Acronis

acronis.com

Cyberbescherming

24.04

Gebruikershandleiding

REVISIE: 9-5-2024

Inhoudsopgave

Aan de slag met Cyber Protection

Het account activeren

Wanneer een beheerder een account voor u maakt, wordt een e-mailbericht naar uw e-mailadres verzonden. Het bericht bevat de volgende informatie:

- **Uw gebruikersnaam.** Dit is de gebruikersnaam die u gebruikt om u aan te melden. Uw gebruikersnaam wordt ook weergegeven op de pagina voor accountactivering.
- De knop **Account activeren**. Klik op de knop en stel het wachtwoord voor uw account in. Het wachtwoord moet minimaal bestaan uit negen tekens. Zie "Wachtwoordvereisten" (p. 19) voor meer informatie over het wachtwoord.

Als uw beheerder tweeledige verificatie heeft ingeschakeld, wordt u gevraagd om tweeledige verificatie in te stellen voor uw account. Zie "Tweeledige verificatie" (p. 19) voor meer informatie hierover.

Wachtwoordvereisten

Het wachtwoord voor een gebruikersaccount moet uit ten minste 9 tekens bestaan. Wachtwoorden worden ook gecontroleerd op complexiteit: er zijn drie categorieën:

- Zwak
- Medium
- Sterk

U kunt geen zwak wachtwoord opslaan, zelfs als het uit 9 tekens of meer bestaat. Wachtwoorden die de gebruikersnaam, het wachtwoord, het e-mailadres van de gebruiker of de naam van de tenant van het gebruikersaccount bevatten, worden altijd als zwak beschouwd. Vaak gebruikte wachtwoorden worden ook als zwak beschouwd.

Als u een sterker wachtwoord wilt, voegt u meer tekens toe. Het gebruik van verschillende soorten tekens, zoals cijfers, hoofdletters, kleine letters en speciale tekens, is niet verplicht, maar resulteert wel in sterkere wachtwoorden die ook korter kunnen zijn.

Tweeledige verificatie

Tweeledige verificatie (2FA) biedt extra bescherming tegen ongeautoriseerde toegang tot uw account. Wanneer 2FA is ingesteld, moet u uw wachtwoord en een eenmalige code invoeren (deze twee vormen samen de twee factoren van tweeledige verificatie) om u aan te melden bij de Cyber Protect-console. De eenmalige code wordt gegenereerd door een speciale toepassing die moet worden geïnstalleerd op uw mobiele telefoon of een van uw andere apparaten. Zelfs als iemand uw gebruikersnaam en wachtwoord te weten komt, kan deze persoon zich nog steeds niet aanmelden zonder toegang tot uw 'tweede-factor-apparaat'.

Tweeledige verificatie instellen voor uw account

U moet 2FA instellen voor uw account als de beheerder dit voor uw organisatie heeft ingeschakeld. Als de beheerder 2FA heeft ingeschakeld terwijl u bent aangemeld bij de Cyber Protect-console, moet u 2FA instellen na afloop van uw huidige sessie.

Vereisten

- Tweeledige verificatie is ingeschakeld voor uw organisatie door een beheerder.

Tweeledige verificatie instellen voor uw account

1. Installeer een verificatie-app op uw mobiele apparaat.
   Voorbeelden van verificatie-apps:
   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
2. Scan de QR-code met uw verificatie-app en voer vervolgens de 6-cijferige code in die wordt weergegeven in de verificatie-app, in het venster **Tweeledige verificatie instellen**.
3. Klik op **Volgende**.
   De instructies voor het herstellen van de toegang tot uw account als u uw 2FA-apparaat kwijtraakt of de verificatie-app verwijdert, worden weergegeven.
4. Sla het PDF-bestand op of druk het af.

   Opmerking
   Bewaar het PDF-bestand op een veilige plaats of druk het af om later te kunnen raadplegen. Dit is de beste manier om uw toegang te herstellen.

5. Ga terug naar de aanmeldingspagina van de Cyber Protect-console en voer de gegenereerde code in.
   De eenmalige code is 30 seconden geldig. Als u langer dan 30 seconden wacht, gebruik dan de volgende gegenereerde code.

Wanneer u zich de volgende keer aanmeldt, kunt u het selectievakje **Deze browser vertrouwen...** inschakelen. Als u dit doet, is de code niet vereist wanneer u zich de volgende keer aanmeldt via deze browser op deze machine.

Opmerking
We raden u aan dit selectievakje leeg te laten. Anders hebt u geen toegang meer tot 2FA voor uw account.

Tweeledige verificatie (2FA) herstellen op een nieuw apparaat:

Als u toegang hebt tot de eerder ingestelde verificatie-app voor mobiel

1. Installeer een verificatie-app op uw nieuwe apparaat.
2. Gebruik het PDF-bestand dat u hebt opgeslagen tijdens de configuratie van 2FA op uw apparaat. Dit bestand bevat de 32-cijferige code die u moet invoeren in de verificatie-app om de app weer

te koppelen aan uw Acronis-account.

Belangrijk
Als de code niet werkt, controleer dan of de tijd in de mobiele verificatie-app is gesynchroniseerd met uw apparaat.

Als u tijdens de installatie het PDF-bestand niet hebt opgeslagen:

a. Klik op **2FA opnieuw instellen** en voer vervolgens het eenmalige wachtwoord in dat wordt weergegeven in de mobiele verificatie-app.
b. Volg de instructies op het scherm.

Als u geen toegang hebt tot de eerder ingestelde mobiele verificatie-app

1. Neem een nieuw mobiel apparaat.
2. Gebruik het opgeslagen PDF-bestand om een nieuw apparaat te koppelen (standaardnaam van het bestand is `cyberprotect-2fa-backupcode.pdf`).
3. Herstel de toegang tot uw account vanaf een back-up. Controleer of back-ups worden ondersteund door uw mobiele app.
4. Open de app voor hetzelfde account vanaf een ander mobiel apparaat (als dit wordt ondersteund door de app).

Privacyinstellingen

Met privacyinstellingen kunt u aangeven of u al dan niet toestemming geeft voor het verzamelen, gebruiken en openbaar maken van uw persoonlijke gegevens.

Afhankelijk van het land waarin u Cyber Protect Cloud gebruikt en het Cyber Protect Cloud-datacenter dat services aan u levert, wordt u bij de eerste lancering van Cyber Protect Cloud mogelijk gevraagd om te bevestigen of u akkoord gaat met het gebruik van Google Analytics in Cyber Protect Cloud.

Google Analytics helpt ons het gedrag van gebruikers beter te begrijpen en de gebruikerservaring in Cyber Protect Cloud te verbeteren door gepseudonimiseerde gegevens te verzamelen.

Als u Google Analytics hebt ingeschakeld of niet hebt willen inschakelen bij de eerste lancering van Cyber Protect Cloud, kunt u uw besluit later op elk gewenst moment wijzigen.

Google Analytics in- of uitschakelen:

1. Klik in de Cyber Protect-console op **Account beheren**.
2. Klik op het accountpictogram in de rechterbovenhoek.
3. Selecteer **Mijn privacyinstellingen**. Het venster **Mijn privacyinstellingen** wordt weergegeven.
4. Klik in het gedeelte **Google Analytics-gegevensverzameling** op een van de volgende knoppen:
   - **Aan** om Google Analytics in te schakelen
   - **Uit** om Google Analytics uit te schakelen

In het gedeelte **Cookies verwijderen** kunt u cookies controleren en beheren rechtstreeks vanuit uw browser.

Opmerking
Als u het gedeelte Google Analytics niet ziet, betekent dit dat Google Analytics niet wordt gebruikt in uw land.

In het gedeelte **In-product onboarding en interactieve hulp** in het product, dat aanvankelijk tijdens de proefperiode wordt weergegeven, kunt u kiezen of u de informatie over de verbeteringen en nieuwe functies van het programma in de toekomst wilt stopzetten of blijven ontvangen. De functie is standaard ingeschakeld, maar u kunt deze uitschakelen door de schakelaar in te stellen op **Uit**.

Toegang tot de Cyber Protection-service

Wanneer uw account is geactiveerd, kunt u toegang krijgen tot de Cyber Protection-service door u aan te melden bij de Cyber Protect-console of via de beheerportal.

Aanmelden bij de Cyber Protect-console

1. Ga naar de aanmeldingspagina voor de Cyber Protection-service.
2. Typ uw gebruikersnaam en klik op **Volgende**.
3. Typ uw wachtwoord en klik op **Volgende**.
4. [Als u meer dan één Cyber Protect Cloud-service gebruikt] Klik op **Cyber Protection**.
   Gebruikers die alleen toegang hebben tot de Cyber Protection-service, melden zich direct aan op de Cyber Protect-console.
   Als **Cyber Protection** niet de enige service is waartoe u toegang hebt, kunt u schakelen tussen de services via het pictogram  in de rechterbovenhoek. Beheerders kunnen dit pictogram ook gebruiken om over te schakelen naar de beheerportal.

De time-outperiode voor de Cyber Protect-console is 24 uur voor actieve sessies en 1 uur voor niet-actieve sessies.

U kunt de taal van de webinterface wijzigen door te klikken op het accountpictogram in de rechterbovenhoek.

Toegang tot de Cyber Protect-console via de beheerportal

1. Ga in de beheerportal naar **Controle** > **Gebruik**.
2. Selecteer onder **Cyber Protect** de optie **Bescherming** en klik op **Service beheren**.
   Of ga naar **Klanten**, selecteer een klant en klik vervolgens op **Service beheren**.

U wordt dan omgeleid naar de Cyber Protect-console.

Belangrijk
Als de klant gebruikmaakt van de **Selfservice** beheermodus, kunt u geen services voor de klant beheren. Alleen de klantbeheerders kunnen de klantmodus wijzigen in **Beheerd door serviceprovider**. Vervolgens kunnen ze de services beheren.

Uw wachtwoord opnieuw instellen

1. Ga naar de aanmeldingspagina voor de Cyber Protection-service.
2. Typ uw gebruikersnaam en klik op **Volgende**.
3. Klik op **Wachtwoord vergeten?**
4. Klik op **Verzenden** om te bevestigen dat u verdere instructies wilt.
5. Volg de instructies in de e-mail die u hebt ontvangen.
6. Stel uw nieuwe wachtwoord in.

Softwarevereisten

Ondersteunde webbrowsers

De Cyber Protect-console gebruikt het TLS 1.2-protocol en ondersteunt de volgende webbrowsers:

- Google Chrome 29 of later
- Mozilla Firefox 23 of later
- Opera 16 of later
- Microsoft Edge 25 of later
- Safari 8 of later uitgevoerd op de besturingssystemen macOS en iOS

Het is mogelijk dat de gebruikersinterface in andere webbrowsers (inclusief Safari-browsers die worden uitgevoerd op andere besturingssystemen) niet goed wordt weergegeven of dat bepaalde functies niet beschikbaar zijn.

Ondersteunde besturingssystemen en omgevingen

Agent voor Windows

Deze agent bevat een onderdeel voor Antivirus- en antimalwarebeveiliging en URL-filtering. Zie "Ondersteunde beschermingsfuncties per besturingssysteem" (p. 45) voor meer informatie over ondersteunde functionaliteit per besturingssysteem.

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows Server 2003 SP1/2003 R2 en later – Standard en Enterprise Edition (x86, x64)
- Windows Small Business Server 2003/2003 R2

- Windows Server 2008, Windows Server 2008 SP2* – Standard, Enterprise, Datacenter, Foundation en Web Edition (x86, x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7 – alle edities

Opmerking
Als u Cyber Protection wilt gebruiken met Windows 7, moet u de volgende updates van Microsoft installeren voordat u de beveiligingsagent installeert:

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

Zie dit Knowledge Base-artikel voor meer informatie over de vereiste updates.

- Windows Server 2008 R2* – Standard, Enterprise, Datacenter, Foundation en Web Edition
- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011* – alle edities
- Windows 8/8.1 – alle edities (x86, x64), met uitzondering van de Windows RT-edities.
- Windows Server 2012/2012 R2 – alle edities
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Home-, Pro-, Education-, Enterprise-, IoT Enterprise- en LTSC (vroeger LTSB)-editie
- Windows Server 2016 – alle installatieopties, met uitzondering van Nano Server
- Windows Server 2019 – alle installatieopties, met uitzondering van Nano Server
- Windows 11 – alle edities
- Windows Server 2022 – alle installatieopties, met uitzondering van Nano Server

Opmerking
* Als u Cyber Protection met deze versie van Windows wilt gebruiken, moet u de SHA2-ondersteuningsupdate voor codeondertekening van Microsoft (KB4474419) installeren voordat u de beveiligingsagent installeert.

Zie dit Knowledge Base-artikel voor informatie over problemen met de update voor ondersteuning van handtekening bij SHA2-programmacode.

Agent voor SQL, Agent voor Active Directory, Agent voor Exchange (voor databaseback-up en applicatiegerichte back-up)

Elk van deze agenten kan worden geïnstalleerd op een machine met een van de hier vermelde besturingssystemen en een ondersteunde versie van de betreffende applicatie.

Agent voor preventie van gegevensverlies

Apparaatbesturing

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

Opmerking
Agent voor preventie van gegevensverlies voor macOS ondersteunt alleen x64-processors. Apple silicon ARM-processors worden niet ondersteund.

Preventie van gegevensverlies

- Microsoft Windows 7 Service Pack 1 en later
- Microsoft Windows Server 2008 R2 en later

Opmerking
Agent voor preventie van gegevensverlies is een integraal onderdeel van Agent voor Mac en kan daarom worden geïnstalleerd op macOS-systemen die niet door de agent worden ondersteund. In dit geval zal de Cyber Protect-console aangeven dat Agent voor preventie van gegevensverlies is geïnstalleerd op de computer, maar de functie voor apparaatbeheer en preventie van gegevensverlies zal niet werken. De functie voor apparaatbeheer werkt alleen op macOS-systemen die worden ondersteund door Agent voor preventie van gegevensverlies.

Agent voor Advanced Data Loss Prevention

- Microsoft Windows 7 Service Pack 1 en later
- Microsoft Windows Server 2008 R2 en later

Agent voor File Sync & Share

Zie de Cyber Files Cloud-gebruikershandleiding voor de lijst met ondersteunde besturingssystemen.

Agent voor Exchange (voor postvakback-ups)

- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation en Web Edition (x86, x64)
- Windows Small Business Server 2008
- Windows 7 – alle edities

- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation en Web Edition
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – alle edities
- Windows 8/8.1 – alle edities (x86, x64), met uitzondering van de Windows RT-edities.
- Windows Server 2012/2012 R2 – alle edities
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – Home, Pro, Education en Enterprise Edition
- Windows Server 2016 – alle installatieopties, met uitzondering van Nano Server
- Windows Server 2019 – alle installatieopties, met uitzondering van Nano Server
- Windows 11 – alle edities
- Windows Server 2022 – alle installatieopties, met uitzondering van Nano Server

Agent voor Microsoft 365

- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation en Web Edition (alleen x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation en Web Edition
- Windows Home Server 2011
- Windows Small Business Server 2011 – alle edities
- Windows 8/8.1 – alle edities (alleen x64), met uitzondering van de Windows RT-edities
- Windows Server 2012/2012 R2 – alle edities
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (alleen x64)
- Windows 10 – Home, Pro, Education en Enterprise Edition (alleen x64)
- Windows Server 2016 – alle installatieopties (alleen x64), met uitzondering van Nano Server
- Windows Server 2019 – alle installatieopties (alleen x64), met uitzondering van Nano Server
- Windows 11 – alle edities
- Windows Server 2022 – alle installatieopties, met uitzondering van Nano Server

Agent voor Oracle

- Windows Server 2008R2 – Standard, Enterprise, Datacenter en Web Edition (x86, x64)
- Windows Server 2012R2 – Standard, Enterprise, Datacenter en Web Edition (x86, x64)
- Linux – elke kernel en distributie ondersteund door Agent voor Linux (zie hieronder)

Agent voor MySQL/MariaDB

- Linux – elke kernel en distributie ondersteund door Agent voor Linux (zie hieronder)

Agent voor Linux

Deze agent bevat een onderdeel voor Antivirus- en antimalwarebeveiliging en URL-filtering. Zie "Ondersteunde beschermingsfuncties per besturingssysteem" (p. 45) voor meer informatie over ondersteunde functionaliteit per besturingssysteem.

De volgende Linux-distributies en -kernelversies zijn specifiek getest. Zelfs als uw Linux-distributie of -kernelversie hieronder niet wordt vermeld, kan deze toch correct werken in alle vereiste scenario's, vanwege de specifieke kenmerken van de Linux-besturingssystemen.

Als u problemen ondervindt bij het gebruik van Cyber Protection met uw combinatie van Linux-distributie en -kernelversie, neem dan contact op met het ondersteuningsteam voor verder onderzoek.

Linux met kernel van 2.6.9 tot 5.19 en glibc 2.3.4 of later, inclusief de volgende x86- en x86_64-distributies:

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

Belangrijk
Configuraties met Btrfs worden niet ondersteund voor SUSE Linux Enterprise Server 12 en SUSE Linux Enterprise Server 15.

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

Opmerking
Bij de installatie van de beveiligingsagent in Oracle Linux 8.6 en hoger, waarop Secure Boot is ingeschakeld, moet u de kernelmodules handmatig ondertekenen. Zie dit Knowledge Base-artikel voor meer informatie over het ondertekenen van een kernelmodule.

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

- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

  * Vanaf versie 8.4 alleen ondersteuning met kernels van 4.18 tot 5.19

Agent voor Mac

Deze agent bevat een onderdeel voor Antivirus- en antimalwarebeveiliging en URL-filtering. Zie "Ondersteunde beschermingsfuncties per besturingssysteem" (p. 45) voor meer informatie over ondersteunde functionaliteit per besturingssysteem.

Zowel x64- als ARM-architectuur (gebruikt in Apple silicon processors zoals Apple M1 en M2) wordt ondersteund.

Opmerking
Back-ups op schijfniveau van Macs met Intel naar Macs met een Apple Silicon-processor (en omgekeerd) kunnen niet worden hersteld. U kunt bestanden en mappen herstellen.

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

Belangrijk
Vanaf versie C23.07 biedt Cyber Protect Cloud geen ondersteuning meer voor de volgende besturingssystemen: OS X Yosemite 10.10, OS X El Capitan 10.11 en macOS Sierra 10.12.

We raden u sterk aan om uw besturingssysteem te upgraden naar een ondersteunde versie om de compatibiliteit te waarborgen en de volledige functionaliteit van Cyber Protect Cloud te kunnen benutten.

Agent voor VMware (Virtual Appliance)

Deze agent wordt geleverd als virtuele toepassing die kan worden uitgevoerd op een ESXi-host.

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

Agent voor VMware (Windows)

Deze agent wordt geleverd als een Windows-toepassing die kan worden uitgevoerd op alle vermelde besturingssystemen voor Agent voor Windows, met de volgende uitzonderingen:

- 32-bits besturingssystemen worden niet ondersteund.
- Windows XP, Windows Server 2003/2003 R2 en Windows Small Business Server 2003/2003 R2 worden niet ondersteund.

Agent voor Hyper-V

- Windows Server 2008 (alleen x64) met Hyper-V-rol, inclusief Server Core-installatiemodus
- Windows Server 2008 R2 met Hyper-V-rol, inclusief Server Core-installatiemodus
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 met Hyper-V-rol, inclusief Server Core-installatiemodus
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (alleen x64) met Hyper-V
- Windows 10 – Pro, Education en Enterprise Edition met Hyper-V
- Windows Server 2016 met Hyper-V-rol – alle installatieopties, met uitzondering van Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 met Hyper-V-rol – alle installatieopties, met uitzondering van Nano Server
- Microsoft Hyper-V Server 2019
- Windows Server 2022 – alle installatieopties, met uitzondering van Nano Server

Agent voor Virtuozzo

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

Agent voor Virtuozzo Hybrid Infrastructure

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

Agent voor Scale Computing HC3

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

Agent voor oVirt

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agent voor Synology

DiskStation Manager 6.2.x, 7.x

Agent voor Synology ondersteunt alleen NAS-apparaten met x86_64-processors. ARM-processors worden niet ondersteund.

Cyber Protect Monitor

- Windows 7 en later
- Windows Server 2008 R2 en later
- Alle macOS-versies die worden ondersteund door Agent voor Mac

Ondersteunde versies van Microsoft SQL Server

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

De SQL Server Express-edities van de bovenstaande SQL-serverversies worden ook ondersteund.

Opmerking
Microsoft SQL-back-up wordt alleen ondersteund voor databases die worden uitgevoerd op NFTS-, REFS- en FAT32-bestandssystemen. ExFat wordt niet ondersteund.

Ondersteunde versies van Microsoft Exchange Server

- Microsoft Exchange Server 2019 – alle edities.
- Microsoft Exchange Server 2016 – alle edities.
- Microsoft Exchange Server 2013 – alle edities, Cumulative Update 1 (CU1) en later.
- Microsoft Exchange Server 2010 – alle edities, alle servicepacks. Back-up van postvakken en gedetailleerd herstel vanaf databaseback-ups worden ondersteund vanaf Service Pack 1 (SP1).
- Microsoft Exchange Server 2007 – alle edities, alle servicepacks. Back-up van postvakken en gedetailleerd herstel vanaf databaseback-ups worden niet ondersteund.

Ondersteunde versies van Microsoft SharePoint

Cyber Protection ondersteunt de volgende versies van Microsoft SharePoint:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1

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

*Als u SharePoint Explorer wilt gebruiken voor deze versies, hebt u een SharePoint-herstelfarm nodig waaraan u de databases kunt koppelen.

De back-ups of databases waarvan u gegevens uitpakt, moeten afkomstig zijn van dezelfde SharePoint-versie als de versie waarvoor SharePoint Explorer is geïnstalleerd.

Ondersteunde versies van Oracle Database

- Oracle Database versie 11g, alle edities
- Oracle Database versie 12c, alle edities
- Oracle Database versie 19c, alle edities
- Oracle Database versie 21c, alle edities

Alleen configuraties met een enkelvoudig exemplaar worden ondersteund.

Ondersteunde SAP HANA-versies

HANA 2.0 SPS 03 geïnstalleerd in RHEL 7.6 op een fysieke machine of virtuele VMware ESXi-machine.

Herstel van multitenant-databasecontainers via momentopnamen van de opslag wordt niet ondersteund door SAP HANA, dus deze oplossing is alleen voor SAP HANA-containers met slechts één tenantdatabase.

Ondersteunde MySQL-versies

- 5.5.x − Community Server-, Enterprise-, Standard- en Classic-edities
- 5.6.x − Community Server-, Enterprise-, Standard- en Classic-edities
- 5.7.x − Community Server-, Enterprise-, Standard- en Classic-edities
- 8.0.x − Community Server-, Enterprise-, Standard- en Classic-edities

Ondersteunde MariaDB-versies

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

- 10.6.x
- 10.7.x

Ondersteunde virtualisatieplatforms

D volgende tabel geeft weer op welke manier verschillende virtualisatieplatforms worden ondersteund.

Zie "Back-ups met en zonder agent" (p. 63) voor meer informatie over de verschillen tussen back-up met agent en zonder agent.

