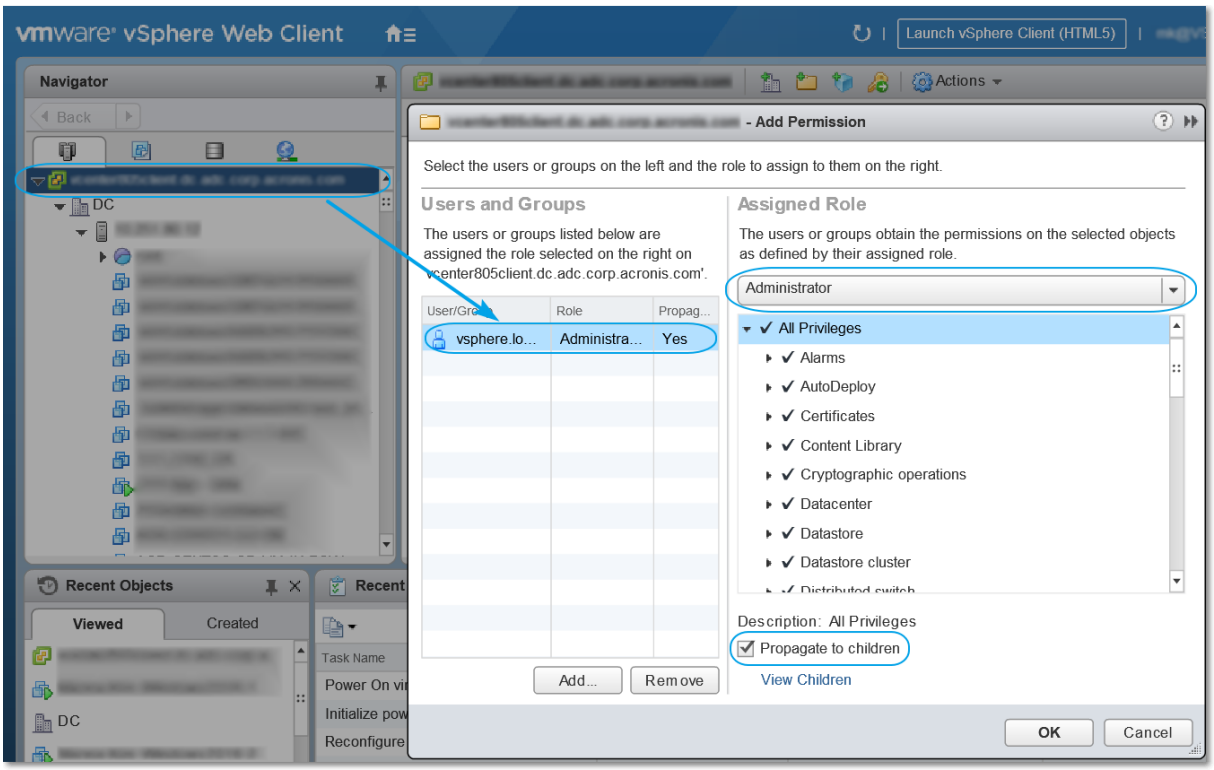
Tentukan akun vSphere dengan privilese yang diperlukan selama instalasi atau konfigurasi Agen untuk VMware. Jika Anda perlu mengubah akun di lain waktu, lihat bagian "Mengelola lingkungan virtualisasi".

Untuk menetapkan izin kepada pengguna vSphere di tingkat vCenter, lakukan hal berikut:

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**	**Penyebaran VA**
Operasi kriptografis (mulai dengan vSphere 6.5)	**Tambah disk**	+*				
	Akses Langsung	+*				
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 autostart VM**					+
	Konfigurasi partisi penyimpanan				+	
Host > **Inventori**	**Ubah klaster**					+
Host > **Operasi lokal**	**Buat VM**				+	+
	Hapus VM				+	+
	Konfigurasi ulang VM				+	+
Jaringan	**Tetapkan jaringan**		+	+	+	+
Sumber daya	**Tetapkan VM ke pool sumber daya**		+	+	+	+
	Impor					+
Mesin Virtual > **Konfigurasi**	**Tambah disk yang ada**	+	+		+	
	Tambah disk baru		+	+	+	+
	Tambah atau		+		+	+

	hapus perangkat					
	Tingkat lanjut	+	+	+		+
	Ubah jumlah CPU		+			
	Pelacakan perubahan disk	+		+		
	Sewa disk	+		+		
	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		+	+		
	Interaksi konsol					+
	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		+	+	+	+
	Pindah					+
	Daftar				+	
	Hapus		+	+	+	+
	Batalkan pendaftaran				+	
Mesin virtual > **Provisi**	**Izinkan akses ke disk**		+	+	+	
	Izinkan akses disk hanya-baca	+		+		
	Izinkan unduhan mesin virtual	+	+	+	+	
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. Mendaftarkan semua agen di server manajemen.

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 yang dicadangkan ke mesin virtual Hyper-V *baru*, atau melakukan konversi pada mesin virtual Hyper-V dalam rencana proteksi, 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

Opsi pencadangan **Penjadwalan** menetapkan berapa banyak mesin virtual yang dapat dicadangkan agen secara bersamaan saat mengeksekusi rencana proteksi tertentu.

Jika beberapa rencana proteksi tumpang tindih di saat bersamaan, jumlah yang ditentukan dalam opsi pencadangan akan ditambah. Meskipun jumlah total yang dihasilkan secara terprogram terbatas hingga 10, rencana yang tumpang tindih dapat memengaruhi performa pencadangan dan membebani host serta penyimpanan mesin virtual.

Anda selanjutnya dapat mengurangi jumlah total mesin virtual yang dapat dicadangkan oleh Agen untuk VMware atau Agen untuk Hyper-V secara bersamaan.

Untuk membatasi jumlah total mesin virtual yang dapat dicadangkan oleh Agen untuk VMware (Windows) atau Agen untuk Hyper-V

1. Pada mesin yang menjalankan agen, 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\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. Lakukan langkah berikut untuk memulai kembali agen:
   a. Pada menu **Start**, klik **Run**, lalu ketik: **cmd**
   b. Klik **OK**.
   c. Jalankan perintah berikut:

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

Untuk membatasi jumlah total mesin virtual yang dapat dicadangkan oleh Agen untuk VMware (Virtual Appliance) atau Agen untuk VMware (Linux)

1. Pada mesin yang menjalankan agen, mulai command shell:
   - **Agen untuk VMware (Peralatan Virtual):** tekan CTRL+SHIFT+F2 saat berada di UI alat virtual.
   - **Agen untuk VMware (Linux):** masuk sebagai pengguna root ke mesin yang menjalankan alat Acronis Cyber Protect. Kata sandi sama dengan yang dipakai untuk konsol web Cyber Protect.
2. Buka file **/etc/Acronis/MMS.config** pada editor teks, seperti **vi**.
3. Temukan bagian berikut:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Ganti `10` dengan nilai desimal dari batas yang ingin Anda tetapkan.
5. Simpan file.
6. Mulai ulang agen:
   - **Agen untuk VMware (Alat Virtual):** jalankan perintah `boot ulang`.
   - **Agen untuk VMware (Linux):** eksekusi perintah berikut:

```
sudo service acronis_mms restart
```

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	Mesin virtual Virtuozzo*	Kontainer Virtuozzo*	Mesin Virtual Virtuozzo Hybrid Infrastructure*	Mesin virtual Scale Computing HC3	Mesin virtual RHV/oVirt*
Mesin fisik	+	+	+	-	-	+	+	+
Mesin virtual VMware ESXi	+	+	+	-	-	+	+	+
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*	+	+	+	-	-	+	+	+

* Hanya tersedia dengan penyebaran awan.

Untuk petunjuk cara melakukan migrasi, lihat bagian berikut:

- Fisik-ke-virtual (P2V) – "Memulihkan mesin fisik ke mesin virtual" (hlm. 309)
- Virtual-ke-virtual (V2V) – "Memulihkan mesin virtual" (hlm. 311)
- Virtual-ke-fisik (V2P) – "Memulihkan mesin virtual" (hlm. 311) atau "Memulihkan disk dan volume dengan menggunakan media yang dapat di-boot" (hlm. 315)

Meskipun dimungkinkan untuk melakukan migrasi V2P di antarmuka web, kami menyarankan untuk menggunakan media yang dapat di-boot dalam kasus spesifik. Terkadang, Anda mungkin ingin menggunakan media untuk migrasi ke ESXi atau Hyper-V.

Media memungkinkan Anda untuk melakukan hal berikut:

- Lakukan migrasi P2V dan V2P dari mesin Linux yang berisi volume logis (LVM). Gunakan Agen untuk Linux atau media yang dapat di-boot untuk mencadangkan dan media yang dapat di-boot untuk memulihkan.
- Menyediakan driver untuk perangkat keras spesifik yang sangat penting untuk bootabilitas sistem.

Mesin virtual Windows Azure dan Amazon EC2

Untuk mencadangkan mesin virtual Windows Azure atau Amazon EC2, instal agen perlindungan pada mesin. Operasi pencadangan dan pemulihan sama dengan mesin fisik. Meskipun demikian, mesin dianggap sebagai virtual ketika Anda menetapkan kuota untuk jumlah mesin dalam penyebaran awan.

Perbedaan dari mesin fisik adalah bahwa mesin virtual Windows Azure dan Amazon EC2 tidak dapat di-boot dari media yang dapat di-boot. Jika Anda perlu memulihkan ke mesin virtual Windows Azure atau Amazon EC2 baru, ikuti prosedur di bawah ini.

Untuk memulihkan mesin sebagai mesin virtual Windows Azure atau Amazon EC2

1. Buat mesin virtual baru dari gambar/templat di Windows 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.

Persyaratan jaringan

Agen yang diinstal pada mesin yang dicadangkan harus dapat berkomunikasi dengan server manajemen melalui jaringan.

Penyebaran di lokasi

- Jika agen dan server manajemen diinstal di awan Azure/EC2, semua mesin sudah berada di jaringan yang sama. Tidak diperlukan tindakan tambahan.
- Jika server manajemen berada di luar awan Azure/EC2, mesin di awan tidak akan memiliki akses jaringan ke jaringan lokal tempat server manajemen diinstal. Agar agen yang diinstal pada mesin tersebut dapat berkomunikasi dengan server manajemen, koneksi jaringan privat virtual (VPN) antara jaringan lokal (lokal) dan awan (Azure/EC2) harus dibuat. Untuk instruksi tentang cara membuat koneksi VPN, lihat artikel berikut:

Amazon EC2: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

Windows Azure: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

Penyebaran awan

Pada penyebaran awan, server manajemen berada di salah satu pusat data Acronis dan oleh karenanya dapat dijangkau oleh agen. Tidak diperlukan tindakan tambahan.

Perlindungan SAP HANA

Perlindungan SAP HANA dijelaskan dalam dokumen terpisah yang tersedia di https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_SAP_HANA_whitepaper_en-US.pdf.

Perlindungan antimalware dan perlindungan web

Perlindungan antimalware dalam Cyber Protect memberi Anda manfaat berikut:

- Perlindungan teratas di semua tahap: proaktif, aktif, dan reaktif.
- Empat teknologi antimalware dalam sistem untuk memberikan perlindungan multilapisan terbaik di kelasnya.
- Pengelolaan Microsoft Security Essentials dan Windows Defender Antivirus.

Perlindungan Antivirus & Antimalware

Modul perlindungan Antivirus dan Antimalware memungkinkan Anda untuk melindungi mesin Windows dan macOS dari semua ancaman malware terbaru. Perhatikan bahwa fungsi Active Protection yang merupakan bagian dari proteksi antimalware tidak didukung di mesin macOS. Lihat daftar lengkap tentang fitur antimalware yang didukung: Fitur yang didukung oleh sistem operasi.

Acronis Cyber Protect didukung dan terdaftar di Pusat Keamanan Windows.

Jika mesin Anda sudah dilindungi dengan antivirus pihak ketiga saat menerapkan modul perlindungan Antivirus dan Antimalware pada mesin, sistem akan menghasilkan peringatan dan akan menghentikan perlindungan waktu nyata untuk mencegah potensi masalah kompatibilitas dan performa. Anda harus menonaktifkan atau menghapus instalasi antivirus pihak ketiga untuk mengaktifkan perlindungan Antivirus dan Antimalware Acronis Cyber Protect yang berfungsi penuh.

Kemampuan antimalware berikut tersedia untuk Anda:

- Deteksi malware dalam file pada mode perlindungan waktu nyata dan sesuai permintaan (untuk Windows, macOS)
- Deteksi perilaku berbahaya ketika proses (untuk Windows)
- Memblokir akses ke URL berbahaya (untuk Windows)
- Memindahkan file berbahaya ke karantina
- Menambahkan aplikasi korporat tepercaya ke daftar putih

Modul perlindungan Antivirus dan Antimalware memberi Anda dua tipe pemindaian:

- Pemindaian perlindungan waktu nyata
- Pemindaian malware sesuai permintaan

Pemindaian perlindungan waktu nyata

Perlindungan waktu nyata memeriksa semua file yang sedang dieksekusi atau dibuka pada mesin untuk mencegah ancaman malware.

Anda dapat memilih salah satu dari tipe pemindaian berikut:

- Deteksi saat akses 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.
- Deteksi dalam eksekusi 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 malware sesuai permintaan

Pemindaian antimalware dilakukan sesuai jadwal.

Anda dapat memantau hasil pemindaian antimalware di widget **Dasbor** > **Ikhtisar** > Terdampak baru-baru ini.

Pengaturan perlindungan Antivirus & Antimalware

Untuk mempelajari cara membuat rencana proteksi dengan modul perlindungan Antivirus & Antimalware, lihat "Membuat rencana proteksi".

Pengaturan berikut dapat ditetapkan untuk modul perlindungan Antivirus & Antimalware.

Active Protection

Active Protection melindungi sistem dari ransomware dan malware penggalian cryptocurrency. Ransomware mengenkripsi file dan meminta tebusan agar pemilik file mendapatkan kunci enkripsi. Malware Cryptomining melakukan perhitungan matematika di latar belakang, sehingga dapat mencuri daya pemrosesan dan lalu lintas jaringan.

Dalam edisi Cyber Backup pada Acronis Cyber Protect, 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. Dalam edisi Protect pada Acronis Cyber Protect, Active Protection adalah bagian dari modul proteksi Antivirus & Antimalware.

Active Protection tersedia untuk mesin yang menjalankan sistem operasi berikut:

- Sistem operasi desktop: Windows 7 Service Pack 1 dan versi setelahnya
  Pada mesin yang berjalan dengan Windows 7, pastikan bahwa Pembaruan untuk Windows 7 (KB2533623) sudah diinstal.
- Sistem operasi server: Windows Server 2008 R2 dan versi lebih baru.

Agen untuk Windows harus diinstal pada mesin.

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, jika ditentukan oleh konfigurasi.

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 default: **Aktif**.

Pengaturan Active Protection

Pada **Tindakan saat deteksi**, pilih tindakan yang akan dilakukan perangkat lunak saat mendeteksi aktivitas ransomware, lalu klik **Selesai**.

Anda dapat memilih salah satu dari tindakan berikut:

- **Hanya beri tahu**
  Perangkat lunak akan mengeluarkan peringatan tentang proses.
- **Hentikan proses**
  Perangkat lunak akan mengeluarkan peringatan dan menghentikan proses.
- **Kembalikan menggunakan cache**
  Perangkat lunak akan mengeluarkan peringatan, menghentikan proses, dan mengembalikan perubahan file menggunakan cache layanan.

Pengaturan default: **Kembalikan menggunakan cache**.

Perlindungan folder jaringan

Opsi **Lindungi folder jaringan yang dipetakan sebagai drive lokal** menentukan apakah perlindungan Antivirus & Antimalware melindungi dari folder jaringan proses berbahaya lokal yang dipetakan sebagai drive lokal.

Opsi 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 opsi ini. Folder default adalah **C:\ProgramData\Acronis\Restored Network Files**. 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**.

Perlindungan sisi server

Opsi ini menentukan apakah perlindungan Antivirus & Antimalware melindungi folder jaringan yang Anda bagikan dari koneksi masuk eksternal dari server lain dalam jaringan yang berpotensi membawa ancaman.

Pengaturan default: **Dinonaktifkan**.

Mengatur koneksi tepercaya dan koneksi yang diblokir

Pada tab **Tepercaya**, Anda dapat menentukan koneksi yang diperbolehkan untuk memodifikasi data apa pun. Anda harus menentukan nama pengguna dan alamat IP.

Pada tab **Diblokir**, Anda dapat menentukan koneksi yang tidak akan dapat memodifikasi data apa pun. Anda harus menentukan nama pengguna dan alamat IP.

Perlindungan diri

Perlindungan diri mencegah perubahan tidak sah pada proses perangkat lunak itu sendiri, catatan registri, file yang dapat dieksekusi dan konfigurasi, Secure Zone, serta cadangan yang terletak di folder lokal. Kami tidak merekomendasikan Anda untuk menonaktifkan fitur ini.

Pengaturan default: **Aktif**.

Memungkinkan proses untuk memodifikasi cadangan

Opsi **Izinkan proses tertentu untuk memodifikasi cadangan** berlaku saat **Perlindungan diri** diaktifkan.

Opsi ini berlaku untuk file yang memiliki ekstensi .tibx, .tib, .tia, dan yang berada di folder lokal.

Opsi ini memungkinkan Anda untuk menentukan proses yang diizinkan untuk memodifikasi file cadangan, meskipun file tersebut dilindungi oleh perlindungan diri. Opsi ini berguna, misalnya, jika Anda menghapus file cadangan atau memindahkannya ke lokasi lain menggunakan skrip.

Jika opsi 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 opsi 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**.

Deteksi proses cryptomining

Opsi ini menentukan apakah perlindungan Antivirus & Antimalware mendeteksi potensi malware cryptomining.

Malware Cryptomining menurunkan performa aplikasi yang berfungsi, menaikkan tagihan listrik, menyebabkan crash sistem, bahkan merusak perangkat keras karena penyalahgunaan. Kami menyarankan Anda untuk menambahkan malware cryptomining ke daftar proses **Berbahaya** untuk mencegahnya agar tidak berjalan.

Pengaturan default: **Aktif**.

Pengaturan deteksi proses cryptomining

Pilih tindakan yang akan dilakukan perangkat lunak saat aktivitas cryptomining terdeteksi, lalu klik **Selesai**. Anda dapat memilih salah satu dari tindakan berikut:

- **Hanya beri tahu**
  Perangkat lunak tersebut mengeluarkan peringatan tentang proses yang dicurigai sebagai aktivitas cryptomining.
- **Hentikan proses**
  Perangkat lunak ini mengeluarkan peringatan dan menghentikan proses yang dicurigai sebagai aktivitas cryptomining.

Pengaturan default: **Hentikan proses**.

Karantina

Karantina adalah folder untuk mengisolasi file yang mencurigakan (mungkin terinfeksi) atau berpotensi berbahaya.

Hapus file yang dikarantina setelah – Menentukan periode dalam hari yang setelahnya file yang dikarantina akan dihapus.

Pengaturan default: **30 hari**.

Deteksi perilaku

Acronis Cyber Protect melindungi sistem Anda dengan menggunakan heuristik perilaku untuk mengidentifikasi proses berbahaya: perangkat lunak ini membandingkan rangkaian tindakan yang dilakukan oleh proses dengan rangkaian tindakan yang terekam dalam database pola perilaku berbahaya. Dengan demikian, malware baru terdeteksi dari perilaku khasnya.

Pengaturan default: **Aktif**.

Pengaturan deteksi perilaku

Pada **Tindakan saat deteksi**, pilih tindakan yang akan dilakukan perangkat lunak saat mendeteksi aktivitas malware, lalu klik **Selesai**.

Anda dapat memilih salah satu dari tindakan berikut:

- **Hanya beri tahu**
  Perangkat lunak akan membuat peringatan tentang dugaan proses aktivitas malware.
- **Hentikan proses**

Perangkat lunak akan membuat peringatan dan menghentikan dugaan proses aktivitas malware.

- **Karantina**
  Perangkat lunak akan mengeluarkan peringatan, menghentikan proses, dan memindahkan file yang dapat dieksekusi ke folder karantina.

Pengaturan default: **Karantina**.

Perlindungan waktu nyata

Perlindungan waktu nyata secara terus-menerus memeriksa sistem mesin Anda dari virus dan ancaman lainnya selama sistem Anda dihidupkan.

Pengaturan default: **Aktif**.

Mengonfigurasi tindakan saat deteksi untuk perlindungan Waktu nyata

Pada **Tindakan saat deteksi**, pilih tindakan yang akan dilakukan perangkat lunak saat ancaman virus atau ancaman berbahaya lainnya terdeteksi, lalu klik **Selesai**.

Anda dapat memilih salah satu dari tindakan berikut:

- **Blokir dan beri tahu**
  Perangkat lunak memblokir proses tersebut dan mengeluarkan peringatan tentang proses yang dicurigai sebagai aktivitas malware.
- **Karantina**
  Perangkat lunak mengeluarkan peringatan, menghentikan proses, dan memindahkan file yang dapat dieksekusi ke folder karantina.

Pengaturan default: **Karantina**.

Mengonfigurasi mode pemindaian untuk perlindungan Waktu nyata

Pada **Mode pemindaian**, pilih tindakan yang akan dilakukan perangkat lunak saat ancaman virus atau ancaman berbahaya lainnya terdeteksi, lalu klik **Selesai**.

Anda dapat memilih salah satu dari tindakan berikut:

- **Smart on-access** – Memantau semua aktivitas sistem dan secara otomatis memindai file saat diakses untuk membaca atau menulis, atau setiap kali program diluncurkan.
- **Saat eksekusi** – Secara otomatis hanya memindai file yang dapat dieksekusi saat diluncurkan untuk memastikan bahwa file tersebut bersih dan tidak akan menyebabkan kerusakan apa pun pada komputer atau data Anda.

Pengaturan default: **Smart on-access**.

Jadwalkan pemindaian

Anda dapat menentukan jadwal sesuai dengan mesin Anda yang akan diperiksa terhadap malware, dengan mengaktifkan pengaturan **Jadwalkan pemindaian**.

Tindakan saat deteksi:

- **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.

Pengaturan default: **Karantina**.

Jenis pemindaian:

- **Penuh**
  Pemindaian penuh membutuhkan waktu lebih lama untuk selesai dibandingkan dengan pemindaian cepat karena setiap file akan diperiksa.
- **Cepat**
  Pemindaian cepat hanya memindai area umum tempat malware biasanya berada di mesin.
- **Kustom**
  Pemindaian kustom memeriksa file/folder yang dipilih oleh administrator untuk Rencana proteksi.

Anda dapat menjadwalkan ketiga pemindaian, yaitu pemindaian **Cepat**, **Penuh**, dan **Kustom** dalam satu rencana proteksi.

Pengaturan default:

- Pemindaian **Cepat** dan **Penuh** dijadwalkan.
- Pemindaian **Kustom** dinonaktifkan secara default.

Jadwalkan operasi tugas menggunakan peristiwa berikut:

- **Jadwalkan berdasarkan waktu** – Tugas akan dijalankan berasarkan 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.

Pengaturan default: **Jadwalkan berdasarkan waktu**.

Jenis jadwal:

- **Bulanan** – Pilih bulan dan minggu atau hari dalam sebulan saat tugas akan berjalan.
- **Harian** – Pilih hari dalam pekan saat tugas akan berjalan.
- **Per jam** – Pilih hari dalam pekan, jumlah pengulangan, dan interval waktu tugas akan berjalan.

Pengaturan default: **Harian**.

Mulai pada – Pilih waktu spesifik saat tugas akan berjalan.

Jalankan dalam rentang tanggal – Atur rentang saat jadwal yang dikonfigurasi akan berlaku.

Persyaratan awal – Tentukan semua persyaratan yang harus dipenuhi secara bersamaan agar tugas dapat berjalan.

Persyaratan awal untuk pemindaian antimalware mirip dengan persyaratan awal untuk modul Cadangan yang dijelaskan di "Persyaratan untuk memulai" (hlm. 238). 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 penundaan adalah 60 menit, maka tugas akan dimulai antara pukul 10.00 dan 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.

Pindai hanya file baru dan file yang diubah – Hanya file yang baru dibuat dan diubah yang akan dipindai.

Pengaturan default: **Aktif**.

Saat menjadwalkan **Pemindaian penuh**, Anda memiliki dua opsi tambahan:

- **Pindai file arsip**
  Pengaturan default: **Aktif**.
  - **Maks kedalaman rekursi**
    Berapa banyak tingkat arsip tersemat yang dapat dipindai. Misalnya, dokumen MIME > arsip ZIP > arsip Office > isi dokumen.
    Pengaturan default: **16**.
  - **Ukuran maks**
    Ukuran maksimum file arsip yang akan dipindai.
    Pengaturan default: **Tidak terbatas**.
- **Pindai drive yang dapat dilepas**
  Pengaturan default: **Dinonaktifkan**.

- **Drive jaringan yang dipetakan (jarak jauh)**
- **Perangkat penyimpanan USB** (seperti flash drive dan hard drive eksternal)
- **CD/DVD**

Pengecualian

Untuk meminimalkan sumber daya yang digunakan oleh analisis heuristik, dan untuk menghilangkan positif palsu ketika program yang dipercaya dianggap ransomware, Anda dapat menentukan pengaturan berikut:

Pada tab **Tepercaya**, Anda dapat menentukan:

- Proses yang tidak akan dianggap sebagai malware. Proses yang ditandai oleh Microsoft adalah selalu tepercaya.
- Folder tempat perubahan file tidak akan dipantau.
- File dan folder tempat pemindaian terjadwal tidak akan dilakukan.

Pada tab **Diblokir**, Anda dapat menentukan:

- Processes yang akan selalu diblokir. Proses ini tidak akan bisa dimulai selama Active Protection diaktifkan pada mesin.
- Folder tempat dilakukannya proses akan diblokir.

Tentukan jalur lengkap ke proses yang dapat dieksekusi, dimulai dengan huruf drive. Misalnya: `C:\Windows\Temp\er76s7sdkh.exe`.

Untuk menentukan folder, Anda dapat menggunakan karakter wildcard * dan ?. Tanda bintang (*) menggantikan nol atau lebih banyak karakter. Tanda tanya (?) menggantikan satu karakter. Variabel lingkungan, seperti `%AppData%`, tidak dapat digunakan.

Pengaturan default: Tidak ada pengecualian yang ditentukan secara default.

Pemfilteran URL

Harap lihat Pemfilteran URL untuk mengetahui penjelasan lengkapnya.

Active Protection

Dalam edisi Cyber Backup pada Acronis Cyber Protect, Active Protection adalah modul terpisah dalam rencana proteksi. Modul ini memiliki pengaturan berikut ini:

- Tindakan saat deteksi
- Perlindungan diri
- Perlindungan folder jaringan
- Perlindungan sisi server

- Deteksi proses cryptomining
- Pengecualian

Dalam edisi Protect pada Acronis Cyber Protect, Active Protection adalah bagian dari modul proteksi Antivirus & Antimalware.

Active Protection tersedia untuk mesin yang menjalankan sistem operasi berikut:

- Sistem operasi desktop: Windows 7 Service Pack 1 dan versi setelahnya
  Pada mesin yang berjalan dengan Windows 7, pastikan bahwa Pembaruan untuk Windows 7 (KB2533623) sudah diinstal.
- Sistem operasi server: Windows Server 2008 R2 dan versi lebih baru.

Agen untuk Windows harus diinstal pada mesin.

Untuk mempelajari lebih lanjut tentang Active Protection dan pengaturannya, lihat "Pengaturan perlindungan Antivirus & Antimalware" (hlm. 504).

Windows Defender Antivirus

Windows Defender Antivirus adalah komponen antimalware Microsoft Windows bawaan yang diberikan mulai dari Windows 8.

Modul Windows Defender Antivirus memungkinkan Anda untuk mengonfigurasi kebijakan keamanan Windows Defender Antivirus dan melacak statusnya melalui konsol web Cyber Protect.

Modul ini berlaku untuk mesin dengan Windows Defender Antivirus yang telah diinstal.

Jadwalkan pemindaian

Tetapkan jadwal untuk pemindaian terjadwal.

Mode pemindaian:

- **Penuh** – pemeriksaan menyeluruh semua file dan folder sebagai tambahan item yang dipindai dalam pemindaian cepat. Mode ini memerlukan lebih banyak sumber daya mesin dibandingkan dengan pemindaian cepat.
- **Cepat** – pemeriksaan cepat proses dan folder dalam memori di mana malware biasanya ditemukan. Mode ini memerlukan lebih sedikit sumber daya mesin.

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 jadwal Windows 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** – bersihkan malware yang terdeteksi di mesin.
- **Karantina** – masukkan malware yang terdeteksi ke folder karantina tapi tidak menghapusnya.
- **Hapus** – hapus malware yang terdeteksi dari mesin.
- **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 Windows Defender Antivirus, lihat https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings.

Perlindungan waktu nyata

Aktifkan **Perlindungan waktu nyata** untuk mendeteksi dan menghentikan malware menginstal atau berjalan pada mesin.

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 Windows 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** – termasuk arsip file 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 Windows Defender Antivirus tidak akan tersedia bagi pengguna. Anda dapat mengelola kebijakan Windows Defender Antivirus melalui konsol web 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.
  - **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 detail 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 Windows 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 Windows Defender Antivirus, lihat https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings.

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 untuk mengonfigurasi kebijakan keamanan Microsoft Security Essentials dan melacak statusnya melalui konsol web Cyber Protect.

Modul ini berlaku untuk mesin tempat Microsoft Security Essentials diinstal.

Pengaturan Microsoft Security Essentials hampir sama dengan Microsoft Windows Defender Antivirus kecuali tidak adanya pengaturan perlindungan real-time dan ketidakmampuan untuk menetapkan pengecualian melalui konsol web Cyber Protect.

Pemfilteran URL

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 memblokir akses 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 kebijakan akses untuk lebih dari 40 kategori situs web.

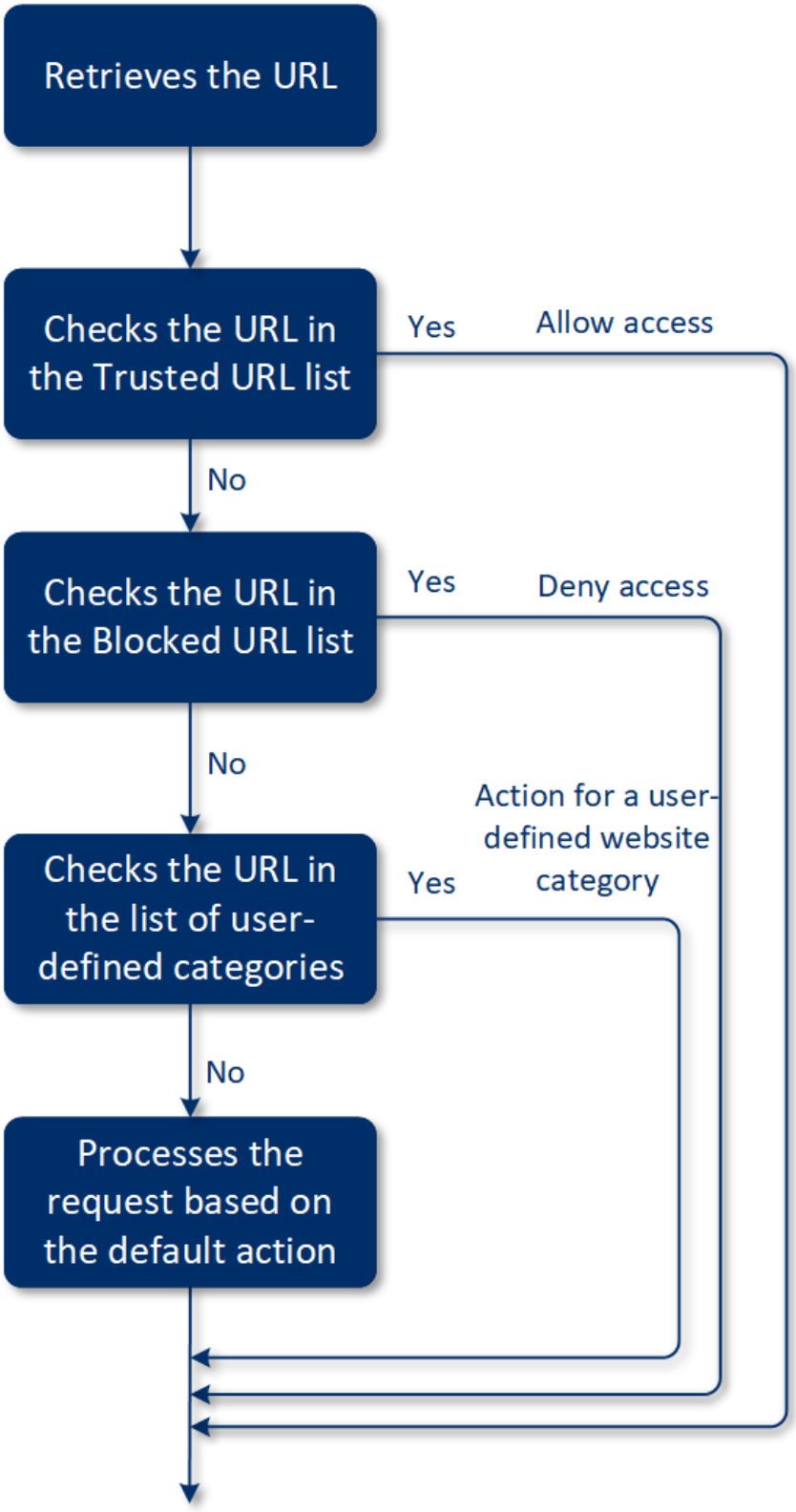
Saat ini, koneksi HTTP dan HTTPS dari mesin Windows diperiksa oleh agen perlindungan.