Opmerking
Als u een virtualisatieplatform of versie gebruikt die niet hieronder wordt vermeld, kan de methode **Back-up met agent (Back-up van binnen een gastbesturingssysteem)**, mogelijk toch correct werken in alle vereiste scenario's. Als u problemen ondervindt met back-up met agent, neemt u contact op met het ondersteuningsteam voor verder onderzoek.

VMware

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
VMware vSphere-versies: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 **VMware vSphere-edities:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **VMware ESXi** > **Agent voor installatie in Windows** of **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **VMware ESXi** > **Virtual appliance (OVF)**	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
VMware vSphere Hypervisor (Free ESXi)**	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
VMware Server (VMware Virtual server:) VMware Workstation VMware ACE	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
VMware Player		

* HotAdd-transport voor virtuele schijven wordt in deze edities alleen ondersteund voor vSphere 5.0 en later. Back-ups worden mogelijk trager uitgevoerd in versie 4.1.

** Back-up op hypervisorniveau wordt niet ondersteund voor vSphere Hypervisor, omdat dit product alleen toegang tot de Remote Command Line Interface (RCLI) biedt in de modus Alleen-lezen. De agent werkt tijdens de vSphere Hypervisor-evaluatieperiode zolang er geen seriële sleutel is opgegeven. Zodra u een seriële sleutel opgeeft, werkt de agent niet meer.

Opmerking
Cyber Protect Cloud biedt officieel ondersteuning voor elke update binnen de ondersteunde primaire versie van vSphere.

Ondersteuning voor vSphere 8.0 omvat bijvoorbeeld ondersteuning voor elke update binnen deze versie, tenzij anders vermeld. vSphere 8.0 Update 1 wordt bijvoorbeeld ook ondersteund in combinatie met de oorspronkelijke release van vSphere 8.0.

Ondersteuning voor een specifieke VMware vSphere-versie houdt in dat vSAN van de overeenkomstige versie ook wordt ondersteund. Ondersteuning voor vSphere 8.0 houdt bijvoorbeeld in dat vSAN 8.0 ook wordt ondersteund.

Beperkingen

- **Fouttolerante machines**
  Met Agent voor VMware kunnen back-ups van fouttolerante machines alleen worden gemaakt als fouttolerantie is ingeschakeld in VMware vSphere 6.0 en later. Als u een upgrade uitvoert van een eerdere versie van vSphere, kunt u volstaan met het uitschakelen en inschakelen van fouttolerantie voor elke machine. Als u een eerdere versie van vSphere gebruikt, installeert u een agent in het gastbesturingssysteem.
- **Onafhankelijke schijven en RDM**
  Agent voor VMware maakt geen back-ups van RDM-schijven (Raw Device Mapping) in de fysieke compatibiliteitsmodus of van onafhankelijke schijven. De agent slaat deze schijven over en voegt waarschuwingen toe aan het logboek. U kunt de waarschuwingen voorkomen door onafhankelijke schijven en RDM's in de fysieke compatibiliteitsmodus uit te sluiten van het beschermingsschema. Als u back-ups wilt maken van deze schijven of de gegevens op deze schijven, installeert u een agent in het gastbesturingssysteem.
- **iSCSI-gastverbinding**
  Agent voor VMware maakt geen back-up van LUN-volumes die zijn verbonden via een iSCSI-initiator binnen het gastbesturingssysteem. De ESXi-hypervisor herkent dergelijke volumes niet, dus de volumes worden niet opgenomen in momentopnamen op hypervisor-niveau en worden

zonder waarschuwing weggelaten uit een back-up. Als u back-ups wilt maken van deze volumes of de gegevens op deze volumes, installeert u een agent in het gastbesturingssysteem.

- **Versleutelde virtuele machines** (beschikbaar vanaf VMware vSphere 6.5)
  - De back-ups van versleutelde virtuele machines zijn niet versleuteld. Als versleuteling essentieel is voor u, moet u versleuteling van back-ups inschakelen wanneer u een beschermingsschema maakt.
  - Herstelde virtuele machines zijn nooit versleuteld. U kunt versleuteling handmatig inschakelen nadat het herstel is voltooid.
  - Als u back-ups maakt van versleutelde virtuele machines, raden we u aan om ook de virtuele machine met Agent voor VMware te versleutelen. De bewerkingen met versleutelde machines zijn anders mogelijk trager dan verwacht. Gebruik vSphere Web Client om het **Versleutelingsbeleid voor virtuele machines** toe te passen op de machine met de agent.
  - Back-ups van versleutelde virtuele machines worden gemaakt via LAN, zelf als u de SAN-transportmodus configureert voor de agent. De agent maakt dan gebruik van NBD-transport, want VMware biedt geen ondersteuning voor SAN-transport voor het maken van back-ups van versleutelde virtuele schijven.
- **Secure Boot**
  - Virtuele VMware-machines: (vanaf VMware vSphere 6.5) **Secure Boot** wordt uitgeschakeld nadat een virtuele machine is hersteld als nieuwe virtuele machine. U kunt deze optie handmatig inschakelen nadat het herstel is voltooid. Deze beperking is van toepassing op VMware.
  - Virtuele Hyper-V-machines: Secure Boot wordt uitgeschakeld voor alle virtuele machines van generatie 2 nadat de machine is hersteld als nieuwe virtuele machine of als bestaande virtuele machine.
- **Back-up van ESXi-configuratie** wordt niet ondersteund voor VMware vSphere 7.0 of hoger.
- **Virtuele machines met een lege exemplaar-UUID worden niet weergegeven in de Cyber Protect-console.**

  Virtuele VMware-machines met een lege vSphere-eigenschap `exemplaar-UUID` (`vc.uuid`) worden niet weergegeven in de Cyber Protect-console. Zie dit Knowledge Base-artikel voor meer informatie over het oplossen van dit probleem.
- **Netwerkinstellingen voor de beveiligingsagent**

  Een back-up van een virtuele VMware-machine kan mislukken als de beveiligingsagent de naam van de ESXi-host die is geregistreerd in vCenter, niet kan omzetten naar een IP-adres, zelfs als de hostnaam in vCenter wel kan worden omgezet. De volgende foutmelding wordt weergegeven: 'You do not have access rights to this file' (u hebt geen toegangsrechten voor dit bestand).

  Als u het probleem wilt oplossen, bewerkt u de netwerkinstellingen van de beveiligingsagent door het DNS te configureren of het bestand `/etc/hosts` te wijzigen. Voer de volgende opdracht uit op de machine met de beveiligingsagent om de oplossing te verifiëren:

  ```
  ping <ESXi host name>
  ```
- **Ondersteunde bewerkingen voor machines met logische volumes**

Back-up en herstel van workloads met logische volumes, zoals LDM in Windows (dynamische schijven) en LVM in Linux, worden ondersteund met enkele beperkingen. Zie "Ondersteunde bewerkingen met logische volumes" (p. 58) voor meer informatie over de beperkingen.

Microsoft

Hyper-V virtuele machines die worden uitgevoerd op een hypergeconvergeerd cluster met Storage Spaces Direct (S2D) worden ondersteund. Storage Spaces Direct wordt ook ondersteund als back-upopslag.

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Windows Server 2008 (x64) met Hyper-V Windows Server 2008 R2 met Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 met Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) met Hyper-V Windows 10 met Hyper-V Windows Server 2016 met Hyper-V – alle installatieopties, met uitzondering van Nano Server Microsoft Hyper-V Server 2016 Windows Server 2019 met Hyper-V – alle installatieopties, met uitzondering van Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 met Hyper-V – alle installatieopties, met uitzondering van Nano Server	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Hyper-V**	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Microsoft Virtual Server 2005	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**

Opmerking
Virtuele Hyper-V-machines die worden uitgevoerd op een hypergeconvergeerd cluster met Storage Spaces Direct (S2D), worden ondersteund. Storage Spaces Direct wordt ook ondersteund als back-upopslag.

Beperkingen

- **Doorgangsschijven**
  Agent voor Hyper-V maakt geen back-ups van doorgangsschijven. De agent slaat deze schijven over tijdens de back-up en voegt waarschuwingen toe aan het logboek. U kunt de waarschuwingen voorkomen door doorgangsschijven uit te sluiten van het beschermingsschema. Als u back-ups wilt maken van deze schijven of de gegevens op deze schijven, installeert u een agent in het gastbesturingssysteem.
- **Hyper-V-gastclustering**
  Agent voor Hyper-V ondersteunt geen back-ups van virtuele Hyper-V-machines die knooppunten zijn van een failoverclustering van Windows Server. Mogelijk wordt de externe quorumschijf zelfs tijdelijk van het cluster losgekoppeld door een VSS-momentopname. Als u back-ups wilt maken van deze machines, moet u agenten installeren in de gastbesturingssystemen.
- **iSCSI-gastverbinding**
  Agent voor Hyper-V maken geen back-up van LUN-volumes die zijn verbonden via een iSCSI-initiator binnen het gastbesturingssysteem. De Hyper V-hypervisor herkent dergelijke volumes niet, dus de volumes worden niet opgenomen in momentopnamen op hypervisor-niveau en worden zonder waarschuwing weggelaten uit een back-up. Als u back-ups wilt maken van deze volumes of de gegevens op deze volumes, installeert u een agent in het gastbesturingssysteem.
- **VHD/VHDX-bestandsnamen met en-tekens**
  Op Hyper-V-hosts met Windows Server 2016 of hoger kunt u geen back-up maken van oudere virtuele machines (versie 5.0) die oorspronkelijk zijn gemaakt met Hyper-V 2012 R2 of ouder, als de namen van de betreffende VHD/VHDX-bestanden het en-teken (&) bevatten.
  Als u een back-up van dergelijke machines wilt maken, koppelt u in Hyper-V Manager de betreffende virtuele schijf los van de virtuele machine, bewerkt u de VHD/VHDX-bestandsnaam door het en-teken te verwijderen en koppelt u de schijf vervolgens weer aan de virtuele machine.
- **Afhankelijkheid van het Microsoft WMI-subsysteem**
  Back-ups zonder agent van virtuele Hyper-V-machines zijn afhankelijk van het Microsoft WMI-subsysteem, en in het bijzonder van de klasse `Msvm_VirtualSystemManagementService`. Als de WMI-

query's niet correct worden uitgevoerd, mislukken ook de back-ups. Voor meer informatie over de klasse `Msvm_VirtualSystemManagementService`: zie de Microsoft-documentatie.

- **Virtuele machines met PMEM-schijven**

  Back-up van virtuele Hyper-V-machines met schijven met permanent geheugen (PMEM) wordt niet ondersteund.
- **Platformonafhankelijk herstel**

  Als Agent voor Hyper-V een back-up herstelt die door een andere agent is gemaakt als nieuwe virtuele Hyper-V-machine, is de resulterende machine Generatie 1.
- **Secure Boot**

  Secure Boot is uitgeschakeld om het opstarten te waarborgen van virtuele Hyper-V-machines van generatie 2 die zijn hersteld. U kunt dit handmatig opnieuw inschakelen in de Hyper-V-beheertool. Zie de Microsoft-documentatie voor meer informatie over Secure Boot en virtuele machines van generatie 2.
- **Crashconsistente back-ups van virtuele Linux-machines**

  Back-ups van Linux virtuele machines op een Hyper-V 2019-host mislukken en er wordt een failover uitgevoerd naar crashconsistente momentopnamen, vanwege een beperking van Microsoft (kan geen productiecontrolepunten maken voor virtuele Linux-machines). Als u waarschuwingen tijdens een back-up wilt voorkomen, schakelt u de back-upoptie VSS voor virtuele machines uit in het beschermingsplan.
- **Een virtuele machine uitvoeren vanaf een back-up**

  Het uitvoeren van een virtuele machine vanaf een back-up op een Hyper-V-host mislukt als de back-up zich op hetzelfde volume bevindt als het pad dat is geselecteerd voor de gekoppelde VM-schijven. U kunt dat probleem oplossen door een ander volume te selecteren voor het pad van de gekoppelde VM-schijven. De ruimte wordt alleen gebruikt voor wijzigingen die worden gegenereerd in de gekoppelde virtuele machine en deze blijft kleiner dan de volledige opslagruimte van de virtuele schijf.
- **Ondersteunde bewerkingen voor machines met logische volumes**

  Back-up en herstel van workloads met logische volumes, zoals LDM in Windows (dynamische schijven) en LVM in Linux, worden ondersteund met enkele beperkingen. Zie "Ondersteunde bewerkingen met logische volumes" (p. 58) voor meer informatie over de beperkingen.

Scale Computing

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Scale Computing HC3**	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**

Beperkingen

Ondersteunde bewerkingen voor machines met logische volumes

Back-up en herstel van workloads met logische volumes, zoals LDM in Windows (dynamische schijven) en LVM in Linux, worden ondersteund met enkele beperkingen. Zie "Ondersteunde bewerkingen met logische volumes" (p. 58) voor meer informatie over de beperkingen.

Citrix

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Citrix XenServer/Citrix Hypervisor 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2	Niet ondersteund	Alleen ondersteund voor volledig gevirtualiseerde gasten (HVM). Paravirtual gasten (PV) worden niet ondersteund. **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Citrix XenServer** > **Windows** of **Linux**

Red Hat en Linux

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
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	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
Red Hat-virtualisatie (beheerd met oVirt) 4.2, 4.3, 4.4, 4.5	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Red Hat Virtualization (oVirt)**	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
Kernel-based Virtual Machines (KVM)	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **KVM** > **Windows** of **Linux**
Kernel-based Virtual Machines	Ondersteund	Ondersteund

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
(KVM) beheerd met oVirt 4.3 en uitgevoerd op Red Hat Enterprise Linux 7.6, 7.7 of CentOS 7.6, 7.7	**Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Red Hat Virtualization (oVirt)**	**Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
Kernel-based Virtual Machines (KVM) beheerd met oVirt 4.4 en uitgevoerd op Red Hat Enterprise Linux 8.x of CentOS Stream 8.x	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts**> **Red Hat Virtualization (oVirt)**	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
Kernel-based Virtual Machines (KVM) beheerd met oVirt 4.5 en uitgevoerd op Red Hat Enterprise Linux 8.x of CentOS Stream 8.x	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Red Hat Virtualization (oVirt)**	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**

Beperkingen

Ondersteunde bewerkingen voor machines met logische volumes

Back-up en herstel van workloads met logische volumes, zoals LDM in Windows (dynamische schijven) en LVM in Linux, worden ondersteund met enkele beperkingen. Zie "Ondersteunde bewerkingen met logische volumes" (p. 58) voor meer informatie over de beperkingen.

Parallels

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Parallels Workstation	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
Parallels Server 4 Bare Metal	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**

Oracle

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Oracle Virtualization Manager (gebaseerd op oVirt)* 4.3	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Red Hat Virtualization (oVirt)**	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
Oracle VM Server 3.0, 3.3, 3.4	Niet ondersteund	Alleen ondersteund voor volledig gevirtualiseerde gasten (HVM). Paravirtual gasten (PV) worden niet ondersteund. **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Oracle** > **Windows** of **Linux**
Oracle VM VirtualBox 4.x	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Oracle** > **Windows** of **Linux**

*Oracle Virtualization Manager wordt ondersteund door Agent voor oVirt.

Beperkingen

Ondersteunde bewerkingen voor machines met logische volumes

Back-up en herstel van workloads met logische volumes, zoals LDM in Windows (dynamische schijven) en LVM in Linux, worden ondersteund met enkele beperkingen. Zie "Ondersteunde bewerkingen met logische volumes" (p. 58) voor meer informatie over de beperkingen.

Nutanix

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Nutanix Acropolis Hypervisor (AHV) 20160925.x tot en met 20180425.x	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Nutanix AHV** > **Windows** of **Linux**

Virtuozzo

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Virtuozzo**	Alleen ondersteund voor virtuele machines. Containers worden niet ondersteund. **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
Virtuozzo 7.0.13, 7.0.14	Alleen ondersteund voor ploop-containers. Virtuele machines worden niet ondersteund. **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Virtuozzo**	Alleen ondersteund voor virtuele machines. Containers worden niet ondersteund. **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**
Virtuozzo Hybrid Server 7.5	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatiehosts** > **Virtuozzo**	Alleen ondersteund voor virtuele machines. Containers worden niet ondersteund. **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**

Beperkingen

Ondersteunde bewerkingen voor machines met logische volumes

Back-up en herstel van workloads met logische volumes, zoals LDM in Windows (dynamische schijven) en LVM in Linux, worden ondersteund met enkele beperkingen. Zie "Ondersteunde bewerkingen met logische volumes" (p. 58) voor meer informatie over de beperkingen.

Virtuozzo Hybrid Infrastructure

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0	Ondersteund **Apparaten** > **Toevoegen** > **Virtualisatie hosts** > **Virtuozzo hybride infrastructuur**	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**

Beperkingen

- **Back-up zonder agent van VM's met schijven op een externe iSCSI-opslag**
  U kunt geen back-up maken van VM's vanuit Virtuozzo Hybrid Infrastructure als VM-schijven zijn geplaatst op externe iSCSI-volumes (gekoppeld aan het VHI-cluster).
- **Ondersteunde bewerkingen voor machines met logische volumes**
  Back-up en herstel van workloads met logische volumes, zoals LDM in Windows (dynamische schijven) en LVM in Linux, worden ondersteund met enkele beperkingen. Zie "Ondersteunde bewerkingen met logische volumes" (p. 58) voor meer informatie over de beperkingen.

Amazon

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Amazon EC2-exemplaren	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**

Microsoft Azure

Platform	Back-up zonder agent (Back-up op hypervisorniveau)	Back-up met agent (Back-up van binnen een gastbesturingssysteem)
Virtuele Azure-machines	Niet ondersteund	Ondersteund **Apparaten** > **Toevoegen** > **Werkstations** of **Servers** > **Windows** of **Linux**

Compatibiliteit met versleutelingssoftware

Er zijn geen beperkingen voor het maken van back-ups en het herstel van gegevens die zijn versleuteld met software voor versleuteling op *bestandsniveau*.

Met software voor versleuteling op *schijfniveau* worden gegevens direct versleuteld. Daarom worden de gegevens in de back-up niet versleuteld. Software voor versleuteling op schijfniveau brengt vaak wijzigingen aan in systeemgebieden: opstartrecords, partitietabellen of bestandssysteemtabellen. Deze factoren zijn van invloed op het maken van back-ups en herstel op schijfniveau, en bepalen ook of het herstelde systeem kan worden opgestart en toegang heeft tot Secure Zone.

Het is mogelijk een back-up te maken van gegevens die zijn versleuteld met de volgende software voor versleuteling op schijfniveau:

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

Volg de volgende algemene regels en softwarespecifieke aanbevelingen om betrouwbaar herstel op schijfniveau te waarborgen.

Algemene regel voor installatie

We raden u sterk aan de versleutelingssoftware te installeren voordat u de beveiligingsagenten installeert.

Gebruiksmethode voor Secure Zone

Secure Zone moet niet worden versleuteld met versleuteling op schijfniveau. De enige manier om Secure Zone te gebruiken is als volgt:

1. Installeer de versleutelingssoftware en installeer vervolgens de agent.
2. Maak Secure Zone.
3. Sluit Secure Zone uit wanneer u de schijf of schijfvolumes versleutelt.

Algemene regel voor het maken van back-ups

U kunt een back-up op schijfniveau maken in het besturingssysteem.

Softwarespecifieke herstelprocedures

Microsoft BitLocker Drive Encryption

Een systeem herstellen dat is versleuteld met BitLocker:

1. Start op vanaf de opstartmedia.
2. Herstel het systeem. De herstelde gegevens worden ontsleuteld.
3. Start het herstelde systeem opnieuw op.
4. Schakel BitLocker in.

Als u slechts één partitie van een schijf met meerdere partities wilt herstellen, kunt u dit doen via het besturingssysteem. Als u herstelt met opstartmedia, kan Windows de herstelde partitie mogelijk niet detecteren.

McAfee Endpoint Encryption en PGP Whole Disk Encryption

U kunt een versleutelde systeempartitie alleen herstellen via opstartmedia.

Als het herstelde systeem niet kan worden opgestart, bouwt u de Master Boot Record opnieuw op, zoals beschreven in het volgende Microsoft Knowledge Base-artikel: https://support.microsoft.com/kb/2622803

Compatibiliteit met Dell EMC Data Domain-opslag

U kunt Dell EMC Data Domain-apparaten gebruiken als back-upopslag.

Bij deze opslag is het aanbevolen om een back-upschema te gebruiken dat regelmatig volledige back-ups maakt, bijvoorbeeld **Altijd volledig**. Voor meer informatie over de beschikbare back-upschema's: zie "Back-upschema's" (p. 445).

Retentievergrendeling

Retentievergrendeling (Governancemodus) wordt ondersteund. Als retentievergrendeling is ingeschakeld in de Data Domain-opslag, moet u de omgevingsvariabele `AR_RETENTION_LOCK_SUPPORT` toevoegen aan de machine met de beschermingsagent die deze opslag gebruikt als back-upbestemming. Voor meer informatie: zie "De variabele AR_RETENTION_LOCK_SUPPORT toevoegen" (p. 44).

Opmerking
Dell EMC Data Domain-opslag met ingeschakelde retentievergrendeling wordt niet ondersteund door Agent voor Mac.

Als retentievergrendeling is ingeschakeld in de Data Domain-opslag, worden de back-ups in de opslag niet verwijderd door de retentieregels in het beschermingsplan. Er wordt geen fout weergegeven. De back-ups worden verwijderd wanneer de retentievergrendeling verloopt en de retentieregels weer worden toegepast.

Afhankelijk van de configuratie van het beschermingsplan worden er bewaarregels toegepast op een archief voor of na een back-up.

De variabele AR_RETENTION_LOCK_SUPPORT toevoegen

Als retentievergrendeling is ingeschakeld op de Data Domain-opslag, moet u de omgevingsvariabele `AR_RETENTION_LOCK_SUPPORT` toevoegen aan de machine met de beveiligingsagent die deze opslag gebruikt als back-upbestemming.

De omgevingsvariabele `AR_RETENTION_LOCK_SUPPORT` toevoegen:

In Windows

1. Meld u aan als beheerder op de machine met de beveiligingsagent.
2. Ga in het **Configuratiescherm** naar **Systeem en beveiliging** > **Systeem** > **Geavanceerde systeeminstellingen**.
3. Klik op het **tabblad Geavanceerd** op **Omgevingsvariabelen**.
4. Klik in het deelvenster **Systeemvariabelen** op **Nieuw**.

5. Voeg in het venster **Nieuwe systeemvariabele** de nieuwe variabele als volgt toe:
   - Naam van variabele: `AR_RETENTION_LOCK_SUPPORT`
   - Waarde van variabele: `1`
6. Klik op **OK**.
7. Klik in het venster **Omgevingsvariabelen** op **OK**.
8. Start de machine opnieuw op.

In Linux

1. Meld u aan als beheerder op de machine met de beveiligingsagent.
2. Ga naar de directory `/sbin` en open vervolgens het bestand `acronis_mms` om het te bewerken.
3. Voeg boven de regel `export LD_LIBRARY_PATH` de volgende regel toe:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Sla het bestand `acronis_mms` op.
5. Start de machine opnieuw op.

Op een virtueel apparaat

1. Meld u aan als beheerder op de machine met het virtuele apparaat.
2. Ga naar de directory `/bin` en open vervolgens het bestand `autostart` om het te bewerken.
3. Voeg onder de regel `export LD_LIBRARY_PATH` de volgende regel toe:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Sla het bestand `autostart` op.
5. Start de virtuele toepassing opnieuw op.

Ondersteunde beschermingsfuncties per besturingssysteem

Dit onderwerp bevat informatie over de beschermingsfuncties van Cyber Protect Cloud. De back-up- en herstelfuncties worden hier niet behandeld.

De beschermingsfuncties worden alleen ondersteund op machines waarop een beveiligingsagent is geïnstalleerd. Ze zijn niet beschikbaar voor virtuele machines waarvan een back-up wordt gemaakt in de modus zonder agent, bijvoorbeeld door Agent voor Hyper-V, Agent voor VMware, Agent voor Virtuozzo Hybrid Infrastructure, Agent voor Scale Computing of Agent voor oVirt.

Voor sommige functies zijn mogelijk extra licenties vereist, afhankelijk van het toegepaste licentiemodel.

Ondersteunde besturingssystemen en versies

Windows

De volgende Windows-versies worden ondersteund (tenzij anders vermeld voor een specifieke functieset):

- Windows 7 Service Pack 1 en later
- Windows Server 2008 R2 Service Pack 1 en later

Opmerking
Voor Windows 7 moet u de volgende updates van Microsoft installeren voordat u de beveiligingsagent installeert.

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

Zie dit Knowledge Base-artikel voor meer informatie over de vereiste updates.

Linux

Welke Linux-distributies en -versies worden ondersteund, varieert per functieset (zie onderaan elke tabel).

macOS

Welke macOS-versies worden ondersteund, varieert per functieset (zie onderaan elke tabel).

Functieset	Windows	Linux	macOS
Standaardbeschermingsschema's			
Medewerkers op afstand	Ja	Nee	Nee
Medewerkers op kantoor (antivirus van derden)	Ja	Nee	Nee
Medewerkers op kantoor (Cyber Protect-antivirus)	Ja	Nee	Nee
Cyber Protect Essentials (alleen voor de Cyber Protect Essentials-editie)	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functieset	Windows	Linux	macOS
Forensische back-up			
Geheugendump genereren	Ja	Nee	Nee

Functieset	Windows	Linux	macOS
Forensische back-up			
Momentopname van actieve processen	Ja	Nee	Nee
Notarisatie van forensische back-up van lokale installatiekopie	Ja	Nee	Nee
Notarisatie van forensische back-up van installatiekopie in de cloud	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functies	Windows	Linux	macOS
Continue gegevensbescherming (CDP)			
CDP voor bestanden en mappen	Ja	Nee	Nee
CDP voor gewijzigde bestanden via applicatie-tracking	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functieset	Windows	Linux	macOS
Automatische detectie en externe installatie			
Netwerkdetectie	Ja	Nee	Nee
Active Directory-detectie	Ja	Nee	Nee
Sjabloondetectie (machines importeren uit een bestand)	Ja	Nee	Nee
Handmatig toevoegen van apparaten	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functieset	Windows	Linux	macOS
Active Protection			
Detectie van procesinjectie	Ja	Nee	Nee
Automatisch herstel van getroffen bestanden uit de lokale cache	Ja	Ja	Ja
Zelfverdediging voor Acronis Backup-bestanden	Ja	Nee	Nee
Zelfverdediging voor Acronis-software	Ja	Nee	Ja (Alleen Active

Functieset	Windows	Linux	macOS
Active Protection			
			Protection en antimalware-onderdelen)
Beheer van vertrouwde/geblokkeerde processen	Ja	Nee	Ja
Proces-/mapuitsluitingen	Ja	Ja	Ja
Detectie van ransomware op basis van procesgedrag (gebaseerd op AI)	Ja	Ja	Ja
Detectie van cryptomining-processen op basis van procesgedrag	Ja	Nee	Nee
Bescherming van externe stations (HDD, flashstations, SD-kaarten)	Ja	Nee	Ja
Netwerkmapbescherming	Ja	Ja	Ja
Bescherming op server	Ja	Nee	Nee
Bescherming van Zoom, Cisco Webex, Citrix Workspace en Microsoft Teams	Ja	Nee	Nee
Zie "Ondersteunde platforms" (p. 863) voor meer informatie over de ondersteunde besturingssystemen en versies.			

Functieset	Windows	Linux	macOS
Antivirus- en antimalwarebeveiliging			
Volledig geïntegreerde Active Protection-functionaliteit	Ja	Nee	Nee
Realtime antimalwarebeveiliging	Ja	Ja, met het Geavanceerde antimalware-pakket	Ja, met het Geavanceerde antimalware-pakket
Geavanceerde realtime antimalwarebeveiliging met lokale detectie op basis van handtekeningen	Ja	Ja	Ja
Statische analyse voor draagbare uitvoerbare bestanden	Ja	Nee	Ja*
Antimalwarescan op aanvraag	Ja	Ja**	Ja

Functieset	Windows	Linux	macOS
Antivirus- en antimalwarebeveiliging			
Netwerkmapbescherming	Ja	Ja	Nee
Bescherming op server	Ja	Nee	Nee
Scan van archiefbestanden	Ja	Nee	Ja
Scan van verwisselbare stations	Ja	Nee	Ja
Scan van alleen nieuwe en gewijzigde bestanden	Ja	Nee	Ja
Bestand-/mapuitsluitingen	Ja	Ja	Ja***
Procesuitsluitingen	Ja	Nee	Ja
Engine voor gedragsanalyse	Ja	Nee	Ja
Preventie tegen aanvallen	Ja	Nee	Nee
Quarantaine	Ja	Ja	Ja
Automatische opschoning in quarantaine	Ja	Ja	Ja
URL-filtering (http/https)	Ja	Nee	Nee
Witte lijst van het bedrijf	Ja	Nee	Ja
Firewallbeheer****	Ja	Nee	Nee
Microsoft Defender Antivirus-beheer*****	Ja	Nee	Nee
Microsoft Security Essentials-beheer	Ja	Nee	Nee
Antivirus- en antimalwarebeveiliging registreren en beheren via Windows Security Center	Ja	Nee	Nee
Zie "Ondersteunde platforms" (p. 863) voor meer informatie over de ondersteunde besturingssystemen en versies.			

* Statische analyse voor draagbare uitvoerbare bestanden wordt alleen ondersteund voor geplande scans op macOS.

** Startvoorwaarden worden niet ondersteund voor scannen op aanvraag in Linux.

*** Uitsluitingen van bestanden/mappen worden alleen ondersteund wanneer u bestanden en mappen opgeeft die niet worden gescand door realtime bescherming of geplande scans op macOS.

**** Firewallbeheer wordt ondersteund voor Windows 8 en later. Windows Server wordt niet ondersteund.

***** Microsoft Defender Antivirus-beheer wordt ondersteund voor Windows 8.1 en later.

Functieset	Windows	Linux	macOS
Evaluatie van beveiligingsproblemen			
Evaluatie van beveiligingsproblemen van het besturingssysteem en de systeemeigen toepassingen	Ja	Ja******	Ja
Evaluatie van beveiligingsproblemen voor toepassingen van derden	Ja	Nee	Ja
Zie "Ondersteunde producten van Microsoft en derden" (p. 1020), "Ondersteunde Linux-producten" (p. 1022) en "Ondersteunde producten van Apple en derden" (p. 1021) voor meer informatie over de ondersteunde besturingssystemen en versies.			

****** De evaluatie van beveiligingsproblemen hangt af van de beschikbaarheid van officiële beveiligingsadviezen voor een specifieke distributie, bijvoorbeeld https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce, enzovoort.

Functieset	Windows	Linux	macOS
Patchbeheer			
Automatische patchgoedkeuring	Ja	Nee	Nee
Automatische patchinstallatie	Ja	Nee	Nee
Patchtest	Ja	Nee	Nee
Handmatige patchinstallatie	Ja	Nee	Nee
Patchplanning	Ja	Nee	Nee
Foutveilig patchen: back-up maken van de machine voordat patches worden geïnstalleerd als onderdeel van het beschermingsschema	Ja	Nee	Nee
Opnieuw opstarten van een machine annuleren als er een back-up wordt uitgevoerd	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functies	Windows	Linux	macOS
Overzicht van gegevensbescherming			
Aanpasbare definitie van belangrijke bestanden	Ja	Nee	Nee

Functies	Windows	Linux	macOS
Overzicht van gegevensbescherming			
Machines scannen om onbeschermde bestanden te vinden	Ja	Nee	Nee
Overzicht van onbeschermde locaties	Ja	Nee	Nee
Mogelijkheid om de beschermingsactie te starten vanuit de widget Overzicht van gegevensbescherming (actie **Alle bestanden beschermen**)	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functieset	Windows	Linux	macOS
Schijfintegriteit			
Op AI gebaseerd beheer van HDD- en SSD-schijfintegriteit	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functies	Windows	Linux	macOS
Slimme beschermingsschema's op basis van Acronis Cyber Protection Operations Center (CPOC)-waarschuwingen			
Bedreigingsfeed	Ja	Nee	Nee
Herstelwizard	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functieset	Windows	Linux	macOS
Back-upscan			
Antimalwarescan van systeemkopieback-ups als onderdeel van het back-upschema	Ja	Nee	Nee
Systeemkopieback-ups scannen op malware in de cloud	Ja	Nee	Nee
Malwarescan van versleutelde back-ups	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functieset	Windows	Linux	macOS
Veilig herstel			
Antimalwarescan met antivirus- en antimalwarebeveiliging tijdens het herstelproces	Ja	Nee	Nee
Veilig herstel voor versleutelde back-ups	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functieset	Windows	Linux	macOS
Verbinding met extern bureaublad			
Verbinding via NEAR	Ja	Ja	Ja
Verbinding via RDP	Ja	Nee	Nee
Verbinding via Schermdeling van Apple	Nee	Nee	Ja
Verbinding via webclient	Ja	Nee	Nee
Verbinding via Quick Assist	Ja	Ja	Ja
Hulp op afstand	Ja	Ja	Ja
Bestandsoverdracht	Ja	Ja	Ja
Overdracht van momentopname	Ja	Ja	Ja
Zie "Ondersteunde platforms" (p. 1060) voor meer informatie over de ondersteunde besturingssystemen en versies.			

Functieset	Windows	Linux	macOS
#CyberFit-score			
Status van #CyberFit-score	Ja	Nee	Nee
Stand-alone tool voor #CyberFit-score	Ja	Nee	Nee
Aanbevelingen van #CyberFit-score	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functieset	Windows	Linux	macOS
Preventie van gegevensverlies			
Apparaatbesturing	Ja	Nee	Ondersteund op

Functieset	Windows	Linux	macOS
Preventie van gegevensverlies			
			Macs met Intel-processors met macOS 10.15 en later of macOS 11.2.3 of later. Niet ondersteund op Apple silicon ARM-processors, zoals Apple M1/M2.
Advanced Data Loss Prevention	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46).			

Functieset	Windows	Linux	macOS
Beheeropties			
Upsellscenario's om Cyber Protect-edities te promoten	Ja	Ja	Ja
Webgebaseerde centrale en externe beheerconsole	Ja	Ja	Ja
Ondersteunde besturingssystemen en versies: Platformonafhankelijk.			

Functieset	Windows	Linux	macOS
Beschermingsopties			
Extern wissen	Ja	Nee	Nee
Ondersteund voor Windows 10 en later.			

Functieset	Windows	Linux	macOS
Cyber Protect Monitor			
Cyber Protect-app	Ja	Nee	Ja
Beveiligingsstatus voor Zoom	Ja	Nee	Nee
Beveiligingsstatus voor Cisco Webex	Ja	Nee	Nee
Beveiligingsstatus voor Citrix Workspace	Ja	Nee	Nee

Functieset	Windows	Linux	macOS
Cyber Protect Monitor			
Beveiligingsstatus voor Microsoft Teams	Ja	Nee	Nee
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46). Op macOS: Cyber Protect Monitor wordt ondersteund voor alle versies waarop u Agent voor Mac kunt installeren. Zie "Agent voor Mac" (p. 28) voor meer informatie.			

Functieset	Windows	Linux	macOS
Software-inventaris			
Software-inventarisscan	Ja	Nee	Ja
Software-inventarisbewaking	Ja	Nee	Ja
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46). Op macOS: Software-inventaris wordt ondersteund voor versies 10.13.x − 13.x.			

Functieset	Windows	Linux	macOS
Hardware-inventaris			
Hardware-inventarisscan	Ja	Nee	Ja
Hardware-inventarisbewaking	Ja	Nee	Ja
Zie de ondersteunde Windows-versies in "Ondersteunde besturingssystemen en versies" (p. 46). Op macOS: Hardware-inventaris wordt ondersteund voor versies 10.13.x − 13.x.			

Ondersteunde bestandssystemen

Met een beveiligingsagent kunt u een back-up maken van elk bestandssysteem dat toegankelijk is vanuit het besturingssysteem waar de agent is geïnstalleerd. Agent voor Windows kan bijvoorbeeld back-ups maken en herstelbewerkingen uitvoeren voor een ext4-bestandssysteem als het toepasselijke stuurprogramma is geïnstalleerd in Windows.

In de volgende tabel ziet u de bestandssystemen waarvoor back-ups en herstelbewerkingen kunnen worden uitgevoerd (op opstartmedia zijn alleen herstelbewerkingen nodig). De beperkingen zijn zowel van toepassing op de agenten als op opstartmedia.

Bestandssysteem	Ondersteund door			Beperkingen
	Agenten	Opstartmedia voor Windows en Linux	Opstartmedia voor Mac	
FAT16/32	Alle agenten	+	+	Geen beperkingen
NTFS	Alle agenten	+	+	
ext2/ext3/ext4	Alle agenten	+	-	
HFS+	Agent voor Mac	-	+	
APFS	Agent voor Mac	-	+	• Ondersteund vanaf macOS High Sierra 10.13 • De schijfconfiguratie moet handmatig opnieuw worden gemaakt wanneer u herstelt naar bare metal of een machine die niet de oorspronkelijke machine is.
JFS	Agent voor Linux	+	-	• Bestandsfilters (opnemen/uitsluiten) worden niet ondersteund • Snelle incrementele/differentiële back-up kan niet worden ingeschakeld
ReiserFS3	Agent voor Linux	+	-	
ReiserFS4	Agent voor Linux	+	-	• Bestandsfilters (opnemen/uitsluiten) worden niet ondersteund • Snelle incrementele/differentiële back-up kan niet worden ingeschakeld • De grootte van volumes kan niet worden aangepast tijdens een

Bestandssysteem	Ondersteund door			Beperkingen
	Agenten	Opstartmedia voor Windows en Linux	Opstartmedia voor Mac	
				herstelbewerking
ReFS	Alle agenten	+	+	• Bestandsfilters (opnemen/uitsluiten) worden niet ondersteund • Snelle incrementele/differentiële back-up kan niet worden ingeschakeld • De grootte van volumes kan niet worden aangepast tijdens een herstelbewerking • Tijdens een bestandsherstel vanaf een ReFS-back-up wordt alleen de inhoud hersteld. Toegangsbeheerlijsten (ACL) en alternatieve streams worden niet hersteld. Tijdelijke bestanden worden hersteld als reguliere bestanden.
XFS	Alle agenten	+	+	• Bestandsfilters (opnemen/uitsluiten) worden niet ondersteund • Snelle incrementele/differentiële back-up kan niet worden ingeschakeld • De grootte van volumes kan niet worden aangepast tijdens een herstelbewerking • De modus snelle incrementele back-up wordt niet ondersteund voor het XFS-

Bestandssysteem	Ondersteund door			Beperkingen
	Agenten	Opstartmedia voor Windows en Linux	Opstartmedia voor Mac	
				bestandssysteem. Incrementele en differentiële back-ups van XFS-volumes naar de cloud kunnen aanzienlijk trager zijn dan vergelijkbare ext4-back-ups die de snelle incrementele modus gebruiken.
Linux swap	Agent voor Linux	+	-	Geen beperkingen
exFAT	Alle agenten	+ Opstartmedia kunnen niet worden gebruikt voor herstel als de back-up *is opgeslagen op* exFAT	+	• Alleen een schijf-/volumeback-up wordt ondersteund • Bestandsfilters (opnemen/uitsluiten) worden niet ondersteund • Er kunnen geen afzonderlijke bestanden worden hersteld vanaf een back-up

De software schakelt automatisch over naar de modus sector-voor-sector wanneer een back-up wordt gemaakt van stations met niet-herkende of niet-ondersteunde bestandssystemen (bijvoorbeeld Btrfs). Een back-up sector-voor-sector is mogelijk voor elk bestandssysteem dat aan de volgende voorwaarden voldoet:

- gebaseerd op blokken
- geplaatst op één schijf
- standaard MBR/GPT-partitioneringsschema

Als het bestandssysteem niet aan deze vereisten voldoet, mislukt de back-up.

Gegevensdeduplicatie

In Windows Server 2012 en later kunt u de functie Gegevensontdubbeling inschakelen voor een NTFS-volume. Met gegevensdeduplicatie vermindert u de gebruikte ruimte op het volume doordat dubbele fragmenten van de bestanden op het volume slechts één keer worden opgeslagen.

Als een volume geschikt is voor gegevensdeduplicatie, kunt u hiervan zonder beperkingen een back-up maken en het herstellen. Back-up op bestandsniveau wordt ondersteund, behalve bij gebruik van Acronis VSS Provider. Als u bestanden van een schijfback-up wilt herstellen, kunt u een virtuele machine uitvoeren vanaf uw back-up of u kunt de back-up koppelen op een machine met Windows Server 2012 of later en vervolgens de bestanden kopiëren vanaf het gekoppelde volume.

De functie Gegevensontdubbeling van Windows Server staat los van de functie Acronis Backup-deduplicatie.

Ondersteunde bewerkingen met logische volumes

Back-up en herstel van workloads met logische volumes, zoals LDM in Windows (dynamische schijven) en LVM in Linux, worden ondersteund met de volgende beperkingen.

Back-up

Back-up met agent is een back-up gemaakt door een beveiligingsagent die is geïnstalleerd in de workload of door een opstartmedium.

Back-up zonder agent is alleen beschikbaar voor virtuele machines. De back-up zonder agent wordt uitgevoerd op hypervisorniveau door een agent die een back-up kan maken en herstel kan uitvoeren voor alle virtuele machines in de omgeving. Er worden geen afzonderlijke agenten geïnstalleerd op de beschermde virtuele machines.

Zie "Back-ups met en zonder agent" (p. 63) voor meer informatie over de verschillen tussen back-up met agent en zonder agent.

Back-up met agent	Back-up zonder agent
• Back-ups van logische volumes worden gemaakt per volume. • Bestandsfilters (opnemen/uitsluiten) worden ondersteund.	• Wanneer er een logisch volume wordt gedetecteerd op een schijf, wordt er een back-up van de schijf gemaakt in de modus per sector (RAW). De partitiestructuur van de schijf wordt niet geanalyseerd en er worden geen afzonderlijke volume-images opgeslagen. • Afzonderlijke LDM- of LVM-volumes kunnen niet worden geselecteerd als back-upbron – noch door directe selectie, noch via beleidsregels. Alleen **Hele machine** is beschikbaar in het gedeelte **Back-up maken van** van een beschermingsplan.

Back-up met agent	Back-up zonder agent
	• Bestandsfilters (opnemen/uitsluiten) worden niet ondersteund. Eventueel geconfigureerde items voor opnemen of uitsluiten worden genegeerd.

Herstel

Herstel met agent is een herstelbewerking uitgevoerd door een agent die is geïnstalleerd in de workload of door een opstartmedium.

Herstel zonder agent ondersteunt alleen virtuele machines als doel. Herstel zonder agent wordt uitgevoerd op hypervisorniveau door een agent die een back-up kan maken en herstel kan uitvoeren voor alle virtuele machines in de omgeving. U hoeft niet handmatig een doelmachine te maken waarop de back-up wordt hersteld.

	Vanuit back-up met agent	Vanuit back-up zonder agent
Herstel met agent	• Herstel per volume is beschikbaar. • Bestand- en mapherstel is beschikbaar.	• Herstel per volume is niet beschikbaar. • Bestand- en mapherstel is beschikbaar.
Herstel zonder agent	• Machinemigratie (P2V, V2P en V2V) wordt niet ondersteund. Als u gegevens wilt herstellen vanuit een back-up met agent, moet u opstartmedia gebruiken. • De bewerking **Uitvoeren als VM** wordt niet ondersteund. • Bestand- en mapherstel is beschikbaar.	• Herstel per volume is niet beschikbaar. • Herstel van volledige machine is beschikbaar. • Bestand- en mapherstel is beschikbaar. • De bewerking **Uitvoeren als VM** wordt ondersteund. Als u de virtuele machine opstartbaar wilt maken, moet u mogelijk de opstartvolgorde wijzigen. Zie dit Knowledge Base-artikel voor meer informatie. • Conversie naar de volgende typen virtuele machines wordt ondersteund: ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ Scale Computing HC3

Cyber Protection-agents installeren en implementeren

Voordat u start

Voorbereiding

Stap 1

Kies een agent, afhankelijk waarvan u een back-up wilt maken. Zie Welke agent heb ik nodig? voor meer informatie over de mogelijke opties.

Stap 2

Controleer of er voldoende vrije schijfruimte is op uw harde schijf om een agent te installeren. Zie "Systeemvereisten voor agenten" (p. 68) voor gedetailleerde informatie over de vereiste schijfruimte.

Stap 3

Download het installatieprogramma. Voor de downloadlinks klikt u op **Alle apparaten** > **Toevoegen**.

De pagina **Apparaten toevoegen** bevat webinstallers voor elke agent die is geïnstalleerd in Windows. Een webinstaller is een klein uitvoerbaar bestand dat het hoofdinstallatieprogramma van internet downloadt en opslaat als een tijdelijk bestand. Dit bestand wordt na de installatie meteen weer verwijderd.

Als u de installatieprogramma's lokaal wilt opslaan, gebruikt u de link onder aan de pagina **Apparaten toevoegen** om een pakket te downloaden met alle agenten voor installatie in Windows. Zowel 32-bits als 64-bits pakketten zijn beschikbaar. Met deze pakketten kunt u de lijst met te installeren onderdelen aanpassen. Met deze pakketten kunt u ook een installatie zonder toezicht uitvoeren, bijvoorbeeld via Groepsbeleid. Dit geavanceerde scenario wordt beschreven in "Beveiligingsagents via Groepsbeleid implementeren" (p. 140).

Als u het installatieprogramma voor Agent voor Microsoft 365 wilt downloaden, klikt u op het accountpictogram in de rechterbovenhoek en vervolgens op **Downloads** > **Agent voor Microsoft 365**.

De installatie in Linux en macOS wordt uitgevoerd met de gebruikelijke installatieprogramma's.

Voor alle installatieprogramma's is een internetverbinding vereist om de machine bij de Cyber Protection-service te registreren. Zonder internetverbinding mislukt de installatie.

Stap 4

Voor Cyber Protect-functies is Microsoft Visual C++ 2017 Redistributable vereist. Zorg ervoor dat dit pakket al op uw machine is geïnstalleerd of installeer het voordat u de agent installeert. Na de installatie van Microsoft Visual C++ moet mogelijk opnieuw worden opgestart. U kunt het Microsoft Visual C++ Redistributable-pakket hier vinden https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Stap 5

Controleer of uw firewalls en andere onderdelen van uw netwerkbeveiligingssysteem (zoals een proxyserver) uitgaande verbindingen toelaten via de volgende TCP-poorten.