Fitur pemfilteran URL memerlukan koneksi internet agar dapat berfungsi.

Catatan
Konflik dapat terjadi jika pemfilteran URL digunakan secara paralel dengan solusi antivirus pihak ketiga yang juga menggunakan fitur pemfilteran URL. Anda dapat menentukan status solusi antivirus terinstal lainnya melalui Pusat Keamanan Windows.
Jika terjadi masalah kompatibilitas atau kinerja, hapus instalasi solusi pihak ketiga atau nonaktifkan modul pemfilteran URL dalam rencana proteksi Anda

Cara kerjanya

Pengguna mengikuti tautan atau memasukkan URL dalam bilah alamat di browser. Interceptor mendapatkan URL dan mengirimnya kepada agen perlindungan. Agen perlindungan menguraikan URL, memeriksa database, kemudian mengembalikan putusan kepada Interceptor. Jika URL dilarang, Interceptor memblokir akses ke URL dan memberi tahu pengguna bahwa konten ini tidak diizinkan untuk dilihat.



Untuk mengonfigurasi pemfilteran URL

1. Buat rencana proteksi dengan modul pemfilteran URL yang diaktifkan.
2. Konfigurasi pengaturan pemfilteran URL (lihat di bawah).

3. Tetapkan rencana proteksi pada mesin yang Anda inginkan.

Untuk memeriksa URL mana yang telah diblokir, buka **Dasbor** > **Peringatan**.

Pengaturan pemfilteran URL

Pengaturan berikut dapat dikonfigurasikan untuk modul pemfilteran URL.

Akses situs web berbahaya

Tentukan tindakan mana yang akan dilakukan saat pengguna mencoba membuka situs web berbahaya:

- **Blokir** – Akses ke situs web berbahaya akan diblokir dan peringatan akan dibuat.
- **Selalu tanya pengguna** – Pengguna akan diminta untuk memilih apakah akan melanjutkan ke situs web atau kembali.

Kategori yang akan difilter

Ada 44 kategori situs web kategori yang dapat Anda konfigurasi kebijakan aksesnya. Secara default, akses ke situs web dari semua kategori diizinkan.

	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 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 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.
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. Disarankan untuk 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 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. 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.

Jika Anda mengaktifkan kotak centang **Tampilkan semua pemberitahuan untuk URL yang diblokir berdasarkan kategori**, pemberitahuan untuk URL yang diblokir berdasarkan kategori akan ditampilkan di tray. Jika situs web memiliki beberapa subdomain, pemberitahuan juga akan dibuat, maka jumlahnya akan besar.

Pengecualian

URL yang diketahui aman dapat ditambahkan ke daftar URL tepercaya. URL yang merepresentasikan ancaman dapat ditambahkan ke daftar URL yang diblokir.

Untuk menambahkan URL ke daftar

1. Dalam modul pemfilteran URL dari rencana proteksi, klik **Pengecualian**.
2. Pilih daftar yang diinginkan: **Tepercaya** atau **Diblokir**.
3. Klik **Tambah**.
4. Tentukan URL atau alamat IP, kemudian klik tanda centang.

Contoh pengecualian URL:

- Jika Anda menambahkan xyz.com sebagai tepercaya/tidak tepercaya, semua alamat di domain xyz.com akan diperlakukan sebagai tepercaya atau tidak tepercaya tergantung di mana Anda ingin menambahkannya.
- Jika Anda ingin menambahkan subdomain tertentu, Anda dapat menambahkan **mail.xyz.com** sebagai tepercaya/tidak tepercaya, dan ini tidak akan menyebabkan semua alamat **xyz.com** dipercaya atau tidak dipercaya.
- Jika Anda ingin menambahkan IPv4 sebagai dipercaya/tidak dipercaya, format berikut harus digunakan agar valid: **20.53.203.50**.
- Jika Anda ingin menambahkan beberapa pengecualian URL sekaligus, pastikan untuk menambahkan setiap entri pada baris baru:

  acronis.com

  mail.xyz.com

  20.53.203.50

Karantina

Karantina adalah folder terisolasi khusus di hard disk mesin untuk menyimpan file mencurigakan yang terdeteksi oleh perlindungan Antivirus & 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.

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 Anti-malware** > **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.
- **Pulihkan** – memulihkan file yang dikarantina ke lokasi aslinya tanpa modifikasi apa pun. Jika saat ini terdapat file dengan nama yang sama di lokasi asli, file tersebut akan ditimpa dengan file yang dipulihkan.

Lokasi karantina di mesin

Lokasi default file yang dikarantina adalah:

Untuk mesin Windows: `%ProgramData%\%product_name%\Quarantine`

Untuk mesin Mac/Linux: `/usr/local/share/%product_name%/quarantine`

Daftar putih perusahaan

Penting
Daftar putih perusahaan mengharuskan Layanan Pemindaian diinstal ke server manajemen.

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.

Cyber Protect 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 dapat diaktifkan dan dinonaktifkan. Saat dinonaktifkan, file yang ditambahkan padanya akan disembunyikan untuk sementara.

Penambahan otomatis ke daftar putih

1. Jalankan pemindaian awan dari cadangan pada setidaknya dua mesin. Anda dapat melakukannya menggunakan "Rencana pemindaian cadangan" (hlm. 344).
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 web Cyber Protect, buka **Perlindungan Antimalware** > **Daftar yang Diizinkan**.
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 web 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 waktu dan pemeriksaan dalam jumlah yang signifikan. 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 ditambahkan ke daftar putih lebih cepat, 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.

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

Untuk mencegah pemulihan file yang terinfeksi dari cadangan, Anda dapat memindai cadangan untuk malware. Pemindaian cadangan hanya didukung untuk sistem operasi Windows. Pemindaian ini hanya tersedia jika Layanan Pemindaian diinstal di Server Manajemen Cyber Protect.

Untuk memindai cadangan dari malware, buat rencana pemindaian cadangan.

Catatan
Demi keamanan dan kinerja, sebaiknya Anda menggunakan mesin khusus untuk keperluan pemindaian. Mesin ini akan memiliki akses ke semua cadangan yang dipindai.

Anda dapat memeriksa hasil pemindaian di widget "Detail pemindaian cadangan" di Dasbor. Selain itu, Anda dapat melihat status cadangan di **Penyimpanan cadangan** > **Lokasi** > **<nama cadangan>**. Jika pemindaian cadangan tidak dilakukan, cadangan tersebut berstatus **Tidak dipindai**. Setelah pemindaian cadangan dilakukan, cadangan memiliki status yang diperbarui:

- **Tidak ada malware**
- **Malware terdeteksi**

Pembatasan

- Hanya cadangan jenis **Seluruh mesin** atau **Disk/volume** yang dapat dipindai untuk malware.
- Hanya volume dengan sistem file NTFS dengan partisi GPT dan MBR yang akan dipindai.
- Lokasi cadangan yang didukung adalah: **Penyimpanan awan**, **Folder lokal**, dan **Folder jaringan**.
- Cadangan dengan Titik pemulihan perlindungan data berkelanjutan (CDP) dapat dipilih untuk pemindaian, tetapi titik pemulihan ini akan dikecualikan dari pemindaian. Hanya titik pemulihan reguler yang akan dipindai.
- Jika cadangan CDP dipilih untuk pemulihan aman seluruh mesin, mesin akan dipulihkan dengan aman tanpa data di titik pemulihan CDP. Untuk memulihkan data CDP, jalankan pemulihan **File/folder**.

Perlindungan aplikasi kolaborasi dan komunikasi

Zoom, Cisco Webex Meetings, dan Microsoft Teams sekarang banyak digunakan untuk konferensi dan komunikasi video/web. Cyber Protect memungkinkan Anda melindungi alat bantu kolaborasi Anda.

Perlindungan untuk Zoom, Cisco Webex Meetings, 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 di mesin tempat aplikasi kolaborasi diinstal.
2. Masuk ke konsol web Cyber Protect dan terapkan rencana proteksi dengan 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

Penilaian kerentanan dan manajemen patch

Penilaian kerentanan (VA) adalah proses mengidentifikasi, mengukur, dan memprioritaskan kerentanan yang ditemukan dalam sistem. Dengan menggunakan modul penilaian Kerentanan dalam rencana proteksi, Anda dapat memindai mesin Anda untuk menemukan kerentanan, dan memeriksa apakah sistem operasi dan aplikasi yang diinstal sudah diperbarui dan berfungsi dengan benar.

Pemindaian penilaian kerentanan didukung untuk mesin yang menjalankan sistem operasi berikut:

- Windows. Untuk informasi lebih lanjut, lihat "Produk Microsoft dan produk pihak ketiga yang didukung" (hlm. 530).
- Mesin Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Untuk informasi lebih lanjut, lihat "Produk Linux yang didukung" (hlm. 531).

Gunakan fungsionalitas **Manajemen patch** (PM) untuk mengelola patch (pembaruan) untuk 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 penginstalan pembaruan di mesin Anda.

Manajemen patch didukung untuk mesin yang menjalankan Windows. Untuk informasi lebih lanjut, lihat "Produk Microsoft dan produk pihak ketiga yang didukung" (hlm. 530).

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.
3. Agen menerima 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 di widget penilaian kerentanan dan daftar kerentanan yang ditemukan.
6. Dengan menggunakan informasi ini, Anda dapat memutuskan kerentanan yang mana yang harus diperbaiki.

Anda dapat memantau hasil pemindaian penilaian kerentanan di widget **Dasbor** > **Ikhtisar** > **Kerentanan/Kerentanan yang ada**.

Produk Microsoft dan produk pihak ketiga yang didukung

Produk Microsoft dan produk pihak ketiga untuk sistem operasi Windows berikut didukung untuk penilaian kerentanan.

Produk Microsoft yang didukung

Sistem operasi desktop

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

Sistem operasi server

- 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

- Internet Explorer
- Microsoft Edge
- Windows Media Player
- .NET Framework
- Visual Studio dan Aplikasi
- Komponen sistem operasi

Aplikasi server

- 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 Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

Produk pihak ketiga yang didukung untuk Windows

Cyber Protect mendukung penilaian kerentanan dan patch untuk berbagai aplikasi pihak ketiga, termasuk alat bantu kolaborasi dan klien VPN, yang sangat penting dalam skenario kerja jarak jauh.

Untuk daftar lengkap tentang produk pihak ketiga untuk Windows, lihat https://kb.acronis.com/content/62853.

Produk Linux yang didukung

Distribusi dan versi Linux berikut ini didukung untuk penilaian kerentanan:

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10 (320)
- Virtuozzo 7.0.9 (539)
- Virtuozzo 7.0.8 (524)
- CentOS 7.x
- Cyber Infrastructure 3.x Acronis
- Penyimpanan 2.4.0 Acronis
- Penyimpanan 2.2.0 Acronis

Pengaturan penilaian kerentanan

Untuk mempelajari cara membuat rencana proteksi dengan modul penilaian Kerentanan, lihat "Membuat rencana proteksi" (hlm. 202). Anda dapat melakukan pemindaian penilaian kerentanan 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, lihat https://kb.acronis.com/content/62853.
- Mesin Linux:
  - **Pindai paket Linux**

Jadwal

Tetapkan jadwal untuk melakukan pemindaian penilaian kerentanan pada mesin yang dipilih:

Jadwalkan operasi tugas menggunakan peristiwa berikut:

- **Jadwalkan berdasarkan waktu** – Tugas akan dijalankan berasarkan 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.

Pengaturan default: **Jadwalkan berdasarkan waktu**.

Jenis jadwal:

- **Bulanan** – Pilih bulan dan minggu atau hari dalam sebulan saat tugas akan berjalan.
- **Harian** – Pilih hari dalam pekan saat tugas akan berjalan.
- **Per jam** – Pilih hari dalam pekan, jumlah pengulangan, dan interval waktu tugas akan berjalan.

Pengaturan default: **Harian**.

Mulai pada – Pilih waktu spesifik saat tugas akan berjalan.

Jalankan dalam rentang tanggal – Atur rentang saat jadwal yang dikonfigurasi akan berlaku.

Persyaratan awal – Tentukan semua persyaratan yang harus dipenuhi secara bersamaan agar tugas dapat berjalan.

Persyaratan awal untuk pemindaian antimalware mirip dengan persyaratan awal untuk modul Cadangan yang dijelaskan di "Persyaratan untuk memulai" (hlm. 238). 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 penundaan adalah 60 menit, maka tugas akan dimulai antara pukul 10.00 dan 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.

Penilaian kerentanan untuk mesin Windows

Anda dapat memindai mesin Windows dan produk pihak ketiga untuk Windows guna menemukan kerentanan.

1. Di konsol web Cyber Protect, buat rencana proteksi, lalu 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. 531).
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 **Dasbor** > **Gambaran Umum** > **Kerentanan/Kerentanan yang ada**.

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 web Cyber Protect, buat rencana proteksi, lalu 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. 531).

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 **Dasbor** > **Gambaran Umum** > **Kerentanan/Kerentanan yang ada**.

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 kerentanan, baik yang disarankan untuk patch, maupun yang tidak disarankan. Anda dapat menggunakan filter untuk menampilkan kerentanan dengan patch yang ada 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**
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 web Cyber Protect, buka **Manajemen perangkat lunak** > **Kerentanan**.
2. Pilih kerentanan di dalam daftar lalu klik **Instal patch**. Wizard perbaikan kerentanan akan terbuka.
3. Pilih patch untuk diinstal. Klik **Berikutnya**.
4. Pilih mesin yang ingin Anda instal dengan patch.
5. Pilih apakah Anda ingin boot ulang mesin setelah penginstalan patch:
   - **Tidak** – boot ulang tidak akan pernah dimulai setelah instalasi patch.
   - **Bila perlu** – boot ulang dilakukan hanya bila diperlukan untuk menerapkan pembaruan.
   - **Ya** – boot ulang akan selalu dimulai setelah instalasi patch. Akan tetapi, Anda dapat menentukan penundaan.

   Jangan boot ulang hingga pencadangan selesai – jika proses pencadangan sedang berlangsung, boot ulang mesin akan tertunda hingga pencadangan selesai.
6. Klik **Instal patch**.

Hasilnya, patch yang dipilih akan diinstal pada mesin yang dipilih.

Manajemen patch

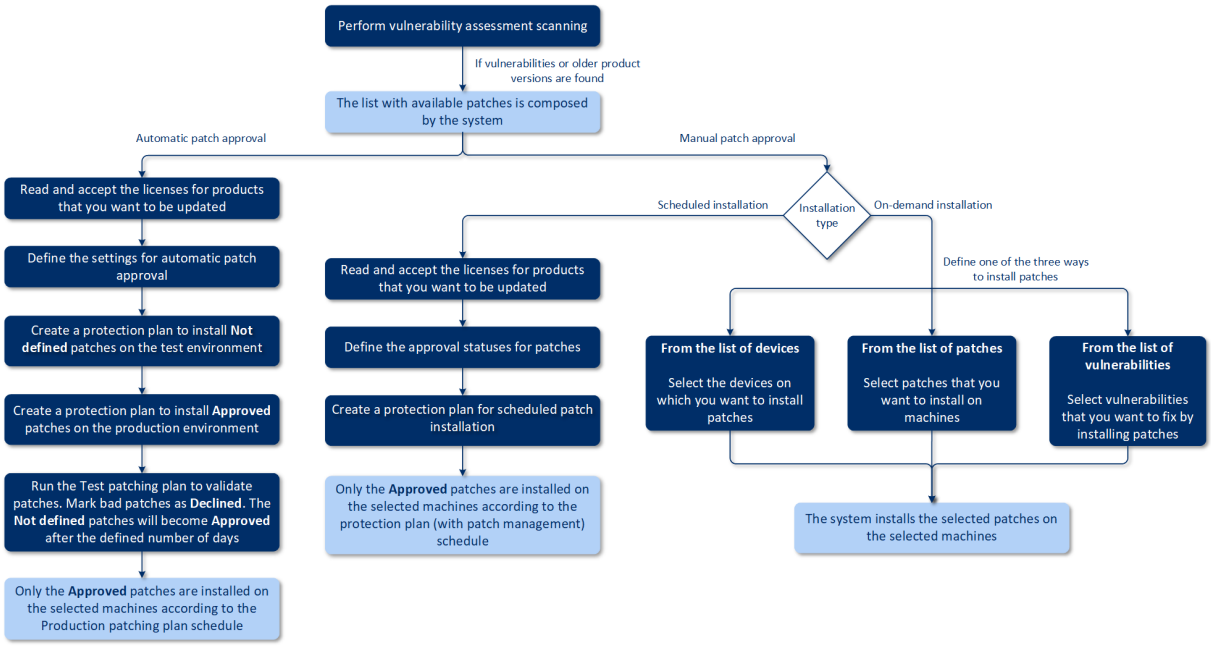
Gunakan fungsionalitas manajemen patch untuk:

- Menginstal pembaruan pada tingkat OS dan aplikasi
- Menyetujui patch secara manual atau otomatis
- Menginstal patch sesuai permintaan dan berdasarkan jadwal
- Menentukan secara akurat patch mana yang akan diterapkan berdasarkan berbagai kriteria: keparahan, kategori, dan status persetujuan
- Jalankan pencadangan pra-pembaruan guna mencegah kemungkinan pembaruan yang tidak berhasil
- Menentukan opsi boot ulang yang akan diterapkan setelah instalasi patch

Cyber Protect 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.

Cara kerjanya

Anda dapat mengonfigurasi persetujuan patch otomatis atau manual. Pada skema di bawah ini, Anda dapat melihat alur kerja persetujuan patch otomatis dan manual.



1. Pertama, Anda harus melakukan setidaknya satu pemindaian penilaian kerentanan menggunakan rencana proteksi dengan modul **Penilaian kerentanan** yang diaktifkan. Setelah pemindaian dilakukan, daftar kerentanan yang ditemukan dan patch yang tersedia dibuat oleh sistem.
2. Kemudian, Anda dapat mengonfigurasi persetujuan patch otomatis atau menggunakan pendekatan persetujuan patch manual.
3. Tetapkan cara menginstal patch – berdasarkan jadwal atau sesuai permintaan. Instalasi patch sesuai permintaan dapat dilakukan dalam tiga cara berdasarkan preferensi Anda:
   - Buka daftar patch (**Manajemen perangkat lunak** > **Patch**) dan instal patch yang diperlukan.
   - Buka daftar kerentanan (**Manajemen perangkat lunak** > **Kerentanan**) dan mulailah proses perbaikan yang juga termasuk instalasi patch.
   - Buka daftar perangkat (**Perangkat** > **Semua perangkat**), pilih mesin tertentu yang ingin Anda perbarui, dan instal patch pada mesin tersebut.

Anda dapat memantau hasil instalasi patch di widget **Dasbor** > **Ikhtisar** > **Riwayat instalasi patch**.

Pengaturan manajemen patch

Untuk mempelajari cara membuat rencana proteksi dengan modul manajemen Patch, lihat "Membuat rencana proteksi". Menggunakan rencana proteksi, Anda dapat menetapkan pembaruan untuk produk Microsoft dan produk pihak ketiga lainnya untuk Windows OS yang akan diinstal secara otomatis pada mesin yang ditentukan.

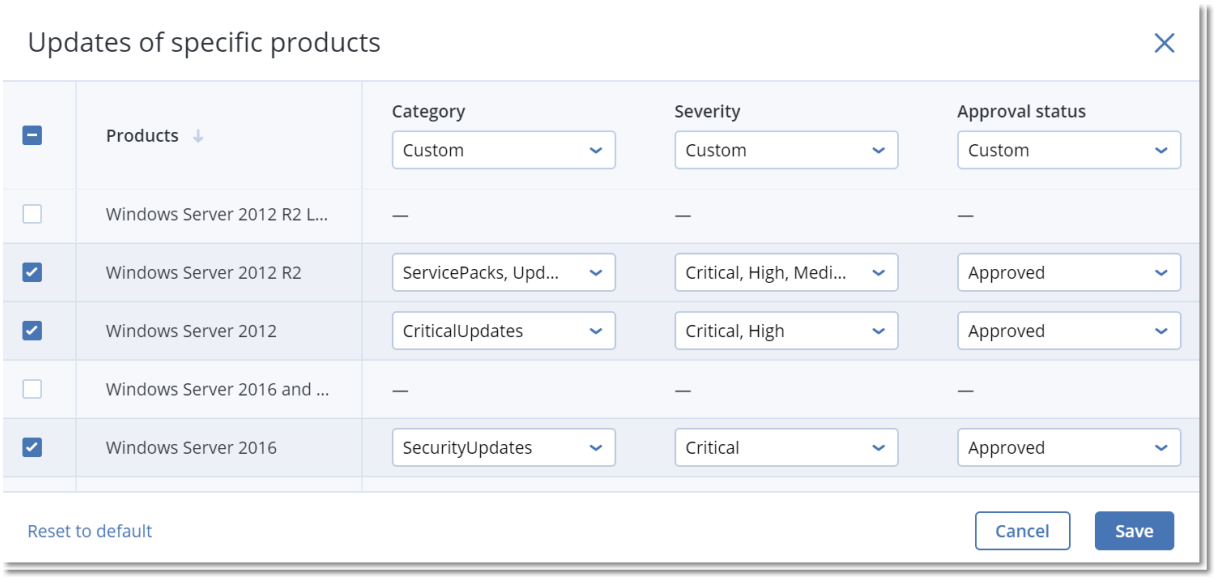
Pengaturan berikut dapat ditetapkan untuk modul manajemen Patch.

Produk Microsoft

Untuk menginstal pembaruan Microsoft di mesin yang dipilih, aktifkan opsi **Perbarui produk Microsoft**.

Pilih pembaruan mana yang ingin Anda instal:

- **Semua pembaruan**
- **Hanya pembaruan Penting dan Keamanan**
- **Pembaruan produk spesifik**: Anda dapat menetapkan pengaturan khusus untuk produk yang berbeda-beda. Jika Anda ingin memperbarui produk spesifik, Anda dapat menetapkan pembaruan mana yang akan diinstal untuk setiap produk berdasarkan kategori, keparahan, atau status persetujuan.

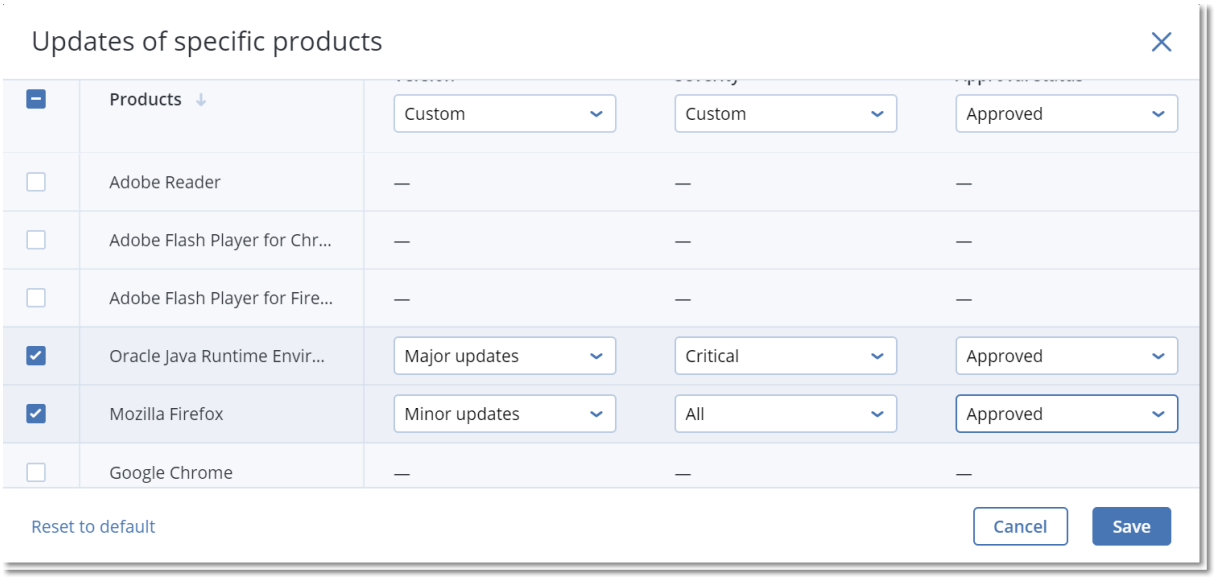


Produk pihak ketiga Windows

Untuk menginstal pembaruan pihak ketiga untuk Windows OS di mesin yang dipilih, aktifkan opsi **Produk pihak ketiga Windows**.

Pilih pembaruan mana yang ingin Anda instal:

- **Hanya pembaruan berat** yang memungkinkan Anda untuk menginstal versi pembaruan terakhir yang tersedia.
- **Hanya pembaruan ringan terakhir** yang memungkinkan Anda untuk menginstal versi ringan dari pembaruan.
- **Pembaruan produk spesifik**: Anda dapat menetapkan pengaturan khusus untuk produk yang berbeda-beda. Jika Anda ingin memperbarui produk spesifik, Anda dapat menetapkan pembaruan mana yang akan diinstal untuk setiap produk berdasarkan kategori, keparahan, atau status persetujuan.



Jadwal

Tetapkan jadwal untuk menginstal pembaruan pada mesin yang dipilih.

Jadwalkan operasi tugas menggunakan peristiwa berikut:

- **Jadwalkan berdasarkan waktu** – Tugas akan dijalankan berasarkan 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.

Pengaturan default: **Jadwalkan berdasarkan waktu**.

Jenis jadwal:

- **Bulanan** – Pilih bulan dan minggu atau hari dalam sebulan saat tugas akan berjalan.
- **Harian** – Pilih hari dalam pekan saat tugas akan berjalan.
- **Per jam** – Pilih hari dalam pekan, jumlah pengulangan, dan interval waktu tugas akan berjalan.

Pengaturan default: **Harian**.

Mulai pada – Pilih waktu spesifik saat tugas akan berjalan.

Jalankan dalam rentang tanggal – Atur rentang saat jadwal yang dikonfigurasi akan berlaku.

Persyaratan awal – Tentukan semua persyaratan yang harus dipenuhi secara bersamaan agar tugas dapat berjalan.

Persyaratan awal untuk pemindaian antimalware mirip dengan persyaratan awal untuk modul Cadangan yang dijelaskan di "Persyaratan untuk memulai" (hlm. 238). 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 penundaan adalah 60 menit, maka tugas akan dimulai antara pukul 10.00 dan 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.

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. Tindakan ini memungkinkan Anda membatalkan ke keadaan sebelumnya apabila penginstalan patch gagal. Agar opsi **Pencadangan prapembaruan** dapat berfungsi, mesin yang terkait harus memiliki manajemen Patch dan modul Cadangan 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**.

Mengelola daftar patch

Setelah penilaian kerentanan selesai, Anda akan menemukan patch yang tersedia di **Manajemen perangkat lunak** > **Patch**.

Nama	Deskripsi
Nama	Nama patch
Tingkat keparahan	Tingkat keparahan patch: • **Kritis** • **Tinggi** • **Sedang** • **Rendah** • **Tidak ada**

Vendor	Vendor patch
Produk	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.
Microsoft KB	Jika patch adalah untuk produk Microsoft, ID artikel KB diberikan
Tanggal rilis	Tanggal saat patch dirilis
Mesin	Jumlah mesin yang terdampak
Status persetujuan	Status persetujuan diperlukan terutama untuk skenario persetujuan otomatis dan untuk dapat menentukan pembaruan mana yang akan diinstal berdasarkan status dalam rencana proteksi.

	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 • **Belum ditentukan** – status patch tidak jelas dan harus divalidasi
Perjanjian lisensi	• Baca dan terima • Tidak disetujui. Jika Anda tidak menyetujui perjanjian lisensi, status patch menjadi **Ditolak** dan tidak akan diinstal
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

Persetujuan patch otomatis

Persetujuan patch otomatis memungkinkan Anda untuk menginstal pembaruan pada mesin dengan lebih mudah. Mari kita lihat contoh cara kerjanya.

Cara kerjanya

Anda harus memiliki dua lingkungan: uji dan produksi. Lingkungan uji digunakan untuk menguji instalasi patch dan memastikan bahwa patch tidak mengganggu apa pun. Setelah menguji instalasi patch pada lingkungan uji, Anda dapat secara otomatis menginstal patch aman ini pada lingkungan produksi.

Mengonfigurasi persetujuan patch otomatis

Untuk mengonfigurasi persetujuan patch otomatis

1. Anda harus membaca dan menerima perjanjian lisensi dari setiap vendor yang produknya akan Anda perbarui. Atau, instalasi patch otomatis tidak akan memungkinkan.
2. Konfigurasi pengaturan untuk persetujuan otomatis.
3. Siapkan rencana proteksi (misalnya, "Patch uji") dengan modul **Manajemen patch** yang diaktifkan dan menerapkannya pada mesin dalam lingkungan uji. Tentukan kondisi instalasi patch berikut: status persetujuan patch harus **Belum ditentukan**. Langkah ini diperlukan untuk memvalidasi patch dan memeriksa apakah mesin bekerja dengan benar setelah instalasi patch.

4. Siapkan rencana proteksi (misalnya, "Patch produksi") dengan modul **Manajemen patch** yang diaktifkan dan menerapkannya pada mesin dalam lingkungan produksi. Tentukan kondisi instalasi patch berikut: status persetujuan patch harus **Disetujui**.
5. Jalankan Rencana patch uji dan periksa hasilnya. Status persetujuan untuk mesin-mesin tersebut tidak memiliki masalah yang dapat dinilai sebagai **Belum ditentukan** sedangkan status untuk mesin yang tidak bekerja dengan benar harus diatur menjadi **Ditolak**.
6. Berdasarkan jumlah hari yang ditentukan dalam opsi **Persetujuan otomatis**, patch yang **Belum ditentukan** akan menjadi **Disetujui**.
7. Saat Rencana patch produksi diluncurkan, hanya patch yang **Disetujui** yang akan diinstal di mesin produksi.

Langkah-langkah manualnya tercantum di bawah ini.

Langkah 1. Baca dan terima perjanjian lisensi untuk produk yang ingin Anda perbarui

1. Di konsol web Cyber Protect, buka **Manajemen perangkat lunak** > **Patch**.
2. Pilih patch, lalu baca dan terima perjanjian lisensi.

Langkah 2. Konfigurasi pengaturan untuk persetujuan otomatis

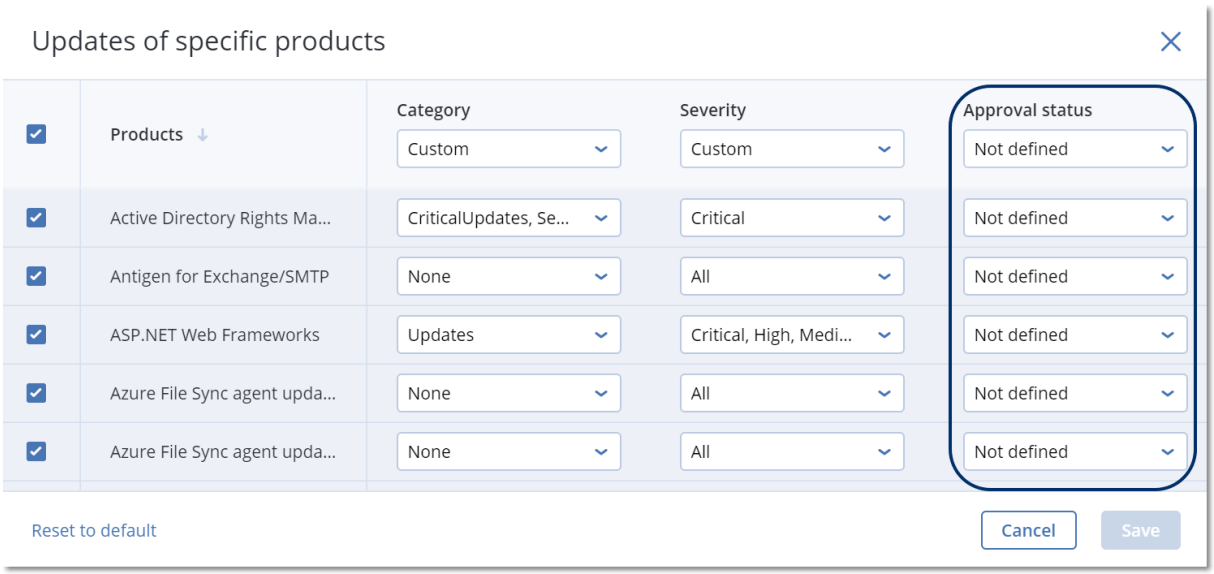
1. Di konsol web Cyber Protect, buka **Manajemen perangkat lunak** > **Patch**.
2. Klik **Pengaturan**.
3. Aktifkan opsi **Persetujuan otomatis** dan tentukan jumlah hari. Ini berarti bahwa setelah jumlah hari yang ditentukan sejak upaya pertama instalasi patch, patch dengan status **Belum ditentukan** akan menjadi **Disetujui** secara otomatis.