- Poorten **443** en **8443**

  Deze poorten worden gebruikt voor toegang tot de Cyber Protect-console, registratie van agents, downloads van certificaten, gebruikersautorisatie en downloads van bestanden uit de cloudopslag.
- Poorten in het bereik **7770** – **7800**

  Deze poorten worden door de agents gebruikt voor communicatie met de beheerserver.
- Poorten **44445** en **55556**

  Deze poorten worden door de agents gebruikt voor gegevensoverdracht tijdens back-up- en herstelbewerkingen.

Als er een proxyserver is ingeschakeld in uw netwerk, raadpleegt u "Proxyserverinstellingen configureren" (p. 74) om te weten of u deze instellingen moet configureren op elke machine waarop een beveiligingsagent wordt uitgevoerd.

De minimale snelheid van de internetverbinding die is vereist om een agent vanuit de cloud te beheren, is 1 Mbit/s (deze waarde is niet gelijk aan de gegevensoverdrachtsnelheid die acceptabel is voor back-ups naar de cloud). Houd hier rekening mee u een verbindingstechnologie met lage bandbreedte zoals ADSL gebruikt.

Voor back-up en replicatie van virtuele VMware-machines zijn TCP-poorten vereist

- Poort **443**

  Agent voor VMware (zowel Windows als Virtual Appliance) maakt verbinding met deze poort op de ESXi-host/vCenter-server om bewerkingen voor VM-beheer uit te voeren, zoals het maken, bijwerken en verwijderen van VM's op vSphere tijdens back-up, herstel en VM-replicatie.
- Poort **902**

  Agent voor VMware (zowel Windows als Virtual Appliance) maakt verbinding met deze poort op de ESXi-host om NFC-verbindingen tot stand te brengen voor het lezen/schrijven van gegevens op VM-schijven tijdens back-up, herstel en VM-replicatie.
- Poort **3333**

  Als de Agent voor VMware (Virtual Appliance) wordt uitgevoerd op de ESXi-host/cluster die het doel is voor VM-replicatie, gaat het VM-replicatieverkeer niet rechtstreeks naar de ESXi-host op

poort **902**. In plaats daarvan gaat het verkeer van de bronagent voor VMware naar TCP-poort **3333** op de Agent voor VMware (Virtual Appliance) op de doel-ESXi-host/cluster.

Alle locaties en typen zijn toegestaan voor de bronagent voor VMware die gegevens van de oorspronkelijke VM-schijven leest: Virtual Appliance of Windows.

De service die VM-replicatiegegevens accepteert op de doelagent voor VMware (Virtual Appliance) wordt 'Replica-schijfserver' genoemd. Deze service levert de WAN-optimalisatietechnieken, zoals verkeerscompressie en deduplicatie tijdens VM-replicatie, inclusief replica seeding (zie Seeding van een eerste replica). Als er geen Agent voor VMware (Virtual Appliance) op de doel-ESXi-host wordt uitgevoerd, is deze service niet beschikbaar en wordt het scenario met replica seeding niet ondersteund.

Poorten vereist voor het onderdeel Downloadprogramma

Het onderdeel Downloadprogramma wordt gebruikt om updates te leveren aan een computer en de updates te distribueren naar andere exemplaren van het Downloadprogramma. Het programma kan worden uitgevoerd in de modus met agent, waardoor de computer verandert in de agent voor het Downloadprogramma. De agent voor het Downloadprogramma downloadt updates van internet en servers als de bron voor de distributie van updates naar andere computers. Voor een goede werking van het Downloadprogramma zijn de volgende poorten vereist.

- (Inkomende) TCP- en UDP-poort **6888**
  Gebruikt door BitTorrent-protocol voor torrent peer-to-peer-updates.
- UDP-poort **6771**
  Gebruikt als de lokale poort voor peer-detectie. Wordt ook gebruikt voor peer-to-peer-updates.
- TCP-poort **18018**
  Gebruikt voor communicatie tussen updaters die in verschillende modi werken: Updater en UpdaterAgent.
- TCP-poort **18019**
  Lokale poort, gebruikt voor communicatie tussen de updater en de beveiligingsagent.

Stap 6

Controleer of de volgende lokale poorten niet worden gebruikt door andere processen op de machine waarop u de beveiligingsagent wilt installeren.

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

Opmerking
U hoeft ze niet te openen in de firewall.

De poorten wijzigen die door de beveiligingsagent worden gebruikt

Sommige poorten die zijn vereist voor de beveiligingsagent, worden mogelijk gebruikt door andere toepassingen in uw omgeving. Als u conflicten wilt voorkomen, moet u de standaardpoorten wijzigen die door de beveiligingsagent worden gebruikt. Dit doet u door de volgende bestanden te wijzigen.

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

Back-ups met en zonder agent

In het geval van back-ups met agent moet er een beveiligingsagent zijn geïnstalleerd op elke beschermde machine. Back-ups met agent worden ondersteund op alle fysieke en virtuele machines. Voor meer informatie over welke agent u nodig hebt en waar u deze moet installeren: zie "Welke agent heb ik nodig?" (p. 64)

Back-up zonder agent wordt ondersteund door sommige virtualisatieplatforms en is niet beschikbaar voor fysieke machines. Bij een back-up zonder agent is slechts één beveiligingsagent vereist, die op een speciale machine in de virtuele omgeving wordt geïnstalleerd. Deze agent maakt een back-up van alle andere virtuele machines in deze omgeving. Zie "Ondersteunde virtualisatieplatforms" (p. 32) voor meer informatie over de ondersteunde back-uptypen per virtualisatieplatform.

Voor sommige virtualisatieplatforms zijn virtuele toepassingen beschikbaar. Een virtueel apparaat (VA) is een kant-en-klare virtuele machine die een beveiligingsagent bevat. De virtuele apparaten zijn beschikbaar in specifieke indelingen voor hypervisors, zoals .ovf, .ova of .qcow.

Welk type back-up heb ik nodig?

Back-up met agent wordt aanbevolen als u het volgende nodig hebt:

- Extra beschermingsfunctionaliteit, zoals antivirus en antimalware, patchbeheer of verbinding met extern bureaublad. Voor meer informatie over deze functies: zie "Ondersteunde beschermingsfuncties per besturingssysteem" (p. 45).
- U moet de virtuele machines op tenantniveau scheiden, bijvoorbeeld omdat u de gebruikers in de tenant alleen toegang wilt geven tot hun eigen back-ups.
- Back-ups op bestandsniveau die u kunt herstellen op de gastbesturingssystemen.

Back-up zonder agent wordt aanbevolen als u het volgende nodig hebt:

- Alleen back-up, zonder enige extra beschermingsfuncties.
- Vereenvoudigd beheer: u kunt een back-up maken van meerdere virtuele machines door slechts één agent te installeren en configureren.
- Minimaal gebruik van resources: één speciale agent gebruikt minder CPU en RAM dan meerdere agents waarbij op elke virtuele machine in uw omgeving een agent is geïnstalleerd.

- Specifieke back-upinstellingen, zoals back-up zonder LAN. Voor meer informatie over deze functie: zie "Agent voor VMware – back-up zonder LAN" (p. 726).
- Minder configuratie-overhead. De speciale agent maakt een back-up van de virtuele machines op hypervisorniveau, ongeacht de gastbesturingssystemen.

Welke agent heb ik nodig?

Welke agent u selecteert, hangt af van de items waarvan u een back-up wilt maken. De onderstaande tabel bevat een overzicht van de informatie op basis waarvan u een besluit kunt nemen.

In Windows moet voor de installatie van Agent voor Exchange, Agent voor SQL, Agent voor Active Directory en Agent voor Oracle ook Agent voor Windows worden geïnstalleerd. Als u dan bijvoorbeeld Agent voor SQL installeert, kunt u ook een volledige back-up maken van de machine waarop de agent is geïnstalleerd.

We raden aan om ook Agent voor Windows te installeren wanneer u Agent voor VMware (Windows) en Agent voor Hyper-V installeert.

In Linux werken Agent voor Oracle, Agent voor MySQL/MariaDB en Agent voor Virtuozzo alleen als ook Agent voor Linux (64 bits) is geïnstalleerd. Deze agents zijn te vinden in de bundel met het installatiebestand van Agent voor Linux (64-bits).

Waar wilt u een back-up van maken?	Welke agent moet u installeren?	Waar moet de agent worden geïnstalleerd?
Fysieke machines		
Fysieke machines met Windows	Agent voor Windows	Op de machine waarvan een back-up wordt gemaakt.
Fysieke machines met Linux	Agent voor Linux	
Fysieke machines met macOS	Agent voor Mac	
Databases		
SQL-databases	Agent voor SQL	Op de machine met Microsoft SQL Server.
MySQL-databases	Agent voor MySQL/MariaDB (te vinden in de bundel met het installatiebestand van Agent voor Linux (64-bits))	Op de machine met MySQL Server.

MariaDB-databases	Agent voor MySQL/MariaDB (te vinden in de bundel met het installatiebestand van Agent voor Linux (64-bits))	Op de machine met MariaDB Server.
Exchange-databases	Agent voor Exchange	Op de machine met de rol Postvak van Microsoft Exchange Server.*
Oracle-databases	Agent voor Oracle (In Linux: te vinden in de bundel met het installatiebestand van Agent voor Linux (64-bits))	Op de machine met Oracle Database.
Cloud-naar-cloud workloads		
Microsoft 365-postvakken (Cloudagent of lokale agent)	Cloudagent (Geen installatie vereist)	Deze functionaliteit is beschikbaar met een cloudagent die wordt geïmplementeerd in het datacentrum. Zie "De cloudagent voor Microsoft 365 gebruiken" (p. 642) voor meer informatie.
	Agent voor Office 365	Op een machine met Windows en een verbinding met internet. Zie "Lokale Agent voor Office 365 gebruiken" (p. 637) voor meer informatie.
Microsoft 365 OneDrive-bestanden en SharePoint Online-sites	Cloudagent (Geen installatie vereist)	Deze functionaliteit is beschikbaar met een cloudagent die wordt

		geïmplementeerd in het datacentrum. Zie "De cloudagent voor Microsoft 365 gebruiken" (p. 642) voor meer informatie.
Google Workspace Gmail-postvakken, Google Drive-bestanden en gedeelde Drive-bestanden	Cloudagent (Geen installatie vereist)	Deze functionaliteit is beschikbaar met een cloudagent die wordt geïmplementeerd in het datacentrum. Zie "Google Workspace-gegevens beveiligen" (p. 677) voor meer informatie.
Active Directory		
Machines met Active Directory Domain Services	Agent voor Active Directory	Op de domeincontroller.
Virtuele machines		
Virtuele VMware ESXi-machines	Agent voor VMware (Windows)	Op een Windows-machine met netwerktoegang tot de vCenter-server en de virtuele machineopslag.**
	Agent voor VMware (Virtual Appliance)	Op de ESXi-host.
Virtuele Hyper-V-machines	Agent voor Hyper-V	Op de Hyper-V-host.
Virtuele Scale Computing HC3-machines	Agent voor Scale Computing HC3 (Virtual Appliance)	Op de Scale Computing HC3-host.
Virtuele Red Hat Virtualization-machines (beheerd met oVirt)	Agent voor oVirt (Virtual Appliance)	Op de Red Hat Virtualization-host.
Virtuele Virtuozzo-machines en -containers***	Agent voor Virtuozzo	Op de Virtuozzo-host.

	(te vinden in de bundel met het installatiebestand van Agent voor Linux (64-bits))	
Virtuele Virtuozzo Hybrid Infrastructure-machines	Agent voor Virtuozzo Hybrid Infrastructure (Virtual Appliance)	Op de Virtuozzo Hybrid Infrastructure-host.
Virtuele machines gehost op Amazon EC2	Hetzelfde als voor fysieke machines****	Op de machine waarvan een back-up wordt gemaakt.
Virtuele machines gehost op Windows Azure		
Virtuele Citrix XenServer-machines		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
Kernel-based Virtual Machines (KVM), niet beheerd met oVirt		
Virtuele Oracle-machines, niet beheerd met oVirt		
Virtuele Nutanix AHV-machines		
Red Hat Virtualization (RHV/RHEV), beheerd door oVirt	Agent voor oVirt (Virtual Appliance)	Op de virtualisatiehost.
Kernel-based Virtual Machines (KVM), beheerd met oVirt		
Virtuele Oracle-machines, beheerd met oVirt		
Mobiele apparaten		
Mobiele apparaten met Android	Mobiele app voor Android	Op het mobiele apparaat waarvan een back-up wordt gemaakt.
Mobiele apparaten met iOS	Mobiele app voor iOS	

*Tijdens de installatie controleert Agent voor Exchange of er voldoende vrije schijfruimte is op de machine waar de agent wordt uitgevoerd. Vrije schijfruimte gelijk aan 15 procent van de grootste Exchange-database is tijdelijk nodig tijdens een gedetailleerd herstel.

**Als voor uw ESXi een opslag wordt gebruikt die is gekoppeld via SAN, installeert u de agent op een machine die is aangesloten op hetzelfde SAN. De agent maakt rechtstreeks vanuit de opslag een back-up van de virtuele machines en niet via de ESXi-host en het LAN. Zie "Agent voor VMware – back-up zonder LAN" (p. 726) voor gedetailleerde instructies.

***Alleen ploop-containers worden ondersteund voor Virtuozzo 7. Virtuele machines worden niet ondersteund.

****Een virtuele machine wordt als virtueel beschouwd als de back-up van de machine wordt uitgevoerd door een externe agent. Als er een agent op het gastsysteem is geïnstalleerd, worden

back-ups en herstel op dezelfde manier uitgevoerd als voor een fysieke machine. Maar als Cyber Protection een virtuele machine kan identificeren via de CPUID-instructie, wordt hieraan een servicequota voor de virtuele machine toegewezen. Als u direct doorsturen gebruikt of een andere optie die de id van de CPU-fabrikant maskeert, kunnen alleen servicequota's voor fysieke machines worden toegewezen.

Systeemvereisten voor agenten

Agent	Vereiste schijfruimte voor installatie
Agent voor Windows	1,2 GB
Agent voor Linux	2 GB
Agent voor Mac	1 GB
Agent voor SQL en Agent voor Windows	1,2 GB
Agent voor Agent voor Exchange en Agent voor Windows	1,3 GB
Agent voor preventie van gegevensverlies	500 MB
Agent voor Microsoft 365	500 MB
Agent voor Active Directory en Agent voor Windows	2 GB
Agent voor VMware en Agent voor Windows	1,5 GB
Agent voor Hyper-V en Agent voor Windows	1,5 GB
Agent voor Virtuozzo en Agent voor Linux	1 GB
Agent voor Virtuozzo Hybrid Infrastructure	700 MB
Agent voor Oracle en Agent voor Windows	2,2 GB
Agent voor Oracle en Agent voor Linux	2 GB
Agent voor MySQL/MariaDB en Agent voor Linux	2 GB

Voor back-upbewerkingen, inclusief het verwijderen van back-ups, is ongeveer 1 GB RAM per 1 TB back-upgrootte vereist. Het geheugenverbruik kan variëren, afhankelijk van de hoeveelheid en het type gegevens die door de agenten worden verwerkt.

Opmerking
Het RAM-gebruik kan toenemen wanneer back-ups worden gemaakt voor zeer grote back-upsets (4 TB en meer).

Voor opstartmedia of schijfherstel met opnieuw opstarten is minimaal 2 GB geheugen vereist op x64-systemen.

In workloads met moderne processors (zoals 11e generatie Intel Core of AMD Ryzen 7) die CET-technologie ondersteunen, zijn sommige functies van de Agent voor preventie van gegevensverlies uitgeschakeld om conflicten te voorkomen. De volgende tabel bevat een overzicht van de beschikbaarheid van Apparaatbeheer en Advanced DLP-functies op systemen met dergelijke CPU's.

Functies	Apparaatbesturing	Advanced DLP
Lokale kanalen		
Verwisselbare opslag	N.v.t.	Ja
Versleutelde verwisselbare opslag	Ja	N.v.t.
Printers	N.v.t.	Nee
Omgeleide toegewezen stations	N.v.t.	Ja
Omgeleid klembord	N.v.t.	Nee
Netwerkcommunicatie		
SMTP-e-mails	N.v.t.	Ja
Microsoft Outlook (MAPI)	N.v.t.	Ja
IBM-notities	N.v.t.	Nee
Webmails	N.v.t.	Ja
Chatberichten (ICQ)	N.v.t.	Nee
Chatberichten (Viber)	N.v.t.	Nee
Chatberichten (IRC, Jabber, Skype, Viber)	N.v.t.	Ja
Services voor bestanden delen	N.v.t.	Ja
Sociale netwerken	N.v.t.	Ja
Delen van bestanden via een lokaal netwerk (SMB)	N.v.t.	Ja
Webtoegang (HTTP/HTTPS)	N.v.t.	Ja
Bestandsoverdrachten (FTP/FTPS)	N.v.t.	Ja
Gegevensoverdracht plaatsen op acceptatielijst		
Acceptatielijst voor apparaattypen	N.v.t.	Ja
Acceptatielijst voor netwerkcommunicatie	N.v.t.	Ja
Acceptatielijst voor externe hosts	N.v.t.	Ja

Acceptatielijst voor toepassingen	N.v.t.	Ja
Randapparaten		
Verwisselbare opslag	Ja	Ja
Versleutelde verwisselbare opslag	Ja	Ja
Printers	Nee	Nee
Via MTP verbonden mobiele apparaten	Nee	Nee
Bluetooth-adapters	Ja	Ja
Optische stations	Ja	Ja
Diskettestations	Ja	Ja
Windows-klembord	Nee	Nee
Schermopname	Nee	Nee
Omgeleide toegewezen stations	Ja	Ja
Omgeleid klembord	Nee	Nee
Cyber Protect Agent-zelfbescherming		
Bescherming tegen reguliere eindgebruikers	Ja	Ja
Bescherming tegen lokale systeembeheerders	Ja	Ja

Beveiligingsagents downloaden

Voordat u een agent installeert, moet u het betreffende installatiebestand downloaden vanuit de Cyber Protect-console.

Een agent downloaden terwijl u een workload toevoegt om te beschermen

1. Ga in de Cyber Protect-console, naar **Apparaten** > **Alle apparaten**.
2. Klik rechtsboven op **Apparaat toevoegen**.
3. Ga in het deelvenster **Apparaten toevoegen** naar het vervolgkeuzemenu **Releasekanaal** en selecteer een agentversie.
   - **Vorige release**: download de agentversie van de vorige release.
   - **Huidige**: download de meest recente agentversie die beschikbaar is.
4. Select de agent voor het besturingssysteem van de workload die u wilt toevoegen.
   Het dialoogvenster **Opslaan als** wordt geopend.
5. [Alleen voor Macs met Apple Silicon-processors (zoals Apple M1)] Klik op **Annuleren**. Klik in het deelvenster **Mac toevoegen** dat wordt geopend, op de link **ARM-installatieprogramma**

downloaden.

6. Selecteer een locatie om het installatiebestand van de agent op te slaan en klik op **Opslaan**.

Een agent downloaden voor later gebruik

1. Klik in de rechterbovenhoek van de Cyber Protect-console op het pictogram **Gebruiker**.
2. Klik op **Downloads**.
3. Ga in het dialoogvenster **Downloads** naar het vervolgkeuzemenu **Releasekanaal** en selecteer een agentversie.
   - **Vorige release**: download de agentversie van de vorige release.
   - **Huidige**: download de meest recente agentversie die beschikbaar is.
4. Scrol door de lijst met beschikbare installatieprogramma's om het nodige installatieprogramma van de agent te vinden en klik op het downloadpictogram aan het einde van de betreffende rij. Het dialoogvenster **Opslaan als** wordt geopend.
5. Selecteer een locatie om het installatiebestand van de agent op te slaan en klik op **Opslaan**.

Linux-pakketten

Om de benodigde modules aan de Linux-kernel toe te voegen, heeft het installatieprogramma de volgende Linux-pakketten nodig:

- Het pakket met de kernelheaders of -bronnen. De pakketversie moet overeenkomen met de kernelversie.
- Het GCC-compileersysteem (GNU Compiler Collection). De kernel moet zijn gecompileerd met de GCC-versie.
- De tool Make.
- De Perl-interpreter.
- De bibliotheken `libelf-dev`, `libelf-devel` of `elfutils-libelf-devel` voor het bouwen van kernels vanaf versie 4.15 en geconfigureerd met CONFIG_UNWINDER_ORC=y. Voor sommige distributies, zoals Fedora 28, moeten deze apart van de kernelheaders worden geïnstalleerd.

De namen van deze pakketten kunnen variëren, afhankelijk van de Linux-distributie.

In Red Hat Enterprise Linux, CentOS en Fedora worden de pakketten doorgaans geïnstalleerd door het installatieprogramma. In andere distributies moet u de pakketten zelf installeren als ze nog niet zijn geïnstalleerd of de vereiste versie niet aanwezig is.

Zijn de vereiste pakketten al geïnstalleerd?

Voer de volgende stappen uit om te controleren of de pakketten al zijn geïnstalleerd:

1. Voer de volgende opdracht uit om de kernel- en GCC-versie te bepalen:

```
cat /proc/version
```

Deze opdracht retourneert regels die vergelijkbaar zijn met de volgende: `Linux-versie 2.6.35.6` en `gcc version 4.5.1`

2. Voer de volgende opdracht uit om te controleren of de tool Make en het GCC-compileerprogramma zijn geïnstalleerd:

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

Gcc: controleer of de versie die door de opdracht wordt geretourneerd, overeenkomt met de `gcc-versie` in stap 1. **Make**: controleer alleen of de opdracht wordt uitgevoerd.

3. Controleer of de juiste versie van het pakket voor het bouwen van kernelmodules is geïnstalleerd:
   - Voer in Red Hat Enterprise Linux, CentOS en Fedora de volgende opdracht uit:

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

   - Voer in Ubuntu de volgende opdrachten uit:

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

   Zorg er in beide gevallen voor dat de pakketversies overeenkomen met de `Linux-versie` in stap 1.

4. Voer de volgende opdracht uit om te controleren of de Perl-interpreter is geïnstalleerd:

```
perl --version
```

   Als er informatie over de Perl-versie wordt weergegeven, is de interpreter geïnstalleerd.

5. Voer in Red Hat Enterprise Linux, CentOS en Fedora de volgende opdracht uit om te controleren of `elfutils-libelf-devel` is geïnstalleerd:

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

   Als er informatie over de bibliotheekversie wordt weergegeven, is de bibliotheek geïnstalleerd.

De pakketten installeren vanuit de opslagplaats

De volgende tabel toont u hoe u de vereiste pakketten in de verschillende Linux-distributies installeert.

Linux-distributie	Pakketnamen	Installeren
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	De pakketten worden automatisch door het installatieprogramma gedownload en geïnstalleerd door gebruik te maken van uw Red Hat-abonnement.

	perl	Voer de volgende opdracht uit: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	De pakketten worden automatisch door het installatieprogramma gedownload en geïnstalleerd.
	perl	Voer de volgende opdracht uit: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Voer de volgende opdrachten uit:
		`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`

De pakketten worden gedownload uit de opslagplaats van de distributie en vervolgens geïnstalleerd.

Voor andere Linux-distributies raadpleegt u de documentatie van de distributie voor de exacte namen van de vereiste pakketten en de installatie-instructies.