   Misalnya, Anda menentukan selama 10 hari. Anda menjalankan Rencana patch uji untuk mesin uji dan patch yang diinstal. Anda menandai patch yang merusak mesin sebagai **Ditolak**, sedangkan patch lainnya tetap berstatus **Belum ditentukan**. Setelah 10 hari berlalu, patch dengan status **Belum ditentukan** akan secara otomatis berubah menjadi **Disetujui**.
4. Aktifkan opsi **Secara otomatis menerima perjanjian lisensi**. Ini diperlukan untuk penerimaan lisensi otomatis selama instalasi patch, tidak ada konfirmasi yang diperlukan dari pengguna.

Langkah 3. Siapkan Rencana proteksi patch uji

1. Di konsol web Cyber Protect, buka **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 keterangan lebih lanjut tentang pengaturan ini, lihat "Pengaturan manajemen patch".

Penting
Untuk semua produk yang akan diperbarui, tetapkan **Status persetujuan** menjadi **Belum ditentukan**. Ketika waktu pembaruan tiba, agen hanya akan menginstal patch yang **Tidak ditentukan** pada mesin yang dipilih di lingkungan uji.

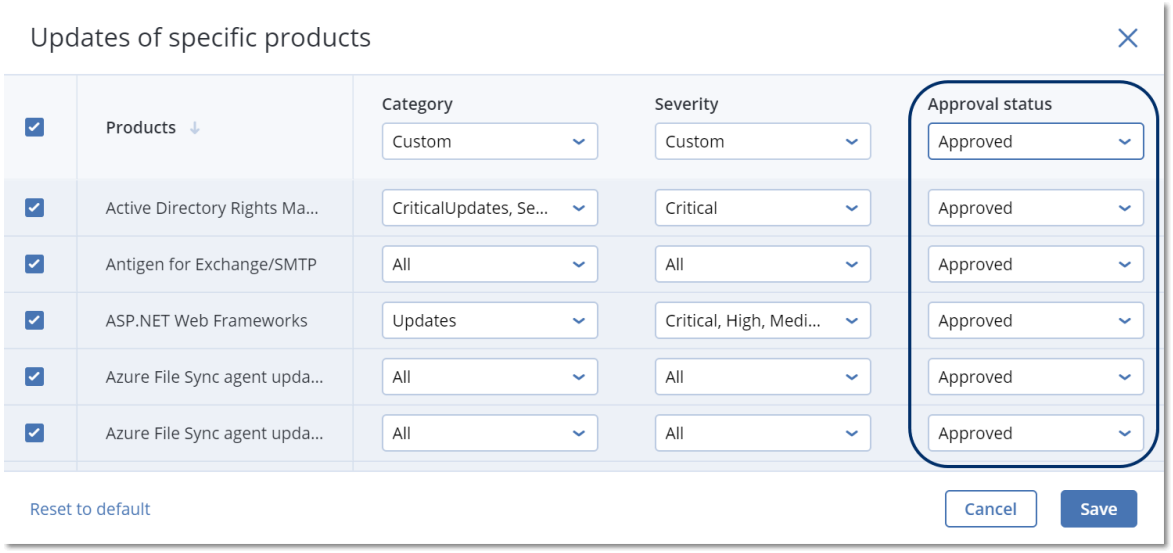


Langkah 4. Siapkan Rencana proteksi patch produksi

1. Di konsol web Cyber Protect, buka **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 keterangan lebih lanjut tentang pengaturan ini, lihat "Pengaturan manajemen patch".

Penting
Untuk semua produk yang akan diperbarui, tetapkan **Status persetujuan** menjadi **Disetujui**. Ketika waktu pembaruan tiba, agen hanya akan menginstal patch yang **Disetujui** pada mesin yang dipilih di lingkungan produksi.

Catatan



Langkah 5. Jalankan Rencana proteksi patch uji dan periksa hasilnya

1. Jalankan Rencana proteksi patch uji (berdasarkan jadwal atau sesuai permintaan).
2. Kemudian, periksa patch terinstal mana yang aman dan tidak aman.
3. Buka **Manajemen perangkat lunak** > **Patch** dan atur **Status persetujuan** menjadi **Ditolak** untuk patch yang tidak aman.

Persetujuan patch manual

Proses persetujuan patch manual adalah seperti berikut:

1. Di konsol web Cyber Protect, buka **Manajemen perangkat lunak** > **Patch**.
2. Pilih patch yang ingin Anda instal, lalu baca dan terima perjanjian lisensinya.
3. Atur **Status persetujuan** menjadi **Disetujui** untuk patch yang Anda setujui untuk diinstal.
4. Buat rencana proteksi dengan modul Manajemen patch yang diaktifkan. Anda dapat mengonfigurasi jadwal atau memulai rencana sesuai permintaan dengan mengklik **Jalankan sekarang** dalam pengaturan modul manajemen Patch.

Hasilnya, hanya patch yang disetujui yang akan diinstal pada mesin terpilih.

Instalasi patch sesuai permintaan

Instalasi patch sesuai permintaan dapat dilakukan dalam tiga cara berdasarkan preferensi Anda:

- Buka daftar patch (**Manajemen perangkat lunak** > **Patch**) dan instal patch yang diperlukan.
- Buka daftar kerentanan (**Manajemen perangkat lunak** > **Kerentanan**) dan mulailah proses perbaikan yang juga termasuk instalasi patch.

- Buka daftar perangkat (**Perangkat** > **Semua perangkat**), pilih mesin tertentu yang ingin Anda perbarui, dan instal patch pada mesin tersebut.

Mari pertimbangkan instalasi patch dari daftar patch:

1. Di konsol web Cyber Protect, buka **Manajemen perangkat lunak** > **Patch**.
2. Terima perjanjian lisensi untuk patch yang ingin Anda instal.
3. Pilih patch yang ingin Anda instal dan klik **Instal**.
4. Pilih mesin untuk tempat menginstal patch.
5. Tentukan apakah boot ulang dimulai setelah menginstal patch:
   - **Tidak pernah** – boot ulang tidak akan pernah diinisiasi setelah patch.
   - **Bila perlu** – boot ulang dilakukan hanya bila diperlukan untuk menerapkan patch.
   - **Selalu** – boot ulang akan selalu dimulai setelah patch diinstal. Anda selalu dapat menetapkan penundaan boot ulang.

   Jangan boot ulang hingga pencadangan selesai – jika proses pencadangan sedang berlangsung, boot ulang mesin akan tertunda hingga pencadangan selesai.
6. Klik **Instal patch**.

Patch yang dipilih akan diinstal pada mesin terpilih.

Masa aktif patch dalam daftar

Agar daftar patch tetap mutakhir, buka **Manajemen perangkat lunak** > **Patch** > **Pengaturan** dan tentukan opsi **Masa aktif dalam daftar**.

Opsi **Masa aktif dalam daftar** menjelaskan berapa lama patch tersedia yang terdeteksi akan tetap dalam daftar patch. Biasanya, patch dihapus dari daftar jika berhasil diinstal di semua mesin di mana ketidakadaannya terdeteksi atau waktu yang ditentukan sudah berlalu.

- **Selamanya** – patch selalu berada dalam daftar.
- **7 hari** – patch dihapus tujuh hari setelah penginstalan pertamanya.
  Misalnya, Anda memiliki dua mesin di mana patch harus diinstal. Salah satunya online, yang lain – offline. Patch diinstal di mesin pertama. Setelah 7 hari, patch akan dihapus dari daftar patch meskipun tidak diinstal di mesin kedua karena berstatus offline.
- **30 hari** – patch dihapus tiga puluh hari setelah penginstalan pertamanya.

Proteksi cerdas

Umpan ancaman

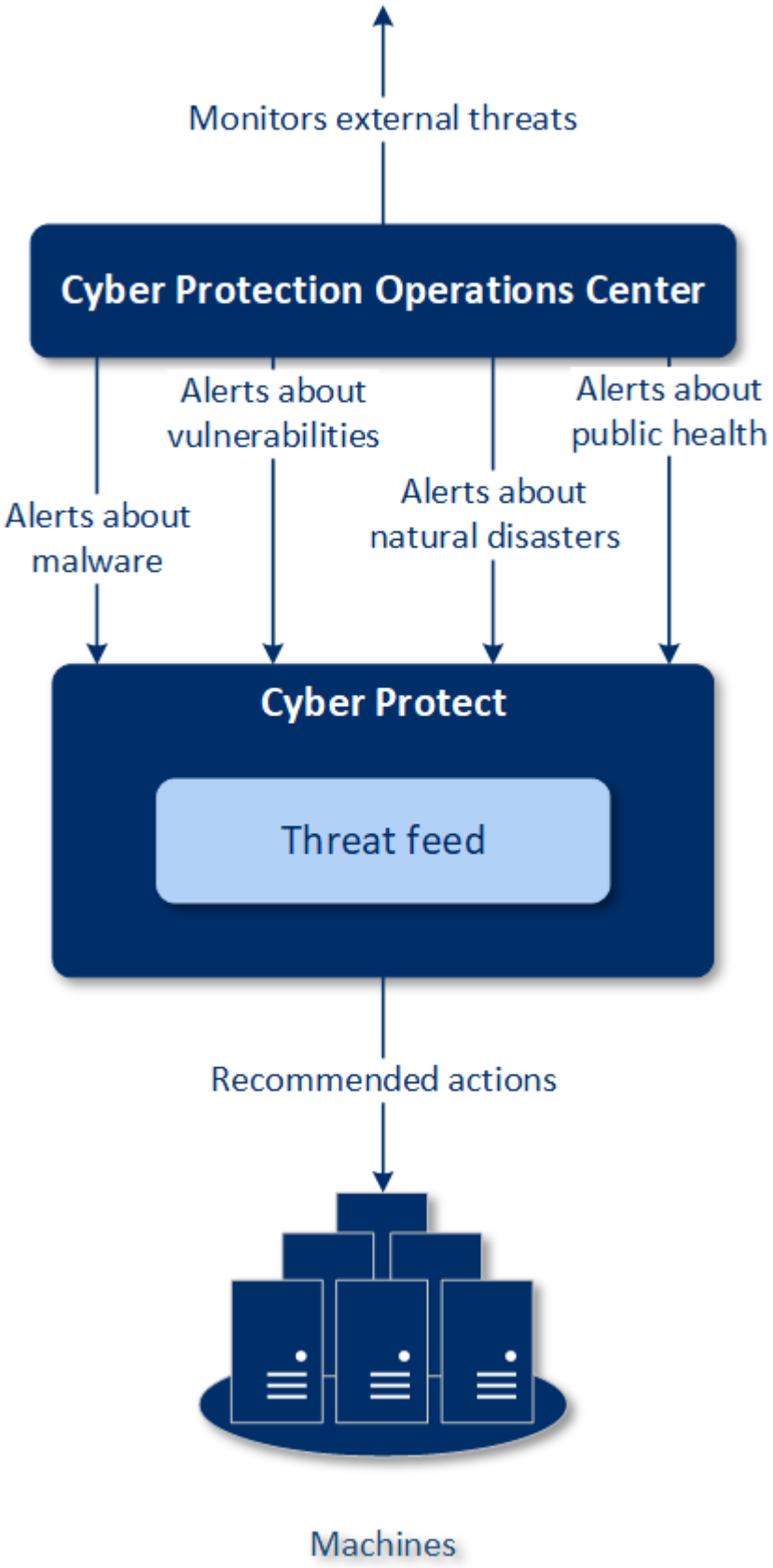
Acronis Pusat Operasi Perlindungan Cyber (CPOC) mengeluarkan peringatan keamanan yang dikirimkan hanya ke wilayah yang terkait secara geografis. Peringatan keamanan ini menyediakan informasi tentang malware, kerentanan, bencana alam, kesehatan publik, dan jenis peristiwa global lainnya yang dapat berdampak pada perlindungan data Anda. Umpan ancaman memberi tahu Anda tentang potensi ancaman dan memungkinkan Anda untuk mencegahnya.

Peringatan keamanan dapat diselesaikan dengan sejumlah tindakan spesifik yang ditentukan oleh ahli keamanan. Terdapat beberapa peringatan yang digunakan hanya untuk memberi tahu Anda tentang ancaman yang akan datang tetapi tidak tersedia tindakan yang direkomendasikan.

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 web 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.



Untuk menjalankan tindakan yang direkomendasikan pada peringatan yang diterima dari Pusat Operasi Perlindungan Cyber Acronis, lakukan hal-hal berikut:

1. Di konsol web Cyber Protect, buka **Dasbor** > **Umpan ancaman** untuk memeriksa apakah terdapat peringatan keamanan.

2. Pilih peringatan dalam daftar dan tinjau detail yang diberikan.

3. Klik **Mulai** untuk membuka wizard.

4. Aktifkan tindakan yang ingin Anda lakukan dan pilih 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 Anti-malware** – untuk menjalankan pemindaian menyeluruh pada mesin yang dipilih
- **Cadangan mesin yang dilindungi atau tidak dilindungi** – untuk mencadangkan mesin yang dilindungi/tidak dilindungi

5. Klik **Mulai**.

6. Di halaman **Aktivitas**, verifikasi bahwa aktivitas berhasil dilakukan.

Menghapus semua peringatan

Peringatan umpan ancaman secara otomatis dibersihkan setelah periode 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:

- Mendapatkan informasi detail tentang data yang disimpan (klasifikasi, lokasi, status proteksi, dan informasi tambahan) di mesin Anda.
- Mendeteksi apakah data dilindungi atau tidak. Data dianggap dilindungi jika dilindungi dengan cadangan (rencana proteksi dengan modul Cadangan yang diaktifkan).
- Untuk melakukan tindakan perlindungan data.

Cara kerjanya

1. Pertama, Anda membuat rencana proteksi dengan modul Peta perlindungan 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.

Mengelola file yang tidak terlindungi yang terdeteksi

Untuk melindungi file penting yang terdeteksi sebagai tidak terlindungi, lakukan hal berikut:

1. Di konsol web 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 klik **Lindungi semua file**. Anda akan dialihkan ke daftar rencana di mana Anda dapat membuat rencana proteksi dengan modul Cadangan yang diaktifkan.

   Untuk menghapus perangkat tertentu dengan file yang tidak terlindungi dari daftar, klik **Sembunyikan hingga penemuan data berikutnya**.
2. Untuk melihat informasi detail tentang file yang tidak terlindungi pada perangkat tertentu, klik nama perangkat ini.

   Anda akan melihat daftar file yang tidak terlindungi per ekstensi dan per lokasi. Anda dapat memfilter daftar ini berdasarkan ekstensi file.
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 Cadangan 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.

Jadwalkan operasi tugas menggunakan peristiwa berikut:

- **Jadwalkan berdasarkan waktu** – Tugas akan dijalankan berasarkan 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.

Pengaturan default: **Jadwalkan berdasarkan waktu**.

Jenis jadwal:

- **Bulanan** – Pilih bulan dan minggu atau hari dalam sebulan saat tugas akan berjalan.
- **Harian** – Pilih hari dalam pekan saat tugas akan berjalan.
- **Per jam** – Pilih hari dalam pekan, jumlah pengulangan, dan interval waktu tugas akan berjalan.

Pengaturan default: **Harian**.

Mulai pada – Pilih waktu spesifik saat tugas akan berjalan.

Jalankan dalam rentang tanggal – Atur rentang saat jadwal yang dikonfigurasi akan berlaku.

Persyaratan awal – Tentukan semua persyaratan yang harus dipenuhi secara bersamaan agar tugas dapat berjalan.

Persyaratan awal untuk pemindaian antimalware mirip dengan persyaratan awal untuk modul Cadangan yang dijelaskan di "Persyaratan untuk memulai" (hlm. 238). 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 penundaan adalah 60 menit, maka tugas akan dimulai antara pukul 10.00 dan 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.

Aturan pengecualian dan ekstensi

Pada tab **Ekstensi** , Anda dapat menentukan 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 status proteksinya tidak ingin diperiksa 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.

Akses desktop jarak jauh

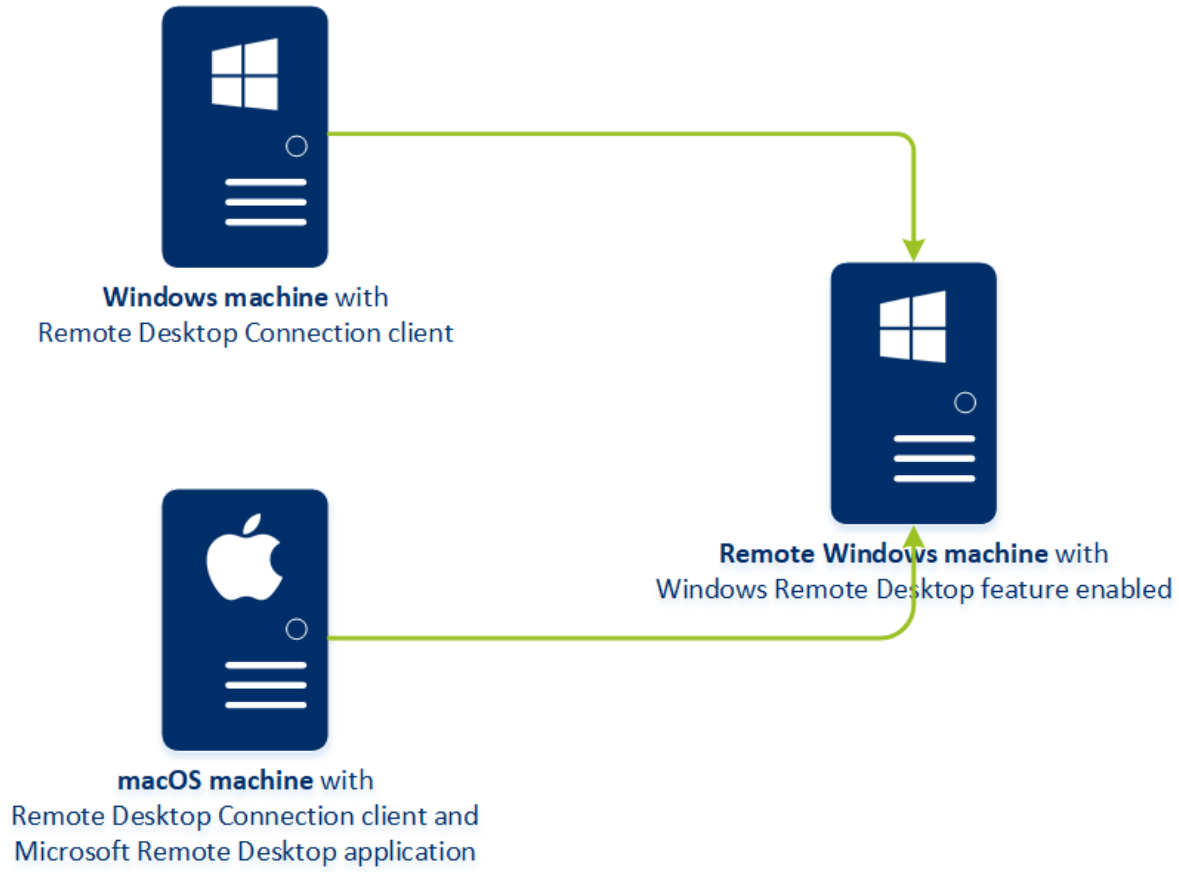
Akses jarak jauh (klien RDP dan HTML5)

Cyber Protect memberi Anda kemampuan untuk melakukan akses jarak jauh. Anda dapat menghubungkan dan mengelola mesin pengguna Anda dari jarak jauh langsung dari konsol web. Ini memungkinkan Anda dengan mudah membantu pengguna dalam menyelesaikan masalah pada mesin mereka.

Prasyarat:

- Agen perlindungan diinstal di mesin jarak jauh dan terdaftar di server manajemen.
- Mesin memiliki lisensi Cyber Protect yang sesuai.
- Klien Koneksi Desktop Jarak Jauh diinstal pada mesin tempat koneksi diinisialisasi.
- Mesin tempat koneksi RDP diinisialisasi harus dapat mengakses server manajemen dengan nama hostnya. Pengaturan DNS harus dikonfigurasi dengan benar atau nama host server manajemen harus dimasukkan ke dalam file host.

Koneksi jarak jauh dapat dilakukan dari mesin Windows dan macOS.



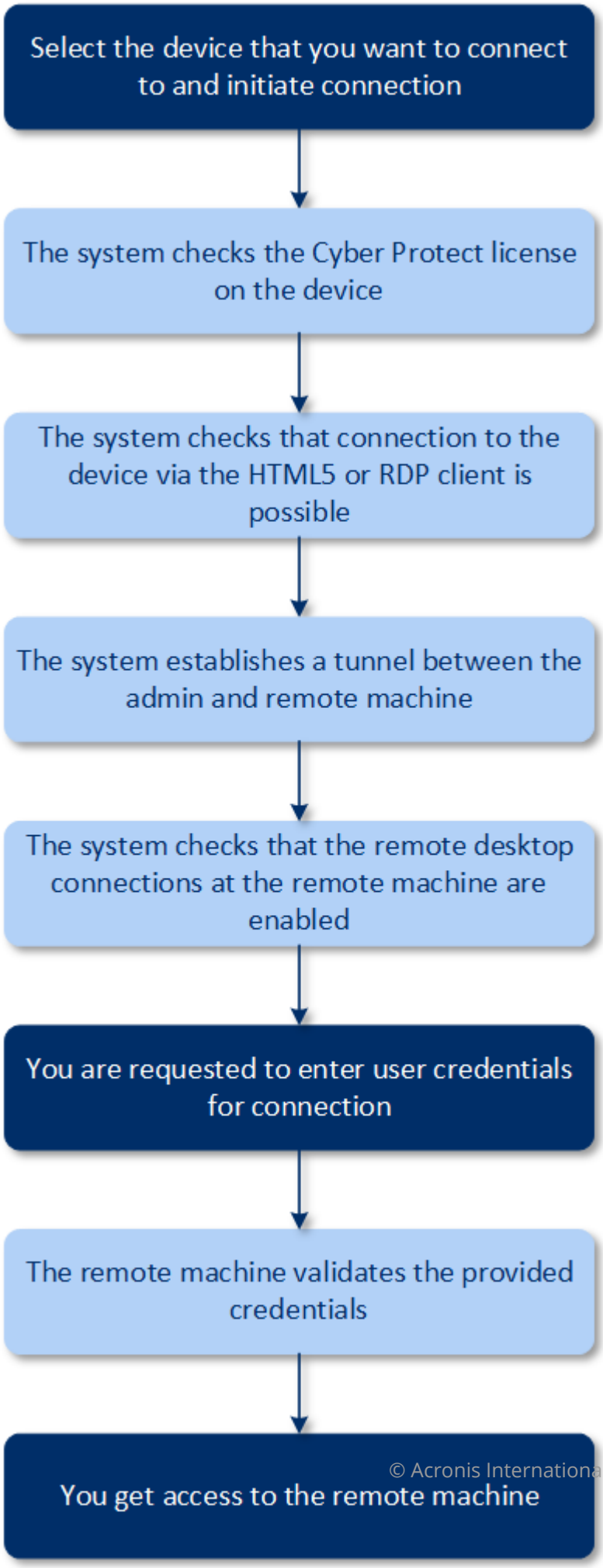
Fungsi akses jarak jauh dapat digunakan untuk koneksi ke mesin Windows dengan fitur Windows Remote Desktop yang tersedia. Itulah mengapa akses jarak jauh tidak mungkin dilakukan, misalnya, ke sistem Windows 10 Home atau macOS.

Untuk melakukan koneksi dari mesin macOS ke sebuah mesin jarak jauh, pastikan bahwa aplikasi berikut ini telah diinstal pada mesin macOS:

- Klien Koneksi Desktop Jarak Jauh
- Aplikasi Microsoft Remote Desktop

Cara kerjanya

Jika Anda mencoba menyambungkan ke mesin jarak jauh, sistem akan memeriksa apakah mesin ini memiliki lisensi Cyber Protect terlebih dahulu. Kemudian, sistem akan memeriksa apakah koneksi melalui klien HTML5 atau RDP mungkin dilakukan. Anda memulai sambungan melalui klien RDP atau HTML5. Sistem membuat terowongan ke mesin jarak jauh dan memeriksa apakah koneksi desktop jarak jauh diaktifkan pada mesin jarak jauh. Kemudian, Anda memasukkan kredensial dan, setelah validasi, Anda dapat mengakses mesin jarak jauh.



Cara menghubungkan ke mesin jarak jauh

Lakukan hal berikut untuk menghubungkan ke mesin jarak jauh:

1. Di konsol web Cyber Protect, buka **Perangkat** > **Semua perangkat.**
2. Klik pada mesin yang ingin Anda sambungkan dari jarak jauh, lalu klik **Desktop Perlindungan Cyber** > **Sambungkan melalui klien RDP** atau **Sambungkan melalui klien HTML5**.

   Catatan
   Koneksi melalui klien HTML5 hanya tersedia jika server manajemen diinstal di mesin Linux.

3. [Opsional, hanya untuk koneksi melalui klien RDP] Unduh dan instal klien Koneksi Desktop Jarak Jauh. Memulai koneksi ke mesin jarak jauh.
4. Tentukan login dan kata sandi untuk mengakses mesin jarak jauh, dan kemudian klik **Sambungkan**.

Hasilnya, Anda tersambung ke mesin jarak jauh dan dapat mengelolanya.

Berbagi koneksi jarak jauh

Karyawan yang bekerja dari rumah mungkin memerlukan akses ke komputer kantor mereka, tetapi mungkin saja organisasi Anda tidak mengonfigurasi VPN atau alat bantu lain untuk koneksi jarak jauh. Cyber Protect memberi Anda kemampuan untuk berbagi tautan RDP dengan pengguna Anda, sehingga memberi mereka akses jarak jauh ke mesin mereka.

Untuk mengaktifkan fungsionalitas berbagi koneksi jarak jauh

1. Di konsol web Cyber Protect, buka **Pengaturan** > **Perlindungan** > **Koneksi jarak jauh**.
2. Pilih kotak centang **Bagikan koneksi desktop jarak jauh**.

Hasilnya, saat Anda memilih perangkat di konsol web Cyber Protect, opsi baru **Bagikan koneksi jarak jauh** akan muncul.

Untuk berbagi koneksi jarak jauh dengan pengguna Anda

1. Di konsol web Cyber Protect, buka **Perangkat** > **Semua perangkat**.
2. Pilih perangkat yang ingin Anda berikan koneksi jarak jauh.
3. Klik **Bagikan koneksi jarak jauh**.
4. Klik **Dapatkan tautan**. Pada jendela yang dibuka, salin tautan yang telah dihasilkan. Tautan ini dapat dibagikan dengan pengguna yang membutuhkan akses jarak jauh ke perangkat. Tautan ini valid selama 10 jam.

Setelah mendapatkan tautannya, Anda dapat membagikannya melalui email atau alat komunikasi lainnya. Pengguna yang diberikan link tersebut, harus mengkliknya, lalu memilih jenis koneksi:

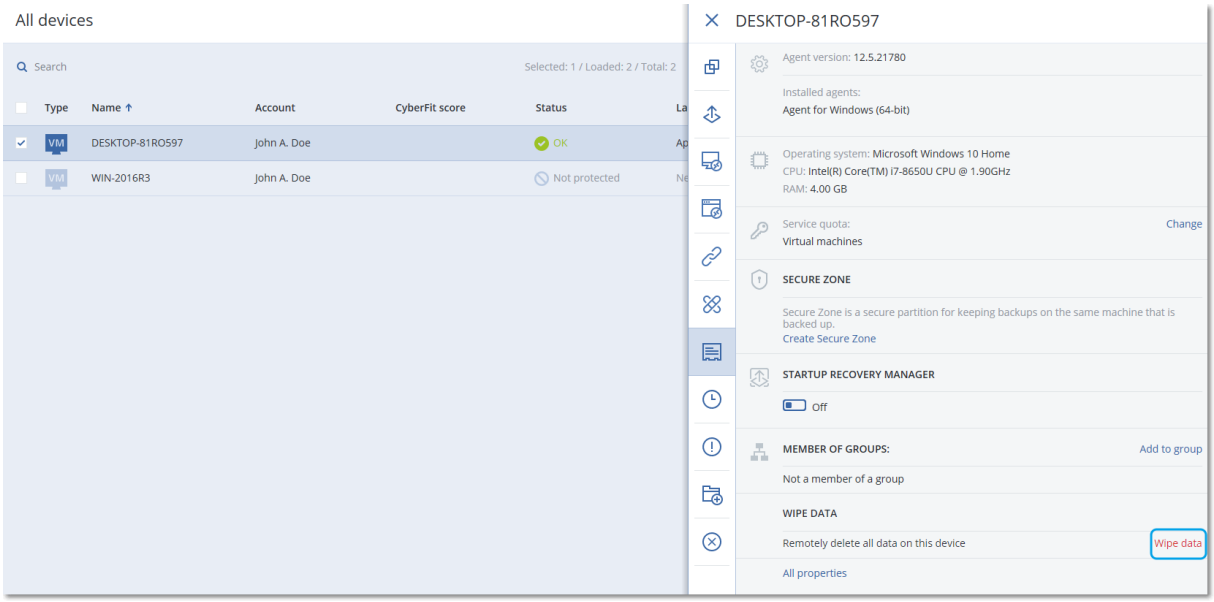
- Sambungkan melalui klien RDP.
  Koneksi ini akan meminta untuk mengunduh dan menginstal klien Koneksi Jarak Jauh.

- Sambungkan melalui klien HTML5.
  Koneksi ini tidak memerlukan penginstalan klien RDP apa pun di mesin pengguna. Pengguna akan diarahkan ke layar masuk dan harus memasukkan kredensial untuk mengakses mesin.

Penghapusan jarak jauh

Penghapusan jarak jauh memungkinkan administrator layanan Cyber Protect 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 pada mesin yang menggunakan Windows 10. Untuk menerima perintah penghapusan, mesin harus menyala dan terhubung ke Internet.



Untuk menghapus data dari mesin

1. Di konsol web 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 dan siapa yang memulainya dalam **Dasbor** > **Aktivitas**.

Grup perangkat

Grup perangkat dirancang untuk mempermudah manajemen sejumlah besar perangkat terdaftar.

Anda dapat menerapkan rencana proteksi pada suatu grup. Setelah perangkat baru muncul di grup, perangkat akan terlindungi oleh rencana. Jika perangkat dihapus dari grup, perangkat tidak akan lagi terlindungi oleh rencana. Rencana yang diterapkan pada grup tidak dapat dicabut dari anggota grup, hanya dari grup itu sendiri.

Hanya perangkat dengan jenis sama yang dapat ditambahkan ke grup. Misalnya, pada **Hyper-V** Anda dapat membuat grup mesin virtual Hyper-V. Pada **Mesin dengan agen**, Anda dapat membuat grup mesin dengan agen yang diinstal. Pada **Semua perangkat**, Anda tidak dapat membuat grup.

Perangkat tunggal dapat menjadi anggota lebih dari satu grup.

Grup bawaan

Setelah terdaftar, perangkat akan muncul di salah satu grup root bawaan pada tab **Perangkat**.

Grup root *tidak dapat* diedit atau dihapus. Anda *tidak dapat* menerapkan rencana untuk me-root grup.

Beberapa grup root berisi grup sub-root bawaan. Grup ini *tidak dapat* diedit atau dihapus. Namun, Anda *dapat* menerapkan rencana ke sub-root grup bawaan.

Grup kustom

Melindungi semua perangkat dalam grup bawaan dengan rencana proteksi tunggal mungkin tidak berhasil karena peran mesin yang berbeda. Data yang dicadangkan spesifik untuk setiap departemen; beberapa data harus sering dicadangkan, sedangkan data lainnya dicadangkan dua kali setahun. Dengan demikian, Anda mungkin perlu membuat beberapa rencana proteksi yang berlaku untuk sejumlah perangkat mesin yang berbeda. Dalam hal ini, pertimbangkan untuk membuat grup kustom.

Grup kustom dapat berisi satu atau beberapa grup bersarang. Setiap grup kustom dapat diedit atau dihapus. Ada beberapa jenis grup kustom:

- **Grup statis**

  Grup statis berisi mesin yang ditambahkan secara manual ke dalamnya. Konten grup statis tidak pernah berubah kecuali jika Anda secara eksplisit menambah atau menghapus mesin.

  Contoh: Anda membuat grup kustom untuk departemen akuntansi dan secara manual menambahkan mesin akuntan ke grup ini. Setelah Anda menerapkan rencana proteksi pada grup, mesin akuntan akan terlindungi. Jika terdapat akuntan baru, Anda harus menambahkan mesin baru ke grup secara manual.
- **Grup dinamis**

Grup dinamis berisi mesin yang ditambahkan secara otomatis sesuai dengan kriteria pencarian yang ditentukan saat membuat grup. Konten grup dinamis berubah secara otomatis. Mesin akan tetap berada di grup saat memenuhi kriteria yang ditentukan.

Contoh 1: Nama host dari mesin yang dimiliki oleh departemen akuntansi mengandung kata "accounting". Anda menentukan nama mesin parsial sebagai kriteria keanggotaan grup dan menerapkan rencana proteksi pada grup. Jika terdapat akuntan baru, mesin baru akan ditambahkan ke grup segera setelah terdaftar, dan dengan demikian akan secara otomatis terlindungi.

Contoh 2: Departemen akuntansi membentuk unit organisasi (OU) Active Directory yang terpisah. Anda menetapkan OU akuntansi sebagai kriteria keanggotaan grup dan menerapkan rencana proteksi pada grup. Jika terdapat akuntan baru, mesin baru akan ditambahkan ke grup segera setelah terdaftar dan ditambahkan ke OU (mana pun yang terjadi lebih dahulu), dan dengan demikian akan secara otomatis terlindungi.

Membuat grup statis

1. Klik **Perangkat**, lalu pilih grup bawaan yang berisi perangkat yang ingin Anda buat grup statisnya.
2. Klik ikon roda gigi di sebelah grup tempat Anda ingin membuat grup.
3. Klik **Grup baru**.
4. Tentukan nama grup, lalu klik **OK**.
   Grup baru akan muncul di pohon grup.

Menambahkan perangkat ke grup statis

1. Klik **Perangkat**, lalu pilih satu atau beberapa perangkat yang ingin Anda tambahkan ke grup.
2. Klik **Tambahkan ke grup**.
   Perangkat lunak akan menampilkan pohon grup yang dapat ditambah dengan perangkat yang dipilih.
3. Jika Anda ingin membuat grup baru, lakukan langkah berikut. Jika tidak, lewati langkah ini.
   a. Pilih grup tempat Anda ingin membuat grup.
   b. Klik **Grup baru**.
   c. Tentukan nama grup, lalu klik **OK**.
4. Pilih grup yang ingin Anda tambahkan perangkat, lalu klik **Selesai**.

Cara lain untuk menambah perangkat ke grup statis adalah memilih grup dan klik **Tambah perangkat**.

Membuat grup dinamis

1. Klik **Perangkat**, lalu pilih grup yang berisi perangkat yang ingin Anda buat grup dinamisnya.
2. Cari perangkat menggunakan bidang pencarian. Anda dapat menggunakan beberapa atribut dan operator yang dijelaskan di bawah ini.
3. Klik **Simpan sebagai** di sebelah bidang pencarian.

   Catatan
   Beberapa atribut tidak didukung untuk pembuatan grup. Lihat tabel di bagian kueri Pencarian di bawah.

4. Tentukan nama grup, lalu klik **OK**.

Kueri pencarian

Tabel berikut merangkum atribut tersedia yang dapat Anda gunakan dalam kueri pencarian.

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
`name`	• Nama host untuk mesin fisik • Nama mesin virtual • Nama database • Alamat email untuk kotak surat	`name = 'en-00'`	Iya
`parameters.MacAddress`	Alamat MAC.	`parameters.MacAddress LIKE '00-22-4D-50-25-E5'`	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	`comment = 'important machine'` `comment = ''` (semua mesin tanpa komentar)	Iya

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	setiap 15 menit. • Kosong untuk perangkat lain. **Catatan** Jika Anda menambahkan teks secara manual di kolom komentar, sinkronisasi otomatis deskripsi Windows akan dinonaktifkan. Untuk mengaktifkannya kembali, hapus komentar yang Anda tambahkan. Untuk melakukan refresh komentar yang disinkronisasi secara otomatis pada perangkat Anda, mulai kembali Managed Machine Service di **Layanan Windows** atau jalankan perintah berikut ini di jendela perintah: `net stop mms` `net start mms` Untuk melihat komentar, pada **Perangkat**, pilih perangkat, klik **Detail**, lalu cari bagian **Komentar**. Untuk menambahkan atau mengubah komentar, klik **Tambah**		

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	atau **Edit**. Untuk perangkat di mana agen proteksi diinstal, ada dua bidang komentar terpisah: • Komentar agen ◦ Untuk mesin fisik yang menjalankan Windows, deskripsi komputer di Windows disalin secara otomatis sebagai komentar. Nilai ini akan disinkronisasi setiap 15 menit. ◦ Kosong untuk perangkat lain. **Catatan** Jika Anda menambahkan teks secara manual di kolom komentar, sinkronisasi otomatis deskripsi Windows akan dinonaktifkan. Untuk mengaktifkannya kembali, hapus komentar yang Anda tambahkan. • Komentar perangkat ◦ Jika komentar agen ditentukan secara otomatis, komentar akan disalin sebagai komentar perangkat. Komentar agen		

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	yang ditambahkan secara manual tidak disalin sebagai komentar perangkat. ◦ Komentar perangkat tidak disalin sebagai komentar agen. Perangkat dapat memiliki salah satu atau kedua komentar yang ditentukan, atau keduanya kosong. Jika 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**.		
`ip`	Alamat IP (hanya untuk mesin fisik).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Iya
`cpuArch`	Arsitektur CPU.	`cpuArch = 'x64'`	Iya

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	Nilai yang dimungkinkan: • `'x64'` • `'x86'`		
`memorySize`	Ukuran RAM dalam megabyte (MiB).	`memorySize < 1024`	Iya
`cpuName`	Nama CPU.	`cpuName LIKE '%XEON%'`	Iya
`insideVm`	Mesin virtual dengan agen di dalamnya. Nilai yang dimungkinkan: • `true` • `false`	`insideVm = true`	Iya
`tzOffset`	Offset zona waktu mesin dalam sekejap.	`tzOffset = 120`	Iya
`parameters.Architecture`	Arsitektur sistem operasi. Nilai yang dimungkinkan: • `'x86'` • `'x64'`	`parameters.Architecture = 'x86'`	Iya
`osName`	Nama sistem operasi	`osName LIKE '%Windows XP%'`	Iya
`osType`	Jenis sistem operasi. Nilai yang dimungkinkan: • `'windows'` • `'linux'` • `'macosx'`	`osType IN ('linux', 'macosx')`	Iya
`osProductType`	Jenis produk sistem operasi. Nilai yang dimungkinkan:	`osProductType = 'server'`	Iya

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	• `'dc'` Singkatan dari Pengontrol Domain. • `'server'` • `'workstation'`		
`virtualType`	Tipe mesin virtual. Nilai yang dimungkinkan: • `'vmwesx'` Mesin virtual VMware. • `'mshyperv'` Mesin virtual Hyper-V. • `'pcs'` Mesin virtual Virtuozzo. • `'hci'` Mesin virtual Virtuozzo Hybrid Infrastructure. • `'scale'` Mesin virtual Scale Computing HC3. • `'ovirt'` Mesin virtual oVirt	`virtualType = 'vmwesx'`	Iya
`osSp`	Pak layanan sistem operasi.	`osSp = 1`	Iya
`osVersionMajor`	Versi besar sistem operasi.	`osVersionMajor = 1`	Iya
`osVersionMinor`	Versi kecil sistem operasi.	`osVersionMminor = 1`	Iya
`isOnline`	Ketersediaan mesin. Nilai yang dimungkinkan: • `true` • `false`	`isOnline = true`	Tidak

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
`tenant`	Nama unit tempat perangkat tersebut berada.	`tenant = 'Unit 1'`	Iya
`tenantId`	Pengidentifikasi unit yang dimiliki perangkat. Untuk mendapatkan ID unit, pada **Perangkat**, pilih perangkat, klik **Detail** > **Semua properti**. ID ditampilkan di bidang `ownerId`.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Iya
`state`	Status perangkat. Nilai yang dimungkinkan: • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`	`state = 'backup'`	Tidak
`status`	Status sumber daya. Nilai yang dimungkinkan: • `'notProtected'` • `'ok'`	`status = 'ok'`	Tidak

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	• `'warning'` • `'error'` • `'critical'`		
`protectedByPlan`	Perangkat yang dilindungi oleh rencana proteksi dengan ID tertentu. Untuk mendapatkan ID rencana, klik **Rencana** > **Cadangan**, pilih rencana, klik pada diagram di kolom **Status**, lalu klik pada 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 memiliki status **OK**.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Tidak
`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	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Tidak

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	dilindungi oleh rencana proteksi dengan ID tertentu dan memiliki status **Interaksi Diperlukan**.		
`ou`	Mesin yang dimiliki unit organisasi Active Directory yang ditentukan.	`ou IN ('RnD', 'Computers')`	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
`lastBackupTime`	Tanggal dan waktu pencadangan terakhir yang berhasil. Formatnya adalah `'YYYY-MM-DD HH: MM'`.	`lastBackupTime > '2022-03-11'` `lastBackupTime <= '2022-03-11 00:15'` `lastBackupTime is null`	Tidak
`lastBackupTryTime`	Waktu percobaan pencadangan terakhir. Formatnya adalah `'YYYY-MM-DD HH: MM'`.	`lastBackupTryTime >= '2022-03-11'`	Tidak
`nextBackupTime`	Waktu pencadangan berikutnya. Formatnya adalah `'YYYY-MM-DD HH: MM'`.	`nextBackupTime >= '2022-08-11'`	Tidak
`agentVersion`	Versi agen perlindungan yang diinstal.	`agentVersion LIKE '12.0.*'`	Iya
`hostId`	ID internal agen perlindungan. Untuk mendapatkan ID agen perlindungan,	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Iya

Atribut	Maksud	Contoh kueri pencarian	Didukung untuk pembuatan grup
	dalam **Perangkat**, pilih mesin, klik **Detail** > **Semua properti**. Gunakan nilai `"id"` properti `agen`.		
`resourceType`	Tipe sumber daya. Nilai yang dimungkinkan: • `'machine'` • `'virtual_machine.vmwesx'` • `'virtual_machine.mshyperv'` • `'virtual_machine.rhev'` • `'virtual_machine.kvm'` • `'virtual_machine.xen'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Iya
`hasAsz`	Agen perlindungan pada mesin fisik dengan AcronisSecure Zone. Nilai yang dimungkinkan: • `true` • `false`	`hasAsz=true`	Iya
`chassis`	Tipe sasis mesin. Nilai yang dimungkinkan: • `unknown` • `laptop` • `desktop` • `server` • `other`	`chassis='laptop'`	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 = 2020-02-20, berarti bahwa hasil pencarian akan mencakup semua cadangan dari interval lastBackupTime >= 2020-02-20 00:00 dan lastBackup time <= 2020-02-20 23:59:59

Operator

Tabel berikut merangkum operator yang tersedia.

Operator	Maksud	Contoh
`AND`	Operator konjungsi logis.	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Operator disjungsi logis.	`state = 'backup' OR state = 'interactionRequired'`
`IN (<value1>,... <valueN>)`	Operator ini digunakan untuk menguji apakah suatu ekspresi cocok dengan setiap nilai dalam daftar nilai.	`osType IN ('windows', 'linux')`
`NOT`	Operator negasi logis.	`NOT(osProductType = 'workstation')`
`NOT IN (<value1>,... <valueN>)`	Operator ini berlawanan dengan operator `IN`.	`NOT osType IN ('windows', 'linux')`
`LIKE 'wildcard pattern'`	Operator ini digunakan untuk menguji apakah suatu ekspresi cocok dengan pola wildcard. Operator wildcard berikut dapat digunakan: • * 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_'`
`RANGE(<starting_value>, <ending_value>)`	Operator ini digunakan untuk menguji apakah suatu ekspresi berada dalam rentang nilai (inklusif).	`ip RANGE ('10.250.176.1','10.250.176.50')`
`= or ==`	Operator *sama dengan*.	`osProductType = 'server'`
!= atau <>	Operator *tidak sama dengan*.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
<	Operator *kurang dari*.	`memorySize < 1024`
>	Operator *lebih besar dari*.	`diskSize > 300 GB`
<=	Operator *kurang dari atau sama dengan*.	`lastBackupTime <= '2022-05-11`

Operator	Maksud	Contoh
		`00:15'`
>=	Operator *lebih dari atau sama dengan*.	`nextBackupTime >= '2022-09-11'`

Menerapkan rencana proteksi pada grup

1. Klik **Perangkat**, lalu pilih grup bawaan yang berisi grup yang ingin Anda terapkan rencana proteksi.

   Perangkat lunak akan menampilkan daftar grup turunan.
2. Pilih grup yang ingin Anda terapkan rencana proteksi.
3. Klik **Pencadangan grup**.

   Perangkat lunak menampilkan daftar rencana proteksi yang dapat diterapkan pada grup.
4. Lakukan salah satu langkah berikut:
   - Perluas rencana proteksi yang sudah ada, lalu klik **Terapkan**.
   - Klik **Buat baru**, lalu buat rencana proteksi baru seperti yang dijelaskan di "Cadangan".

Pemantauan dan pelaporan

Dasbor **Ikhtisar** memungkinkan Anda untuk memantau kondisi terkini dari infrastruktur pencadangan Anda.

Bagian **Laporan** memungkinkan Anda untuk menghasilkan laporan sesuai permintaan dan terjadwal terkait infrastruktur terlindung Anda. Bagian ini hanya tersedia dengan lisensi Lanjutan.

Dasbor Ikhtisar

Dasbor **Ikhtisar** memberikan sejumlah widget yang dapat disesuaikan yang memberikan gambaran tentang infrastruktur terlindung Anda. Anda dapat memilih dari lebih dari 20 widget, yang disajikan sebagai diagram lingkaran, tabel, grafik, diagram batang, dan daftar. Widget memiliki elemen yang dapat diklik sehingga memungkinkan Anda untuk menyelidiki dan menyelesaikan masalah. Informasi dalam widget diperbarui setiap lima menit.

Dengan lisensi Lanjutan, Anda juga dapat mengunduh status dasbor saat ini atau mengirimnya melalui email dalam format .pdf atau/dan .xlsx. Untuk mengirim dasbor melalui email, pastikan pengaturan **Server email** sudah dikonfigurasikan.

Widget yang tersedia bergantung pada edisi Cyber Protect Anda. Widget default tercantum di bawah ini:

Widget	Ketersediaan	Deskripsi
Perlindungan cyber	Tidak tersedia dalam edisi Cyber Backup	Menampilkan keseluruhan informasi mengenai ukuran cadangan, malware yang diblokir, URL yang diblokir, kerentanan yang ditemukan, dan patch yang diinstal.
Status proteksi	Tersedia dalam semua edisi	Menampilkan status proteksi saat ini untuk semua mesin.
Aktivitas	Tersedia dalam semua edisi	Menampilkan ringkasan aktivitas yang dilakukan selama periode waktu tertentu.
Ringkasan peringatan aktif	Tersedia dalam semua edisi	Menampilkan ringkasan peringatan aktif berdasarkan tipe peringatan dan tingkat keparahan.
Status instalasi patch	Tidak tersedia dalam edisi Cyber Backup	Menampilkan jumlah mesin yang dikelompokkan berdasarkan status instalasi patch.
Pembaruan yang tidak ada berdasarkan kategori	Tidak tersedia dalam edisi Cyber Backup	Menampilkan jumlah pembaruan yang tidak ada berdasarkan kategori.
Status kesehatan disk	Tidak tersedia dalam edisi	Menampilkan jumlah disk berdasarkan status.

	Cyber Backup	
Perangkat	Tersedia dalam semua edisi	Menampilkan informasi rinci tentang perangkat di lingkungan Anda.
Detail peringatan aktif	Tersedia dalam semua edisi	Menampilkan informasi rinci tentang peringatan aktif.
Kerentanan yang ada	Tersedia dalam semua edisi	Menampilkan kerentanan yang ada untuk sistem operasi dan aplikasi dalam lingkungan Anda, dan mesin yang terdampak.
Riwayat instalasi patch	Tidak tersedia dalam edisi Cyber Backup	Menampilkan informasi rinci tentang patch yang diinstal.
Baru-baru ini terdampak	Tersedia dalam semua edisi	Menampilkan informasi rinci tentang mesin yang baru-baru ini terdampak.
Ringkasan lokasi	Tersedia dalam semua edisi	Menampilkan informasi rinci tentang lokasi cadangan.

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 ikon pensil saat widget dipilih. Setelah mengedit widget, klik **Selesai**.

Untuk mengatur ulang widget di dasbor

Seret dan lepaskan widget dengan mengklik namanya.

Untuk mengedit widget

Klik ikon pensil di sebelah nama widget. Pengeditan widget memungkinkan Anda untuk mengganti nama, mengubah rentang waktu, mengatur filter, dan mengelompokkan baris.

Untuk menghapus widget

Klik ikon tanda X di sebelah nama widget.

Cyber Protection

Widget ini menampilkan keseluruhan informasi mengenai ukuran cadangan, malware yang diblokir, URL yang diblokir, kerentanan yang ditemukan, dan patch yang diinstal.

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

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.

Mesin yang ditemukan

Widget ini menampilkan daftar mesin yang ditemukan selama rentang waktu tertentu.

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.

Batasan:

- 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.

- Di drive NVMe, pemantauan kesehatan disk hanya didukung untuk drive yang mengomunikasikan data SMART via API Windows. Pemantauan kesehatan disk tidak didukung untuk drive NVMe yang perlu membaca data SMART langsung dari drive.

Kesehatan disk diwakili salah satu status berikut:

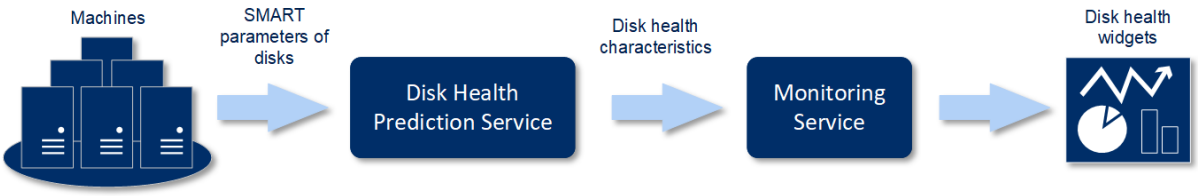
- **OK**
  Kesehatan disk antara 70% dan 100%.
- **Peringatan**
  Kesehatan disk di antara 30% dan 70%.
- **Kritis**
  Kesehatan disk di antara 0% dan 30%.
- **Menghitung data disk**
  Status terkini dan prakiraan disk sedang dihitung

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 seperti berikut:
   - Status terkini kesehatan disk: OK, peringatan, kritis.
   - Prakiraan kesehatan disk: negatif, stabil, positif.
   - Persentase kemungkinan prakiraan kesehatan disk.

   Periode prediksi selalu selama satu bulan.
3. Layanan Pemantauan menerima karakteristik ini, lalu menunjukkan informasi relevan di widget kesehatan disk di konsol web Cyber Protect.



Widget kesehatan disk

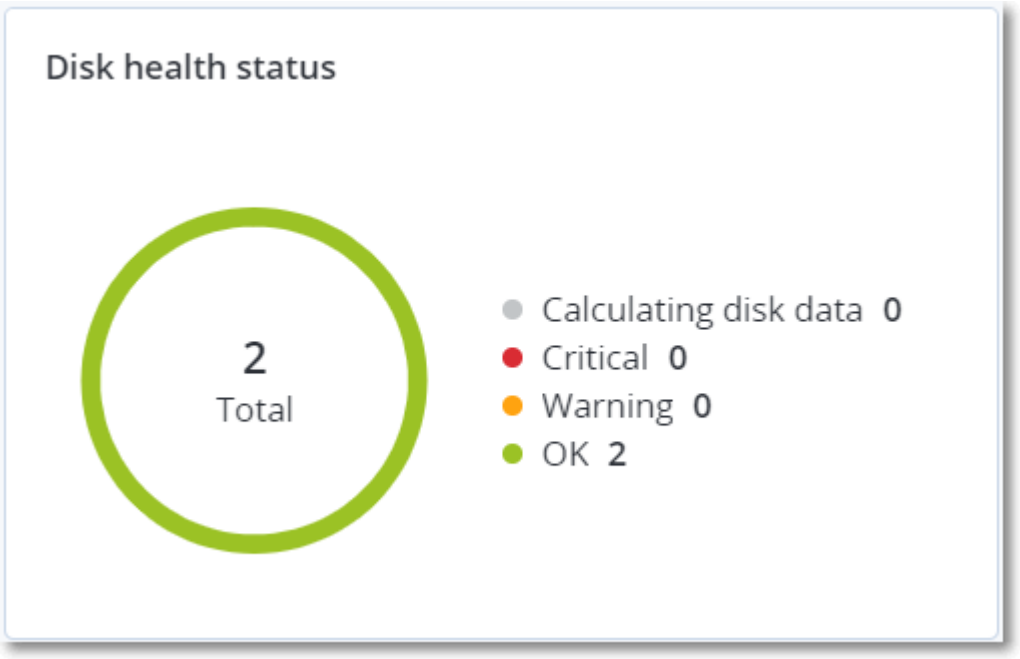
Hasil pemantauan kesehatan disk disajikan di widget berikut yang tersedia di konsol web Cyber Protect.

- **Gambaran kesehatan disk** adalah widget peta hierarki dengan dua tingkat detail yang dapat diaktifkan dengan diperinci.
  - Tingkat mesin
    Menampilkan ringkasan informasi tentang status disk semua mesin di unit organisasi yang 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
- Akan membaik

- **Status kesehatan disk** adalah widget diagram lingkaran yang menunjukkan jumlah disk untuk setiap status.



Peringatan status kesehatan disk

Pemeriksaan kesehatan disk berjalan setiap 30 menit, sedangkan peringatan terkait dihasilkan satu kali sehari. Saat status kesehatan disk berubah dari **Peringatan** ke **Kritis**, peringatan akan selalu 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 <disk name> pada mesin ini berada dalam status kritis dan kemungkinan besar akan gagal dalam waktu dekat. Pencadangan profil disk ini tidak disarankan pada titik ini karena tambahan tekanan dapat menyebabkan disk gagal. Segera cadangkan semua file terpenting pada disk ini lalu ganti disk.

Peta perlindungan data

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 semua file penting yang dimiliki unit/mesin organisasi.

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.

Hasil pemeriksaan perlindungan data dapat ditemukan di dasbor, di widget Peta Perlindungan Data, suatu widget peta pohon yang menunjukkan detail pada tingkat mesin.

Arahkan pointer mouse ke blok berwarna untuk melihat informasi lebih lanjut tentang jumlah file yang tidak terlindungi dan lokasinya. Untuk melindungi file-file tersebut, klik **Lindungi semua file**.

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
- 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.

- **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 berdasarkan status instalasinya.

Riwayat instalasi patch

Widget ini menampilkan informasi detail tentang patch yang diinstal pada mesin.

Pembaruan yang tidak ada berdasarkan kategori

Widget ini menampilkan jumlah pembaruan yang tidak ada per kategori. Kategori berikut ini ditampilkan:

- Pembaruan keamanan
- Pembaruan penting
- Lain

Detail pemindaian cadangan

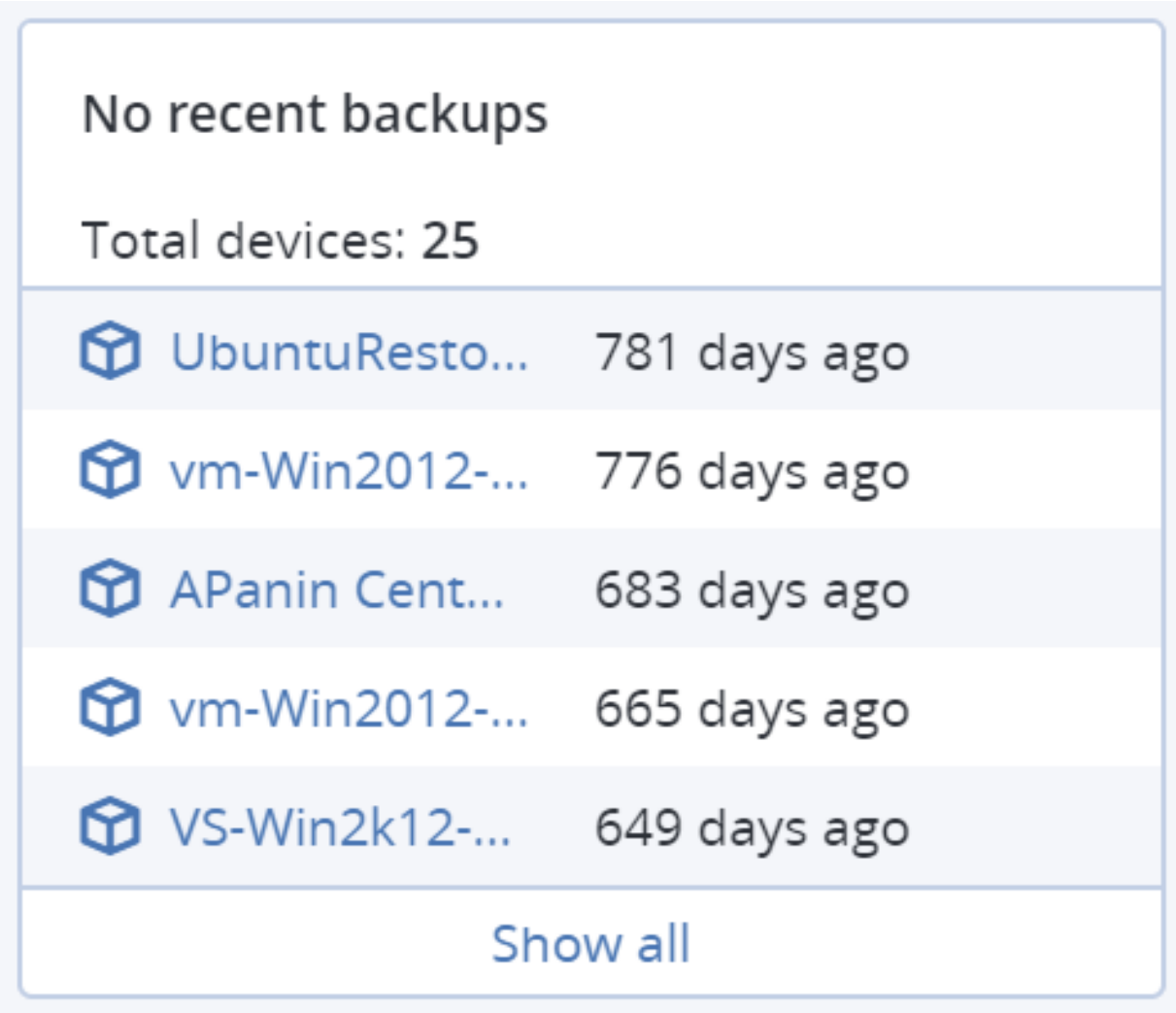
Widget ini tersedia hanya jika Layanan Pemindaian diinstal pada server manajemen. Widget ini menampilkan informasi detail tentang ancaman yang terdeteksi di cadangan.

Baru-baru ini terdampak

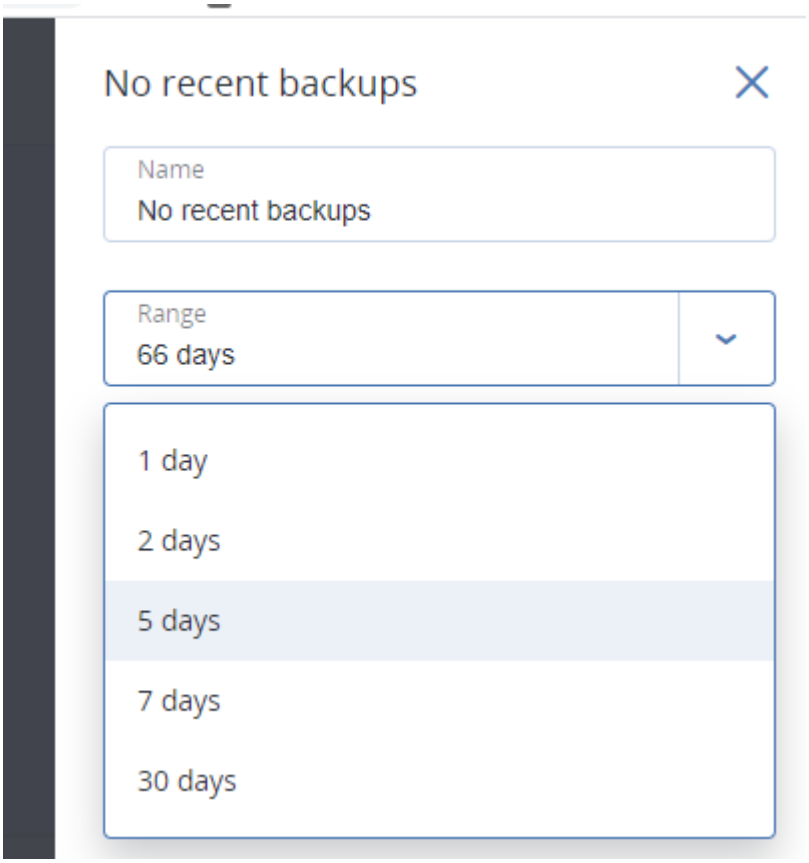
Widget ini menampilkan informasi detail tentang mesin yang baru-baru ini terdampak. Di sini, Anda dapat menemukan informasi tentang ancaman apa yang terdeteksi dan berapa file yang terinfeksi.

Tidak ada cadangan terkini

Widget ini menampilkan beban kerja dengan penerapan rencana proteksi, yang tanggal pencadangan terakhirnya yang berhasil adalah lebih awal dari rentang waktu yang ditentukan dalam pengaturan widget.



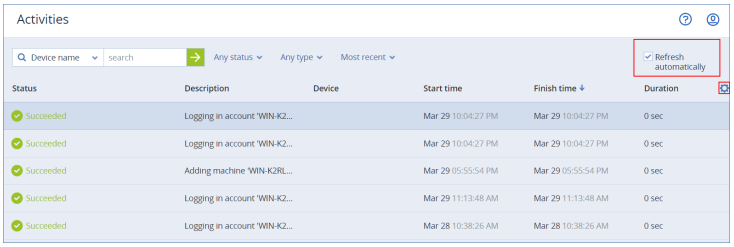
Secara default, saat Anda menambahkan widget ini, widget menampilkan informasi 5 hari terakhir. Anda dapat menggunakan menu drop-down untuk memilih periode lain atau memasukkan jumlah hari secara manual. Jumlah maksimum hari yang dapat Anda masukkan adalah 180.



Tab Aktivitas

Tab **Aktivitas** memberikan gambaran umum tentang aktivitas selama 90 hari terakhir.

Untuk menyesuaikan tampilan tab **Aktivitas**, klik ikon roda gigi dan pilih kolom yang ingin Anda lihat. Untuk melihat kemajuan aktivitas secara real time, pilih kotak centang **Refresh otomatis**. Perhatikan bahwa seringnya memperbarui beberapa aktivitas dapat menurunkan kinerja server manajemen.



Anda dapat mencari aktivitas yang terdaftar dengan kriteria berikut:

- **Nama perangkat**
  Ini adalah mesin tempat aktivitas dilaksanakan.
- **Dimulai oleh**
  Ini adalah akun yang memulai aktivitas.

Anda juga dapat menyaring dengan properti berikut:

- **Status**
  Misalnya, berhasil, gagal, sedang berlangsung, atau 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 mengubah periode retensi default, edit file konfigurasi task_manager.yaml.