De pakketten handmatig installeren

Mogelijk moet u de pakketten in de volgende gevallen **handmatig** installeren:

- De machine heeft geen actief Red Hat-abonnement of actieve internetverbinding.
- Het installatieprogramma kan de **kernel-devel**- of **gcc**-versie niet vinden die overeenkomt met de kernelversie. Als de beschikbare **kernel-devel** nieuwer is dan uw kernel, moet u de kernel bijwerken of de overeenkomende versie van de **kernel-devel** handmatig installeren.
- U hebt de vereiste pakketten op het lokale netwerk en wilt geen tijd besteden om automatisch te zoeken en te downloaden.

Haal de pakketten op van uw lokale netwerk of via de website van een betrouwbare derde partij en installeer ze als volgt:

- In Red Hat Enterprise Linux, CentOS of Fedora voert u de volgende opdracht uit als rootgebruiker:

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

- Voer in Ubuntu de volgende opdracht uit:

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

Voorbeeld: de pakketten handmatig installeren in Fedora 14

Voer de volgende stappen uit om de vereiste pakketten in Fedora 14 op een 32-bits machine te installeren:

1. Voer de volgende opdracht uit om de kernelversie en de vereiste GCC-versie te bepalen:

   ```
   cat /proc/version
   ```

   De uitvoer van deze opdracht bevat onder meer het volgende:

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

2. Haal de **kernel-devel**- en **gcc**-pakketten op die overeenkomen met deze kernelversie:

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

3. Haal het **make**-pakket voor Fedora 14 op:

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

4. Installeer de pakketten door de volgende opdrachten uit te voeren als rootgebruiker:

   ```
   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
   ```

   U kunt al deze pakketten opgeven in één `rpm`-opdracht. Wanneer u deze pakketten installeert, moet u mogelijk aanvullende pakketten installeren om afhankelijkheden op te lossen.

Proxyserverinstellingen configureren

De beveiligingsagenten kunnen gegevens overdragen via een HTTP/HTTPS-proxyserver. De server moet een HTTP-tunnel doorlopen zonder te scannen of het HTTP-verkeer te verstoren. Man-in-the-middle proxy's worden niet ondersteund.

Aangezien de agent zichzelf registreert in de cloud tijdens de installatie, moet u de proxyserverinstellingen opgeven tijdens of voorafgaand aan de installatie.

Voor Windows

Als een proxyserver is geconfigureerd in **Configuratiescherm** > **Internetopties** > **Verbindingen**, worden de proxyserverinstellingen gelezen vanuit het register en automatisch toegepast door het installatieprogramma.

Gebruik deze procedure als u de volgende taken wilt uitvoeren.

- De proxyinstellingen configureren vóór de installatie van de agent.
- De proxyinstellingen bijwerken na de installatie van de agent.

Zie "Beveiligingsagents installeren in Windows" (p. 81) voor het configureren van de proxyinstellingen gedurende de installatie van de agent.

Opmerking
Deze procedure is alleen geldig wanneer het bestand `http-proxy.yaml` niet bestaat op de machine. Als het bestand `http-proxy.yaml` wel bestaat op de machine, moet u de proxyinstellingen in het bestand bijwerken, aangezien hiermee de instellingen in het bestand `aakore.yaml` worden overschreven.

Het bestand `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml` wordt gemaakt wanneer u de instellingen van de proxyserver configureert via Cyber Protection Monitor. Zie "Proxyserverinstellingen configureren in Cyber Protect Monitor" (p. 300) voor meer informatie.

U moet lid zijn van de groep Administrators in Windows om het bestand `http-proxy.yaml` te kunnen openen.

De proxyinstellingen configureren:

1. Maak een nieuw tekstdocument en open het in een teksteditor, zoals Kladblok.
2. Kopieer en plak de volgende regels in het bestand.

```
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. Vervang `proxy.company.com` door de hostnaam/het IP-adres van uw proxyserver en vervang `000001bb` door de hexadecimale waarde van het poortnummer. Voorbeeld: `000001bb` is poort 443.
4. Als uw proxyserver verificatie vereist, vervangt u `proxy_login` en `proxy_password` door de referenties van de proxyserver. Zo niet, dan kunt u deze regels verwijderen uit het bestand.
5. Sla het document op als `proxy.reg`.
6. Voer het bestand uit als beheerder.
7. Bevestig dat u het Windows-register wilt bewerken.

8. Als de agent nog niet is geïnstalleerd voor deze workload, kunt u deze nu installeren. Als de agent wel al is geïnstalleerd voor de workload, gaat u verder met de volgende stap.
9. Open het bestand `%programdata%\Acronis\Agent\etc\aakore.yaml` in een teksteditor.
   U moet lid zijn van de groep Administrators in Windows om dit bestand te kunnen openen.
10. Zoek het gedeelte **env** of maak dit en voeg de volgende regels toe.

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

11. Vervang `proxy_login` en `proxy_password` door de referenties van de proxyserver en vervang `proxy_address:port` door het adres en poortnummer van de proxyserver.
12. Klik in het menu **Start** op **Uitvoeren** en typ **cmd**. Klik vervolgens op **OK**.
13. Start de aakore-service opnieuw met de volgende opdrachten.

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

14. Start de agent opnieuw met de volgende opdrachten.

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

Voor macOS

Gebruik deze procedure als u de volgende taken wilt uitvoeren.

- De proxyinstellingen configureren vóór de installatie van de agent.
- De proxyinstellingen bijwerken na de installatie van de agent.

Zie "Beveiligingsagents installeren in macOS" (p. 86) voor het configureren van de proxyinstellingen gedurende de installatie van de agent.

De proxyinstellingen configureren:

1. Maak het bestand `/Library/Application Support/Acronis/Registry/Global.config` en open het in een teksteditor zoals TextEdit.
2. Kopieer en plak de volgende regels in het bestand.

```
<?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. Vervang `proxy.company.com` door de hostnaam/het IP-adres van uw proxyserver en vervang `443` door de decimale waarde van het poortnummer.
4. Als uw proxyserver verificatie vereist, vervangt u `proxy_login` en `proxy_password` door de referenties van de proxyserver. Zo niet, dan kunt u deze regels verwijderen uit het bestand.
5. Sla het bestand op.
6. Als de agent nog niet is geïnstalleerd voor deze workload, kunt u deze nu installeren. Als de agent wel al is geïnstalleerd voor de workload, gaat u verder met de volgende stap.
7. Open het bestand `/Library/Application Support/Acronis/Agent/etc/aakore.yaml` in een teksteditor.
8. Zoek het gedeelte **env** of maak dit en voeg de volgende regels toe.

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

9. Vervang `proxy_login` en `proxy_password` door de referenties van de proxyserver en vervang `proxy_address:port` door het adres en poortnummer van de proxyserver.
10. Ga naar **Programma's** > **Hulpprogramma's** > **Terminal**.
11. Start de aakore-service opnieuw met de volgende opdrachten.

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

12. Start de agent opnieuw met de volgende opdrachten.

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

Voor Linux

Voer het installatiebestand uit met de parameters `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`. Gebruik de volgende procedure als u de proxyinstellingen wilt bijwerken na installatie van de beveiligingsagent.

De proxyinstellingen configureren:

1. Open het bestand `/etc/Acronis/Global.config` in een teksteditor.
2. Voer een van de volgende handelingen uit:
   - Als de proxyinstellingen zijn opgegeven tijdens de installatie van de agent, gaat u naar het volgende gedeelte.

```
<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>
```

- Als de proxyinstellingen niet zijn opgegeven tijdens de installatie van de agent, kopieert u de volgende regels en plakt u ze in het bestand tussen de tags `<registry name="Global">...</registry>`.

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

3. Vervang `ADDRESS` door de nieuwe waarden voor de hostnaam/het IP-adres van de proxyserver en vervang `PORT` door de decimale waarde van het poortnummer.
4. Als uw proxyserver verificatie vereist, vervangt u `LOGIN` en `PASSWORD` door de referenties van de proxyserver. Zo niet, dan kunt u deze regels verwijderen uit het bestand.
5. Sla het bestand op.
6. Open het bestand `/opt/acronis/etc/aakore.yaml` in een teksteditor.
7. Zoek het gedeelte **env** of maak dit en voeg de volgende regels toe:

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

8. Vervang `proxy_login` en `proxy_password` door de referenties van de proxyserver en vervang `proxy_address:port` door het adres en poortnummer van de proxyserver.
9. Start de aakore-service opnieuw met de volgende opdracht.

```
sudo service aakore restart
```

10. Start de agent opnieuw op door de opdracht uit te voeren in een willekeurige directory.

```
sudo service acronis_mms restart
```

Voor opstartmedia

Wanneer u met opstartmedia werkt, hebt u mogelijk een proxyserver nodig voor toegang tot de cloudopslag. Als u de instellingen voor de proxyserver wilt configureren, klikt u op **Extra** > **Proxyserver** en geeft u de hostnaam/het IP-adres, de poort en de referenties van de proxyserver op.

Dynamisch installeren en verwijderen van onderdelen

Voor Windows-workloads die worden beschermd door agent versie 15.0.26986 (uitgebracht in mei 2021) of later, worden de volgende onderdelen dynamisch geïnstalleerd, maar alleen wanneer dit is vereist door een beschermingsschema:

- Agent voor URL-filtering: vereist om de functies van URL-filtering goed te laten werken.
- Agent voor antimalwarebeveiliging: vereist voor de werking van de functies voor antimalwarebeveiliging.
- Agent voor preventie van gegevensverlies: vereist voor de werking van de functies voor apparaatbeheer.

Deze onderdelen zijn standaard niet geïnstalleerd. Het betreffende onderdeel wordt automatisch geïnstalleerd als een workload wordt beschermd door een schema waarin een van de volgende modules is ingeschakeld:

- Antivirus- en antimalwarebeveiliging
- URL-filtering
- Apparaatbesturing

En als de functies voor antimalwarebeveiliging, URL-filtering of apparaatbeheer in geen enkel beveiligingsschema meer zijn vereist, wordt het betreffende onderdeel automatisch verwijderd.

Het dynamisch installeren of verwijderen van onderdelen duurt maximaal 10 minuten nadat u het beschermingsschema hebt gewijzigd. Als echter een van de volgende bewerkingen wordt uitgevoerd, zal de dynamische installatie of verwijdering starten nadat deze bewerking is voltooid:

- Back-up
- Herstel
- Back-upreplicatie
- Replicatie van virtuele machines
- Replica testen
- Een virtuele machine uitvoeren vanaf een back-up (inclusief voltooiing)
- Failover voor noodherstel
- Failback voor noodherstel
- Een script uitvoeren (voor Cyber Scripting-functionaliteit)
- Patchinstallatie
- Back-up van ESXi-configuratie

De vereiste systeemmachtigingen toekennen aan Connect Agent

Als u alle functies van de functionaliteit voor extern bureaublad wilt inschakelen voor macOS-workloads, moet u naast de machtiging voor volledige schijftoegang de volgende machtigingen toekennen aan Connect Agent:

- Schermopname: maakt schermopname van de macOS-workload mogelijk via NEAR. Totdat deze machtiging is verleend, worden alle verbindingen voor externe besturing geweigerd.
- Toegankelijkheid: maakt externe verbindingen in besturingsmodus mogelijk via NEAR

- Microfoon: maakt omleiding van geluid van de externe macOS-workload naar de lokale workload mogelijk via NEAR. Als u de functie voor het omleiden van geluid wilt inschakelen, moet een stuurprogramma voor het opnemen van geluid zijn geïnstalleerd voor de workload. Zie "Omleiding van extern geluid" (p. 1063) voor meer informatie.
- Automatisering: activeert de actie Prullenbak leegmaken

Nadat u de agent voor de macOS-workload hebt gestart, wordt gecontroleerd of de agent deze rechten heeft en wordt u eventueel gevraagd om de machtigingen te toe te kennen.

De machtiging voor schermopname toekennen:

1. Ga naar het dialoogvenster **Vereiste systeemmachtigingen toekennen** voor Cyber Protect-agent en klik op **Systeemmachtigingen instellen**.
2. Klik in het dialoogvenster **Systeemmachtigingen** op **Machtiging voor schermopname aanvragen**.
3. Klik op **Systeemvoorkeuren openen**.
4. Selecteer **Connect Agent**.

Als de agent geen machtiging heeft wanneer u op afstand toegang probeert te krijgen tot de workload, ziet u het dialoogvenster Machtiging voor schermopname aanvragen. Alleen de lokale gebruiker kan een antwoord geven in dit dialoogvenster.

De machtiging voor toegankelijkheid toekennen:

1. Ga naar het dialoogvenster **Vereiste systeemmachtigingen toekennen** voor Cyber Protect-agent en klik op **Systeemmachtigingen instellen**.
2. Klik in het dialoogvenster **Systeemmachtigingen** op **Machtiging voor toegankelijkheid aanvragen**.
3. Klik op **Systeemvoorkeuren openen**.
4. Klik op het slotpictogram in de linkerbenedenhoek van het venster zodat het verandert in een ontgrendeld slot. U wordt gevraagd om een beheerderswachtwoord om wijzigingen te kunnen aanbrengen.
5. Selecteer **Connect Agent**.

De machtiging voor microfoon toekennen:

1. Ga naar het dialoogvenster **Vereiste systeemmachtigingen toekennen** voor Connect Agent en klik op **Systeemmachtigingen instellen**.
2. Klik in het dialoogvenster **Systeemmachtigingen** op **Machtiging voor microfoon aanvragen**.
3. Klik op **OK**.

Opmerking
U moet ook een stuurprogramma voor het opnemen van geluid installeren voor de macOS-workload, zodat de agent de gegeven machtiging kan gebruiken om het geluid van de workload om te leiden. Zie "Omleiding van extern geluid" (p. 1063) voor meer informatie.

De machtiging voor automatisering toekennen:

1. Ga naar het dialoogvenster **Vereiste systeemmachtigingen toekennen** voor Connect Agent en klik op **Systeemmachtigingen instellen**.
2. Klik in het dialoogvenster **Systeemmachtigingen** op **Machtiging voor automatisering aanvragen**.

Beveiligingsagents installeren via de grafische gebruikersinterface

Beveiligingsagents installeren in Windows

Vereisten

Download de agent die u nodig hebt voor de workload die u wilt beschermen. Zie "Beveiligingsagents downloaden" (p. 70).

Agent voor Windows installeren

1. Zorg dat de machine verbinding heeft met internet.
2. Meld u aan als beheerder en start het installatieprogramma.
3. [Optioneel] Klik op **Installatie-instellingen aanpassen**. Hier kunt u indien gewenst de nodige wijzigingen aanbrengen voor de volgende gevallen:
   - De onderdelen wijzigen die moeten worden geïnstalleerd (bijvoorbeeld om de installatie van Cyber Protection Monitor of het opdrachtregelprogramma uit te schakelen, of om de Agent voor Antimalwarebeveliging of de Agent voor URL-filtering te installeren).

     Opmerking
     Voor de functie van antimalwarebeveiliging op Windows-machines is de installatie van Agent voor Antimalwarebeveiliging vereist, en voor de functie van URL-filtering is de installatie van Agent voor URL-filtering vereist. Deze agents worden automatisch geïnstalleerd voor beschermde workloads als de module **Antivirus- en Antimalwarebeveiliging** en/of **URL-filtering** is ingeschakeld in de betreffende beschermingsplannen.

   - Als u de methode voor registratie van de workload in de Cyber Protection-service wilt wijzigen. U kunt wisselen tussen **Serviceconsole gebruiken** (standaard) en **Referenties gebruiken** of **Registratietoken gebruiken**.
   - Als u het installatiepad wilt wijzigen.
   - Als u het gebruikersaccount wilt wijzigen waarvoor de agentservice wordt uitgevoerd. Zie "Het aanmeldingsaccount voor Windows-machines wijzigen" (p. 82) voor meer informatie.
   - Als u de hostnaam/het IP-adres, de poort of de referenties van de proxyserver wilt verifiëren of wijzigen. Als een proxyserver is ingeschakeld in Windows, wordt deze automatisch gedetecteerd en gebruikt.

4. Klik op **Installeren**.
5. [Alleen voor de installatie van Agent voor VMware] Geef het adres en de toegangsreferenties op voor vCenter Server of de standalone ESXi-host waarop u back-ups van virtuele machines wilt maken en virtuele machines wilt herstellen, en klik vervolgens op **Gereed**.

   We raden u aan een speciaal account te gebruiken voor toegang tot vCenter Server of de ESXi-host, in plaats van een bestaand account met de rol Beheerder. Voor meer informatie: zie "Vereiste bevoegdheden voor Agent voor VMware" (p. 735).
6. [Alleen voor installatie op een domeincontroller] Geef het gebruikersaccount op waarvoor de agentservice wordt uitgevoerd. Klik vervolgens op **Gereed**. Uit veiligheidsoverwegingen worden er niet automatisch nieuwe accounts op een domeincontroller gemaakt door het installatieprogramma.

   Opmerking
   Het gebruikersaccount dat u opgeeft, moet het recht `Aanmelden als service` hebben. U kunt de profielmap op die machine alleen maken als dit account al eerder is gebruikt op de domeincontroller.

   Zie dit Knowledge Base-artikel voor meer informatie over het installeren van de agent op een alleen-lezen domeincontroller.
7. Als u de standaardregistratiemethode **Serviceconsole gebruiken** hebt gekozen bij stap 3, wacht u tot het registratiescherm wordt weergegeven en gaat u verder met de volgende stap. In de andere gevallen hoeft u geen verdere actie te ondernemen.
8. Registreer de agent onder een klanttenantaccount. Voor meer informatie over registratie: zie "Workloads registreren via de grafische gebruikersinterface" (p. 124).
9. [Als de agent is geregistreerd onder een account met tenant in de compliancemodus] Stel het versleutelingswachtwoord in.

Het aanmeldingsaccount voor Windows-machines wijzigen

Geef op het scherm **Onderdelen selecteren** de optie **Aanmeldingsaccount voor de agentservice** op om het account te definiëren waarvoor de services worden uitgevoerd. U kunt een van de volgende opties selecteren:

- **Servicegebruikeraccounts gebruiken** (standaard voor de agentservice)

  Servicegebruikeraccounts zijn Windows-systeemaccounts die worden gebruikt om services uit te voeren. Het voordeel van deze instelling is dat de beleidsregels voor domeinbeveiliging geen invloed hebben op de gebruikersrechten van deze accounts. De agent wordt standaard uitgevoerd onder het **Lokale systeemaccount**.
- **Een nieuw account maken**

  De accountnaam is Agent User voor de agent.
- **Het volgende account gebruiken**

Als u de agent installeert op een domeincontroller, wordt u gevraagd om bestaande accounts (of hetzelfde account) op te geven voor de agent. Uit veiligheidsoverwegingen worden er niet automatisch nieuwe accounts op een domeincontroller.

Het gebruikersaccount dat u opgeeft wanneer het installatieprogramma op een domeincontroller wordt uitgevoerd, moet het recht `Aanmelden als service` hebben. U kunt de profielmap op die machine alleen maken als dit account al eerder is gebruikt op de domeincontroller.

Zie dit Knowledge Base-artikel voor meer informatie over het installeren van de agent op een alleen-lezen domeincontroller.

Als u de optie **Een nieuw account maken** of **Het volgende account gebruiken** kiest, controleert u of de beleidsregels voor domeinbeveiliging geen invloed hebben op de rechten van de gerelateerde accounts. Als een account niet beschikt over de gebruikersrechten die tijdens de installatie zijn toegewezen, werkt het onderdeel mogelijk niet goed of werkt het helemaal niet.

Rechten vereist voor het aanmeldingsaccount

Een beveiligingsagent wordt uitgevoerd als een Managed Machine Service (MMS) op een Windows-computer. Het account waarvoor de agent wordt uitgevoerd, moet specifieke rechten hebben om de agent correct te laten werken. Daarom moet de MMS-gebruiker de volgende rechten krijgen:

1. Moet zijn opgenomen in de groepen **Back-upoperators** en **Administrators**. Op een domeincontroller moet de gebruiker zijn opgenomen in de groep **Domeinadministrators**.
2. Moet de machtiging **Volledig beheer** hebben voor de map `%PROGRAMDATA%\Acronis` (in Windows XP en Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis`) en voor de bijbehorende submappen.
3. Moet de machtiging **Volledig beheer** hebben voor bepaalde registersleutels in de volgende sleutel: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Moet de volgende gebruikersrechten hebben:
   - Aanmelden als service
   - Geheugenquota voor een proces verhogen
   - Token op procesniveau vervangen
   - Omgevingswaarden in firmware wijzigen

Gebruikersrechten toewijzen

Volg de onderstaande instructies om de gebruikersrechten toe te wijzen (in dit voorbeeld wordt het gebruikersrecht **Aanmelden als service** gebruikt; dezelfde stappen zijn van toepassing voor andere gebruikersrechten):

1. Meld u aan bij de computer met een account met administratorbevoegdheden.
2. Open **Systeembeheer** in het **Configuratiescherm** (of klik op Win + R, typ **control admintools** en druk op Enter) en open **Lokaal beveiligingsbeleid**.
3. Vouw **Lokaal beleid** uit en klik op **Toewijzing van gebruikersrechten**.

4. Klik in het rechterdeelvenster met de rechtermuisknop op **Aanmelden als service** en selecteer **Eigenschappen**.
5. Klik op de knop **Gebruiker of groep toevoegen...** om een nieuwe gebruiker toe te voegen.
6. Zoek in het venster **Gebruikers, computers, serviceaccounts of groepen selecteren** de gebruiker die u wilt invoeren en klik op **OK**.
7. Klik op **OK** in de eigenschappen van **Aanmelden als service** om de wijzigingen op te slaan.

Belangrijk
Zorg ervoor dat de gebruiker die u hebt toegevoegd aan het gebruikersrecht **Aanmelden als service**, niet wordt vermeld in het beleid **Aanmelden als service weigeren** in **Lokaal beveiligingsbeleid**.

Let op: we raden u niet aan om aanmeldingsaccounts handmatig te wijzigen nadat de installatie is voltooid.

Beveiligingsagents installeren in Linux

Voorbereiding

- Download de gewenste agent op de machine die u wilt beschermen. Zie "Beveiligingsagents downloaden" (p. 70).
- Controleer of de nodige Linux-pakketten zijn geïnstalleerd op de machine.
- Bij de installatie van de agent in SUSE Linux moet u `su -` gebruiken in plaats van `sudo`. Anders treedt de volgende fout op wanneer u de agent probeert te registreren via de Cyber Protect-console: `Kan de webbrowser niet starten. Geen weergave beschikbaar.`
  Sommige Linux-distributies, zoals SUSE, geven de variabele DISPLAY niet door bij gebruik van sudo en het installatieprogramma kan de browser dan niet openen in de grafische gebruikersinterface (GUI).

Installatie

U hebt minimaal 2 GB vrije schijfruimte nodig om Agent voor Linux te installeren.

Agent voor Linux installeren

1. Zorg dat de machine verbinding heeft met internet.
2. Navigeer als rootgebruiker naar de directory met het installatiebestand, maak het bestand uitvoerbaar en voer het vervolgens uit.

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

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

Als een proxyserver is ingeschakeld in uw netwerk, geeft u bij het uitvoeren van het installatiebestand de hostnaam/het IP-adres en de poort van de server op in de volgende indeling: `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`.