Untuk mengubah periode retensi

1. Di mesin yang menjalankan server manajemen, buka file konfigurasi berikut di editor teks:
   - Di Windows: `%Program Files%\Acronis\TaskManager\task_manager.yaml`
   - Di Linux: `/usr/lib/Acronis/TaskManager/task_manager.yaml`
2. Temukan bagian berikut:

   ```
   database:
     connection-string: ""
     run-cleanup-at: "23:59"
     cleanup-batch-size: 10
     max-cleanup-retries: 10
     log-queries: false
     max-transaction-retries: 10
     shards:
      - connection-string: sqlite://task-manager.sqlite
        days-to-keep: 90
        space: "default"
        key: "00000000-0000-0000-0000-000000000000"
   ```

3. Edit baris `days-to-keep` sesuai keinginan.
   Contoh:

   ```
   days-to-keep: 30
   ```

   Catatan
   Anda dapat mengubah periode retensi sesuai dengan kebutuhan Anda. Meningkatkan periode retensi akan menurunkan kinerja server manajemen.

4. Mulai ulang **Layanan Acronis Service Manager** seperti yang dijelaskan di "Untuk memulai ulang Layanan Acronis Service Manager" (hlm. 197).

Laporan

Anda dapat menggunakan laporan yang telah ditetapkan atau membuat laporan kustom. Laporan dapat mencakup set widget dasbor apa pun.

Anda hanya dapat mengonfigurasi laporan untuk unit yang Anda kelola.

Laporan dapat dikirim melalui email atau diunduh sesuai jadwal. Untuk mengirim laporan melalui email, pastikan bahwa pengaturan **Server email** sudah dikonfigurasi. Jika Anda ingin memproses laporan menggunakan perangkat lunak pihak ketiga, jadwalkan simpan laporan dalam format .xlsx ke folder yang ditentukan.

Laporan yang tersedia bergantung pada edisi Cyber Protect Anda. Laporan default tercantum di bawah ini:

Nama laporan	Ketersediaan	Deskripsi
Peringatan	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan peringatan yang terjadi selama periode waktu tertentu.
Detail pemindaian cadangan	Cyber Protect Advanced	Menampilkan informasi detail tentang ancaman yang terdeteksi di cadangan.
Cadangan	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan detail tentang cadangan saat ini dan titik pemulihan.
Status saat ini	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan status lingkungan Anda saat ini.
Aktivitas sehari-hari	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan ringkasan tentang kegiatan yang dilakukan selama periode waktu tertentu.
Peta perlindungan data	Cyber Protect Advanced	Menampilkan informasi mendetail tentang jumlah, ukuran, lokasi, dan status proteksi semua file penting di mesin.
Ancaman terdeteksi	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan detail tentang mesin yang terpengaruh berdasarkan jumlah ancaman yang diblokir, dan informasi tentang mesin yang sehat dan rentan.
Mesin yang ditemukan	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan semua mesin yang ditemukan di jaringan organisasi.

Prediksi kesehatan disk	Cyber Protect Advanced	Menampilkan prediksi tentang kapan HDD/SSD Anda akan rusak, dan status disk saat ini.
Kerentanan yang ada	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan kerentanan yang ada untuk sistem operasi dan aplikasi dalam lingkungan Anda, dan mesin yang terdampak.
Lisensi	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan rangkuman lisensi yang tersedia.
Lokasi	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan statistik penggunaan untuk lokasi cadangan, untuk periode waktu tertentu.
Rangkuman manajemen patch	Cyber Protect Advanced	Menampilkan jumlah patch yang tidak ada, patch yang diinstal, dan patch yang diterapkan. Anda dapat memperinci laporan untuk mendapatkan informasi patch yang hilang/diinstal dan detail tentang semua sistem.
Ringkasan	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan ringkasan perangkat yang dilindungi, untuk periode waktu tertentu.
Aktivitas pita	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan daftar pita yang digunakan selama 24 jam terakhir.
Aktivitas mingguan	Cyber Backup Lanjutan Cyber Protect Advanced	Menampilkan ringkasan aktivitas yang dilakukan selama periode waktu tertentu.

Operasi dasar dengan laporan

- Untuk menampilkan laporan, klik namanya.
- Untuk operasi tambahan dengan laporan, klik ikon elipsis (...).
  Operasi yang sama tersedia dari dalam laporan.

Untuk menambahkan laporan

1. Klik **Tambah laporan**.
2. Lakukan salah satu langkah berikut:
   - Untuk menambahkan laporan yang telah ditetapkan, klik namanya.
   - Untuk menambahkan laporan kustom, klik **Kustom**. Laporan baru dengan nama **Kustom** ditambahkan ke daftar laporan. Buka laporan ini dan tambahkan widget ke laporan.
3. [Opsional] Seret dan lepas widget untuk menyusunnya kembali.
4. [Opsional] Edit laporan seperti yang dijelaskan di bawah ini.

Untuk mengedit laporan

1. Klik ikon elipsis (...) di samping nama laporan, lalu klik **Pengaturan**.
2. Edit laporan. Anda dapat:
   - Mengganti nama laporan
   - Mengubah rentang waktu untuk semua widget yang disertakan dalam laporan
   - Menjadwalkan pengiriman laporan melalui email dalam format .pdf atau/dan .xlsx
3. Klik **Simpan**.

Untuk menjadwalkan laporan

1. Pilih laporan, lalu klik **Jadwal**.
2. Aktifkan switch **Kirim laporan terjadwal**.
3. Pilih apakah akan mengirim laporan melalui email, menyimpannya ke folder, atau keduanya. Tergantung pada pilihan Anda, tentukan alamat email, jalur folder, atau keduanya.
4. Pilih format laporan: .pdf, .xlsx, atau keduanya.
5. Pilih periode pelaporan: 1 hari, 7 hari, atau 30 hari.
6. Pilih hari dan waktu kapan laporan akan dikirim atau disimpan.
7. Klik **Simpan**.

Mengekspor dan mengimpor struktur laporan

Anda dapat mengekspor dan mengimpor struktur laporan (set widget dan pengaturan jadwal) ke file.json. Hal ini mungkin berguna apabila terjadi instalasi ulang server manajemen atau untuk menyalin struktur laporan ke server manajemen yang berbeda.

Untuk mengekspor struktur laporan, pilih laporan, lalu klik **Ekspor**.

Untuk mengimpor struktur laporan, klik **Buat laporan**, lalu klik **Impor**.

Membuang data laporan

Anda dapat menyimpan buangan data laporan ke file.csv. Buangan mencakup semua data laporan (tanpa pemfilteran) untuk rentang waktu kustom.

Perangkat lunak menghasilkan buangan data pada saat memproses. Jika Anda menetapkan jangka waktu yang lama, tindakan ini mungkin memerlukan waktu lama.

Untuk membuang data laporan

1. Pilih laporan, lalu klik **Buka**.
2. Klik ikon elipsis (...) di sudut kanan atas, lalu klik **Buang data**.
3. Di **Lokasi**, tentukan jalur folder untuk file.csv.
4. Di **Rentang waktu**, tentukan rentang waktunya.
5. Klik **Simpan**.

Mengonfigurasi tingkat keparahan peringatan

Peringatan adalah pesan yang memperingatkan tentang masalah aktual atau potensial. Anda dapat menggunakan peringatan dengan berbagai cara:

- Bagian **Peringatan** dari tab **Ikhtisar** memungkinkan Anda untuk dengan cepat mengidentifikasi dan memecahkan masalah dengan memantau peringatan saat ini.
- Pada **Perangkat**, status perangkat berasal dari peringatan. Kolom **Status** memungkinkan Anda untuk memfilter perangkat yang bermasalah.
- Saat mengonfigurasi notifikasi email, Anda dapat memilih peringatan mana yang akan memicu notifikasi.

Peringatan dapat memiliki salah satu tingkat keparahan berikut:

- **Kritis**
- **Eror**
- **Peringatan**

Anda dapat mengubah tingkat keparahan peringatan atau sepenuhnya menonaktifkan peringatan menggunakan file konfigurasi peringatan seperti yang dijelaskan di bawah ini. Operasi ini mengharuskan server manajemen untuk dimulai ulang.

Mengubah tingkat keparahan peringatan tidak akan memengaruhi peringatan yang sudah dibuat.

File konfigurasi peringatan

File konfigurasi berada di mesin yang menjalankan server manajemen.

- Di Windows: `<installation_path>`**\AlertManager\alert_manager.yaml**
  Di sini, `<installation_path>` adalah jalur instalasi server manajemen. Secara default, direktorinya adalah **%ProgramFiles%\Acronis** .
- Di Linux: **/usr/lib/Acronis/AlertManager/alert_manager.yaml**

File ini disusun sebagai dokumen YAML. Setiap peringatan adalah elemen dalam daftar `alertTypes`.

Kunci `nama` mengidentifikasi peringatan.

Kunci `keparahan` menentukan tingkat keparahan peringatan. Tingkat keparahan harus memiliki salah satu dari nilai berikut: `kritis`, `kesalahan`, atau `peringatan`.

Kunci `diaktifkan` opsional menentukan apakah peringatan diaktifkan atau dinonaktifkan. Nilainya harus `true` atau `false`. Secara default (tanpa kunci ini) semua peringatan diaktifkan.

Untuk mengubah tingkat keparahan atau menonaktifkan peringatan

1. Pada mesin tempat server manajemen diinstal, buka file **alert_manager.yaml** dalam editor teks.
2. Cari peringatan yang ingin Anda ubah atau nonaktifkan.
3. Lakukan salah satu langkah berikut:
   - Untuk mengubah tingkat keparahan peringatan, ubah nilai kunci `keparahan`.
   - Untuk menonaktifkan peringatan, tambahkan kunci `diaktifkan`, lalu tetapkan nilainya ke `false`.
4. Simpan file.
5. Mulai ulang layanan server manajemen seperti dijelaskan di bawah ini.

Untuk memulai ulang layanan server manajemen di Windows

1. Pada menu **Start**, klik **Run**, lalu ketik: **cmd**
2. Klik **OK**.
3. Jalankan perintah berikut:

```
net stop acrmngsrv
net start acrmngsrv
```

Untuk memulai ulang layanan server manajemen di Linux

1. **Terminal** Terbuka.
2. Jalankan perintah berikut di direktori mana pun:

```
sudo service acronis_ams restart
```

Opsi penyimpanan lanjutan

Alat rekaman

Bagian berikut menjelaskan secara terperinci cara menggunakan perangkat pita untuk menyimpan cadangan.

Apa itu perangkat pita?

Perangkat pita adalah istilah generik yang berarti pustaka pita atau drive pita yang berdiri sendiri.

Pustaka pita (pustaka robotik) adalah perangkat penyimpanan berkapasitas tinggi yang berisi:

- satu atau beberapa drive pita
- beberapa (hingga beberapa ribu) slot untuk menampung pita
- satu atau beberapa pengubah (mekanisme robotik) yang ditujukan untuk memindahkan pita antara slot dan drive pita.

Dapat juga berisi komponen lain seperti pembaca barcode atau printer barcode.

Autoloader adalah kotak khusus dari perpustakaan pita. Autooader berisi satu drive, beberapa slot, pengubah dan pembaca barcode (opsional).

Driver pita yang berdiri sendiri (juga disebut **streamer**) berisi satu slot dan hanya dapat menampung satu pita pada satu waktu.

Ikhtisar dukungan pita

Agen perlindungan dapat mencadangkan data ke alat rekaman secara langsung atau melalui simpul penyimpanan. Dalam kedua kasus, operasi sepenuhnya otomatis dari perangkat pita dapat dipastikan. Ketika perangkat pita dengan beberapa drive terpasang ke simpul penyimpanan, beberapa agen akan secara bersamaan mencadangkan ke pita.

Kompatibilitas dengan RSM dan perangkat lunak pihak ketiga

Koeksistensi dengan perangkat lunak pihak ketiga

Tidak dimungkinkan untuk bekerja dengan pita pada mesin di mana perangkat lunak pihak ketiga dengan alat manajemen pita eksklusif diinstal. Untuk menggunakan pita pada mesin seperti itu, Anda harus menghapus instalasi atau menonaktifkan perangkat lunak manajemen pita pihak ketiga.

Interaksi dengan Windows Removable Storage Manager (RSM)

Agen perlindungan dan simpul penyimpanan tidak menggunakan RSM. Ketika mendeteksi perangkat pita, mereka akan menonaktifkan perangkat dari RSM (kecuali jika sedang digunakan oleh perangkat lunak lain). Selama Anda ingin bekerja dengan perangkat pita, pastikan pengguna

maupun perangkat lunak pihak ketiga tidak mengaktifkan perangkat di RSM. Jika perangkat pita diaktifkan di RSM, ulangi deteksi perangkat pita.

Perangkat keras yang didukung

Acronis Cyber Protect mendukung perangkat SCSI eksternal. Ini adalah perangkat yang terhubung ke Fibre Channel atau menggunakan antarmuka SCSI, iSCSI, Serial Attached SCSI (SAS). Acronis Cyber Protect juga mendukung perangkat pita yang tersambung ke USB.

Di Windows, Acronis Cyber Protect dapat mencadangkan ke alat rekaman meskipun driver untuk pengubah perangkat tidak diinstal. Perangkat pita seperti itu ditunjukkan dalam **Manajer Perangkat** sebagai **Pengubah Media yang Tidak Dikenal**. Namun, driver untuk drive perangkat harus diinstal. Di Linux dan di bawah media yang dapat di-boot, tidak dimungkinkan untuk mencadangkan ke perangkat pita tanpa driver.

Pengenalan perangkat IDE atau SATA yang terhubung tidak dijamin. Hal tersebut tergantung apakah driver yang tepat telah diinstal di sistem operasi.

Untuk mengetahui apakah perangkat spesifik Anda didukung, gunakan Alat Kompatibilitas Perangkat Keras seperti yang dijelaskan pada http://kb.acronis.com/content/57237. Anda dapat mengirim laporan tentang hasil pengujian ke Acronis. Perangkat keras dengan dukungan yang dikonfirmasi dapat dilihat dalam Daftar Kompatibilitas Perangkat Keras: https://go.acronis.com/acronis-cyber-protect-advanced-tape-hcl.

Database manajemen pita

Informasi tentang semua perangkat pita yang terpasang pada mesin disimpan dalam database manajemen pita. Jalur database defaultnya adalah sebagai berikut:

- Di Windows XP/Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database`.
- Di Windows 7 dan versi Windows yang lebih baru: `%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database`.
- Di Linux: `/var/lib/Acronis/BackupAndRecovery/ARSM/Database`.

Ukuran database bergantung pada jumlah cadangan yang disimpan pada pita dan sama dengan sekitar 10 MB per seratus cadangan. Ukuran database mungkin akan besar jika pustaka pita berisi ribuan cadangan. Dalam kasus ini, Anda mungkin perlu menyimpan database pita di volume yang berbeda.

Untuk memindahkan database di Windows:

1. Hentikan layanan Removable Storage Management.
2. Pindahkan semua file dari lokasi default ke lokasi baru.
3. Temukan kunci registri `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings`.
4. Tentukan jalur lokasi baru dalam nilai registri `ArsmDmlDbProtocol`. String dapat berisi hingga

32765 karakter.

5. Mulai layanan Removable Storage Management.

Untuk merelokasi database di Linux:

1. Hentikan layanan `acronis_rsm`.
2. Pindahkan semua file dari lokasi default ke lokasi baru.
3. Buka file konfigurasi `/etc/Acronis/ARSM.config` di editor teks.
4. Temukan baris `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Ubah jalur di bawah baris tersebut.
6. Simpan file.
7. Mulai layanan `acronis_rsm`.

Folder TapeLocation

Folder `TapeLocation` berisi cache metadata sistem file dari semua volume yang dicadangkan pada tape.

Jalur folder `TapeLocation` default adalah:

- Di Windows XP/Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation`
- Di Windows 7 dan versi Windows yang lebih baru: `%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation`
- Di Linux: `/var/lib/Acronis/BackupAndRecovery/TapeLocation`

Ukuran folder `TapeLocation` sekitar 0,5-1% kali ukuran semua cadangan yang disimpan di tape. Untuk cadangan tingkat disk dengan opsi pemulihan file diaktifkan, ukuran folder `TapeLocation` mungkin sedikit lebih besar, bergantung pada jumlah file yang dicadangkan.

Parameter untuk menulis ke pita

Parameter penulisan pita (ukuran blok dan ukuran cache) memungkinkan Anda untuk menyetel perangkat lunak agar mencapai performa maksimum. Kedua parameter diperlukan untuk menulis ke pita, tetapi biasanya Anda hanya perlu menyesuaikan ukuran blok. Nilai optimal tergantung pada jenis perangkat pita dan pada data yang dicadangkan, seperti jumlah file dan ukurannya.

Catatan
Ketika perangkat lunak membaca dari pita, perangkat lunak tersebut akan menggunakan ukuran blok yang sama dengan yang digunakan saat menulis ke pita. Jika perangkat pita tidak mendukung ukuran blok ini, pembacaan akan gagal.

Parameter ditetapkan pada setiap mesin yang memiliki perangkat pita terpasang. Perangkat ini dapat menjadi mesin tempat agen atau simpul penyimpanan diinstal. Pada mesin yang

menjalankan Windows, konfigurasi dilakukan di registri; pada mesin Linux, konfigurasi dilakukan dalam file konfigurasi **/etc/Acronis/BackupAndRecovery.config**.

Di Windows, buat masing-masing kunci registri dan nilai DWORD-nya. Di Linux, tambahkan teks berikut di akhir file konfigurasi, tepat sebelum tag `</registry>`:

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Dword">
          "value"
     </value>
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
</key>
```

DefaultBlockSize

Ini adalah ukuran blok (dalam byte) yang digunakan saat menulis ke pita.

Nilai yang dimungkinkan: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576.

Jika nilainya 0 atau jika parameter tidak ada, ukuran blok akan ditentukan sebagai berikut:

- Di Windows, nilainya diambil dari driver perangkat pita.
- Di Linux, nilainya adalah **64 KB**.

Kunci registri (pada mesin yang menjalankan Windows): **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize**

Baris di /etc/Acronis/BackupAndRecovery.config (pada mesin yang menjalankan Linux):

```
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
```

Jika nilai yang ditentukan tidak diterima oleh tape drive, perangkat lunak akan membaginya dengan kelipatan dua hingga nilai yang berlaku tercapai atau nilai mencapai 32 byte. Jika nilai yang berlaku tidak ditemukan, perangkat lunak akan mengalikan nilai yang ditentukan dengan kelipatan dua hingga nilai yang berlaku tercapai atau nilai mencapai 1 MB. Jika tidak ada nilai yang diterima oleh drive, pencadangan akan gagal.

WriteCacheSize

Ini adalah ukuran buffer (dalam byte) yang digunakan saat menulis ke pita.

Nilai yang dimungkinkan: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, tetapi tidak kurang dari nilai parameter **DefaultBlockSize**.

Jika nilainya 0 atau jika parameter tidak ada, ukuran buffer-nya adalah **1 MB**. Jika sistem operasi tidak mendukung nilai ini, perangkat lunak akan membaginya dengan kelipatan dua hingga nilai yang berlaku ditemukan atau nilai parameter **DefaultBlockSize** tercapai. Jika nilai yang didukung oleh sistem operasi tidak ditemukan, pencadangan gagal.

Kunci registri (pada mesin yang menjalankan Windows):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize

Baris di /etc/Acronis/BackupAndRecovery.config (pada mesin yang menjalankan Linux):

```
<value name="WriteCacheSize" type="Dword">
     "value"
</value>
```

Jika Anda menentukan nilai selain nol yang tidak didukung oleh sistem operasi, pencadangan akan gagal.

Opsi pencadangan terkait pita

Anda dapat mengonfigurasi opsi pencadangan **Manajemen pita** untuk menentukan:

- Apakah akan mengaktifkan pemulihan file dari cadangan level disk yang disimpan pada pita.
- Apakah akan mengembalikan pita kembali ke slot setelah rencana proteksi selesai.
- Apakah akan mengeluarkan pita setelah pencadangan selesai.
- Apakah akan menggunakan pita bebas untuk setiap pencadangan penuh.
- Apakah akan menimpa pita saat membuat cadangan penuh (hanya untuk drive pita yang berdiri sendiri).
- Apakah akan menggunakan set pita untuk membedakan pita yang digunakan, misalnya, untuk cadangan yang dibuat pada hari yang berbeda dalam seminggu atau untuk cadangan dari jenis mesin yang berbeda.

Operasi paralel

Acronis Cyber Protect dapat secara bersamaan melakukan operasi dengan berbagai komponen alat rekaman. Selama operasi yang menggunakan drive (mencadangkan, memulihkan, memindai ulang, atau menghapus), Anda dapat meluncurkan operasi yang menggunakan pengubah (memindahkan pita ke slot lain atau mengeluarkan pita) dan sebaliknya. Jika pustaka pita Anda memiliki lebih dari satu drive, Anda juga dapat meluncurkan operasi yang menggunakan salah satu drive selama operasi dengan drive lain. Misalnya, beberapa mesin dapat mencadangkan atau memulihkan secara bersamaan menggunakan drive yang berbeda dari pustaka pita yang sama.

Operasi mendeteksi perangkat pita baru dapat dilakukan bersamaan dengan operasi lainnya. Selama inventarisasi, tidak ada operasi lain yang tersedia kecuali untuk mendeteksi perangkat pita baru.

Operasi yang tidak dapat dilakukan secara paralel akan diantrekan.

Pembatasan

Batasan penggunaan perangkat pita adalah sebagai berikut:

1. Perangkat pita tidak didukung ketika mesin di-boot dari media yang dapat di-boot berbasis Linux 32-bit.
2. Anda tidak dapat mencadangkan jenis data berikut untuk ke pita: Kotak surat Microsoft 365, kotak surat Microsoft Exchange.
3. Anda tidak dapat membuat cadangan keberadaan aplikasi mesin fisik dan virtual.
4. Di macOS, yang didukung hanya pencadangan level file ke lokasi berbasis pita yang dikelola.
5. Konsolidasi cadangan yang terletak di pita tidak dimungkinkan. Hasilnya, skema pencadangan **Selalu inkremental** tidak tersedia saat Anda mencadangkan ke pita.
6. Deduplikasi cadangan yang berada di pita tidak dimungkinkan.
7. Perangkat lunak tidak dapat secara otomatis menimpa pita yang berisi cadangan yang tidak dihapus atau jika ada cadangan dependen pada pita lain.

   Satu-satunya pengecualian untuk aturan ini adalah ketika opsi "Timpa rekaman di tape drive mandiri saat membuat cadangan penuh" diaktifkan.
8. Anda tidak dapat memulihkan pada sistem operasi dari cadangan yang disimpan di pita jika pemulihan mengharuskan reboot sistem operasi. Gunakan media yang dapat di-boot untuk melakukan pemulihan tersebut.
9. Anda dapat memvalidasi cadangan apa pun yang disimpan pada pita, tetapi Anda tidak dapat memilih untuk memvalidasi seluruh lokasi atau perangkat berbasis pita.
10. Lokasi berbasis pita yang dikelola tidak dapat dilindungi dengan enkripsi. Namun, Anda dapat melakukan enkripsi cadangan.
11. Perangkat lunak tidak dapat secara bersamaan menulis satu cadangan ke beberapa pita atau beberapa cadangan melalui drive yang sama ke pita yang sama.
12. Perangkat yang menggunakan Network Data Management Protocol (NDMP) tidak didukung.
13. Printer barcode tidak didukung.
14. Pita berformat Linear Tape File System (LTFS) tidak didukung.

Keterbacaan pita yang ditulis oleh produk Acronis versi lama

Tabel berikut merangkum keterbacaan pita yang ditulis oleh rangkaian produk Acronis True Image Echo, Acronis True Image 9.1, Acronis Backup & Recovery 10, Acronis Backup & Recovery 11, Acronis Backup 11.5, 11.7, dan 12.5 di Acronis Cyber Protect. Tabel tersebut juga menjelaskan kompatibilitas pita yang ditulis oleh berbagai komponen Acronis Cyber Protect.

Anda dapat menambahkan cadangan bertahap dan diferensial ke cadangan yang dipindai ulang yang dibuat oleh Acronis Backup 11.5, 11.7, dan 12.5.

	...dapat dibaca pada alat rekaman yang terpasang pada mesin dengan...

			Acronis Cyber Protect Media yang Dapat Di-Boot	Agen Acronis Cyber Protect untuk Windows	Agen Acronis Cyber Protect untuk Linux	Acronis Cyber Protect Simpul Penyimpanan
Pita yang ditulis pada perangkat pita yang terpasang secara lokal (drive pita atau pustaka pita) oleh...	Media yang dapat di-boot	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
	Agen untuk Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
	Agen untuk Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-

Pita yang ditulis pada alat rekaman melalui...	Server Pencadangan	9.1	-	-	-	-
		Echo	-	-	-	-
	Simpul Penyimpanan	ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	+

Memulai dengan perangkat pita

Mencadangkan mesin ke perangkat pita yang terpasang secara lokal

Prasyarat

- Perangkat pita terpasang ke mesin sesuai dengan instruksi produsen.
- Agen perlindungan diinstal pada mesin.

Sebelum mencadangkan

1. Muat pita ke perangkat pita.
2. Masuk ke konsol web Cyber Protect.
3. Pada **Pengaturan** > **Manajemen pita**, perluas simpul mesin, lalu klik **Perangkat pita**.
4. Pastikan perangkat pita yang terpasang ditampilkan. Jika tidak, klik **Deteksi perangkat**.
5. Lakukan inventaris pita:
   a. Klik nama perangkat pita.
   b. Klik **Inventaris** untuk mendeteksi pita yang dimuat. Biarkan **Inventaris penuh** dihidupkan. Jangan menghidupkan **Pindahkan pita yang tidak dikenal atau yang diimpor ke pool 'Pita bebas'**. Klik **Mulai inventarisasi sekarang**.
   Hasil. Pita yang dimuat telah dipindahkan ke pool yang tepat seperti yang ditentukan dalam bagian "Inventarisasi".

   Catatan
   Inventarisasi penuh untuk seluruh perangkat pita mungkin membutuhkan waktu yang cukup lama.

   c. Jika pita yang dimuat dikirim ke **Pita yang tidak dikenal** atau **Pita yang diimpor** dan Anda ingin menggunakannya untuk mencadangkan, pindah pita tersebut ke pool **Pita bebas** secara manual.

Catatan
Pita yang dikirim ke pool **Pita yang diimpor** berisi cadangan yang ditulis oleh perangkat lunak Acronis. Sebelum memindahkan pita tersebut ke pool **Pita bebas**, pastikan Anda sudah tidak memerlukan cadangan ini.

Mencadangkan

Buat rencana proteksi seperti yang dijelaskan di bagian "Cadangan". Saat menentukan lokasi pencadangan, pilih **Pool pita 'Acronis'**.

Hasil

- Untuk mengakses lokasi tempat cadangan akan dibuat, klik **Penyimpanan cadangan** > **Pool pita 'Acronis'**.
- Pita dengan cadangan akan dipindahkan ke pool **Acronis**.

Mencadangkan ke perangkat pita yang terpasang pada simpul penyimpanan

Prasyarat

- Simpul penyimpanan terdaftar di server manajemen.
- Perangkat pita terpasang ke simpul penyimpanan sesuai dengan instruksi produsen.

Sebelum mencadangkan

1. Muat pita ke perangkat pita.
2. Masuk ke konsol web Cyber Protect.
3. Klik **Pengaturan** > **Manajemen pita**, perluas simpul dengan nama simpul penyimpanan, lalu klik **Perangkat pita**.
4. Pastikan perangkat pita yang terpasang ditampilkan. Jika tidak, klik **Deteksi perangkat**.
5. Lakukan inventaris pita:
   a. Klik nama perangkat pita.
   b. Klik **Inventaris** untuk mendeteksi pita yang dimuat. Biarkan **Inventaris penuh** dihidupkan. Jangan menghidupkan **Pindahkan pool pita yang tidak dikenal atau yang diimpor ke pool 'Pita bebas'**. Klik **Mulai inventarisasi sekarang**.
   Hasil. Pita yang dimuat telah dipindahkan ke pool yang tepat seperti yang ditentukan dalam bagian "Inventarisasi".

Catatan
Inventarisasi penuh untuk seluruh perangkat pita mungkin membutuhkan waktu yang cukup lama.

c. Jika pita yang dimuat dikirim ke **Pita yang tidak dikenal** atau **Pita yang diimpor** dan Anda ingin menggunakannya untuk mencadangkan, pindah pita tersebut ke pool **Pita bebas** secara manual.

> **Catatan**
> Pita yang dikirim ke pool **Pita yang diimpor** berisi cadangan yang ditulis oleh perangkat lunak Acronis. Sebelum memindahkan pita tersebut ke pool **Pita bebas**, pastikan Anda sudah tidak memerlukan cadangan ini.

d. Putuskan apakah Anda ingin mencadangkan ke pool **Acronis** atau ke buat pool baru.

Detail. Dengan memiliki beberapa pool, Anda dimungkinkan untuk menggunakan set pita terpisah untuk setiap mesin atau setiap departemen di perusahaan Anda. Dengan menggunakan beberapa pool, Anda dapat mencegah cadangan yang dibuat melalui rencana proteksi berbeda agar tidak tercampur dalam satu pita.

e. Jika pool yang dipilih dapat mengambil pita dari pool **Pita bebas** bila diperlukan, lewati langkah ini.

Jika tidak, pindahkan pita dari pool **Pita bebas** ke pool yang dipilih.

Tips. Untuk mengetahui apakah suatu pool dapat mengambil pita dari pool **Pita bebas**, klik pool tersebut lalu klik **Info**.

Mencadangkan

Buat rencana proteksi seperti yang dijelaskan di bagian "Cadangan". Saat menentukan lokasi pencadangan, pilih pool pita yang dibuat.

Hasil

- Untuk mengakses lokasi tempat cadangan akan dibuat, klik **Cadangan**, lalu klik nama pool pita yang dibuat.
- Pita dengan cadangan akan dipindahkan ke pool yang dipilih.

Tips untuk penggunaan pustaka pita lebih lanjut

- Anda tidak perlu melakukan inventarisasi penuh setiap kali Anda memuat pita baru. Untuk menghemat waktu, ikuti prosedur yang dijelaskan dalam "Inventarisasi" pada "Kombinasi inventaris cepat dan penuh".
- Anda dapat membuat pool lain di pustaka pita yang sama dan memilih salah satu darinya sebagai tujuan untuk pencadangan.

Pemulihan di bawah sistem operasi dari perangkat pita

Untuk memulihkan di bawah sistem operasi dari perangkat pita:

1. Masuk ke konsol web Cyber Protect.
2. Klik **Perangkat**, lalu pilih mesin yang dicadangkan.

3. Klik **Pemulihan**.
4. Pilih titik pemulihan. Perlu dicatat bahwa titik pemulihan difilter berdasarkan lokasi.
5. Perangkat lunak ini menunjukkan daftar pita yang diperlukan untuk pemulihan. Pita yang tidak ditemukan akan berwarna abu-abu. Jika perangkat pita Anda memiliki slot kosong, masukkan pita ini ke dalam perangkat.
6. Konfigurasi pengaturan pemulihan lainnya.
7. Klik **Mulai pemulihan** untuk memulai operasi pemulihan.
8. Jika salah satu pita yang diperlukan tidak dimuat karena alasan tertentu, perangkat lunak akan menampilkan pesan dengan pengidentifikasi pita yang dibutuhkan. Lakukan langkah berikut:
   a. Muat pita.
   b. Lakukan inventarisasi cepat.
   c. Klik **Ikhtisar** > **Aktivitas**, lalu klik aktivitas pemulihan dengan status **Interaksi diperlukan**.
   d. Klik **Tampilkan detail**, lalu klik **Coba lagi** untuk melanjutkan pemulihan.

Bagaimana jika saya tidak melihat cadangan yang tersimpan di pita?

Hal ini mungkin menunjukkan bahwa database dengan konten pita hilang atau rusak karena suatu alasan.

Untuk memulihkan database, lakukan langkah berikut:

1. Lakukan inventarisasi cepat.

   Peringatan!
   Selama inventarisasi, *jangan* hidupkan **Pindahkan pita yang tidak dikenal dan diimpor ke pool 'Pita bebas'**. Jika switch dihidupkan, Anda dapat kehilangan semua cadangan.

2. Pindai ulang pool **Pita yang tidak dikenal**. Hasilnya, Anda akan mendapatkan konten dari pita yang dimuat.
3. Jika salah satu cadangan yang terdeteksi melanjutkan pada pita lain yang belum dipindai ulang, muat pita ini seperti yang diminta, lalu pindai ulang.

Pemulihan di bawah media yang dapat di-boot dari perangkat pita yang terpasang secara lokal

Untuk memulihkan di bawah media yang dapat di-boot dari perangkat pita yang terpasang secara lokal:

1. Muat pita yang diperlukan untuk pemulihan ke perangkat pita.
2. Boot mesin dari media yang dapat di-boot.
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 perangkat pita terhubung menggunakan antarmuka iSCSI, konfigurasikan perangkat seperti yang dijelaskan dalam "Mengonfigurasi perangkat iSCSI dan NDAS".
5. Klik **Manajemen pita**.
6. Klik **Inventaris**.
7. Pada **Objek yang akan diinventarisasi**, pilih perangkat pita.
8. Klik **Mulai** untuk memulai inventarisasi.
9. Setelah inventaris selesai, klik **Tutup**.
10. Klik **Tindakan** > **Pulihkan**.
11. Klik **Pilih data**, lalu klik **Jelajahi**.
12. Perluas **Perangkat pita**, lalu pilih perangkat yang diperlukan. Sistem akan meminta konfirmasi pemindaian ulang. Klik **Ya**.
13. Pilih pool **Pita yang tidak dikenal**.
14. Pilih pita yang akan dipindai ulang. Untuk memilih semua pool pita, pilih kotak centang di sebelah header kolom **Nama pita**.
15. Jika pita berisi cadangan yang dilindungi kata sandi, pilih kotak centang yang sesuai, lalu tentukan kata sandi untuk cadangan di kotak **Kata Sandi**. Jika Anda tidak menentukan kata sandi, atau kata sandi salah, cadangan tidak akan terdeteksi. Harap perhatikan hal ini jika Anda tidak melihat cadangan setelah pemindaian ulang.

    Tips. Jika pita berisi beberapa cadangan yang dilindungi berbagai kata sandi, Anda harus mengulangi pemindaian ulang beberapa kali dengan menetapkan setiap kata sandi secara bergantian.
16. Klik **Mulai** untuk memulai pemindaian ulang. Hasilnya, Anda akan mendapatkan konten dari pita yang dimuat.
17. Jika salah satu cadangan yang terdeteksi melanjutkan pada pita lain yang belum dipindai ulang, muat pita ini seperti yang diminta, lalu pindai ulang.
18. Setelah pemindaian ulang selesai, klik **OK**.
19. Pada **Tampilan arsip**, pilih cadangan yang datanya akan dipulihkan, lalu pilih data yang ingin Anda pulihkan. Setelah Anda mengklik **OK**, halaman **Pulihkan data** akan menampilkan daftar pita yang diperlukan untuk pemulihan. Pita yang tidak ditemukan akan berwarna abu-abu. Jika perangkat pita Anda memiliki slot kosong, masukkan pita ini ke dalam perangkat.
20. Konfigurasi pengaturan pemulihan lainnya.
21. Klik **OK** untuk memulai pemulihan.
22. Jika salah satu pita yang diperlukan tidak dimuat karena alasan tertentu, perangkat lunak akan menampilkan pesan dengan pengidentifikasi pita yang dibutuhkan. Lakukan langkah berikut:
    a. Muat pita.
    b. Lakukan inventarisasi cepat.
    c. Klik **Ikhtisar** > **Aktivitas**, lalu klik aktivitas pemulihan dengan status **Interaksi diperlukan**.
    d. Klik **Tampilkan detail**, lalu klik **Coba lagi** untuk melanjutkan pemulihan.

Memulihkan di bawah media yang dapat di-boot dari perangkat pita yang terpasang ke simpul penyimpanan

Untuk memulihkan di bawah media yang dapat di-boot dari perangkat pita yang terpasang ke simpul penyimpanan:

1. Muat pita yang diperlukan untuk pemulihan ke perangkat pita.
2. Boot mesin dari media yang dapat di-boot.
3. Klik **Kelola mesin ini secara lokal** atau klik **Selamatkan Media yang Dapat Di-Boot** dua kali, tergantung jenis media yang Anda gunakan.
4. Klik **Pulihkan**.
5. Klik **Pilih data**, lalu klik **Jelajahi**.
6. Pada kotak **Jalur**, ketik `bsp://<alamat simpul penyimpanan><nama pool>`, di mana `<alamat simpul penyimpanan>` adalah alamat IP simpul penyimpanan yang berisi cadangan yang diperlukan, dan `<nama pool>` adalah nama pool pita. Klik **OK** dan tentukan kredensial untuk pool.
7. Pilih cadangan, lalu pilih data yang ingin Anda pulihkan. Setelah Anda mengklik **OK**, halaman **Pulihkan data** akan menampilkan daftar pita yang diperlukan untuk pemulihan. Pita yang tidak ditemukan akan berwarna abu-abu. Jika perangkat pita Anda memiliki slot kosong, masukkan pita ini ke dalam perangkat.
8. Konfigurasi pengaturan pemulihan lainnya.
9. Klik **OK** untuk memulai pemulihan.
10. Jika salah satu pita yang diperlukan tidak dimuat karena alasan tertentu, perangkat lunak akan menampilkan pesan dengan pengidentifikasi pita yang dibutuhkan. Lakukan langkah berikut:
    a. Muat pita.
    b. Lakukan inventarisasi cepat.
    c. Klik **Ikhtisar** > **Aktivitas**, lalu klik aktivitas pemulihan dengan status **Interaksi diperlukan**.
    d. Klik **Tampilkan detail**, lalu klik **Coba lagi** untuk melanjutkan pemulihan.

Manajemen pita

Mendeteksi perangkat pita

Saat mendeteksi perangkat pita, perangkat lunak pencadangan akan menemukan perangkat pita yang terpasang ke mesin dan menempatkan informasi tentangnya dalam database manajemen pita. Perangkat pita yang terdeteksi dinonaktifkan dari RSM.

Biasanya, perangkat pita langsung terdeteksi secara otomatis segera terpasang ke mesin dengan produk yang diinstal. Namun Anda mungkin perlu mendeteksi perangkat pita dalam kasus berikut:

- Setelah Anda memasang atau memasang kembali perangkat pita.
- Setelah Anda menginstal atau menginstal ulang perangkat lunak pencadangan pada mesin tempat alat rekaman terpasang.

Untuk mendeteksi perangkat pita

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin tempat perangkat pita terpasang.
3. Klik **Deteksi perangkat**. Anda akan melihat perangkat pita yang terhubung, beserta drive dan slotnya.

Pool tape

Perangkat lunak pencadangan menggunakan pool pita yang merupakan grup logis dari pita. Perangkat lunak ini berisi pool pita yang telah ditentukan sebelumnya: **Pita yang tidak dikenal**, **Pita yang diimpor**, **Pita bebas**, dan **Acronis**. Anda juga dapat membuat pool kustom sendiri.

Pool dan pool kustom **Acronis** juga digunakan sebagai lokasi pencadangan.

Pool yang telah ditentukan sebelumnya

Pita yang tidak dikenal

Pool berisi pita yang ditulis oleh aplikasi pihak ketiga. Untuk menulis ke pita tersebut, Anda perlu memindahkannya ke **Pita bebas** secara eksplisit. Anda tidak dapat memindahkan pita dari pool ini ke pool lain, kecuali untuk pool **Pita bebas**.

Pita yang diimpor

Pool berisi pita yang ditulis oleh Acronis Cyber Protect di alat rekaman yang terpasang pada agen simpul atau simpul penyimpanan lain. Untuk menulis ke pita tersebut, Anda perlu memindahkannya ke **Pita bebas** secara eksplisit. Anda tidak dapat memindahkan pita dari pool ini ke pool lain, kecuali untuk pool **Pita bebas**.

Pita bebas

Pool berisi pita bebas (kosong). Anda dapat memindahkan pita ke pool ini secara manual dari pool lain.

Saat Anda memindahkan pita ke pool **Pita bebas**, perangkat lunak akan menandainya sebagai kosong. Jika pita berisi cadangan, pita tersebut ditandai dengan ikon  . Ketika perangkat lunak mulai menimpa pita, data yang terkait dengan cadangan akan dihapus dari database.

Acronis

Pool digunakan untuk mencadangkan secara default, ketika Anda tidak ingin membuat pool Anda sendiri. Biasanya, ini berlaku untuk satu drive pita dengan pita dalam jumlah kecil.

Pool kustom

Anda perlu membuat beberapa pool jika ingin memisahkan cadangan data yang berbeda. Misalnya, Anda mungkin ingin membuat pool kustom untuk memisahkan:

- cadangan dari berbagai departemen perusahaan Anda
- cadangan dari mesin yang berbeda
- cadangan volume sistem dan data pengguna.

Operasi dengan pool

Membuat pool

Untuk membuat pool

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Pool pita** di bawah mesin ini.
3. Klik **Buat pool**.
4. Tentukan nama pool.
5. [Opsional] Kosongkan kotak centang **Ambil pita dari pool 'Pita bebas' secara otomatis....** Jika dikosongkan, hanya pita yang dimasukkan ke dalam pool baru pada saat tertentu yang akan digunakan untuk mencadangkan.
6. Klik **Buat**.

Mengedit pool

Anda dapat mengedit parameter pool **Acronis** atau pool kustom Anda sendiri.

Untuk mengedit pool:

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Pool pita** di bawah mesin ini.
3. Pilih pool yang diperlukan, lalu klik **Edit pool**.
4. Anda dapat mengubah nama atau pengaturan pool. Untuk informasi lebih lanjut tentang pengaturan pool, lihat "Membuat pool".
5. Klik **Simpan** untuk menyimpan perubahan.

Menghapus pool

Anda hanya dapat menghapus pool kustom. Pita yang telah ditentukan sebelumnya (**Pita tidak dikenal**, **Pita yang diimpor**, **Pita bebas**, dan **Acronis**) tidak dapat dihapus.

Catatan
Setelah pool dihapus, jangan lupa untuk mengedit rencana proteksi yang memiliki pool sebagai lokasi cadangan. Jika tidak, rencana proteksi ini akan gagal.

Untuk menghapus pool:

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Pool pita** di bawah mesin ini.
3. Pilih pool yang diperlukan, lalu klik **Hapus**.
4. Pilih pool yang akan ditempati pool pita yang dihapus setelah penghapusan.
5. Klik **OK** untuk menghapus pool.

Operasi dengan pita

Memindahkan ke slot lain

Gunakan operasi ini dalam situasi berikut:

- Anda harus mengeluarkan beberapa pita dari perangkat pita secara bersamaan.
- Perangkat pita Anda tidak memiliki slot surat dan pita yang akan dikeluarkan berada di magazin slot yang tidak dapat dilepas.

Anda harus memindahkan pita ke slot dari satu magazin slot, lalu mengeluarkan magazin secara manual.

Untuk memindahkan pita ke slot lain

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Pool pita** di bawah mesin ini.
3. Klik pool yang berisi pita yang diperlukan, lalu pilih pita yang diperlukan.
4. Klik **Pindah ke slot**.
5. Pilih slot baru untuk tujuan pemindahan pita yang dipilih.
6. Klik **Pindah** untuk memulai operasi.

Memindahkan ke pool lain

Operasi ini memungkinkan Anda untuk memindahkan satu atau beberapa pita dari satu pool ke pool lainnya.

Saat Anda memindahkan pita ke pool **Pita bebas**, perangkat lunak akan menandainya sebagai kosong. Jika pita berisi cadangan, pita tersebut ditandai dengan ikon  . Ketika perangkat lunak mulai menimpa pita, data yang terkait dengan cadangan akan dihapus dari database.

Catatan tentang jenis pita tertentu

- Anda tidak dapat memindahkan pita WORM (Write-Once-Read-Many) yang diproteksi dan pernah direkam ke pool **Pita bebas**.
- Membersihkan pita selalu ditampilkan di pool **Pita yang tidak dikenal**; Anda tidak dapat memindahkannya ke pool lain.

Untuk memindahkan pita ke pool lain

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Pool pita** di bawah mesin ini.
3. Klik pool yang berisi pita yang diperlukan, lalu pilih pita yang diperlukan.
4. Klik **Pindah ke pool**.
5. [Opsional] Klik **Buat pool baru** jika Anda ingin membuat pool lain untuk pita yang dipilih. Lakukan tindakan yang dijelaskan di bagian "Membuat pool".
6. Pilih pool untuk memindahkan tape.
7. Klik **Pindah** untuk menyimpan perubahan.

Catatan
Jika memiliki cadangan yang dapat dipulihkan pada tape dan Anda memindahkan tape ke pool lainnya, pastikan Anda me-refresh kubah di bawah penyimpanan cadangan setelah menyelesaikan operasi pemindahan. Cadangan akan tersedia di pool kedua meskipun terdapat tujuan cadangan asli.

Melakukan inventasisasi

Operasi inventarisasi akan mendeteksi pita yang dimuat ke dalam perangkat pita dan memberi nama pita yang belum bernama.

Metode inventarisasi

Ada dua metode inventarisasi.

Inventarisasi cepat

Agen atau simpul penyimpanan memindai pita untuk barcode. Dengan barcode, perangkat lunak dapat dengan cepat mengembalikan pita ke pool sebelumnya.

Pilih metode ini untuk mengenali pita yang digunakan oleh perangkat pita terpasang yang sama pada mesin yang sama. Pita lain akan dikirim ke pool **Pita yang tidak dikenal**.

Jika pustaka pita Anda tidak berisi pembaca barcode, semua pita akan dikirim ke pool **Pita yang tidak dikenal**. Untuk mengenali pita Anda, lakukan inventarisasi penuh atau kombinasikan inventaris cepat dan penuh seperti yang dijelaskan di bagian ini berikutnya.

Inventarisasi penuh

Agen atau simpul penyimpanan membaca tag tertulis sebelumnya dan menganalisis informasi lain tentang konten pita yang dimuat. Pilih metode ini untuk mengenali pita dan pita kosong yang ditulis oleh perangkat lunak yang sama pada perangkat pita dan mesin apa pun.

Tabel berikut menunjukkan pool yang untuknya pita yang dikirim sebagai hasil inventarisasi penuh.

Pita digunakan oleh...	Pita dibaca oleh...	Pita dikirim ke pool...
Agen	Agen yang sama	Lokasi pita sebelumnya
	Agen lain	**Pita yang diimpor**
	Simpul penyimpanan	**Pita yang diimpor**
Simpul penyimpanan	Simpul penyimpanan yang sama	Lokasi pita sebelumnya
	Simpul penyimpanan yang lain	**Pita yang diimpor**
	Agen	**Pita yang diimpor**
Aplikasi pencadangan pihak ketiga	Agen atau simpul penyimpanan	**Pita yang tidak dikenal**

Pita jenis tertentu dikirim ke pool spesifik:

Jenis pita	Pita dikirim ke pool...
Pita kosong	**Pita bebas**
Pita kosong yang dilindungi dari menulis	**Pita yang tidak dikenal**
Membersihkan pita	**Pita yang tidak dikenal**

Inventarisasi cepat dapat diterapkan ke seluruh perangkat pita. Inventarisasi penuh dapat diterapkan ke seluruh perangkat pita, drive individual, atau slot. Untuk pita drive yang berdiri sendiri, inventarisasi penuh selalu dilakukan, meskipun inventarisasi cepat dipilih.

Kombinasi inventaris cepat dan penuh

Inventarisasi penuh untuk seluruh perangkat pita mungkin membutuhkan waktu yang cukup lama. Jika Anda hanya perlu melakukan inventarisasi beberapa pita, lakukan dengan langkah berikut:

1. Lakukan inventarisasi cepat pada perangkat pita.
2. Klik pool **Pita yang tidak dikenal**. Temukan pita yang ingin Anda inventarisasi dan perhatikan slot mana yang ditempati.
3. Lakukan inventarisasi penuh slot ini.

Apa yang harus dilakukan setelah inventarisasi

Jika Anda ingin mencadangkan ke pita yang ditempatkan di pool **Pita yang tidak dikenal** atau **Pita yang diimpor**, pindah ke pool **Pita bebas**, lalu ke pool **Acronis** atau pool kustom. Jika pool yang

menjadi tujuan pencadangan adalah pool yang dapat diisi ulang, Anda dapat membiarkan pita tersebut di pool **Pita bebas**.

Jika Anda ingin memulihkan dari pita yang ditempatkan di **Pita yang tidak dikenal** atau **Pita yang diimpor**, Anda perlu memindainya ulang. Pita akan dipindahkan ke pool yang telah Anda pilih selama pemindaian ulang, dan pencadangan yang disimpan pada pita tersebut akan muncul di lokasi.

Urutan tindakan

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin yang terpasang perangkat pita, lalu pilih perangkat pita yang ingin Anda inventarisasi.
3. Klik **Inventaris**.
4. [Opsional] Untuk memilih inventaris cepat, matikan **Inventaris penuh**.
5. [Opsional] Hidupkan **Pindahkan pita yang tidak dikenal dan pita yang diimpor ke pool 'Pita bebas'**.

   Peringatan!
   Hanya aktifkan switch ini jika Anda benar-benar yakin bahwa data yang disimpan di pita Anda dapat ditimpa.

6. Klik **Mulai inventarisasi sekarang** untuk memulai inventarisasi.

Pemindaian ulang

Informasi tentang konten pita disimpan dalam database khusus. Operasi pemindaian ulang akan membaca konten pita dan memperbarui database jika informasi di dalamnya tidak cocok dengan data yang disimpan dalam pita. Cadangan yang terdeteksi sebagai hasil operasi ditempatkan di pool yang ditentukan.

Dalam satu operasi, Anda dapat memindai ulang pita dari satu pool. Hanya pita online yang dapat dipilih untuk operasi.

Untuk memindai ulang pita dengan pencadangan multistreaming atau multiplexing dan multistreaming, Anda memerlukan minimal jumlah drive yang sama yang digunakan untuk membuat cadangan ini. Pencadangan tersebut tidak dapat dipindai ulang melalui drive pita yang berdiri sendiri.

Jalankan pemindaian ulang:

- Jika database dari simpul penyimpanan atau mesin yang dikelola hilang atau rusak.
- Jika informasi tentang pita dalam database sudah tidak berlaku (misalnya, konten pita diubah oleh simpul atau agen penyimpanan lain).
- Untuk mendapatkan akses ke cadangan yang disimpan di pita saat bekerja di bawah media yang dapat di-boot.

- Jika Anda tidak sengaja menghapus informasi tentang pita dari database. Saat Anda memindai ulang pita yang dihapus, cadangan yang disimpan di dalamnya akan muncul kembali dalam database dan tersedia untuk pemulihan data.
- Jika cadangan dihapus dari pita baik secara manual atau melalui aturan retensi tetapi Anda ingin cadangan menjadi dapat diakses untuk pemulihan data. Sebelum memindai ulang pita tersebut, keluarkan pita, hapus informasi tentangnya dari database, lalu masukkan lagi pita ke dalam perangkat pita.

Untuk memindai ulang pita

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Perangkat pita** di bawah mesin ini.
3. Pilih perangkat pita tempat Anda memuat pita.
4. Lakukan inventarisasi cepat.

   Catatan
   Selama inventarisasi, *jangan* mengaktifkan switch **Pindahkan pita yang tidak dikenal dan pita yang diimpor ke 'Pita bebas'**.

5. Pilih pool **Pita yang tidak dikenal**. Ini adalah pool yang merupakan tujuan dari sebagian besar pita yang dikirim sebagai hasil inventarisasi cepat. Memindai ulang pool yang lain juga dimungkinkan.
6. [Opsional] Hanya untuk memindai ulang pita individual, pilih opsi tersebut.
7. Klik **Pindai ulang**.
8. Pilih pool lokasi pencadangan yang baru terdeteksi akan ditempatkan.
9. Jika perlu, pilih kotak centang **Aktifkan pemulihan file dari cadangan disk yang disimpan pada pita**.

   Detail. Jika kotak centang dipilih, perangkat lunak akan membuat file tambahan khusus pada hard disk mesin tempat perangkat pita terpasang. Pemulihan file dari pencadangan disk dimungkinkan selama file tambahan ini masih utuh. Pastikan untuk memilih kotak centang jika pita berisi cadangan keberadaan aplikasi. Jika tidak, Anda tidak akan dapat memulihkan data aplikasi dari cadangan ini.
10. Jika pita berisi cadangan yang dilindungi kata sandi, pilih kotak centang yang sesuai, lalu tentukan kata sandi untuk cadangan. Jika Anda tidak menentukan kata sandi, atau kata sandi salah, cadangan tidak akan terdeteksi. Harap perhatikan hal ini jika Anda tidak melihat cadangan setelah pemindaian ulang.

    Tips. Jika pita berisi cadangan yang dilindungi oleh berbagai kata sandi, Anda perlu mengulang pemindaian ulang beberapa kali dengan menetapkan setiap kata sandi secara bergantian.
11. Klik **Mulai pemindaian ulang** untuk memulai pemindaian ulang.

Hasil. Pita yang dipilih dipindahkan ke pool yang dipilih. Cadangan yang disimpan di pita dapat ditemukan di pool ini. Cadangan yang tersebar di beberapa pita tidak akan muncul di pool hingga semua pita ini dipindai ulang.

Mengganti nama

Ketika pita baru terdeteksi oleh perangkat lunak, pita akan secara otomatis diberi nama dalam format berikut: **Tape XXX**, di mana **XXX** adalah nomor unik. Pita diberi nomor secara berurutan. Operasi penggantian nama memungkinkan Anda mengubah nama pita secara manual.

Untuk mengganti nama pita

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Pool pita** di bawah mesin ini.
3. Klik pool yang berisi pita yang diperlukan, lalu pilih pita yang diperlukan.
4. Klik **Ganti nama**.
5. Ketik nama baru untuk pita yang dipilih.
6. Klik **Ganti nama** untuk menyimpan perubahan.

Menghapus

Menghapus pita secara fisik akan menghapus semua cadangan yang tersimpan di pita dan menghapus informasi tentang cadangan tersebut dari database. Namun, informasi tentang pita akan tetap ada dalam database.

Setelah menghapus, pita yang berada di pool **Pita yang tidak dikenal** atau **Pita yang diimpor** akan dipindahkan ke pool **Pita bebas**. Pita yang berada di pool lain tidak akan dipindahkan.

Untuk menghapus pita

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Pool pita** di bawah mesin ini.
3. Klik pool yang berisi pita yang diperlukan, lalu pilih pita yang diperlukan.
4. Klik **Hapus**. Sistem akan meminta konfirmasi operasi.
5. Pilih metode penghapusan: cepat atau penuh.
6. Klik **Hapus** untuk memulai operasi.
   Detail. Anda tidak dapat membatalkan operasi penghapusan.

Mengeluarkan

Agar pita dapat dikeluarkan dari pustaka pita, pustaka pita harus memiliki slot surat dan slot tidak boleh dikunci oleh pengguna atau perangkat lunak lain.

Untuk mengeluarkan pita

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Pool pita** di bawah mesin ini.
3. Klik pool yang berisi pita yang diperlukan, lalu pilih pita yang diperlukan.
4. Klik **Keluarkan**. Perangkat lunak akan meminta Anda untuk memberikan deskripsi pita. Kami menyarankan Anda untuk menjelaskan lokasi fisik di mana pita akan disimpan. Selama pemulihan, perangkat lunak akan menampilkan deskripsi ini sehingga Anda dapat dengan mudah menemukan pita.
5. Klik **Keluarkan** untuk memulai operasi.

Setelah pita dikeluarkan, baik secara manual atau secara otomatis, Anda disarankan untuk menulis namanya pada pita tersebut.

Menghapus

Operasi penghapusan akan menghapus informasi tentang pencadangan yang disimpan pada pita yang dipilih dan tentang pita itu sendiri dari database.

Anda hanya dapat menghapus pita offline (dikeluarkan).

Untuk menghapus pita

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Pool pita** di bawah mesin ini.
3. Klik pool yang berisi pita yang diperlukan, lalu pilih pita yang diperlukan.
4. Klik **Hapus**. Sistem akan meminta konfirmasi operasi.
5. Klik **Hapus** untuk menghapus pita itu.

Apa yang harus dilakukan jika saya tidak sengaja menghapus pita?

Tidak seperti pita yang dihapus, data dari pita yang dihapus tidak akan secara fisik terhapus. Oleh karena itu, Anda dapat menyediakan cadangan yang disimpan di pita tersebut kembali. Untuk melakukannya:

1. Masukkan pita ke dalam perangkat pita Anda.
2. Lakukan inventarisasi cepat untuk mendeteksi pita tersebut.

   Catatan
   Selama inventarisasi, *jangan* mengaktifkan switch **Pindahkan pita yang tidak dikenal dan pita yang diimpor ke 'Pita bebas'**.

3. Lakukan pemindaian ulang untuk mencocokkan data yang disimpan pada pita dengan database.

Menentukan set pita

Operasi ini memungkinkan Anda untuk menentukan set pita untuk pita.

Set pita adalah sekelompok pita dalam satu pool.