Als u de standaardmethode voor registratie van de machine in de Cyber Protection-service wilt wijzigen, voert u het installatiebestand uit met een van de volgende parameters:

- `--register-with-credentials`: als u wilt dat er om een gebruikersnaam en wachtwoord wordt gevraagd tijdens de installatie
- `--token=STRING`: als u een registratietoken wilt gebruiken
- `--skip-registration`: als u de registratie wilt overslaan

3. Schakel de selectievakjes in voor de agenten die u wilt installeren. De volgende agenten zijn beschikbaar:
   - Agent voor Linux
   - Agent voor Virtuozzo
   - Agent voor Oracle
   - Agent voor MySQL/MariaDB

   Agent voor Virtuozzo, Agent voor Oracle en Agent voor MySQL/MariaDB werken alleen als ook Agent voor Linux (64-bits) is geïnstalleerd.
4. Als u de standaardregistratiemethode hebt gekozen bij stap 2, gaat u verder met de volgende stap. In de andere gevallen voert u de gebruikersnaam en het wachtwoord voor de Cyber Protection-service in of wacht u tot de machine wordt geregistreerd met behulp van het token.
5. Registreer de agent onder een klanttenantaccount. Voor meer informatie over registratie: zie "Workloads registreren via de grafische gebruikersinterface" (p. 124).
6. [Als de agent is geregistreerd onder een account met tenant in de compliancemodus] Stel het versleutelingswachtwoord in.
7. Als UEFI Secure Boot is ingeschakeld op de machine, krijgt u een melding dat u het systeem na de installatie opnieuw moet opstarten. Onthoud welk wachtwoord (dat van de rootgebruiker of 'acronis') moet worden gebruikt.

   Opmerking
   De installatie genereert een nieuwe sleutel die wordt gebruikt voor het ondertekenen van de kernelmodules. U moet deze nieuwe sleutel registreren in de lijst van Machine Owner Key (MOK) door de machine opnieuw op te starten. Als u de sleutel niet registreert, kan de agent niet werken. Als u UEFI Secure Boot inschakelt na installatie van de agent, moet u de agent opnieuw installeren.

8. Wanneer de installatie is voltooid, voert u een van de volgende handelingen uit:
   - Klik op **Opnieuw opstarten**, als hierom werd gevraagd bij de vorige stap.

Wanneer het systeem opnieuw wordt opgestart, kiest u MOK-beheer (Machine Owner Key) en **MOK registreren**. Registreer de sleutel vervolgens met het in de vorige stap aanbevolen wachtwoord.

- Klik anders op **Afsluiten**.

Informatie voor het oplossen van problemen vindt u in het volgende bestand:
`/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

Beveiligingsagents installeren in macOS

Vereisten

Download de agent die u nodig hebt voor de workload die u wilt beschermen. Zie "Beveiligingsagents downloaden" (p. 70).

Agent voor Mac (x64 of ARM64) installeren

1. Zorg dat de machine verbinding heeft met internet.
2. Dubbelklik op het installatiebestand (.dmg).
3. Wacht totdat het besturingssysteem de image van de installatieschijf heeft gekoppeld.
4. Dubbelklik op **Installeren**.
5. Als een proxyserver is ingeschakeld in uw netwerk, klikt u op **Beveiligingsagent** in de menubalk en op **Proxyserverinstellingen**. Vervolgens geeft u de hostnaam/het IP-adres, de poort en de referenties van de proxyserver op.
6. Geef desgevraagd de beheerdersreferenties op.
7. Klik op **Doorgaan**.
8. Wacht tot het registratiescherm wordt weergegeven.
9. Registreer de agent onder een klanttenantaccount. Voor meer informatie over registratie: zie "Workloads registreren via de grafische gebruikersinterface" (p. 124).
10. [Als de agent is geregistreerd onder een account met tenant in de compliancemodus] Stel het versleutelingswachtwoord in.
11. Als u macOS-versie Mojave 10.14.x of later gebruikt, moet u de beveiligingsagent volledige schijftoegang geven om back-upbewerkingen mogelijk te maken.
    Voor instructies raadpleegt u De machtiging 'Volledige schijftoegang' verlenen aan de Cyber Protection-agent (64657).
12. Als u de functionaliteit voor extern bureaublad wilt gebruiken, moet u de vereiste systeemmachtigingen toekennen aan Connect Agent. Zie "De vereiste systeemmachtigingen toekennen aan Connect Agent" (p. 79) voor meer informatie.

Agenten verwijderen

Wanneer u een agent verwijdert uit een workload, wordt de workload automatisch verwijderd uit de Cyber Protect-console. Als de workload nog steeds wordt weergegeven nadat u de agent hebt

verwijderd, bijvoorbeeld vanwege een netwerkprobleem, verwijdert u deze workload handmatig uit de console. Zie "Workloads verwijderen uit de Cyber Protect-console" (p. 323) voor meer informatie over hoe u dit kunt doen.

Opmerking
Als u een agent verwijdert, worden er geen plannen of back-ups verwijderd.

Een agent verwijderen

Windows

1. Meld u aan als beheerder op de machine met de agent.
2. Ga in **Configuratiescherm** naar **Programma's en onderdelen** (**Programma's toevoegen of verwijderen** in Windows XP).
3. Klik met de rechtermuisknop op **Acronis Cyber Protect** en selecteer vervolgens **Verwijderen**.
4. [Voor agents met wachtwoordbeveiliging] Geef het wachtwoord op dat nodig is om de agent te verwijderen en klik vervolgens op **Volgende**.
5. [Optioneel] Schakel het selectievakje **De logboeken en configuratie-instellingen verwijderen** in.
   Als u van plan bent de agent opnieuw te installeren, laat u dit selectievakje uitgeschakeld. Als u het selectievakje inschakelt en de agent vervolgens opnieuw installeert, wordt deze workload mogelijk gedupliceerd in de Cyber Protect-console en worden de oude back-ups mogelijk niet hieraan gekoppeld.
6. Klik op **Verwijderen**.

Linux

1. Ga naar de machine met de agent en voer `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` uit als rootgebruiker.
2. [Optioneel] Schakel het selectievakje **Alle producttraceringen opschonen (Logboeken, taken, kluizen en configuratie-instellingen van het product verwijderen)** in.
   Als u van plan bent de agent opnieuw te installeren, laat u dit selectievakje uitgeschakeld. Als u het selectievakje inschakelt en de agent vervolgens opnieuw installeert, wordt deze workload mogelijk gedupliceerd in de Cyber Protect-console en worden de oude back-ups mogelijk niet hieraan gekoppeld.
3. Bevestig uw beslissing.

macOS

1. Dubbelklik op de machine met de agent op het .dmg-installatiebestand.
2. Wacht totdat het besturingssysteem de image van de installatieschijf heeft gekoppeld.
3. Dubbelklik in de image op **Verwijderen**.
4. Geef desgevraagd de beheerdersreferenties op.
5. Bevestig uw beslissing.

Onderdelen verwijderen die zijn gebundeld met Agent voor Windows:

U kunt afzonderlijke onderdelen verwijderen die zijn gebundeld met Agent voor Windows, zoals Cyber Protect Monitor, Agent voor preventie van gegevensverlies of Bootable Media Builder, zonder dat u Agent voor Windows hoeft te verwijderen.

1. Meld u als beheerder aan op de machine met de agent.
2. Voer het installatieprogramma uit en klik vervolgens op **Geïnstalleerde onderdelen wijzigen**.
3. Schakel de selectievakjes uit naast de onderdelen die u wilt verwijderen en klik vervolgens op **Gereed**.

Agent voor VMware (Virtual Appliance) verwijderen:

1. Meld u via vSphere Client aan bij vCenter Server.
2. [Als de virtuele toepassing is ingeschakeld] Klik met de rechtermuisknop op de virtuele toepassing en klik vervolgens op **Aan/uit** > **Uitschakelen**. Bevestig uw beslissing.
3. [Als de virtuele toepassing een lokaal gekoppelde opslag op een virtuele schijf gebruikt en u gegevens op die schijf wilt bewaren] Verwijder de virtuele opslag uit de virtuele toepassing.
   a. Klik met de rechtermuisknop op de virtuele toepassing en klik op **Instellingen bewerken**.
   b. Selecteer de schijf met de opslag en klik op **Verwijderen**.
   c. Klik onder **Opties voor verwijderen** op **Verwijderen van virtuele machine**.
   d. Klik op **OK**.

   Het resultaat is dat de schijf in de gegevensopslag blijft. U kunt de schijf koppelen aan een andere virtuele toepassing.
4. Klik met de rechtermuisknop op de virtuele toepassing en klik vervolgens op **Verwijderen van schijf**. Bevestig uw beslissing.
5. [Optioneel] [Als u niet van plan bent deze toepassing opnieuw te gebruiken] Ga in de Cyber Protect-console naar **Back-upopslag** > **Locaties** en verwijder vervolgens de locatie die overeenkomt met de lokaal gekoppelde opslag.

Beveiligingsagents installeren en verwijderen via de opdrachtregelinterface

Beveiligingsagents installeren en verwijderen in Windows

In Windows kunt u een installatie zonder toezicht uitvoeren of een installatie verwijderen op de volgende manieren:

- Door het EXE-bestand van het installatieprogramma te gebruiken en de installatieparameters op de opdrachtregel op te geven.
- Door een MSI-bestand te gebruiken dat u uitpakt uit het installatieprogramma en de installatieparameters op te geven op een van de volgende manieren:

- In een MST-bestand
- Rechtstreeks op de opdrachtregel

Installatie zonder toezicht met een EXE-bestand en installatie verwijderen

Voor dit type installatie zonder toezicht downloadt u het installatieprogramma en start u het, met de vereiste installatieparameters, vanaf de opdrachtregel. Zie "Parameters voor installatie zonder toezicht (EXE)" (p. 91) voor meer informatie over de parameters die u kunt gebruiken.

U hoeft installatiepakketten, MSI- en MST-bestanden niet vooraf uit te pakken.

Agents en onderdelen installeren en verwijderen (EXE)

Als u een installatie zonder toezicht wilt uitvoeren met een EXE-bestand, voert u het installatieprogramma uit en geeft u de installatieparameters op de opdrachtregel op.

Als u het installatieprogramma wilt downloaden, klikt u in de Cyber Protect-console op het accountpictogram in de rechterbovenhoek en vervolgens op **Downloads**. De downloadlink is ook beschikbaar in het deelvenster **Apparaten toevoegen**.

Agents en onderdelen installeren

1. Start de opdrachtregelinterface als beheerder en navigeer vervolgens naar het EXE-bestand van het installatieprogramma.
2. Start het installatieprogramma en geef de installatieparameters op met de volgende opdracht:

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

   Gebruik spaties om de parameters van elkaar te scheiden en komma's zonder spaties om de waarden voor een parameter van elkaar te scheiden. Bijvoorbeeld:

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

   Zie "Parameters voor installatie zonder toezicht (EXE)" (p. 91) voor de beschikbare parameters en bijbehorende waarden.

Voorbeelden

- Agent voor Windows, Agent voor Antimalware, Agent voor URL-filtering, opdrachtregelprogramma en Cyber Protect Monitor installeren. De workload registreren in de Cyber Protection-service met behulp van een gebruikersnaam en wachtwoord.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,agentForAmp,commandLine,trayMonitor --install-
  ```

```
dir="C:\Program Files\BackupClient" --agent-account=system --reg-
address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
```

- Agent voor Windows, opdrachtregelprogramma en Cyber Protect Monitor installeren. Een nieuw aanmeldingsaccount maken voor de agentservice in Windows. De workload registreren in de Cyber Protection-service met behulp van een token.

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

- Agent voor Windows, opdrachtregelprogramma, Agent voor Oracle en Cyber Protect Monitor installeren. De machine registreren in de Cyber Protection-service met een gebruikersnaam en wachtwoord.

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

- Agent voor Windows, opdrachtregelprogramma en Cyber Protect Monitor installeren. De taal van de gebruikersinterface instellen op Duits. De machine registreren in de Cyber Protection-service met behulp van een token. Een HTTP-proxy instellen.

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

Een geïnstalleerd onderdeel verwijderen

1. Start de opdrachtregelinterface als beheerder en ga vervolgens naar `%ProgramFiles%\BackupClient\RemoteInstall`.
2. Voer de volgende opdracht uit:

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

   Zie "Parameters voor installatie zonder toezicht (EXE)" (p. 91) voor de beschikbare parameters en bijbehorende waarden.

Voorbeeld

- Cyber Protect Monitor verwijderen.

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

Een agent verwijderen

1. Start de opdrachtregelinterface als beheerder en ga vervolgens naar `%Program Files%\Common Files\Acronis\BackupAndRecovery`.
2. Voer de volgende opdracht uit:

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

   Zie "Parameters voor installatie zonder toezicht (EXE)" (p. 91) voor de beschikbare parameters en bijbehorende waarden.

Voorbeelden

- Agent voor Windows en alle bijbehorende onderdelen verwijderen. Hiermee worden alle logboeken, taken en configuratie-instellingen verwijderd.

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

- Een met een wachtwoord beveiligde Agent voor Windows en alle bijbehorende onderdelen verwijderen. Hiermee worden alle logboeken, taken en configuratie-instellingen verwijderd.

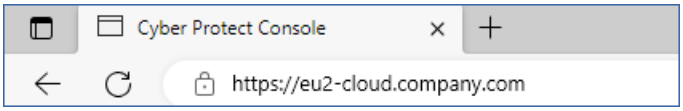
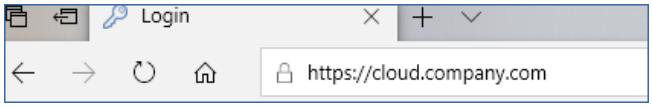
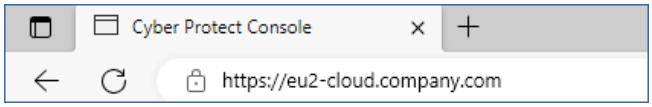
  ```
  C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --anti-tamper-password=<password> --quiet --delete-all-settings
  ```

Parameters voor installatie zonder toezicht (EXE)

De volgende tabel bevat een overzicht van de parameters voor een installatie zonder toezicht met een EXE-bestand.

Parameters	Beschrijving
Algemene parameters	
`--add-components=` <onderdeel1,onderdeel2,...,onderdeelN>	De onderdelen die worden geïnstalleerd: Zie "Onderdelen voor installatie zonder toezicht (EXE)" (p. 96) voor de volledige lijst met beschikbare onderdelen. Wanneer u meerdere onderdelen opgeeft, moet u ze van elkaar scheiden met komma's. Voeg geen spaties toe voor of na de komma. Als u onderdelen opgeeft die al zijn geïnstalleerd, worden deze onderdelen gerepareerd of bijgewerkt, afhankelijk van de versie van het installatieprogramma en de versie van de geïnstalleerde onderdelen. Als u deze parameter niet opgeeft, wordt een standaardset van onderdelen geïnstalleerd, afhankelijk van de machine waarop u de installatie uitvoert. Agent voor SQL wordt

Parameters	Beschrijving
	bijvoorbeeld alleen geïnstalleerd op machines met MS SQL Server.
`--install-dir=`<path>	De map waarin de geselecteerde onderdelen worden geïnstalleerd. Als de opgegeven map niet bestaat, wordt deze gemaakt. Als u deze parameter niet opgeeft, wordt een standaardmap gebruikt: `C:\Program Files\BackupClient`.
`--log-dir=`<pad>	De map waarin de installatielogboeken worden opgeslagen. Als u deze parameter niet opgeeft, wordt een standaardmap gebruikt: `%ProgramData%\ Acronis\ InstallationLogs`.
`--language=`<code>	De taal van het product. De volgende waarden zijn beschikbaar: en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Als u deze parameter niet opgeeft, wordt de systeemtaal gebruikt van de machine waarop u de installatie uitvoert (indien die taal hierboven wordt vermeld). In alle andere gevallen wordt de waarde ingesteld op en.
`--quiet`	Gebruik deze parameter om het installatieprogramma uit te voeren zonder de gebruikersinterface weer te geven. Gebruik deze niet in combinatie met de parameter `--register-only`.
`--help`	Gebruik deze parameter om een lijst te zien met alle beschikbare parameters die u op de opdrachtregel kunt gebruiken, samen met de bijbehorende beschrijvingen.
`--fss-onboarding-auto-start`	Gebruik deze parameter in combinatie met de parameter `--quiet` om na een installatie zonder toezicht de File Sync & Share-wizard voor onboarding weer te geven.
Registratieparameters	
`--registration=`{skip | by-credentials | by-token | device-flow}	Gebruik deze parameter om te kiezen hoe u de agent wilt registreren na de installatie. Als u de registratie wilt overslaan, geeft u `skip` op. U kunt de agent later registreren met behulp van de parameter `--register-only`. Als u de agent wilt registreren met behulp van referenties, geeft u `by-credentials` op en gebruikt u vervolgens de

Parameters	Beschrijving
	parameters `--reg-login` en `--reg-password`. U kunt ook alleen de parameters `--reg-login` en `--reg-password` gebruiken. De parameter `--registration=by-credentials` is dan optioneel. Als u de agent wilt registreren met een registratietoken, geeft u `by-token` op en vervolgens gebruikt de parameter `--reg-token`. U kunt ook alleen de parameter `--reg-token` gebruiken. De parameter `--registration=by-token` is dan optioneel. Als u de agent wilt registreren met behulp van het OAuth 2.0-protocol, geeft u `device-flow` op. Wanneer de installatie is voltooid, wordt de registratiepagina automatisch geopend. Wanneer u `--registration=device-flow` gebruikt, geeft u het exacte adres van het datacenter op als waarde voor de parameter `--reg-address`. Dit is de URL die u ziet **nadat u zich hebt aangemeld** bij de Cyber Protection-service. Bijvoorbeeld: `https://eu2-cloud.company.com`.  Gebruik `--registration=device-flow` niet samen met de parameter `--quiet`.
`--reg-address=<url>`	De URL van de Cyber Protection-service. U kunt deze parameter gebruiken met de parameters `--reg-login` en `--reg-password` of met de parameter `--reg-token`. • Wanneer u deze gebruikt met de parameters `--reg-login` en `--reg-password`, geeft u het adres op dat u gebruikt voor **aanmelding** bij de Cyber Protection-service. Bijvoorbeeld: `https://cloud.company.com`:  • Wanneer u deze gebruikt met de parameter `--reg-token`, geeft u het exacte adres van het datacenter op. Dit is de URL die u ziet **nadat u zich hebt aangemeld** bij de Cyber Protection-service. Bijvoorbeeld: `https://eu2-cloud.company.com`.  Gebruik niet `https://cloud.company.com` met de parameter `--reg-token`.

Parameters	Beschrijving
`--reg-login=`<gebruikersnaam> `--reg-password=`<wachtwoord>	De referenties voor het account waarvoor de agent wordt geregistreerd in de Cyber Protection-service. Dit mag niet het account van een partnerbeheerder zijn. Wanneer u deze parameters gebruikt, is de parameter `--registration` optioneel. Gebruik deze parameters niet samen met de parameter `--reg-token`.
`--reg-token=`<token>	Het registratietoken. Het registratietoken is een reeks van 12 tekens in drie segmenten, gescheiden door koppeltekens. Zie "Een registratietoken genereren" (p. 126) voor meer informatie over het genereren van een token. Wanneer u deze parameter gebruikt, is de parameter `--registration` optioneel. Gebruik deze parameter niet samen met de parameters `--reg-login` en `--reg-password`.
`--register-only`	Gebruik deze parameter om de installatie over te slaan en de agent te registreren met behulp van het OAuth 2.0-protocol (device-flow). Wanneer de installatie is voltooid, wordt de registratiepagina automatisch geopend. Gebruik `--register-only` niet samen met de parameter `--quiet`.
Aanmeldingsaccount voor de agentservice	
`--agent-account=`{system | new | custom} of `--agent-account-login=`<gebruikersnaam> `--agent-account-password=`<wachtwoord>	Gebruik deze parameter om het aanmeldingsaccount op te geven waarvoor u de agentservice wilt uitvoeren. Zie "Het aanmeldingsaccount voor Windows-machines wijzigen" (p. 82) voor meer informatie over het aanmeldingsaccount. Als u het account **Lokaal Systeem** wilt gebruiken, geeft u de parameter `--agent-account=system` op gebruikt u niet de parameter `'--agent-account` in u w opdracht. Als u de agentservice wilt uitvoeren voor een nieuw, automatisch gemaakt aanmeldingsaccount (**Acronis Agent User**), geeft u `new` op. Als u de agentservice wilt uitvoeren voor een bestaand account, geeft u de accountreferenties op met de parameters `--agent-account-login` en `--agent-account-password`. De parameter `--agent-account=custom` is dan

Parameters	Beschrijving
	optioneel.
vCenter/ESXi-parameters	
`--esxi-address=`<host>	De hostnaam of het IP-adres van vCenter Server of de ESXi-host. Gebruik deze parameter wanneer u Agent voor VMware installeert.
`--esxi-login=`<gebruikersnaam> `--esxi-password=`<wachtwoord>	De toegangsreferenties voor vCenter Server of de ESXi-host. Gebruik deze parameters wanneer u Agent voor VMware installeert.
Proxyparameters	
`--http-proxy=`{none | system | custom}	Gebruik deze parameter om de HTTP-proxyserver op te geven die u wilt gebruiken voor back-ups naar en herstel uit de cloudopslag. Als u de verbindingen met de proxyserver uitschakelt, geeft u `--http-proxy=none` op. Als u een proxyserver voor het hele systeem wilt gebruiken, geeft u `--http-proxy=system` op of gebruikt u niet de parameter `--http-proxy` in uw opdracht. Als u een andere proxyserver wilt gebruiken, geeft u het adres en de referenties van de proxyserver op met behulp van de parameters `--http-proxy-address`, `--http-proxy-login` en `--http-proxy-password`. De parameter `--http-proxy=custom` is dan optioneel.
`--http-proxy-address=`<host>:<poort>	De hostnaam of het IP-adres, en de poort van de aangepaste HTTP-proxyserver.
`--http-proxy-login=`<gebruikersnaam>	Gebruikersnaam voor de aangepaste HTTP-proxyserver.
`--http-proxy-password=`<wachtwoord>	Wachtwoord voor de aangepaste HTTP-proxyserver.
Parameters voor het verwijderen van de installatie	
`--remove-components=` <onderdeel1,onderdeel2,...,onderdeelN>	De onderdelen die worden verwijderd. Zie "Onderdelen voor installatie zonder toezicht (EXE)" (p. 96) voor de volledige lijst met beschikbare onderdelen. Wanneer u meerdere onderdelen opgeeft, moet u ze van elkaar scheiden met komma's. Voeg geen spaties toe voor of na de komma.

Parameters	Beschrijving
	Belangrijk Met deze parameter kunt u alleen onderdelen verwijderen. Als u het product volledig wilt verwijderen, gaat u naar het Configuratiescherm van Windows > Programma's en onderdelen, selecteert u het product en klikt u vervolgens op **Verwijderen**.
`--delete-all-settings`	Gebruik deze optionele parameter wanneer u de parameter `--remove-components` gebruikt om alle productlogboeken, taken en configuratie-instellingen te verwijderen.
`--anti-tamper-password=`<wachtwoord>	Het wachtwoord dat is vereist voor het verwijderen van een met een wachtwoord beveiligde Agent voor Windows of voor het wijzigen van de onderdelen ervan.

Onderdelen voor installatie zonder toezicht (EXE)

De onderstaande tabel bevat een overzicht van de onderdelen die u kunt gebruiken voor installatie zonder toezicht via een EXE-bestand. Gebruik de waardenamen om waarden op te geven voor de parameter `--add-components`.

Zie "Parameters voor installatie zonder toezicht (EXE)" (p. 91)"Parameters voor installatie zonder toezicht (MSI)" (p. 101) voor meer informatie

Waardenaam	Beschrijving van de onderdelen
`agentForWindows`	Agent voor Windows
`agentForSas`	Agent voor Files Sync & Share
`agentForAd`	Agent voor Active Directory
`agentForAmp`	Agent voor antimalwarebeveiliging en Agent voor URL-filtering
`agentForDlp`	Agent voor preventie van gegevensverlies
`agentForEsx`	Agent voor VMware (Windows)
`agentForExchange`	Agent voor Exchange
`agentForHyperV`	Agent voor Hyper-V
`agentForOffice365`	Agent voor Office 365
`agentForOracle`	Agent voor Oracle
`agentForSql`	Agent voor SQL
`commandLine`	Opdrachtregelprogramma

Waardenaam	Beschrijving van de onderdelen
`mediaBuilder`	Bootable Media Builder
`trayMonitor`	Cyber Protect Monitor
`all`	Deze waarde combineert alle onderdelen.
`allAgents`	Deze waarde combineert alle agents.

Installatie zonder toezicht met een MSI-bestand en installatie verwijderen

Gebruik voor dit type installatie zonder toezicht de Windows Installer (het programma `Msiexec`). Pak de installatiepakketten en het MSI-bestand vooraf uit met via de grafische gebruikersinterface van het installatieprogramma.

Wanneer u onderdelen met een MSI-bestand installeert, kunt u een MST-transformatiebestand gebruiken om de installatieparameters aan te passen. Zie "Agents en onderdelen installeren (combinatie van MSI en MST)" (p. 98) voor meer informatie over gebruik van een combinatie van MSI- en MST-bestanden. U kunt deze installatiemethode in een Active Directory-domein gebruiken om beveiligingsagents te installeren via Windows-groepsbeleid. Zie "Beveiligingsagents via Groepsbeleid implementeren" (p. 140) voor meer informatie.

U kunt installatieparameters ook handmatig opgeven op de opdrachtregel. In dit geval hebt u geen MST-bestand nodig. Zie "Voorbeelden" (p. 99) voor meer informatie.

De MSI-, MST- en CAB-bestanden uitpakken

Pak de MSI-, MST- en CAB-bestanden met de installatiepakketten uit via de grafische gebruikersinterface van het installatieprogramma.

De MSI-, MST- en CAB-bestanden uitpakken:

1. Voer de grafische interface van het installatieprogramma uit en klik vervolgens op **MST- en MSI-bestanden maken voor installatie zonder toezicht**.
2. Ga naar **Installatie-items**, selecteer de onderdelen die u wilt installeren en klik op **Gereed**.
   De installatiepakketten voor deze onderdelen worden als CAB-bestanden uitgepakt uit het installatieprogramma.
3. Selecteer in **Registratie-instellingen** de optie **Referenties gebruiken** of **Registratietoken gebruiken**. Geef de referenties of het registratietoken op (afhankelijk van de geselecteerde onderdelen) en klik vervolgens op **Gereed**.
   Zie "Een registratietoken genereren" (p. 126) voor meer informatie over het genereren van een registratietoken.
4. [Alleen bij installatie op een domeincontroller] Selecteer in **Aanmeldingsaccount voor de agentservice** de optie **Het volgende account gebruiken**. [Alleen voor installatie op een domeincontroller] Geef het gebruikersaccount op waarvoor de agentservice wordt uitgevoerd. Klik vervolgens op **Gereed**. Uit veiligheidsoverwegingen worden er niet automatisch nieuwe

accounts op een domeincontroller gemaakt door het installatieprogramma.

Opmerking
Het gebruikersaccount dat u opgeeft, moet het recht `Aanmelden als service` hebben. U kunt de profielmap op die machine alleen maken als dit account al eerder is gebruikt op de domeincontroller.

Zie dit Knowledge Base-artikel voor meer informatie over het installeren van de agent op een alleen-lezen domeincontroller.

5. Controleer of wijzig de installatie-instellingen die aan het MST-bestand worden toegevoegd en klik vervolgens op **Doorgaan**.
6. Selecteer de map waarin de MSI-, MST- en CAB-bestanden worden uitgepakt en klik vervolgens op **Genereren**.

Agents en onderdelen installeren (combinatie van MSI en MST)

Gebruik het MST-bestand om de installatie-instelling voor het MSI-bestand aan te passen. Gebruik de combinatie van MSI en MST wanneer u agents op meerdere machines installeert via een Windows-groepsbeleid. Zie "Beveiligingsagents via Groepsbeleid implementeren" (p. 140) voor meer informatie.

Onderdelen met MSI- en MST-bestanden installeren:

1. Pak de MSI- en MST-bestanden uit zoals beschreven in "De MSI-, MST- en CAB-bestanden uitpakken" (p. 97).
2. Voer de volgende opdracht uit op de opdrachtregelinterface van de machine waarop u onderdelen wilt installeren:

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

Bijvoorbeeld:

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

Agents en onderdelen installeren en verwijderen (MSI en rechtstreekse selectie)

Voer het MSI-bestand uit, selecteer handmatig de onderdelen die u wilt installeren en voer de gewenste installatieparameters in op de opdrachtregel. In dit geval hebt u het MST-bestand niet nodig.

Agents en onderdelen installeren

1. Pak het MSI-bestand en de installatiepakketten (CAB-bestanden) uit zoals beschreven in "De MSI-, MST- en CAB-bestanden uitpakken" (p. 97).

   Voor deze installatiemethode hebt u alleen de MSI- en CAB-bestanden nodig. Het MST-bestand is niet nodig.
2. Voer op de opdrachtregelinterface van de machine de volgende opdracht uit:

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

Gebruik spaties om de parameters van elkaar te scheiden en komma's zonder spaties om de waarden voor een parameter van elkaar te scheiden. Bijvoorbeeld:

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

Zie "Parameters voor installatie zonder toezicht (MSI)" (p. 101) voor de beschikbare parameters en bijbehorende waarden.

Voorbeelden

- Agent voor Windows, Agent voor Antimalware, Agent voor URL-filtering, opdrachtregelprogramma en Cyber Protect Monitor installeren. De workload registreren in de Cyber Protection-service met behulp van een gebruikersnaam en wachtwoord.

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

- Agent voor Windows, opdrachtregelprogramma en Cyber Protect Monitor installeren. Een nieuw aanmeldingsaccount maken voor de agentservice in Windows. De workload registreren in de Cyber Protection-service met behulp van een 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
  ```

- Agent voor Windows, opdrachtregelprogramma, Agent voor Oracle en Cyber Protect Monitor installeren. De machine registreren in de Cyber Protection-service met behulp van een gebruikersnaam en gecodeerd met een base64-wachtwoord. Mogelijk moet u uw wachtwoord coderen als het speciale tekens of spaties bevat. Zie "Wachtwoorden met speciale tekens of spaties gebruiken" (p. 130) voor meer informatie over het coderen van een wachtwoord.

  ```
  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==
  ```

- Agent voor Windows, opdrachtregelprogramma en Cyber Protect Monitor installeren. De machine registreren in de Cyber Protection-service met behulp van een token. Een HTTP-proxy

instellen.

```
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
```

Een geïnstalleerd onderdeel verwijderen

1. Pak het MSI-bestand en de installatiepakketten (CAB-bestanden) uit zoals beschreven in "De MSI-, MST- en CAB-bestanden uitpakken" (p. 97).

   Voor deze installatiemethode hebt u alleen de MSI- en CAB-bestanden nodig. Het MST-bestand is niet nodig.
2. Voer op de opdrachtregelinterface van de machine de volgende opdracht uit:

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

   Zie "Parameters voor installatie zonder toezicht (MSI)" (p. 101) voor de beschikbare parameters en bijbehorende waarden.

Voorbeeld

- Cyber Protect Monitor verwijderen.

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

Een agent verwijderen

1. Pak het MSI-bestand en de installatiepakketten (CAB-bestanden) uit zoals beschreven in "De MSI-, MST- en CAB-bestanden uitpakken" (p. 97).

   Voor deze installatiemethode hebt u alleen de MSI- en CAB-bestanden nodig. Het MST-bestand is niet nodig.
2. Voer op de opdrachtregelinterface van de machine de volgende opdracht uit:

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

   Zie "Parameters voor installatie zonder toezicht (MSI)" (p. 101) voor de beschikbare parameters en bijbehorende waarden.

Voorbeelden

- Agent voor Windows en alle bijbehorende onderdelen verwijderen. Hiermee worden alle logboeken, taken en configuratie-instellingen verwijderd.

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

- Een met een wachtwoord beveiligde Agent voor Windows en alle bijbehorende onderdelen verwijderen. Hiermee worden alle logboeken, taken en configuratie-instellingen verwijderd.

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

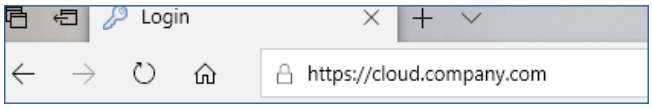
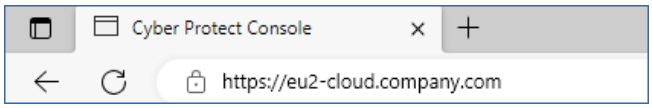
Parameters voor installatie zonder toezicht (MSI)

De volgende tabel bevat een overzicht van de parameters voor installatie zonder toezicht wanneer u een MSI-bestand gebruikt.

U kunt ook nog andere `msiexec`-parameters gebruiken. Gebruik bijvoorbeeld `/qn` om te voorkomen dat GUI-elementen worden weergegeven. Voor meer informatie over de `msiexec`-parameters raadpleegt u de Microsoft-documentatie.

Parameters	Beschrijving
Algemene parameters	
`ADDLOCAL=` <onderdeel1,onderdeel2,...,onderdeelN>	De onderdelen die worden geïnstalleerd: Zie "Onderdelen voor installatie zonder toezicht (MSI)" (p. 105) voor de volledige lijst met beschikbare onderdelen. Wanneer u meerdere onderdelen opgeeft, moet u ze van elkaar scheiden met komma's. Voeg geen spaties toe voor of na de komma. **Opmerking** U moet de installatiebestanden uitpakken voor alle onderdelen die u wilt installeren. Zie "De MSI-, MST- en CAB-bestanden uitpakken" (p. 97) voor meer informatie over het uitpakken.
`TARGETDIR=`<path>	De map waarin de geselecteerde onderdelen worden geïnstalleerd. Als de opgegeven map niet bestaat, wordt deze gemaakt. Als u deze parameter niet opgeeft, wordt een standaardmap gebruikt: `C:\Program Files\BackupClient`.
`REBOOT=ReallySuppress`	Geef deze parameter op als u onderdelen wilt installeren zonder de machine opnieuw op te starten.
`/l*v` <logbestand>	Geef deze parameter op om een uitgebreid logboek op te slaan. Dit logboek is nodig als u installatieproblemen wilt onderzoeken.

Parameters	Beschrijving
CURRENT_LANGUAGE=<taal-id>	De taal van het product. De volgende waarden zijn beschikbaar: en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Als u deze parameter niet opgeeft, wordt de systeemtaal gebruikt van de machine waarop u de installatie uitvoert (indien die taal hierboven wordt vermeld). In alle andere gevallen wordt de waarde ingesteld op en.
SKIP_SHA2_KB_CHECK={0,1}	Gebruik deze parameter om aan te geven of u wilt controleren of de update voor ondersteuning van handtekening bij SHA2-programmacode van Microsoft (KB4474419) is geïnstalleerd op de machine. De controle wordt alleen uitgevoerd op besturingssystemen waarvoor deze update is vereist. Zie "Ondersteunde besturingssystemen en omgevingen" (p. 23) om te controleren of deze is vereist voor uw besturingssysteem. Gebruik deze parameter met de waarde ingesteld op 1 als u de controle wilt overslaan. Als u de parameter niet opgeeft of de waarde ervan niet instelt op 0, en de update voor ondersteuning van handtekening bij SHA2-programmacode niet is gevonden op de machine, mislukt de installatie.
FSS_ONBOARDING_AUTO_START={0,1}	Gebruik deze parameter met de waarde ingesteld op 1 om de File Sync & Share-wizard voor onboarding weer te geven na een installatie zonder toezicht. Als u deze parameter niet opgeeft of de waarde ervan niet instelt op 0, wordt de wizard voor onboarding niet weergegeven.
Registratieparameters	
REGISTRATION_ADDRESS	De URL van de Cyber Protection-service. U kunt deze parameter gebruiken met de parameters REGISTRATION_LOGIN en REGISTRATION_PASSWORD of met de parameter REGISTRATION_TOKEN. • Wanneer u deze gebruikt met de parameters REGISTRATION_LOGIN en REGISTRATION_PASSWORD, moet u het adres opgeven dat u gebruikt voor **aanmelding** bij de Cyber Protection-service. Bijvoorbeeld: https://cloud.company.com:

Parameters	Beschrijving
	 • Wanneer u deze gebruikt met de parameter `REGISTRATION_TOKEN`, geeft u het exacte adres van het datacenter op. Dit is de URL die u ziet **nadat u zich hebt aangemeld** bij de Cyber Protection-service. Bijvoorbeeld: `https://eu2-cloud.company.com`.  Gebruik `https://cloud.company.com` niet samen met de parameter `REGISTRATION_TOKEN`.

`REGISTRATION_LOGIN`
 	
`REGISTRATION_PASSWORD`
	De referenties voor het account waarvoor de agent wordt geregistreerd in de Cyber Protection-service. Dit mag niet het account van een partnerbeheerder zijn.
	
	Gebruik deze parameters niet met de parameter `REGISTRATION_TOKEN`.

`REGISTRATION_PASSWORD_ENCODED`	Het wachtwoord voor het account waarvoor de agent wordt geregistreerd in de Cyber Protection-service, gecodeerd met base64. Zie "Wachtwoorden met speciale tekens of spaties gebruiken" (p. 130) voor meer informatie over codering van uw wachtwoord.
`REGISTRATION_TOKEN`	Het registratietoken. Het registratietoken is een reeks van 12 tekens in drie segmenten, gescheiden door koppeltekens. Zie "Een registratietoken genereren" (p. 126) voor meer informatie over het genereren van een token. U kunt deze parameter gebruiken met de parameters `REGISTRATION_LOGIN` en `REGISTRATION_PASSWORD`.
`REGISTRATION_REQUIRED={0,1}`	Gebruik deze parameter om te kiezen wat er gebeurt als de registratie mislukt. Als u de waarde instelt op `1`, mislukt de installatie ook. Als u de waarde instelt op `0` of de parameter niet opgeeft, wordt de installatie voltooid, zelfs als de registratie is mislukt.
Aanmeldingsaccount voor de agentservice	
`MMS_USE_SYSTEM_ACCOUNT={0,1}`	Gebruik deze parameter met de waarde `1` als u de service wilt uitvoeren voor het aanmeldingsaccount **Lokaal systeem**.

Parameters	Beschrijving
	Zie "Het aanmeldingsaccount voor Windows-machines wijzigen" (p. 82) voor meer informatie over het aanmeldingsaccount.
MMS_CREATE_NEW_ACCOUNT={0,1}	Gebruik deze parameter met de waarde 1 als u de agentservice wilt uitvoeren voor een nieuw, automatisch gemaakt aanmeldingsaccount (**Acronis Agent User**).
MMS_SERVICE_USERNAME=<gebruikersnaam> MMS_SERVICE_PASSWORD=<wachtwoord>	Gebruik deze parameters om een bestaand aanmeldingsaccount op te geven waarvoor de agent wordt uitgevoerd.
vCenter/ESXi-parameters	
SET_ESX_SERVER={0,1}	Gebruik deze parameter wanneer u Agent voor VMware installeert. Als de waarde 0 is, heeft de Agent voor VMware geen verbinding met vCenter-server of een ESXi-host. Als de waarde 1 is, geeft u de volgende parameters op: ESX_HOST, EXI_USER, ESX_PASSWORD.
ESX_HOST=<host name>	De hostnaam of het IP-adres van vCenter Server of de ESXi-host.
ESX_USER=<user name> ESX_PASSWORD=<password>	De toegangsreferenties voor vCenter Server of de ESXi-host.
Proxyparameters	
HTTP_PROXY_ADDRESS=<IP-adres> HTTP_PROXY_PORT=<poort>	Gebruik deze parameters om de HTTP-proxyserver op te geven die door de agent zal worden gebruikt. Als u geen proxyserver gebruikt, moet u deze parameters niet opgeven.
HTTP_PROXY_LOGIN=<login> HTTP_PROXY_PASSWORD=<password>	De referenties voor de HTTP-proxyserver. Gebruik deze parameters als de proxyserver verificatie vereist.
Parameters voor het verwijderen van de installatie	
REMOVE={<list of components>|ALL}	De onderdelen die worden verwijderd. Wanneer u meerdere onderdelen opgeeft, moet u ze van elkaar scheiden met komma's. Voeg geen spaties toe voor of na de komma. Als u alle onderdelen van het product wilt verwijderen, stelt

Parameters	Beschrijving
	u de waarde in op ALL.
DELETE_ALL_SETTINGS={0, 1}	Als u alle productlogboeken, taken en configuratie-instellingen wilt verwijderen, stelt u de waarde in op 1. Gebruik deze optionele parameter wanneer u de parameter REMOVE gebruikt.
ANTI_TAMPER_PASSWORD=<password>	Het wachtwoord dat is vereist voor het verwijderen van een met een wachtwoord beveiligde Agent voor Windows of voor het wijzigen van de onderdelen ervan.

Onderdelen voor installatie zonder toezicht (MSI)

De onderstaande tabel bevat een overzicht van de onderdelen die u kunt gebruiken voor installatie zonder toezicht via een MSI-bestand. Gebruik de waardenamen om waarden op te geven voor de parameter ADDLOCAL. Zie "Parameters voor installatie zonder toezicht (MSI)" (p. 101) voor meer informatie.

Waardenaam	Beschrijving van de onderdelen	Moet worden geïnstalleerd in combinatie met	Bits
AgentFeature	Kernonderdelen voor agenten		32-bits/64-bits
MmsMspComponents	Kernonderdelen voor back-up	AgentFeature	32-bits/64-bits
BackupAndRecoveryAgent	Agent voor Windows	MmsMspComponents	32-bits/64-bits
AmpAgentFeature	Agent for Antimalware protection	BackupAndRecoveryAgent	32-bits/64-bits
UrlFilteringAgentFeature	Agent for URL Filtering	BackupAndRecoveryAgent	32-bits/64-bits
DlpAgentFeature	Agent voor preventie van gegevensverlies	BackupAndRecoveryAgent	32-bits/64-bits
SasAgentFeature	Agent voor File Sync & Share	TrayMonitor	32-bits/64-

			bits
ArxAgentFeature	Agent voor Exchange	MmsMspComponents	32-bits/64-bits
ArsAgentFeature	Agent voor SQL	BackupAndRecoveryAgent	32-bits/64-bits
ARADAgentFeature	Agent voor Active Directory	BackupAndRecoveryAgent	32-bits/64-bits
ArxOnlineAgentFeature	Agent voor Microsoft 365	MmsMspComponents	32-bits/64-bits
OracleAgentFeature	Agent voor Oracle	BackupAndRecoveryAgent	32-bits/64-bits
AcronisESXSupport	Agent voor VMware ESX (i) (Windows)	BackupAndRecoveryAgent	64 bits
HyperVAgent	Agent voor Hyper-V	BackupAndRecoveryAgent	32-bits/64-bits
CommandLineTool	Opdrachtregelprogramma		32-bits/64-bits
TrayMonitor	Cyber Protect Monitor	AgentFeature	32-bits/64-bits
BackupAndRecoveryBootableComponents	Bootable Media Builder		32-bits/64-bits

Beveiligingsagents installeren en verwijderen in Linux

In dit gedeelte wordt beschreven hoe u beveiligingsagenten in de modus zonder toezicht op een machine met Linux kunt installeren of verwijderen via de opdrachtregel.

Een agent installeren:

1. Open Terminal.

2. Voer een van de volgende handelingen uit:

- Voer de volgende opdracht uit om de installatie te starten met behulp van parameters op de opdrachtregel:

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

  Definities: `<package name>` is de naam van het installatiepakket (een bestand met de extensie .i686 of .x86_64). Alle beschikbare parameters en bijbehorende waarden worden beschreven in "Parameters voor installatie zonder toezicht of installatie verwijderen" (p. 108).
- Voer de volgende opdracht uit om de installatie te starten met parameters die zijn opgegeven in een afzonderlijk tekstbestand:

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

  Deze aanpak kan handig zijn als u geen gevoelige informatie op de opdrachtregel wilt invoeren. In dit geval kunt u de configuratie-instellingen opgeven in een afzonderlijk tekstbestand en ervoor zorgen dat alleen u hiertoe toegang hebt. U moet elke parameter op een nieuwe regel plaatsen, gevolgd door de gewenste waarde, bijvoorbeeld:

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

  of

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

  Als dezelfde parameter zowel op de opdrachtregel als in het tekstbestand is opgegeven, wordt eerst de waarde van de opdrachtregel weergegeven.

3. Als UEFI Secure Boot is ingeschakeld op de machine, krijgt u een melding dat u het systeem na de installatie opnieuw moet opstarten. Onthoud welk wachtwoord (dat van de rootgebruiker of 'acronis') moet worden gebruikt. Wanneer het systeem opnieuw wordt opgestart, kiest u MOK-beheer (Machine Owner Key) en **MOK registreren**. Registreer de sleutel vervolgens met het aanbevolen wachtwoord.

Als u UEFI Secure Boot inschakelt na de installatie van de agent, herhaalt u de installatie, inclusief stap 3. Zo niet, dan zullen nieuwe back-ups mislukken.

Een agent verwijderen

1. Open Terminal.
2. Voer een van de volgende handelingen uit:
   - Als u de agent en alle logboeken, taken en configuratie-instellingen wilt verwijderen, voert u de volgende opdracht uit:

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

   - Als u de agent wilt verwijderen, maar de id wilt behouden (bijvoorbeeld als u van plan bent de agent later te installeren), voert u de volgende opdracht uit:

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

   - Als u de agent wilt verwijderen met behulp van het installatiebestand, voert u de volgende opdracht uit:

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

     Definities: `<package name>` is de naam van het installatiepakket (een bestand met de extensie .i686 of .x86_64). Alle beschikbare parameters en bijbehorende waarden worden beschreven in "Parameters voor installatie zonder toezicht of installatie verwijderen" (p. 108).

     Opmerking
     Gebruik deze opdracht alleen wanneer het installatiepakket dezelfde versie is als de geïnstalleerde agent en als `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstal` beschadigd of niet toegankelijk is.

Parameters voor installatie zonder toezicht of installatie verwijderen

In dit gedeelte worden de parameters beschreven voor een installatie zonder toezicht of het verwijderen van de installatie in Linux.

De configuratie voor installatie zonder toezicht moet ten minste `-a` en registratieparameters bevatten (bijvoorbeeld de parameters `--login` en `--password` of de parameters `--rain` en `--token`). U kunt meer parameters gebruiken om uw installatie aan te passen.