Tidak seperti menentukan set pita di opsi pencadangan, di mana Anda dapat menggunakan variabel, di sini Anda dapat bisa menentukan nilai string.

Lakukan operasi ini jika Anda ingin perangkat lunak mencadangkan ke pita *spesifik* sesuai dengan aturan tertentu (misalnya, jika Anda ingin menyimpan cadangan Senin di pita 1, cadangan Selasa di pita 2, dll). Tentukan satu set pita tertentu untuk setiap pita yang diperlukan, lalu tentukan set pita yang sama atau gunakan variabel yang tepat dalam opsi pencadangan.

Untuk contoh di atas, tentukan set pita `Senin` untuk Pita 1, `Selasa` untuk Pita 2, dst. Dalam opsi pencadangan, tentukan `[Hari Kerja]`. Dalam hal ini, pita yang tepat akan digunakan pada masing-masing hari dalam seminggu.

Untuk menentukan satu set pita untuk satu atau beberapa pita

1. Klik **Pengaturan** > **Manajemen pita**.
2. Pilih mesin atau simpul penyimpanan tempat perangkat pita Anda terpasang, lalu klik **Pool pita** di bawah mesin ini.
3. Klik pool yang berisi pita yang diperlukan, lalu pilih pita yang diperlukan.
4. Klik **Set pita**.
5. Ketik nama set pita. Jika pita lain sudah ditentukan untuk pita yang dipilih, nama tersebut akan diganti. Jika Anda ingin mengecualikan pita dari set pita tanpa menentukan yang lain, hapus nama set pita yang sudah ada.
6. Klik **Simpan** untuk menyimpan perubahan.

Simpul penyimpanan

Simpul penyimpanan adalah server yang dirancang untuk mengoptimalkan penggunaan berbagai sumber daya (seperti kapasitas penyimpanan perusahaan, bandwidth jaringan, dan beban CPU server produksi) yang diperlukan untuk melindungi data perusahaan. Tujuan ini dapat dicapai dengan mengatur dan mengelola lokasi yang berfungsi sebagai lokasi penyimpanan khusus cadangan perusahaan (lokasi yang dikelola).

Tujuan utama Simpul Penyimpanan Acronis adalah untuk mengaktifkan akses terpusat ke tape drive atau pustaka, misalnya, mencadangkan dan memulihkan data dari beberapa perangkat ke tape drive atau pustaka yang sama (kubah yang dikelola pada tape).

Kasus penggunaan lainnya adalah untuk mengaktifkan kemampuan deduplikasi lanjutan di mana data di beberapa perangkat perlu dideduplikasi satu sama lain dan disimpan di satu lokasi (kubah yang dikelola dengan deduplikasi yang diaktifkan).

Menginstal simpul penyimpanan dan layanan katalog

Sebelum menginstal simpul penyimpanan, pastikan mesin memenuhi persyaratan sistem.

Kami menyarankan Anda untuk menginstal simpul penyimpanan dan layanan katalog pada mesin terpisah. Persyaratan sistem untuk mesin yang menjalankan layanan katalog dijelaskan dalam "Praktik terbaik katalogisasi" (hlm. 620).

Untuk menginstal simpul penyimpanan dan/atau layanan katalog

1. Masuk sebagai administrator dan mulai program penyiapan Acronis Cyber Protect.
2. [Opsional] Untuk mengubah bahasa program penyiapan, klik **Pengaturan bahasa**.
3. Terima persyaratan perjanjian lisensi dan pernyataan privasi, lalu klik **Lanjutkan**.
4. Klik **Instal agen perlindungan**.
5. Klik **Sesuaikan pengaturan instalasi**.
6. Di sebelah **Apa yang diinstal**, klik **Ubah**.
7. Pilih komponen yang akan diinstal:
   - Untuk menginstal simpul penyimpanan, pilih kotak centang **Simpul penyimpanan**. Kotak centang **Agen untuk Windows** dipilih secara otomatis.
   - Untuk menginstal layanan katalog, pilih kotak centang **Layanan Katalog**.
   - Jika Anda tidak ingin menginstal komponen lain pada mesin ini, kosongkan kotak centang yang sesuai.

   Klik **Selesai** untuk melanjutkan.
8. Tentukan server manajemen tempat komponen akan didaftarkan:
   a. Di sebelah **Server Manajemen Acronis Cyber Protect**, klik **Tentukan**.
   b. Tentukan nama host atau alamat IP mesin tempat server manajemen diinstal.
   c. Tentukan kredensial administrator server manajemen atau token registrasi.
      Untuk informasi lebih lanjut tentang cara membuat token pendaftaran, lihat "Langkah 1: Membuat token pendaftaran" (hlm. 176).
   d. Klik **Selesai**.
9. Jika diminta, pilih apakah mesin dengan simpul penyimpanan dan/atau layanan katalog akan ditambahkan ke organisasi atau ke salah satu unit.
   Permintaan ini akan muncul jika Anda mengelola lebih dari satu unit, atau organisasi dengan setidaknya satu unit. Jika tidak, mesin akan secara otomatis ditambahkan ke unit atau organisasi yang Anda kelola. Untuk informasi lebih lanjut, lihat "Administrator dan unit".
10. [Opsional] Ubah pengaturan instalasi lain seperti yang dijelaskan dalam "Menyesuaikan pengaturan instalasi".
11. Klik **Instal** untuk melanjutkan instalasi.
12. Setelah instalasi selesai, klik **Tutup**.

Memperbarui layanan katalog dengan Acronis Cyber Protect 15 Update 4

Acronis Cyber Protect 15 Update 4 menggunakan versi baru dari layanan katalog. Versi baru tidak secara langsung kompatibel dengan data katalog yang dibuat oleh versi sebelumnya.

Selama memperbarui ke Acronis Cyber Protect 15 Update 4, Anda dapat memigrasikan data ini secara manual ke versi baru layanan katalog. Atau, Anda dapat melewati migrasi dan membuat ulang data katalog nanti. Membuat ulang data katalog membutuhkan waktu lebih lama daripada migrasinya.

Untuk memigrasikan data katalog

1. Pada mesin tempat layanan katalog diinstal, jalankan program penyiapan Acronis Cyber Protect.
2. Terima persyaratan perjanjian lisensi dan pernyataan privasi, lalu klik **Lanjutkan**.
3. Pilih kotak centang **Saya mengerti**, lalu klik **Perbarui**.
4. Pilih kotak centang **Tentukan folder sementara**.
5. Tentukan folder di mana data katalog akan diekspor.
   Data yang diekspor dienkripsi. Folder sementara secara otomatis dihapus ketika migrasi selesai.
6. Klik **Selesai**.

Untuk melewati migrasi data katalog

1. Pada mesin tempat layanan katalog diinstal, jalankan program penyiapan Acronis Cyber Protect.
2. Terima persyaratan perjanjian lisensi dan pernyataan privasi, lalu klik **Lanjutkan**.
3. Pilih kotak centang **Saya mengerti**, lalu klik **Perbarui**.
4. Kosongkan kotak centang **Tentukan folder sementara**.
5. Klik **Selesai**.
6. Konfirmasi pilihan Anda.

Akibatnya, data katalog yang ada menjadi tidak tersedia setelah pembaruan ke Acronis Cyber Protect 15 Update 4. Untuk membuat ulang data katalog, jalankan pencadangan.

Catatan
Jika layanan katalog, node penyimpanan, dan server manajemen berjalan pada mesin terpisah, pastikan Anda memperbarui semuanya ke Acronis Cyber Protect 15 Update 4, dengan urutan sebagai berikut:

1. Server manajemen
2. Simpul penyimpanan
3. Layanan katalog

Menambahkan lokasi yang dikelola

Lokasi yang dikelola dapat diatur:

- Di folder lokal:
  - Pada hard drive lokal ke simpul penyimpanan
  - Pada penyimpanan SAN yang muncul ke sistem operasi sebagai perangkat yang terpasang secara lokal
- Di folder jaringan:
  - Pada bagian SMB/CIFS
  - Pada penyimpanan SAN yang muncul ke sistem operasi sebagai folder jaringan
  - Pada NAS
- Pada perangkat pita yang terpasang secara lokal ke simpul penyimpanan.

  Lokasi berbasis pita dibuat dalam bentuk pool pita. Satu pool pita ada secara default. Jika perlu, Anda dapat membuat pool pita lain, seperti dijelaskan di bagian ini selanjutnya.

Untuk membuat lokasi yang dikelola di folder lokal atau jaringan

1. Lakukan salah satu langkah berikut:
   - Klik **Penyimpanan cadangan** > **Tambahkan lokasi**, lalu klik **Simpul penyimpanan**.
   - Saat membuat rencana proteksi, klik **Tempat menyimpan cadangan** > **Tambah lokasi**, lalu klik **Simpul penyimpanan**.
   - Klik **Pengaturan** > **Simpul penyimpanan**, pilih simpul penyimpanan yang akan mengelola lokasi, lalu klik **Tambah lokasi**.
2. Di bagian **Nama**, tentukan nama unik untuk lokasi. "Unik" berarti tidak boleh ada lokasi lain dengan nama yang sama, yang dikelola oleh simpul penyimpanan yang sama.
3. [Opsional] Pilih simpul penyimpanan yang akan mengelola lokasi. Jika Anda memilih opsi terakhir pada langkah 1, Anda tidak akan dapat mengubah simpul penyimpanan.
4. Pilih nama simpul penyimpanan atau alamat IP yang akan digunakan agen untuk mengakses lokasi.

   Secara default, nama simpul penyimpanan dipilih. Anda mungkin perlu mengubah pengaturan ini jika server DNS tidak dapat menyelesaikan nama ke alamat IP, yang mengakibatkan kegagalan akses. Untuk mengubah setelan ini di lain waktu, klik **Penyimpanan cadangan** > lokasi > **Edit**, lalu ubah nilai bidang **Alamat**.
5. Masukkan jalur folder atau jelajahi ke folder yang diinginkan.
6. Klik **Selesai**. Perangkat lunak akan memeriksa akses ke folder yang ditentukan.
7. [Opsional] Aktifkan deduplikasi pencadangan di lokasi.

   Deduplikasi meminimalkan lalu lintas pencadangan dan mengurangi ukuran pencadangan yang disimpan di lokasi dengan menghilangkan blok disk duplikat.

   Untuk informasi lebih lanjut tentang pembatasan deduplikasi, lihat "Pembatasan Deduplikasi".
8. [Hanya jika deduplikasi diaktifkan] Tentukan atau ubah nilai bidang **Jalur database deduplikasi**.

   Ini harus berupa folder pada hard drive lokal ke simpul penyimpanan. Untuk meningkatkan performa sistem, kami menyarankan Anda untuk membuat database deduplikasi dan lokasi yang dikelola pada disk yang berbeda.

   Untuk informasi lebih lanjut tentang database deduplikasi, lihat "Praktik terbaik Deduplikasi".

9. [Opsional] Pilih apakah akan melindungi lokasi dengan enkripsi. Semua yang ditulis ke lokasi akan dienkripsi dan apa pun yang dibaca darinya akan didekripsi secara transparan oleh simpul penyimpanan, menggunakan kunci enkripsi spesifik lokasi yang disimpan pada simpul penyimpanan.

   Untuk informasi lebih lanjut tentang enkripsi, lihat "Enkripsi lokasi".
10. [Opsional] Pilih apakah akan membuat katalog cadangan yang disimpan di lokasi. Katalog data memungkinkan Anda dengan mudah menemukan versi data yang diperlukan dan memilihnya untuk pemulihan.

    Jika beberapa layanan katalogisasi terdaftar di server manajemen, Anda dapat memilih layanan yang akan membuat katalog cadangan yang disimpan di lokasi.

    Katalogisasi dapat diaktifkan atau dinonaktifkan di lain waktu, seperti yang dijelaskan dalam "Cara mengaktifkan atau menonaktifkan katalogisasi".
11. Klik **Selesai** untuk membuat lokasi.

Untuk membuat lokasi yang dikelola pada perangkat pita

1. Klik **Penyimpanan cadangan** > **Tambahkan lokasi** atau, saat membuat rencana proteksi, klik **Tempat pencadangan** > **Tambahkan lokasi**.
2. Klik **Pita**.
3. [Opsional] Pilih simpul penyimpanan yang akan mengelola lokasi.
4. Ikuti langkah-langkah yang dijelaskan dalam "Membuat pool", mulai dari langkah 4.

Catatan
Secara default, agen akan menggunakan nama simpul penyimpanan untuk mengakses lokasi berbasis pita terkelola. Untuk membuat agen menggunakan alamat IP simpul penyimpanan, klik **Penyimpanan cadangan** > lokasi > **Edit**, lalu ubah nilai bidang **Alamat**.

Deduplikasi

Pembatasan Deduplikasi

Pembatasan umum

Cadangan yang dienkripsi tidak dapat diduplikasi. Jika Anda ingin menggunakan deduplikasi dan enkripsi secara bersamaan, biarkan pencadangan tidak terenkripsi dan arahkan ke lokasi di mana deduplikasi dan enkripsi diaktifkan.

Cadangan tingkat disk

Deduplikasi blok disk tidak dilakukan jika ukuran unit alokasi volume, atau yang disebut juga sebagai ukuran klaster atau ukuran blok, tidak dapat dibagi dengan 4 KB.

Catatan
Ukuran unit alokasi pada sebagian besar volume NTFS dan ext3 adalah 4 KB. Hal ini memungkinkan deduplikasi level blok. Contoh lain dari ukuran unit alokasi yang memungkinkan untuk deduplikasi level blok adalah 8 KB, 16 KB, dan 64 KB.

Cadangan tingkat file

Deduplikasi file tidak dilakukan jika file dienkripsi.

Deduplikasi dan aliran data NTFS

Dalam sistem file NTFS, file dapat memiliki satu atau beberapa set data tambahan yang terkait dengannya, atau sering disebut juga *aliran data alternatif*.

Ketika file tersebut dicadangkan, aliran data alternatifnya juga ikut dicadangkan. Namun, aliran ini tidak pernah dideduplikasi, meskipun ketika file itu sendiri.

Praktik terbaik deduplikasi

Deduplikasi adalah proses kompleks yang bergantung pada banyak faktor.

Faktor terpenting yang memengaruhi kecepatan deduplikasi adalah:

- Kecepatan akses ke database deduplikasi
- Kapasitas RAM dari simpul penyimpanan
- Jumlah lokasi deduplikasi yang dibuat pada simpul penyimpanan.

Untuk meningkatkan performa deduplikasi, ikuti rekomendasi di bawah ini.

Tempatkan database deduplikasi dan lokasi deduplikasi pada perangkat fisik yang terpisah

Database deduplikasi menyimpan nilai hash dari semua item yang disimpan di lokasi, kecuali untuk item yang tidak dapat dideduplikasi, seperti file yang dienkripsi.

Untuk meningkatkan kecepatan akses ke database deduplikasi, database dan lokasi harus ditempatkan pada perangkat fisik yang terpisah.

Yang terbaik adalah mengalokasikan perangkat khusus untuk lokasi dan database. Jika tidak dimungkinkan, setidaknya jangan tempatkan lokasi atau database pada disk yang sama dengan sistem operasi. Alasannya adalah karena sistem operasi melakukan sejumlah besar operasi baca/tulis hard disk, yang secara signifikan memperlambat deduplikasi.

Memilih disk untuk database deduplikasi

- Database harus berada pada drive tetap. Jangan coba menempatkan database deduplikasi pada drive eksternal yang dapat dilepas.

- Untuk meminimalkan waktu akses ke database, lebih baik simpan di drive yang terhubung langsung daripada di volume jaringan yang terpasang. Latensi jaringan dapat secara signifikan menurunkan performa deduplikasi.
- Ruang disk yang diperlukan untuk database deduplikasi dapat diperkirakan menggunakan rumus berikut:

$$S = U * 90 / 65536 + 10$$

Di sini,

S adalah ukuran disk, dalam GB

U adalah jumlah data unik yang direncanakan di penyimpanan data deduplikasi, dalam GB

Misalnya, jika jumlah data unik yang direncanakan dalam penyimpanan data deduplikasi adalah U=5 TB, database deduplikasi akan membutuhkan ruang bebas minimum, seperti yang ditunjukkan di bawah ini:

$$S = 5000 * 90 / 65536 +10 = 17 GB$$

Memilih disk untuk lokasi deduplikasi

Untuk menghindari hilangnya data, sebaiknya gunakan RAID 10, 5, atau 6. RAID 0 tidak disarankan karena tidak toleran terhadap eror. RAID 1 tidak disarankan karena kecepatannya yang relatif rendah. Tidak ada preferensi untuk disk lokal atau SAN, keduanya bagus.

40 hingga 160 MB RAM per 1 TB data unik

Ketika batas tercapai, deduplikasi akan berhenti tetapi pencadangan dan pemulihan akan terus bekerja. Jika Anda menambahkan lebih banyak RAM ke simpul penyimpanan, setelah pencadangan berikutnya, deduplikasi akan dilanjutkan. Secara umum, semakin banyak RAM yang Anda miliki, semakin besar volume data unik yang dapat Anda simpan.

Hanya satu lokasi deduplikasi pada setiap simpul penyimpanan

Anda sangat disarankan untuk membuat hanya satu lokasi deduplikasi pada simpul penyimpanan. Jika tidak, seluruh volume RAM yang tersedia dapat didistribusikan secara proporsional sesuai jumlah lokasi.

Tidak adanya aplikasi yang berebut sumber daya

Mesin dengan simpul penyimpanan tidak boleh menjalankan aplikasi yang membutuhkan banyak sumber daya sistem; misalnya, sistem Database Management Systems (DBMS) atau Enterprise Resource Planning (ERP).

Prosesor multi-core dengan clock rate minimal 2,5 GHz

Sebaiknya Anda menggunakan prosesor dengan jumlah inti minimal empat dan clock rate minimal 2,5 GHz.

Ruang bebas yang cukup di lokasi

Deduplikasi pada target memerlukan ruang bebas sebanyak mungkin karena data yang dicadangkan akan langsung mengisinya setelah menyimpannya ke lokasi. Tanpa kompresi atau deduplikasi pada sumbernya, nilai ini sama dengan ukuran data asli yang dicadangkan selama operasi pencadangan yang diberikan.

LAN berkecepatan tinggi

Disarankan LAN 1-Gbit. Hal ini akan memungkinkan perangkat lunak untuk melakukan 5-6 pencadangan dengan deduplikasi secara paralel, dan kecepatan tidak akan berkurang secara signifikan.

Cadangkan mesin tipikal sebelum mencadangkan beberapa mesin dengan konten serupa

Saat mencadangkan beberapa mesin dengan konten yang serupa, Anda disarankan untuk mencadangkan satu mesin terlebih dahulu dan menunggu hingga akhir pengindeksan data yang dicadangkan. Setelah itu, mesin lain akan dicadangkan lebih cepat karena efisiensi deduplikasi. Karena pencadangan mesin pertama telah diindeks, sebagian besar data sudah ada di penyimpanan data deduplikasi.

Cadangkan mesin yang berbeda di waktu yang berbeda

Jika Anda mencadangkan sejumlah besar mesin, sebarkan operasi pencadangan dari waktu ke waktu. Untuk melakukannya, buat beberapa rencana proteksi dengan jadwal yang bervariasi.

Enkripsi lokasi

Jika Anda melindungi lokasi dengan enkripsi, semua yang ditulis ke lokasi akan dienkripsi dan apa pun yang dibaca darinya akan didekripsi secara transparan oleh simpul penyimpanan, menggunakan kunci enkripsi khusus lokasi yang disimpan pada simpul. Jika media penyimpanan dicuri atau diakses oleh orang yang tidak berwenang, malefactor tidak akan dapat mendekripsi konten lokasi tanpa akses ke simpul penyimpanan.

Enkripsi ini tidak ada hubungannya dengan enkripsi cadangan yang ditentukan oleh rencana proteksi dan dilakukan oleh agen. Jika pencadangan sudah dienkripsi, enkripsi sisi simpul penyimpanan diterapkan melalui enkripsi yang dilakukan oleh agen.

Untuk melindungi lokasi dengan enkripsi

1. Tentukan dan konfirmasikan kata (kata sandi) yang akan digunakan untuk menghasilkan kunci enkripsi.

   Kata tersebut peka huruf besar-kecil. Anda hanya akan diminta untuk memberikan kata ini ketika memasang lokasi ke simpul penyimpanan lain.
2. Pilih salah satu algoritma enkripsi berikut:

- **AES 128** – konten lokasi akan dienkripsi menggunakan algoritma Advanced Encryption Standard (AES) dengan kunci 128-bit.
- **AES 192** – konten lokasi akan dienkripsi menggunakan algoritma AES dengan kunci 192-bit.
- **AES 256** – konten lokasi akan dienkripsi menggunakan algoritma AES dengan kunci 256-bit.

3. Klik **OK**.

Algoritma kriptografi AES beroperasi dalam mode Cipher-block chaining (CBC) dan menggunakan kunci yang dihasilkan secara acak dengan ukuran yang ditentukan pengguna sebesar 128, 192, atau 256 bit. Semakin besar ukuran kunci, semakin lama program akan mengenkripsi pencadangan yang disimpan di lokasi dan semakin aman pencadangannya.

Kunci enkripsi kemudian dienkripsi dengan AES-256 menggunakan hash SHA-256 dari kata yang dipilih sebagai kunci. Kata itu sendiri tidak disimpan di mana pun pada disk; kata hash digunakan untuk keperluan verifikasi. Dengan keamanan dua level ini, cadangan terlindungi dari akses tidak sah, tetapi Anda tidak dimungkinkan untuk memulihkan kata yang hilang.

Mengkatalogkan

Katalog data

Katalog data memungkinkan Anda dengan mudah menemukan versi data yang diperlukan dan memilihnya untuk pemulihan. Katalog data menampilkan data yang disimpan di lokasi yang dikelola yang untuknya katalogisasi diaktifkan.

Bagian **Katalog** hanya akan muncul di bawah tab **Penyimpanan cadangan** jika setidaknya ada satu layanan katalog terdaftar di server manajemen. Untuk informasi tentang cara menginstal layanan katalog, lihat "Menginstal simpul penyimpanan dan layanan katalog".

Bagian **Katalog** hanya dapat dilihat oleh administrator organisasi.

Pembatasan

Katalogisasi hanya didukung untuk cadangan disk dan file level mesin fisik, serta cadangan mesin virtual.

Data berikut tidak dapat ditampilkan dalam katalog:

- Data dari cadangan terenkripsi
- Data yang dicadangkan ke perangkat pita
- Data dicadangkan ke penyimpanan awan
- Data yang didukung oleh versi produk sebelum Acronis Cyber Protect 12.5

Memilih data yang dicadangkan untuk pemulihan

1. Klik **Penyimpanan cadangan** > **Katalog**.
2. Jika beberapa layanan katalogisasi terdaftar di server manajemen, pilih layanan yang melakukan katalogisasi cadangan yang disimpan di lokasi.

   Catatan
   Untuk melihat layanan mana yang membuat katalogisasi lokasi, pilih lokasi di **PenyimpananCadangan**> **Lokasi** > **Lokasi**, lalu klik **Detail**.

3. Perangkat lunak ini menunjukkan mesin yang dicadangkan ke lokasi yang dikelola yang dikatalogkan oleh layanan katalog yang dipilih.
   Pilih data yang akan dipulihkan dengan menjelajahi atau menggunakan pencarian.
   - **Menjelajahi**
     Klik dua kali pada mesin untuk melihat disk, volume, folder, dan file yang dicadangkan.
     Untuk memulihkan disk, pilih disk yang ditandai dengan ikon berikut: 
     Untuk memulihkan volume, klik dua kali pada disk yang berisi volume, lalu pilih volume.
     Untuk memulihkan file dan folder, jelajahi volume lokasi file dan folder tersebut. Anda dapat menjelajahi volume yang ditandai dengan ikon folder: 
   - **Pencarian**
     Di kolom pencarian, ketik informasi yang membantu mengidentifikasi item data yang diperlukan (informasi ini dapat berupa nama mesin, nama file atau folder, atau label disk) lalu klik **Cari**.
     Anda dapat menggunakan tanda bintang (*) dan tanda tanya (?) sebagai wildcard.
     Sebagai hasil dari pencarian, Anda akan melihat daftar item data yang dicadangkan yang namanya cocok, seluruhnya atau sebagian, dengan nilai yang dimasukkan.
4. Secara default, data akan dikembalikan ke titik waktu terbaru yang memungkinkan. Jika item tunggal dipilih, Anda dapat menggunakan tombol **Versi** untuk memilih titik pemulihan.
5. Setelah memilih data yang diperlukan, lakukan salah satu langkah berikut:
   - Klik **Pulihkan**, lalu konfigurasikan parameter operasi pemulihan seperti yang dijelaskan dalam "Pemulihan".
   - [Hanya untuk file/folder] Jika Anda ingin menyimpan file sebagai file .zip, klik **Unduh**, pilih lokasi untuk menyimpan data, lalu klik **Simpan**.

Praktik terbaik katalogisasi

Untuk meningkatkan performa katalogisasi, ikuti rekomendasi di bawah ini.

Instalasi

Kami menyarankan Anda untuk menginstal layanan katalog dan simpul penyimpanan pada mesin terpisah. Jika tidak, komponen tersebut akan berebut sumber daya CPU dan RAM.

Jika beberapa simpul penyimpanan terdaftar di server manajemen, satu layanan katalog sudah cukup kecuali performa pengindeksan atau pencarian menurun. Misalnya, jika Anda memperhatikan bahwa katalogisasi bekerja 24 jam dan 7 hari (artinya tidak ada jeda di antara kegiatan katalogisasi), instal satu layanan katalog lagi pada mesin terpisah. Kemudian, hapus beberapa lokasi yang dikelola dan buat ulang dengan layanan katalog baru. Cadangan akan disaCadangan yang disimpan di lokasi ini akan tetap utuh.impan.

Persyaratan sistem

Parameter	Nilai minimum	Nilai yang disarankan
Jumlah inti CPU	2	4 dan lebih banyak
RAM	8 GB	16 GB ke atas
Hard disk	7200 rpm HDD	SSD
Koneksi jaringan antara mesin dengan simpul penyimpanan dan mesin dengan layanan katalog	100 Mbps	1 Gbps

Cara mengaktifkan atau menonaktifkan katalogisasi

Jika katalogisasi diaktifkan untuk lokasi yang dikelola, konten setiap pencadangan yang diarahkan ke lokasi akan langsung ditambahkan ke katalog data setelah cadangan dibuat.

Anda dapat mengaktifkan katalogisasi saat menambahkan lokasi yang dikelola atau di lain waktu. Setelah katalogisasi diaktifkan, semua cadangan yang disimpan di lokasi dan yang sebelumnya tidak dikatalogisasi akan dikatalogkan setelah pencadangan berikutnya ke lokasi.

Proses katalogisasi dapat memakan waktu, terutama jika sejumlah besar mesin dicadangkan ke lokasi yang sama. Anda dapat menonaktifkan katalogisasi kapan saja. Katalogisasi cadangan yang dibuat sebelum penonaktifan akan diselesaikan. Cadangan yang baru dibuat tidak akan dikatalogisasi.

Untuk mengonfigurasi katalogisasi lokasi yang ada

1. Klik **Penyimpanan cadangan** > **Lokasi**.
2. Klik **Lokasi**, lalu pilih lokasi yang dikelola yang ingin Anda konfigurasi katalogisasinya.
3. Klik **Edit**.

4. Aktifkan atau nonaktifkan switch **Layanan katalog**.
5. Klik **Selesai**.

Pengaturan sistem

Pengaturan ini hanya tersedia dalam penyebaran di lokasi.

Untuk mengakses pengaturan ini, klik **Pengaturan** > **Pengaturan sistem**.

Bagian **Pengaturan sistem** hanya dapat dilihat oleh administrator organisasi.

Notifikasi email

Anda dapat mengonfigurasi pengaturan global yang umum untuk semua notifikasi email yang dikirim dari server manajemen.

Pada opsi pencadangan default, Anda dapat mengganti pengaturan ini secara eksklusif untuk peristiwa yang terjadi selama pencadangan. Dalam hal ini, pengaturan global akan efektif untuk operasi selain pencadangan.

Saat membuat rencana proteksi, Anda dapat memilih pengaturan mana yang akan digunakan: pengaturan global atau pengaturan yang ditentukan dalam opsi pencadangan default. Anda juga bisa menimpanya dengan nilai kustom yang spesifik hanya untuk rencana.

Penting
Jika pengaturan notifikasi email global diubah, semua rencana proteksi yang menggunakan pengaturan global akan terpengaruh.

Sebelum mengonfigurasi pengaturan ini, pastikan bahwa pengaturan **Server email** telah dikonfigurasi.

Untuk mengonfigurasi pengaturan notifikasi email global

1. Klik **Pengaturan** > **Pengaturan sistem** > **Notifikasi email.**.
2. Di kolom **alamat email Penerima**, masukkan alamat email tujuan. Anda dapat memasukkan beberapa alamat yang dipisahkan dengan tanda titik koma.
3. [Opsional] Di **Subjek**, ubah subjek notifikasi email.
   Anda dapat menggunakan variabel berikut
   - `[Peringatan]` - ringkasan peringatan.
   - `[Perangkat]` - nama perangkat.
   - `[Rencana]` - nama rencana yang menghasilkan peringatan.
   - `[ManagementServer]` - nama host mesin tempat server manajemen diinstal.
   - `[Unit]` - nama unit tempat mesin tersebut berada.

   Subjek default adalah `[Peringatan]` **Perangkat:** `[Perangkat]` **Rencana:** `[Rencana]`
4. [Opsional] Pilih kotak centang **Rekap harian tentang peringatan aktif**, lalu lakukan langkah berikut:

a. Tentukan waktu kapan rekap akan dikirim.

b. [Opsional] Pilih kotak centang **Jangan mengirim pesan 'Tidak ada peringatan aktif**.

5. [Opsional] Pilih bahasa yang akan digunakan dalam notifikasi email.
6. Pilih kotak centang untuk peristiwa yang ingin Anda terima notifikasinya. Anda dapat memilih dari daftar semua peringatan yang mungkin, dikelompokkan berdasarkan tingkat keparahannya.
7. Klik **Simpan**.

Server surel

Anda dapat menentukan server email yang akan digunakan untuk mengirim notifikasi email dari server manajemen.

Untuk menentukan server email

1. Klik **Pengaturan** > **Pengaturan sistem** > **Server email**.
2. Pada **Layanan email**, pilih salah satu opsi berikut:
   - **Kustom**
   - **Gmail**
   - **Yahoo Mail**
   - **Outlook.com**
3. [Hanya untuk layanan email kustom] Tentukan pengaturan berikut:
   - Pada **SMTP server** (Server SMTP), masukkan nama server email keluar (SMTP).
   - Pada **SMTP port** (Port SMTP), atur port dari server email keluar. Secara default, port diatur ke 25.
   - Pilih apakah akan menggunakan enkripsi SSL atau TLS. Pilih **Tidak ada** untuk menonaktifkan enkripsi.
   - Jika server SMTP memerlukan autentikasi, pilih centang kotak **Server SMTP memerlukan autentikasi**, lalu tentukan kredensial akun yang akan digunakan untuk mengirim pesan. Jika Anda tidak yakin apakah server SMTP memerlukan autentikasi, hubungi administrator jaringan atau penyedia layanan email Anda untuk mendapatkan bantuan.
4. [Hanya untuk Gmail, Yahoo Mail, dan Outlook.com] Tentukan kredensial akun yang akan digunakan untuk mengirim pesan.
5. [Hanya untuk layanan email kustom] Pada **Pengirim**, tulis nama pengirim. Nama ini akan ditampilkan di bidang **Dari** dari notifikasi email. Jika Anda membiarkan bidang ini kosong, pesan akan berisi akun yang ditentukan pada langkah 3 atau 4.
6. [Opsional] Klik **Kirim pesan pengujian** untuk memeriksa apakah notifikasi email berfungsi dengan benar dengan pengaturan yang ditentukan. Masukkan alamat email untuk mengirim pesan pengujian.

Keamanan

Gunakan opsi ini untuk meningkatkan keamanan penyebaran lokal Acronis Cyber Protect Anda.

Keluarkan pengguna tidak aktif setelah

Opsi ini memungkinkan Anda untuk menentukan batas waktu untuk keluar otomatis karena ketidakaktifan pengguna. Ketika tersisa satu menit dalam batas waktu yang ditentukan, perangkat lunak akan meminta pengguna untuk tetap masuk. Jika tidak, pengguna akan keluar dan semua perubahan yang belum disimpan akan hilang.

Nilai prasetelnya adalah: **Aktif. Batas waktu: 10 menit.**

Tampilkan notifikasi tentang masuk terakhir dari pengguna saat ini

Opsi ini memungkinkan untuk menampilkan tanggal dan waktu berhasil masuk terakhir pengguna, jumlah kegagalan autentikasi sejak berhasil masuk terakhir, dan alamat IP dari berhasil masuk terakhir. Informasi ini ditampilkan di bagian bawah layar setiap kali pengguna masuk.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Peringatkan tentang masa berlaku kata sandi lokal atau domain

Opsi ini memungkinkan ditampilkannya peringatan ketika kata sandi untuk akses pengguna ke Server Manajemen Acronis Cyber Protect akan kedaluwarsa. Ini adalah kata sandi lokal atau domain yang digunakan pengguna untuk masuk ke mesin tempat server manajemen diinstal. Waktu sebelum kata sandi kedaluwarsa akan ditampilkan di bagian bawah layar dan di menu akun di sudut kanan atas.

Nilai prasetelnya adalah: **Dinonaktifkan**.

Pembaruan

Opsi ini menentukan apakah Acronis Cyber Protect akan memeriksa versi baru setiap kali administrator organisasi masuk ke konsol web Cyber Protect.

Nilai prasetelnya adalah: **Aktif**.

Jika opsi ini dinonaktifkan, administrator dapat memeriksa pembaruan secara manual seperti yang dijelaskan dalam "Memeriksa pembaruan perangkat lunak".

Opsi cadangan default

Nilai default opsi pencadangan bersifat umum untuk semua rencana proteksi di server manajemen. Administrator organisasi dapat mengubah nilai opsi default dari yang sudah ditentukan sebelumnya. Nilai baru akan digunakan secara default di semua rencana proteksi yang dibuat 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. Masuk ke konsol web Cyber Protect sebagai administrator organisasi.
2. Klik **Pengaturan** > **Pengaturan sistem**.
3. Perluas bagian **Opsi pencadangan default**.
4. Pilih opsi, lalu buat perubahan yang diperlukan.
5. Klik **Simpan**.

Pengaturan perlindungan

Untuk mengonfigurasi pengaturan perlindungan, di konsol web Cyber Protect, buka **Pengaturan** > **Perlindungan**.

Untuk informasi lebih lanjut tentang pengaturan dan prosedur tertentu, lihat topik terkait di bagian ini.

Memperbarui definisi perlindungan

Secara default, semua agen perlindungan dapat terhubung ke Internet dan mengunduh pembaruan untuk komponen berikut:

- Antimalware
- Penilaian kerentanan
- Manajemen patch

Agen dengan peran Updater

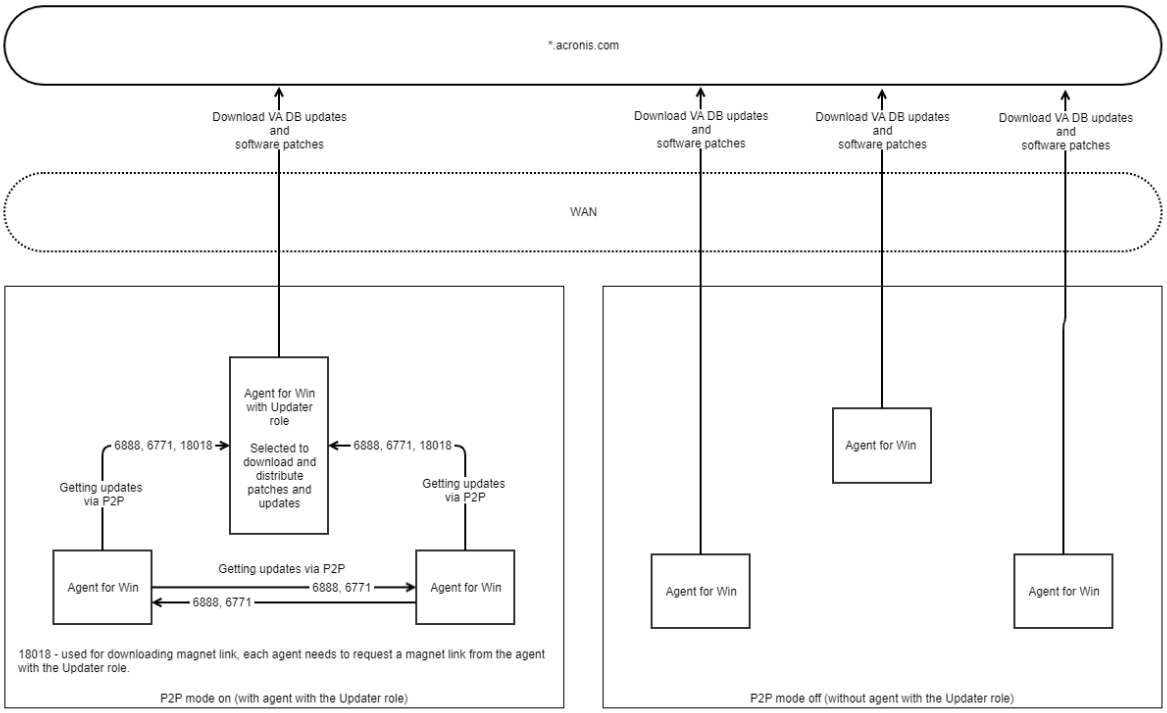
Administrator dapat meminimalkan lalu lintas bandwidth jaringan dengan memilih satu atau beberapa agen di lingkungan dan menetapkan peran Updater ke mereka. Maka, para agen khusus akan terhubung ke Internet dan mengunduh pembaruan. Agen lainnya akan terhubung ke agen pembuat pembaruan khusus menggunakan 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.

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.

Anda dapat menetapkan peran Pembuat Pembaruan ke banyak agen di lingkungan. Maka, jika satu agen dengan peran Updater sedang offline, agen lain dengan peran ini dapat menjadi sumber definisi perlindungan yang diperbarui.

Diagram berikut menggambarkan beberapa opsi untuk mengunduh pembaruan perlindungan. Di sisi kiri, agen ditetapkan peran Updater. Agen itu terhubung ke Internet untuk mengunduh pembaruan perlindungan, dan agen setaranya terhubung ke agen Updater untuk mendapatkan pembaruan terakhir. Di sisi kanan, tidak ada agen yang ditetapkan peran Updater, sehingga semua agen terhubung ke Internet untuk mengunduh pembaruan perlindungan.



Untuk mempersiapkan mesin demi peran Pembuat Pembaruan

1. Di mesin agen tempat agen dengan peran Updater akan berjalan, 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 Layanan Acronis Agent Core.
3. Mulai ulang Layanan Firewall

Jika Anda tidak menerapkan aturan ini dan firewall diaktifkan, agen rekan akan mengunduh pembaruan dari awan.

Untuk menetapkan peran Updater pada agen

1. Di konsol web 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**.

Menjadwalkan pembaruan

Anda dapat menjadwalkan pembaruan otomatis definisi perlindungan pada semua agen atau memperbaruinya secara manual pada agen yang dipilih.

Untuk menjadwalkan pembaruan otomatis

1. Di konsol web Cyber Protect, buka **Pengaturan** > **Perlindungan** > **Pembaruan definisi perlindungan**.
2. Pilih **Jadwal**.
3. Di **Jenis jadwal**, pilih salah satu opsi berikut:
   - **Setiap hari**

     Pilih hari untuk memperbarui definisi perlindungan.

     Di bagian **Mulai pada**, pilih waktu saat pembaruan dimulai.
   - **Per jam**

     Jadwal terperinci untuk pembaruan.

     Di bagian **Jalankan setiap**, tentukan pembaruan periodik.

     Di bagian **Dari** ... **Hingga**, tentukan rentang waktu spesifik untuk pembaruan.

Untuk memperbarui definisi perlindungan secara manual

1. Di konsol web Cyber Protect, buka **Pengaturan** > **Agen**.
2. Pilih mesin agen yang ingin Anda perbarui definisi perlindungannya, lalu klik **Perbarui definisi**.

Mengubah lokasi unduhan

Definisi perlindungan diunduh ke folder sementara default di mesin Anda, lalu disimpan di folder program Acronis.

Untuk mengubah folder unduhan sementara

1. Pada mesin server manajemen, buka file `atp-database-mirror.json` untuk pengeditan.

   Anda dapat menemukan file ini di lokasi berikut:
   - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
2. Ubah nilai `"enable_user_config"` ke `true`.

```
{
"sysconfig":
{
...
"enable_user_config": true
}
...
```

```
}
```

3. Pada mesin server manajemen, buka file `config.json` untuk pengeditan.
   Anda dapat menemukan file ini di lokasi berikut:
   - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
4. Tambahkan baris berikut: `"mirror_temp_dir": "<path_to_new_download_location>"`
   Contoh:

   ```
   {
           "mirror_temp_dir": "C:\\temp"
   }
   ```

   Jalur dapat bersifat absolut atau relatif terhadap folder `AppData`.
   Jika folder tidak dapat dibuat atau server manajemen tidak dapat menulis ke folder tersebut, lokasi default akan digunakan.

Opsi penyimpanan cache

Cache data disimpan di lokasi berikut:

- Windows: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Linux: `/opt/acronis/var/atp-downloader/Cache`
- macOS: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Anda dapat mengonfigurasi jadwal untuk membersihkan cache data lama dan menetapkan batas ukurannya. Anda dapat menetapkan batas yang berbeda untuk mesin dengan agen non-updater dan mesin dengan agen updater.

Sumber definisi perlindungan terbaru

Anda dapat mengunduh definisi perlindungan terbaru dari lokasi berikut:

- **Awan**
  Agen perlindungan terhubung ke Internet dan mengunduh definisi perlindungan terbaru dari Acronis Cloud. Secara default, semua agen yang terdaftar di server manajemen akan memeriksa pembaruan dan mendistribusikannya. Untuk informasi selengkapnya tentang agen dengan peran Updater, lihat "Memperbarui definisi perlindungan" (hlm. 627).
- **Server Manajemen Cyber Protect**
  Dengan opsi ini, agen tidak akan memerlukan akses ke Internet. Mereka hanya terhubung ke server manajemen tempat definisi perlindungan disimpan. Meski demikian, server manajemen harus tersambung ke Internet untuk mengunduh definisi perlindungan terbaru.
- **Server web kustom**

Opsi ini hanya ditujukan untuk pemecahan masalah dan pengujian atau untuk digunakan di lingkungan air-gap. Untuk informasi lebih lanjut, lihat "Memperbarui definisi perlindungan dalam lingkungan air-gap" (hlm. 631). Biasanya, Anda akan perlu memilih opsi ini hanya jika diinstruksikan oleh tim dukungan Acronis.

Koneksi jarak jauh

Ketika Anda mengaktifkan koneksi jarak jauh, opsi **Sambungkan melalui klien RDP** dan **Sambungkan melalui klien HTML5** muncul di konsol web Cyber Protect, di bawah **Desktop Perlindungan Siber** pada menu sebelah kanan. Menu sebelah kanan terbuka saat Anda memilih beban kerja pada tab **Perangkat**.

Mengaktifkan atau menonaktifkan koneksi jarak jauh memengaruhi semua pengguna organisasi Anda.

Untuk mengaktifkan koneksi jarak jauh

1. Di konsol web Cyber Protect, buka **Pengaturan** > **Perlindungan**.
2. Klik **Koneksi jarak jauh**, lalu aktifkan switch **Koneksi desktop jarak jauh**.

Selain itu, Anda dapat mengaktifkan berbagi koneksi jarak jauh. Dengan opsi ini, Anda dapat membuat tautan yang memungkinkan akses beban kerja yang dipilih dari jarak jauh. Anda dapat membagikan tautan ini dengan pengguna lain.

Untuk mengaktifkan berbagi koneksi jarak jauh

1. Di konsol web Cyber Protect, buka **Pengaturan** > **Perlindungan**.
2. Pilih kotak centang **Bagikan koneksi desktop jarak jauh**.

Hasilnya, opsi **Bagikan koneksi jarak jauh** muncul dalam konsol web Cyber Protect, di bawah **Desktop Perlindungan Siber** di menu sebelah kanan.

Memperbarui definisi perlindungan dalam lingkungan air-gap

Acronis Cyber Protect mendukung pembaruan definisi perlindungan dalam lingkungan air-gap.

Untuk memperbarui definisi perlindungan dalam lingkungan air-gap

1. Instal server manajemen kedua yang dapat mengakses Internet, di luar lingkungan dengan air-gap.
   Untuk informasi lebih lanjut tentang cara melakukannya, lihat "Menginstal server manajemen" (hlm. 83).
2. Salin definisi perlindungan dari server manajemen online ke drive yang dapat dilepas, lalu transfer definisi ke server HTTP di lingkungan dengan air-gap.

Untuk informasi lebih lanjut tentang langkah ini, lihat "Mengunduh definisi ke server manajemen online" (hlm. 632) dan "Mentransfer definisi ke server HTTP" (hlm. 633).

3. Pada server manajemen dengan air-gap, konfigurasi server HTTP sebagai sumber definisi perlindungan yang diperbarui.
   Untuk informasi lebih lanjut tentang langkah ini, lihat "Mengonfigurasi sumber definisi pada server manajemen dengan air-gap" (hlm. 634).

Mengunduh definisi ke server manajemen online

Setelah menginstal server manajemen kedua yang dapat mengakses Internet, unduh definisi perlindungan terbaru dan salin ke drive yang dapat dilepas, seperti memori flash USB atau hard drive eksternal.

Untuk mengunduh dan menyalin definisi perlindungan

1. Pada mesin dengan server manajemen online, salin folder `AtpDatabaseMirror` ke lokasi pilihan Anda – misalnya, desktop atau folder `Temp`.
   Anda dapat menemukan folder `AtpDatabaseMirror` di lokasi berikut:
   - Windows: `%ProgramData%\Acronis\`
   - Linux: `/usr/lib/Acronis/`
2. Buka file `atp_database_mirror.json` untuk mengedit. Anda dapat menemukan file di lokasi berikut:
   - Windows: `%Program Files%\Acronis\AtpDatabaseMirror`

     Catatan
     Di Windows, folder ini tidak sama dengan folder di langkah sebelumnya.

   - Linux: `/usr/lib/Acronis/AppDatabaseMonitor`
3. Edit file `atp_database_mirror.json` seperti berikut:
   a. Ubah nilai `"enable_appdata_as_root"` ke `false`.
   b. Ubah nilai dari semua entri `"local_path"` ke jalur absolut lokasi tempat Anda ingin menyimpan definisi perlindungan.
4. Simpan perubahan di file `atp_database_mirror.json`.
5. Pada mesin dengan server manajemen online, hentikan layanan **Server Manajemen Acronis** menggunakan perintah berikut:
   - Windows (Saran Perintah):

     ```
     sc stop AcrMngSrv
     ```

   - Linux (Terminal):

     ```
     sudo systemctl stop acronis_ams.service
     ```

6. Di folder `AtpDatabaseMirror` yang Anda salin ke lokasi pilihan Anda, mulai alat bantu `AtpDatabaseMirror` menggunakan perintah berikut:
   - Windows (Saran Perintah):
     ```
     atp_database_mirror.exe -config atp_database_mirror.json
     ```
   - Linux (Terminal):
     ```
     sudo ./atp_database_mirror -config atp_database_mirror.json
     ```

   Ketika semua pembaruan diunduh ke folder yang Anda tentukan di `"local_path"`, baris berikut akan muncul di jendela Saran Perintah atau Terminal:
   ```
   standing by for 1m0s
   ```
7. Hentikan alat bantu `AtpDatabaseMirror` dengan menekan CTRL+C.
8. Salin file dari folder yang Anda tentukan di `"local_path"` ke drive yang dapat dilepas.

Berikutnya, Anda harus menyalin file dari drive yang dapat dilepas ke server HTTP di lingkungan air-gap. Anda dapat menggunakan server manajemen air-gap sebagai server HTTP. Untuk informasi lebih lanjut, lihat "Mentransfer definisi ke server HTTP" (hlm. 633).

Mentransfer definisi ke server HTTP

Untuk mendistribusikan definisi perlindungan di lingkungan dengan air-gap, Anda memerlukan server HTTP khusus. Anda dapat menggunakan server manajemen air-gap sebagai server HTTP.

Untuk mentransfer definisi ke server HTTP

1. Di mesin tempat Anda menjalankan server HTTP, salin definisi perlindungan ke folder pilihan Anda.
2. Dari folder tempat Anda menyalin definisi perlindungan, mulai server HTTP.
   Misalnya, Anda dapat menggunakan Python dan menjalankan perintah berikut:
   ```
   python -m http.server 8080
   ```

   Catatan
   Anda dapat menggunakan server HTTP apa pun yang Anda inginkan.
3. Di folder tempat Anda menyalin definisi perlindungan, buka file `perbarui-index.json` berikut untuk mengedit:
   - `./ngmp/update-index.json`
   - `./vapm/update-index.json`
4. Di kedua file `update-index.json`, edit semua bidang `products > os > arch > components > versions > url`, seperti berikut:

a. Sebagai nilai `IP` dan `port`, tetapkan alamat IP dan port server HTTP Anda.

b. Jangan mengubah bagian lainnya dari jalur.

Misalnya, `"url": "http://192.168.1.10:8080/ngmp/win64/ngmp.zip"`, where 192.168.1.10 adalah alamat IP server HTTP dan 8080 adalah port-nya. Jangan mengubah bagian `/ngmp/win64/ngmp.zip`.

5. Simpan editan Anda di kedua file `update-index.json`.

Berikutnya, Anda harus mengonfigurasi sumber definisi perlindungan pada server manajemen dengan air-gap. Untuk informasi lebih lanjut, lihat "Mengonfigurasi sumber definisi pada server manajemen dengan air-gap" (hlm. 634).

Mengonfigurasi sumber definisi pada server manajemen dengan air-gap

Setelah mengonfigurasi server HTTP, Anda harus mengonfigurasikannya pada server manajemen dengan air-gap sebagai sumber definisi perlindungan.

Untuk mengonfigurasi sumber definisi perlindungan pada server manajemen dengan air-gap

1. Di konsol web Cyber Protect server manajemen dengan air-gap, buka **Pengaturan** > **Perlindungan** > **Pembaruan definisi perlindungan.**.
2. Pilih **Definisi**.
3. Pilih **Kustom**, lalu tentukan jalur berikut:

- Untuk **Definisi Antivirus dan Antimalware**:
  `http://<IP address of your HTTP server>:8080/scanner`
- Untuk **Definisi deteksi lanjutan**:
  `http://<IP address of your HTTP server>:8080/ngmp`
- Untuk **Definisi penilaian kerentanan dan manajemen patch**:
  `http://<IP address of your HTTP server>:8080/vapm`

Hasilnya, agen di lingkungan air-gap akan mengunduh definisi perlindungan dari server HTTP Anda.

Pengelolaan akun pengguna dan unit organisasi

Penyebaran di lokasi

Fungsi yang dijelaskan dalam bagian ini hanya tersedia untuk administrator organisasi.

Untuk mengakses pengaturan ini, klik **Pengaturan** > **Akun**.

Unit dan akun administratif

Untuk mengelola unit dan akun administratif, di Cyber Protect konsol web, buka **Setelan** > **Akun**. Panel **Akun** menampilkan grup **Organisasi** dengan pohon unit (jika ada), serta daftar akun administratif pada tingkat hierarki yang dipilih.

Unit-unit

Grup **Organisasi** secara otomatis dibuat ketika Anda menginstal server manajemen. Dengan lisensi Acronis Cyber Protect Advanced, Anda dapat membuat grup turunan yang disebut unit, yang biasanya sesuai dengan unit atau departemen organisasi, dan menambahkan akun administratif ke unit tersebut. Dengan cara ini, Anda dapat mendelegasikan manajemen perlindungan kepada orang lain yang izin aksesnya akan dibatasi secara ketat ke unit yang sesuai. Untuk informasi tentang cara membuat unit, lihat "Membuat unit" (hlm. 639).

Setiap unit dapat memilik unit turunan. Akun administratif unit induk memiliki hak yang sama di semua unit turunan. Grup **Organisasi** adalah unit induk tingkat atas, dan akun administratif pada tingkat ini memiliki hak yang sama di semua unit.

Akun administratif

Setiap akun yang dapat masuk ke konsol web Cyber Protect adalah akun administratif.

Di konsol web Cyber Protect, akun administratif apa pun dapat melihat atau mengelola apa pun pada atau di bawah tingkat hierarki unitnya. Misalnya, akun administratif di *organisasi* memiliki akses ke tingkat atas ini dan oleh karena itu akses ke semua unit organisasi ini, sementara akun administratif di *unit* tertentu hanya dapat mengakses unit ini dan unit turunannya.

Akun mana yang dapat menjadi administratif?

Jika server manajemen diinstal pada mesin Windows yang disertakan dalam domain Active Directory, Anda dapat memberikan hak administratif kepada pengguna lokal, atau pengguna dan grup pengguna dalam hutan domain Active Directory.

Secara default, server manajemen membangun koneksi yang terproteksi SSL/TLS ke kontroler domain Active Directory. Jika ini tidak memungkinkan, tidak ada koneksi yang akan dibuat. Namun, Anda dapat mengizinkan koneksi yang tidak aman, dengan mengedit file `auth-connector.json5`.

Untuk menggunakan koneksi yang aman, pastikan bahwa LDAP melalui SSL (LDAP) dikonfigurasi untuk Active Directory Anda.

Untuk mengonfigurasi LDAP untuk Active Directory

1. Pada pengontrol domain, buat dan instal sertifikat LDAP yang memenuhi persyaratan Microsoft.
   Untuk informasi lebih lanjut tentang cara pengoperasian, lihat Mengaktifkan LDAP melalui SSL dengan otoritas sertifikasi pihak ketiga di dokumentasi Microsoft.
2. Pada pengontrol domain, buka **Microsoft Konsol Manajemen** dan verifikasi bahwa sertifikat ada di dalam **Sertifikat (Komputer Lokal)** > **Personal** > **Sertifikat**.
3. Mulai Kembali pengontrol domain.
4. Verifikasi bahwa LDAP diaktifkan.

Untuk mengizinkan koneksi tidak aman ke pengontrol domain

1. Masuk ke mesin tempat server manajemen diinstal.
2. Buka file `auth-connector.json5` untuk diedit.
   File `auth-connector.json5` terletak di `%APPDATA%\Acronis\AuthConnector`
3. Buka bagian **sinkronisasi**, dan di setiap baris **"connectionMode"**, ganti **"ssl_only"** dengan **"auto"**.
   Dalam mode **otomatis**, koneksi tidak aman akan dibuat jika koneksi TLS tidak memungkinkan.
4. Mulai ulang **Layanan Acronis Service Manager** seperti yang dijelaskan di "Untuk memulai ulang Layanan Acronis Service Manager" (hlm. 197).

Catatan
Jika server manajemen tidak disertakan dalam domain Active Directory atau jika diinstal pada mesin Linux, Anda dapat memberikan hak administratif hanya kepada pengguna dan grup lokal.

Untuk mempelajari cara menambahkan akun administratif ke server manajemen, lihat "Menambahkan akun administratif" (hlm. 638).

Peran akun administratif

Setiap akun administratif diberi peran dengan hak yang telah ditentukan sebelumnya, yang diperlukan untuk tugas tertentu. Peran akun administratif adalah sebagai berikut:

- **Administrator**
  Peran ini memberikan akses administratif penuh ke organisasi atau unit.
- **Hanya baca**
  Peran ini menyediakan akses hanya baca ke konsol web Cyber Protect. Ini hanya memungkinkan pengumpulan data diagnostik, seperti laporan sistem. Peran hanya baca tidak mengizinkan penelusuran cadangan atau menelusuri konten kotak surat yang dicadangkan.
- **Auditor**
  Peran ini memberikan akses hanya baca ke tab **Aktivitas** di Cyber Protect konsol web. Untuk

informasi lebih lanjut tentang tab ini, lihat "Tab Aktivitas" (hlm. 582). Peran ini tidak mengizinkan pengumpulan atau ekspor data apa pun, termasuk informasi sistem dari server manajemen.

Setiap perubahan dalam peran ditampilkan di tab **Aktivitas**.

Pewarisan peran

Peran dalam unit induk diwarisi oleh unit turunannya. Jika akun pengguna yang sama memiliki peran berbeda yang ditetapkan di unit induk dan di unit turunan, akun akan memiliki kedua peran tersebut.

Selain itu, peran dapat ditetapkan secara eksplisit ke akun pengguna tertentu atau diwarisi dari grup pengguna. Dengan demikian, akun pengguna dapat memiliki peran yang ditetapkan secara khusus dan yang diwariskan.

Jika akun pengguna memiliki peran berbeda (ditetapkan dan/atau diwariskan), akun tersebut dapat mengakses objek dan melakukan tindakan yang diizinkan oleh salah satu peran ini. Misalnya, akun pengguna dengan peran hanya baca yang ditetapkan dan peran administrator yang diwarisi akan memiliki hak administrator.

Penting
Di konsol web Cyber Protect, hanya peran yang ditetapkan secara eksplisit untuk unit saat ini yang ditampilkan. Semua kemungkinan perbedaan dengan peran yang diwariskan tidak ditampilkan. Kami sangat menyarankan agar Anda menetapkan peran administrator, hanya baca, dan auditor ke akun atau grup terpisah, untuk menghindari kemungkinan masalah dengan peran yang diwariskan.

Administrator default

Di Windows

Ketika server manajemen sedang diinstal pada mesin, hal berikut akan terjadi:

- Grup pengguna **Admin Terpusat Acronis** dibuat di mesin.
  Di pengontrol domain, grup tersebut diberi nama *DCNAME* **$ Acronis Centralized Admins**. Di sini, *DCNAME* adalah singkatan dari nama NetBIOS pengontrol domain.
- Semua anggota grup **Administrator** akan ditambahkan ke grup **Admin Terpusat Acronis**. Jika mesin berada dalam domain tetapi bukan pengontrol domain, pengguna lokal (non-domain) kemudian akan dikecualikan. Pada pengontrol domain, tidak ada pengguna non-domain.
- Grup **Admin Terpusat Acronis** dan **Administrator** ditambahkan ke server manajemen sebagai **administrator organisasi**. Jika mesin berada dalam domain tetapi bukan pengontrol domain, grup **Administrator** tidak akan ditambahkan, sehingga pengguna lokal (non-domain) tidak menjadi administrator organisasi.

Anda dapat menghapus grup **Administrator** dari daftar administrator organisasi. Namun, grup **Admin Terpusat Acronis** tidak dapat dihapus. Jika semua administrator organisasi telah dihapus, Anda dapat menambahkan akun ke grup **Admin Terpusat Acronis** di Windows, kemudian masuk ke konsol web Cyber Protect dengan menggunakan akun ini.

Di Linux

Ketika server manajemen sedang diinstal pada mesin, pengguna **root** akan ditambahkan ke server manajemen sebagai **administrator organisasi**.

Anda dapat menambahkan pengguna Linux lainnya ke daftar administrator server manajemen, seperti yang dijelaskan nanti, dan kemudian menghapus pengguna **root** dari daftar ini. Apabila terjadi penghapusan semua administrator organisasi, Anda dapat memulai kembali layanan `acronis_asm`. Hasilnya, pengguna **root** akan ditambahkan kembali secara otomatis sebagai administrator organisasi.

Akun administratif di berbagai unit

Suatu akun dapat diberikan hak administratif dalam jumlah unit berapa pun. Untuk akun semacam itu, serta untuk akun administratif di tingkat organisasi, pemilih unit ditampilkan di konsol web Cyber Protect. Dengan menggunakan pemilih ini, akun ini dapat melihat dan mengelola setiap unit secara terpisah.

Akun yang memiliki izin untuk semua unit di organisasi tidak memiliki izin untuk organisasi. Akun administratif pada tingkat organisasi harus ditambahkan ke grup **Organisasi** secara eksplisit.

Cara mengisi unit dengan mesin

Ketika administrator menambahkan mesin melalui antarmuka web, mesin akan ditambahkan ke unit yang dikelola oleh administrator. Jika administrator mengelola beberapa unit, mesin akan ditambahkan ke unit yang dipilih dalam pemilih unit. Oleh karena itu, administrator harus memilih unit sebelum mengklik **Tambah**.

Ketika menginstal agen secara lokal, administrator akan memberikan kredensial mereka. Mesin ditambahkan ke unit yang dikelola oleh administrator. Jika administrator mengelola beberapa unit, installer akan meminta Anda memilih unit yang akan ditambahkan mesin untuknya.

Menambahkan akun administratif

Catatan
Fitur ini tidak tersedia pada edisi Standard dan Essentials.

Untuk menambahkan akun

1. Klik **Pengaturan** > **Akun**.
   Perangkat lunak menampilkan daftar administrator server manajemen dan hierarki unit (jika ada).
2. Pilih **Organisasi** atau pilih unit tempat Anda ingin menambahkan administrator.
3. Klik **Tambahkan akun**.

4. Di **Domain**, pilih domain yang berisi akun pengguna yang ingin Anda tambahkan. Jika server manajemen tidak termasuk dalam domain Active Directory atau diinstal di Linux, hanya pengguna lokal yang dapat ditambahkan.
5. Cari nama pengguna atau nama grup pengguna.
6. Klik "+" di sebelah nama pengguna atau grup.
7. Pilih peran untuk akun.
8. Ulangi langkah 4-6 untuk semua pengguna atau grup yang ingin Anda tambahkan.
9. Setelah selesai, klik **Selesai**.
10. [Hanya di Linux] Tambahkan nama pengguna ke konfigurasi Pluggable Authentication Module (PAM) untuk modul Acronis seperti dijelaskan di bawah ini.

Untuk menambahkan nama pengguna ke konfigurasi PAM untuk Acronis

Prosedur ini berlaku untuk server manajemen yang berjalan di mesin Linux dan di All-in-One Appliance Acronis Cyber Protect.

1. Pada mesin yang menjalankan server manajemen, sebagai pengguna root, buka file **/etc/security/acronisagent.conf** dengan editor teks.
2. Dalam file ini, ketikkan nama pengguna yang Anda tambahkan sebagai administrator server manajemen, satu nama per baris.
3. Simpan lalu tutup file.

Membuat unit

1. Klik **Pengaturan** > **Akun**.
2. Perangkat lunak menampilkan daftar administrator server manajemen dan hierarki unit (jika ada).
3. Pilih **Organisasi** atau pilih unit induk untuk unit baru.
4. Klik **Buat unit**.
5. Tentukan nama untuk unit baru, lalu klik **Buat**.

Penyebaran awan

Pengelolaan akun pengguna dan unit organisasi tersedia pada portal manajemen. Untuk mengakses portal manajemen, klik **Portal Manajemen** ketika masuk ke layanan Perlindungan Cyber atau klik ikon  di pojok kanan atas, lalu klik **Portal manajemen**. Hanya pengguna dengan privilese administratif yang dapat mengakses portal ini.

Untuk informasi tentang pengelolaan akun pengguna dan unit organisasi, lihat Panduan Administrator Portal Manajemen. Untuk mengakses dokumen ini, klik ikon tanda tanya pada portal manajemen.

Bagian ini memberikan informasi tambahan terkait dengan pengelolaan layanan Perlindungan Cyber.

Kuota

Kuota memungkinkan Anda untuk membatasi kemampuan pengguna dalam menggunakan layanan. Untuk menetapkan kuota, pilih pengguna pada tab **Pengguna**, lalu klik ikon pensil pada bagian **Kuota**.

Ketika kuota melebihi batas, pemberitahuan akan dikirim ke alamat email pengguna. Jika Anda tidak menetapkan kelebihan kuota, kuota akan dianggap sebagai "lunak". Ini berarti bahwa pembatasan penggunaan layanan Perlindungan Cyber tidak diterapkan.

Anda juga dapat menentukan kelebihan kuota. Kelebihan memungkinkan pengguna untuk melampaui kuota sebesar nilai yang ditentukan. Saat kelebihan terlampaui, pembatasan penggunaan layanan Perlindungan Cyber diterapkan.

Cadangan

Anda dapat menentukan kuota penyimpanan awan, kuota untuk cadangan lokal, dan jumlah mesin/perangkat/kotak surat maksimum yang diizinkan untuk dilindungi oleh pengguna. Kuota berikut tersedia:

- **Penyimpanan awan**
- **Stasiun Kerja**
- **Server**
- **Windows Server Essentials**
- **Host virtual**
- **Universal**
  Kuota ini dapat digunakan sebagai pengganti salah satu dari empat kuota yang ada di atas: Workstations, Servers, Windows Server Essentials, Host Virtual.
- **Perangkat seluler**
- **Kotak surat Microsoft 365**
- **Cadangan lokal**

Mesin/perangkat/kotak surat dianggap terlindungi selama setidaknya memiliki satu rencana proteksi. Perangkat seluler menjadi terlindungi setelah pencadangan pertama.

Ketika kelebihan kuota penyimpanan awan terlampaui, pencadangan akan gagal. Saat kelebihan untuk sejumlah perangkat terlampaui, pengguna tidak dapat menerapkan rencana proteksi ke lebih banyak perangkat.

Kuota **Cadangan lokal** membatasi ukuran total cadangan lokal yang dibuat menggunakan infrastruktur awan. Kelebihan tidak dapat ditetapkan untuk kuota ini.

Pemulihan bencana

Kuota ini diberlakukan oleh penyedia layanan ke seluruh perusahaan. Administrator perusahaan dapat melihat kuota dan penggunaan pada portal manajemen, namun tidak dapat menetapkan kuota bagi pengguna.

- **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 tetap berjalan.

  Ketika kuota dinonaktifkan, semua server akan dihapus. Tab **Situs pemulihan awan** akan hilang dari konsol web Cyber Protect.
- **Titik komputasi**

  Kuota ini membatasi sumber daya CPU dan RAM yang dikonsumsi oleh server utama dan pemulihan selama masa penagihan. Jika kelebihan untuk kuota ini terlampaui, semua server utama dan pemulihan akan dimatikan. Penggunaan server tersebut tidak dimungkinkan hingga awal masa penagihan berikutnya. Masa pembayaran default adalah satu bulan kalender penuh.

  Ketika kuota dinonaktifkan, server tidak dapat digunakan terlepas dari periode pembayarannya.
- **Alamat IP publik**

  Kuota ini membatasi jumlah alamat IP publik yang dapat ditetapkan ke server utama dan pemulihan. Jika kelebihan untuk kuota ini terlampaui, tidak dimungkinkan untuk mengaktifkan alamat IP publik untuk lebih banyak server. Anda dapat menolak server untuk menggunakan alamat IP publik, dengan mengosongkan kotak centang **Alamat IP publik** pada pengaturan server. Setelah itu, Anda dapat mengizinkan server lain untuk menggunakan alamat IP publik, yang biasanya tidak akan sama.

  Ketika kuota dinonaktifkan, semua server akan berhenti menggunakan alamat IP publik, sehingga tidak dapat lagi dijangkau dari internet.
- **Server awan**

  Kuota ini membatasi jumlah total server utama dan pemulihan. Jika kelebihan untuk kuota ini terlampaui, tidak dimungkinkan untuk membuat server utama atau server pemulihan.

  Jika kuota dinonaktifkan, server akan terlihat di konsol web Cyber Protect, tetapi satu-satunya operasi yang tersedia adalah **Hapus**.
- **Akses internet**

  Kuota ini mengaktifkan atau menonaktifkan akses internet dari server utama dan pemulihan.

  Ketika kuota dinonaktifkan, server utama dan pemulihan langsung diputuskan koneksinya dari internet. Switch **Akses internet** pada properti server akan dihapus dan dinonaktifkan.

Pemberitahuan

Untuk mengubah pengaturan pemberitahuan bagi pengguna, pilih pengguna pada tab **Pengguna**, lalu klik ikon pensil pada bagian **Pengaturan**. Pengaturan pemberitahuan berikut tersedia:

- **Pemberitahuan kuota berlebih** (diaktifkan secara default)
  Pemberitahuan tentang penggunaan kuota yang terlampaui.
- **Laporan penggunaan terjadwal**
  Laporan penggunaan yang dijelaskan di bawah ini dikirim pada tanggal satu setiap bulannya.
- **Notifikasi kegagalan**, **Pemberitahuan peringatan**, dan **Pemberitahuan sukses** (dinonaktifkan secara default)
  Pemberitahuan tentang hasil eksekusi rencana proteksi dan hasil operasi pemulihan bencana untuk setiap perangkat.
- **Rekap harian tentang peringatan aktif** (diaktifkan secara default)
  Rekap yang menginformasikan tentang pencadangan yang gagal, pencadangan yang terlewat, dan masalah lainnya. Rekap dikirim pada pukul 10:00 (waktu pusat data). Jika tidak ada masalah, rekap tidak dikirimkan.

Semua pemberitahuan dikirim ke alamat email pengguna.

Laporan

Laporan tentang penggunaan layanan Perlindungan Cyber mencakup data berikut tentang organisasi atau unit:

- Ukuran cadangan berdasarkan unit, pengguna, dan jenis perangkat.
- Jumlah perangkat yang terlindungi berdasarkan unit, pengguna, jenis perangkat.
- Nilai harga berdasarkan unit, pengguna, jenis perangkat.
- Ukuran total cadangan.
- Jumlah total perangkat yang dilindungi.
- Total nilai harga.

Referensi baris perintah

Referensi baris perintah adalah dokumen terpisah yang tersedia di https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect_15_Command_Line_Reference/index.html.

Penyelesaian masalah

Bagian ini menjelaskan cara menyimpan log agen ke file .zip. Jika pencadangan gagal karena alasan yang tidak jelas, file ini akan membantu personel dukungan teknis untuk mengidentifikasi masalah.

Untuk mengumpulkan log

1. Lakukan salah satu langkah berikut:
   - Pada **Perangkat**, pilih mesin yang darinya Anda ingin mengumpulkan log, lalu klik **Aktivitas**.
   - Pada **Pengaturan** > **Agen**, pilih mesin yang darinya Anda ingin mengumpulkan log, lalu klik **Detail**.
2. Klik **Kumpulkan informasi sistem**.
3. Jika diminta oleh browser web Anda, tentukan di mana file tersebut tersimpan.

Glosarium

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.

F

Format cadangan file tunggal

Format cadangan baru, di mana cadangan penuh awal dan inkremental selanjutnya akan disimpan ke file .tib tunggal, bukan rantai file. 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, misalnya server SFTP.

L

Lokasi yang dikelola

Lokasi cadangan yang dikelola oleh simpul penyimpanan. Secara fisik, lokasi yang dikelola dapat berada di jaringan bersama, SAN, NAS, di hard drive lokal ke simpul penyimpanan, atau di pustaka pita yang terpasang secara lokal ke simpul penyimpanan. Simpul penyimpanan melakukan pembersihan dan validasi (jika itu termasuk dalam rencana proteksi) untuk setiap cadangan yang disimpan di lokasi terkelola. Anda dapat menentukan operasi tambahan yang akan dilakukan oleh simpul penyimpanan (deduplikasi, enkripsi).

S

Set cadangan

Sejumlah cadangan yang untuknya aturan retensi individual dapat diterapkan. Untuk skema pencadangan Kustom, set cadangan sesuai dengan metode pencadangan (Penuh, Diferensial, dan Inkremental). Dalam semua kasus lainnya, set cadangannya adalah Bulanan, Harian, Mingguan, dan per Jam. Pencadangan bulanan adalah cadangan pertama yang dibuat pada awal suatu bulan. Pencadangan mingguan adalah cadangan pertama yang dibuat pada hari dalam minggu yang dipilih dalam opsi pencadangan Mingguan (klik ikon roda, lalu Opsi pencadangan > Cadangan mingguan). Apabila pencadangan mingguan adalah cadangan pertama yang dibuat setelah awal suatu bulan, cadangan ini dianggap sebagai cadangan bulanan. Dalam hal ini, pencadangan mingguan akan dibuat

pada hari yang dipilih untuk minggu berikutnya. Pencadangan harian adalah cadangan pertama yang dibuat pada awal suatu hari, kecuali jika cadangan ini termasuk dalam definisi cadangan bulanan atau mingguan. Pencadangan per jam adalah cadangan yang pertama dibuat pada awal suatu jam, kecuali jika cadangan ini termasuk dalam definisi cadangan bulanan, mingguan, atau harian.

Startup Recovery Manager

Modifikasi pada agen yang dapat di-boot yang ada di disk sistem dan dikonfigurasi untuk dimulai pada waktu boot ketika F11 ditekan. Startup Recovery Manager mengeliminasi kebutuhan akan media cadangan atau koneksi jaringan untuk memulai utilitas cadangan yang dapat di-boot. Startup Recovery Manager berguna khususnya bagi pengguna seluler. Jika terjadi kegagalan, pengguna akan mem-boot ulang mesin, menekan F11 pada perintah "Tekan F11 untuk Startup Recovery Manager...", dan melakukan pemulihan data dengan cara yang sama seperti umumnya media yang dapat di-boot. Batasan: memerlukan aktivasi ulang pemuat, selain pemuat Windows dan GRUB.

Indeks

B

C

E

F

G

H

I

M

P

T

U

V

W

Y