Installatieparameters

Basisparameters

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

De onderdelen die worden geïnstalleerd, worden gescheiden door komma's zonder spaties. De volgende onderdelen zijn beschikbaar in het .x86_64-installatiepakket:

Onderdeel	Beschrijving van de onderdelen
BackupAndRecoveryAgent	Agent voor Linux

AgentForPCS	Agent voor Virtuozzo
OracleAgentFeature	Agent voor Oracle
MySQLAgentFeature	Agent voor MySQL/MariaDB

Zonder deze parameter worden alle hier genoemde onderdelen geïnstalleerd.

Agent voor Virtuozzo, Agent voor Oracle en Agent voor MySQL/MariaDB werken alleen als ook Agent voor Linux is geïnstalleerd.

Het .i686-installatiepakket bevat alleen BackupAndRecoveryAgent.

`{-a|--auto}`

Het installatie- en registratieproces wordt voltooid zonder verdere gebruikersinteractie. Wanneer u deze parameter gebruikt, moet u het account opgeven waarvoor de agent wordt geregistreerd in de Cyber Protection-service. Hiervoor gebruikt u de parameter `--token` of de parameters `--login` en `--password`.

`{-t|--strict}`

Als de parameter is opgegeven, resulteert elke waarschuwing tijdens de installatie in een installatiefout. Zonder deze parameter wordt de installatie uitgevoerd, zelfs als er waarschuwingen zijn.

`{-n|--nodeps}`

De afwezigheid van vereiste Linux-pakketten wordt genegeerd tijdens de installatie.

`{-d|--debug}`

Hiermee wordt het installatielogboek weergegeven in de uitgebreide modus.

`--options-file=<locatie>`

De installatieparameters worden gelezen uit een tekstbestand in plaats van de opdrachtregel.

`--language=<taal-id>`

De taal van het product. Beschikbare waarden zijn als volgt: `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`.
Als deze parameter niet is opgegeven, wordt de taal van het product bepaald door uw systeemtaal, op voorwaarde dat deze in de bovenstaande lijst staat. Anders wordt de taal van het product ingesteld op Engels (`en`).

Registratieparameters

Geef een van de volgende parameters op:

- `{-g|--login=}<gebruikersnaam>` en `{-w|--password=}<wachtwoord>`

Referenties voor het account waarvoor de agent wordt geregistreerd in de Cyber Protection-service. Dit mag niet het account van een partnerbeheerder zijn.

- `--token=<token>`

  Het registratietoken is een reeks van 12 tekens in drie segmenten, gescheiden door koppeltekens. U kunt er een genereren in de Cyber Protect-console, zoals beschreven in "Beveiligingsagents via Groepsbeleid implementeren" (p. 140).

  U kunt de parameter `--token` niet samen met de parameters `--login`, `--password` en `--register-with-credentials` gebruiken.

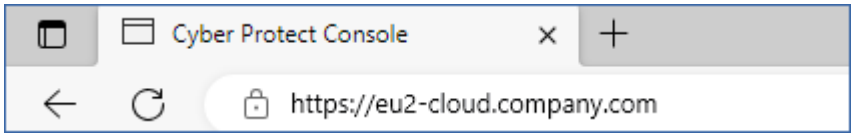
  - `{-C|--rain=}<serviceadres>`

    De URL van de Cyber Protection-service.

    U hoeft deze parameter niet expliciet op te nemen wanneer u de parameters `--login` en `--password` gebruikt voor registratie, omdat het installatieprogramma standaard het juiste adres gebruikt: dit is het adres dat u gebruikt voor **aanmelding** bij de Cyber Protection-service. Bijvoorbeeld:

    Maar wanneer u `{-C|--rain=}` gebruikt met de parameter `--token`, moet u het exacte adres van het datacentrum opgeven. Dit is de URL die u ziet **zodra u bent aangemeld** bij de Cyber Protection-service. Bijvoorbeeld:

- `--register-with-credentials`

Als deze parameter is opgegeven, wordt de grafische interface van het installatieprogramma gestart. Als u de registratie wilt voltooien, voert u de gebruikersnaam en het wachtwoord in voor het account waarvoor de agent wordt geregistreerd in de Cyber Protection-service. Dit mag niet het account van een partnerbeheerder zijn.

- `--skip-registration`

Gebruik deze parameter als u de agent wilt installeren, maar van plan bent om deze later te registreren in de Cyber Protection-service. Voor meer informatie over hoe dit te doen: zie "Workloads registreren en de registratie van workloads ongedaan maken via de opdrachtregelinterface" (p. 129).

Aanvullende parameters

`--http-proxy-host=<IP-adres>` en `--http-proxy-port=<poort>`

De HTTP-proxyserver die door de agent wordt gebruikt voor back-up en herstel vanuit de cloud en voor het maken van verbinding met de beheerserver. Zonder deze parameters wordt geen proxyserver gebruikt.

`--http-proxy-login=<gebruikersnaam>` en `--http-proxy-password=<wachtwoord>`

De referenties voor de HTTP-proxyserver. Gebruik deze parameters als de server authenticatie vereist.

`--tmp-dir=<locatie>`

Hiermee wordt aangegeven in welke map de tijdelijke bestanden worden opgeslagen tijdens de installatie. De standaardmap is **/var/tmp**.

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

Tijdens de installatie worden herdistribueerbare bibliotheken gebruikt, zelfs als ze al aanwezig zijn op uw systeem.

`--skip-prereq-check`

Er wordt niet gecontroleerd of de nodige pakketten voor het compileren van de snapapi-module al zijn geïnstalleerd.

`--force-weak-snapapi`

Er wordt geen snapapi-module gecompileerd door het installatieprogramma. In plaats daarvan wordt een kant-en-klare module gebruikt die mogelijk niet exact overeenkomt met de Linux-kernel. We raden af om deze optie te gebruiken.

`--skip-svc-start`

De services starten niet automatisch na de installatie. Meestal wordt deze parameter gebruikt in combinatie met `--skip-registration`.

Informatieparameters

`{-?|--help}`

Geeft de beschrijving van de parameters weer.

`--usage`

Geeft een korte beschrijving weer van de manier waarop de opdracht wordt gebruikt.

`{-v|--version}`

Geeft de versie van het installatiepakket weer.

`--product-info`

Geeft de productnaam en de versie van het installatiepakket weer.

`--snapapi-list`

Geeft de beschikbare kant-en-klare snapapi-modules weer.

`--components-list`

Geeft de installatieonderdelen weer.

Parameters voor verouderde functies

Deze parameters hebben betrekking op een verouderd onderdeel, namelijk agent.exe.

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

Geeft het pad naar een aangepast certificaatbestand voor SSL-communicatie weer.

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

Geeft de poort weer waarop agent.exe luistert naar verbindingen. De standaardpoort is 9876.

Parameters voor het verwijderen van de installatie

`{-u|--uninstall}`

Hiermee wordt het product verwijderd.

`--purge`

Hiermee wordt het product met de bijbehorende logboeken, taken en configuratie-instellingen verwijderd. U hoeft de parameter `--uninstall` niet expliciet op te geven wanneer u `--purge` gebruikt.

Voorbeelden

- Agent voor Linux installeren zonder deze te registreren.

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

- Agent voor Linux, Agent voor Virtuozzo en Agent voor Oracle installeren en deze registreren met referenties.

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

- Agent voor Oracle en Agent voor Linux installeren en deze registreren met een registratietoken.

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

- Agent voor Linux, Agent voor Virtuozzo en Agent voor Oracle installeren met configuratie-instellingen in een apart tekstbestand.

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

- Agent voor Linux, Agent voor Virtuozzo en Agent voor Oracle verwijderen en alle bijbehorende

logboeken, taken en configuratie-instellingen verwijderen.

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

Beveiligingsagents installeren en verwijderen in macOS

In dit gedeelte wordt beschreven hoe u de beveiligingsagent in de modus zonder toezicht op een machine met macOS kunt installeren en verwijderen via de opdrachtregel.

Vereiste machtigingen

Voordat u een installatie zonder toezicht start voor een Mac-workload, moet u het besturingselement voor het privacyvoorkeurenbeleid aanpassen om app-toegang en kernel- en systeemextensies in het macOS van de workload toe te staan en de installatie van de Cyber Protection-agent mogelijk te maken. Zie "Vereiste machtigingen voor installatie zonder toezicht in macOS" (p. 115).

Nadat u de PPPC-payload hebt geïmplementeerd, kunt u doorgaan met de onderstaande procedures.

Kan het installatiebestand niet downloaden (.dmg)

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op **Toevoegen** en klik vervolgens op **Mac**.

Een agent installeren:

1. Open Terminal.
2. Maak een tijdelijke directory waaraan u het installatiebestand (.dmg) koppelt.

   ```
   mkdir <dmg_root>
   ```

   Voor `<dmg_root>` kunt een naam naar eigen keuze opgeven.
3. Koppel het .dmg-bestand.

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

   `<dmg_file>` is de naam van het installatiebestand. Bijvoorbeeld: **Cyber_Protection_Agent_for_MAC_x64.dmg**.
4. Voer het installatieprogramma uit.
   - Als u een volledig installatieprogramma voor Mac gebruikt, zoals `CyberProtect_AgentForMac_x64.dmg` of `CyberProtect_AgentForMac_arm64.dmg`, voert u de volgende opdracht uit.

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

Opmerking
Als u automatische onboarding wilt inschakelen voor File Sync & Share, voert u in plaats daarvan de volgende opdracht uit. Bij deze optie wordt u om het beheerderswachtwoord gevraagd.

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

- Als u een universeel installatieprogramma voor Mac gebruikt, zoals `CyberProtect_AgentForMac_web.dmg`, voert u de volgende opdracht uit.

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

5. Ontkoppel het installatiebestand (.dmg).

```
hdiutil detach <dmg_root>
```

Voorbeeld

```
mkdir mydirectory
```

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

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

```
hdiutil detach mydirectory
```

Een agent verwijderen

1. Open Terminal.
2. Voer een van de volgende handelingen uit:
   - Als u de agent wilt verwijderen, voert u de volgende opdracht uit:

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

   - Als u de agent en alle logboeken, taken en configuratie-instellingen wilt verwijderen, voert u de volgende opdracht uit:

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

Vereiste machtigingen voor installatie zonder toezicht in macOS

Voordat u een installatie zonder toezicht start voor een Mac-workload, moet u het besturingselement voor het privacyvoorkeurenbeleid aanpassen om app-toegang en kernel- en systeemextensies in het macOS van de workload toe te staan en de installatie van de Cyber Protection-agent mogelijk te maken. U kunt dit doen door een aangepaste PPPC-payload te implementeren of door de voorkeuren in de grafische gebruikersinterface van de workload te configureren. De volgende machtigingen zijn vereist.

Vereisten voor macOS 11 (Big Sur) of later

Tabblad	Gedeelte	Veld	Waarde

Besturingselement voor privacyvoorkeurenbeleid	App-toegang	Id	com.acronis.backup

		Type id	Bundel-id

		Codevereiste	identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP OF SERVICE	SystemPolicyAllFiles
		TOEGANG	Toestaan
	App-toegang	Id	com.acronis.backup.aakore
		Type id	Bundel-id
		Codevereiste	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP OF SERVICE	SystemPolicyAllFiles
		TOEGANG	Toestaan
	App-toegang	Id	com.acronis.backup.activeprotection
		Type id	Bundel-id
		Codevereiste	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP OF SERVICE	SystemPolicyAllFiles
		TOEGANG	Toestaan

	App-toegang	Id	cyber-protect-service
		Type id	Bundel-id
		Codevereiste	`identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6`
		APP OF SERVICE	SystemPolicyAllFiles
		TOEGANG	Toestaan
Systeemextensies		Gebruikers toestaan systeemextensies goed te keuren	Ingeschakeld
	Goedgekeurde team-id's en systeemextensies	Weergavenaam	Systeemextensies voor Acronis Cyber Protection-agent
		Typen systeemextensies	Toegestane team-id's
		Team-id	ZU2TV78AA6

Vereisten voor macOS-versies ouder dan versie 11

Tabblad	Gedeelte	Veld	Waarde

Besturingselement voor privacyvoorkeurenbeleid	App-toegang	Id	com.acronis.backup

		Type id	Bundel-id

		Codevereiste	identifier "com.acronis.backup" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP OF SERVICE	SystemPolicyAllFiles
		TOEGANG	Toestaan
	App-toegang	Id	com.acronis.backup.aakore
		Type id	Bundel-id
		Codevereiste	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP OF SERVICE	SystemPolicyAllFiles
		TOEGANG	Toestaan
	App-toegang	Id	com.acronis.backup.activeprotection
		Type id	Bundel-id
		Codevereiste	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP OF SERVICE	SystemPolicyAllFiles
		TOEGANG	Toestaan

	App-toegang	Id	cyber-protect-service
		Type id	Bundel-id
		Codevereiste	identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		APP OF SERVICE	SystemPolicyAllFiles
		TOEGANG	Toestaan
Goedgekeurde kernelextensies		Gebruikers toestaan kernelextensies goed te keuren	Ingeschakeld
		Standaardgebruikers toestaan om verouderde kernelextensies goed te keuren (macOS 11 of later)	Ingeschakeld
	Goedgekeurde team-id's en kernelextensies	Goedgekeurde team-id - Weergavenaam	Kernelextensies voor Acronis Cyber Protection-agent
		Team-id	ZU2TV78AA6
		Id's van bundel kernelextensies	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
Systeemextensies		Gebruikers toestaan systeemextensies goed te keuren	Ingeschakeld
	Goedgekeurde team-id's en systeemextensies	Weergavenaam	Systeemextensies voor Acronis Cyber Protection-agent
		Typen systeemextensies	Toegestane team-id's
		Team-id	ZU2TV78AA6

Registratie van workloads

Een registratie verbindt een workload waarop een beveiligingsagent is geïnstalleerd, met een gebruikersaccount in een klanttenant. Na voltooiing van de registratie kunt u de workload zien in de Cyber Protect-console, onder **Apparaten** > **Machines met agents**. U kunt geregistreerde workloads beheren door hierop plannen toe te passen.

Wanneer u een beveiligingsagent installeert via de grafische gebruikersinterface, maakt de registratie deel uit van de installatieprocedure.

Wanneer u de opdrachtregelinterface gebruikt, kunt u de registratie uitvoeren als een zelfstandige procedure.

Workloads registreren via de grafische gebruikersinterface

Wanneer u een beveiligingsagent installeert via de grafische gebruikersinterface, maakt de registratie deel uit van de installatieprocedure.

De volgende registratiemethoden zijn beschikbaar:

- Registratie in de Cyber Protect-console
- Registratie met gebruikersaccountreferenties
- Registratie met een registratietoken

De registratie van de agent wordt automatisch ongedaan gemaakt wanneer u de agent verwijdert.

Workloads registreren via de Cyber Protect-console

Deze procedure is van toepassing wanneer u een beveiligingsagent installeert met de standaard installatie-instellingen (**Registratie-instellingen** > **ConsoleCyber Protect gebruiken**).

Een workload registreren vanuit de Cyber Protect-console:

1. Klik in de installatiewizard op **Workload registreren**.
   De Cyber Protect-console wordt geopend.

   Opmerking
   Sluit de installatiewizard niet af voordat de registratie is voltooid. Anders moet u de installatie herhalen en de registratie opnieuw starten.

2. Meld u aan bij de Cyber Protect-console.
3. [Als u zich aanmeldt als beheerder] Ga naar het scherm **Workloadregistratie** en selecteer het account waarvoor u de workload wilt registreren.
   Dit account moet een account zijn in een klanttenant. Partnerbeheerders kunnen de door hen beheerde klanttenants zien en workloads registreren voor accounts in deze tenants.
4. Klik op **Code valideren**.

5. Klik op **Volgende**.
6. [Niet van toepassing op partnerbeheerders] Bekijk de vooraf geselecteerde standaardplannen die op de workload worden toegepast.
   Voor meer informatie over de standaardplannen: zie "Standaardplannen" (p. 212).

   Belangrijk
   Geselecteerde plannen worden alleen toegepast op Windows-workloads.
   in het geval van Linux- en macOS-workloads, moet u de plannen handmatig toepassen wanneer de registratie is voltooid.

7. [Optioneel] [Niet van toepassing op partnerbeheerders] Als u een vooraf geselecteerd plan wilt wijzigen, klik op **Wijzigen**.
   - Als u een ander plan wilt toepassen, selecteert u het plan dat u wilt gebruiken en klikt u vervolgens op **Wijzigen**.
     U kunt een plan van de tenant of een ingebouwd plan selecteren.
     Voor meer informatie over de ingebouwde plannen: zie "Ingebouwde plannen" (p. 203).
   - ALs u de workload wilt registreren zonder een plan toe te passen, selecteert u **Geen beschermingsplan toepassen** en klikt u vervolgens op **Wijzigen**.
8. Klik op **Registreren**.

De workload wordt dan geregistreerd voor het opgegeven gebruikersaccount. Wanneer de registratie is voltooid, worden de geselecteerde plannen automatisch toegepast op Windows-workloads.

Workloads registreren met gebruikersreferenties

U kunt de standaard-installatieprocedure wijzigen en registratie met gebruikersnaam en wachtwoord selecteren in plaats van registratie in de Cyber Protect-console.

Een workload registreren met gebruikersnaam en wachtwoord:

1. Klik in de installatiewizard op **Installatie-instellingen aanpassen**.
2. Klik in het gedeelte **Registratie-instellingen** op **Wijzigen**.
3. Selecteer **Referenties gebruiken**.
4. Geef de gebruikersnaam en het wachtwoord op voor het account waarvoor u de workload wilt registreren.
   Dit account moet een account in een klanttenant zijn.

   Opmerking
   U kunt alleen accounts gebruiken waarvoor tweeledige verificatie niet is ingeschakeld.

5. Klik op **Gereed** en voltooi de installatie.

Workloads registreren met een registratietoken

U kunt de standaard-installatieprocedure wijzigen en registratie met een registratietoken selecteren in plaats van registratie in de Cyber Protect-console.

Een workload registreren met een registratietoken:

1. Klik in de installatiewizard op **Installatie-instellingen aanpassen**.
2. Klik in het gedeelte **Registratie-instellingen** op **Wijzigen**.
3. Selecteer **Registratietoken gebruiken**.
4. Voer het registratietoken in.
5. Klik op **Gereed** en voltooi de installatie.

Een registratietoken genereren

Een registratietoken is een reeks van 12 tekens in drie segmenten, gescheiden door streepjes. Het registratietoken geeft de identiteit van een gebruiker door aan het installatieprogramma van de agent, zonder de gebruikersreferenties voor de Cyber Protect-console op te slaan. Zo kunnen gebruikers workloads registreren voor hun account of beschermingsplannen toepassen op workloads zonder zich aan te melden bij de console.

Opmerking
Beschermingsplannen worden niet automatisch toegepast tijdens de registratie van de workload. Het toepassen van een beschermingsplan is een afzonderlijke taak.

Om veiligheidsredenen hebben tokens een beperkte levensduur, maar u kunt deze aanpassen. De standaardlevensduur is 3 dagen.

Beheerders kunnen registratietokens genereren voor alle gebruikersaccounts in de tenant die zij beheren. Gebruikers kunnen alleen registratietokens voor hun eigen accounts genereren.

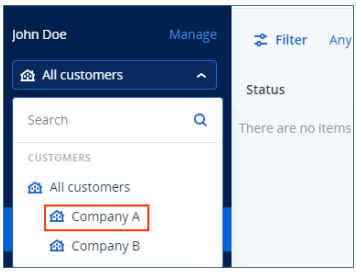
Een registratietoken genereren

Als beheerder

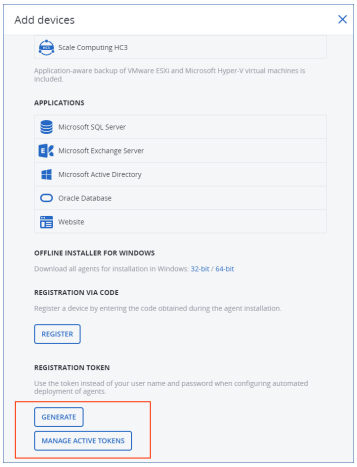
1. Meld u als beheerder aan bij de Cyber Protect-console.
   Als u al bent aangemeld bij de beheerportal, is de Cyber Protect-console toegankelijk via **Controle** > **Gebruik**, het tabblad **Bescherming** en **Service beheren**.

   [Voor partnerbeheerders die klanttenants beheren] Ga naar de Cyber Protect-console en selecteer de tenant met de gebruiker voor wie u een token wilt genereren. U kunt geen token genereren op het niveau **Alle klanten**.



2. Klik onder **Apparaten** op **Alle apparaten** > **Toevoegen**.
   Het deelvenster **Apparaten toevoegen** wordt geopend aan de rechterkant.
3. Blader omlaag naar **Registratietoken** en klik vervolgens op **Genereren**.



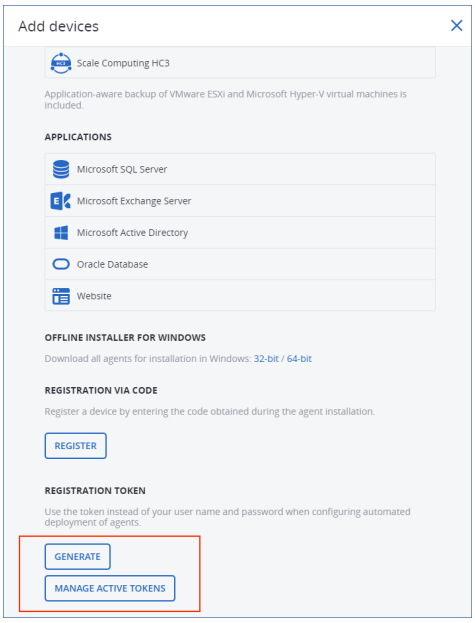
4. Geef de levensduur van het token op.
5. Selecteer de gebruiker voor wie u een token wilt genereren.

> **Opmerking**
> Wanneer u het token gebruikt, worden workloads geregistreerd voor het gebruikersaccount dat u hier selecteert.

6. [Optioneel] Als u wilt dat de gebruiker van het token een beschermingsschema kan toepassen en intrekken voor de toegevoegde workloads, selecteert u het schema in de vervolgkeuzelijst.
   Let op: u moet een script uitvoeren waarmee een beschermingsschema wordt toegepast of ingetrokken voor de toegevoegde workloads. Zie dit Knowledge Base-artikel voor meer informatie.
7. Klik op **Token genereren**.
8. Klik op **Kopiëren** om het token naar het klembord van uw apparaat te kopiëren of noteer het token handmatig.

Als gebruiker

1. Meld u aan bij de Cyber Protect-console.
2. Klik op **Apparaten** > **Alle apparaten** > **Toevoegen**.
   Het deelvenster **Apparaten toevoegen** wordt geopend aan de rechterkant.
3. Blader omlaag naar **Registratietoken** en klik vervolgens op **Genereren**.



4. Geef de levensduur van het token op.
5. Klik op **Token genereren**.
6. Klik op **Kopiëren** om het token naar het klembord van uw apparaat te kopiëren of noteer het token handmatig.

Registratietokens beheren

U kunt de actieve registratietokens bekijken en verwijderen.

Registratietokens bekijken:

1. Meld u aan bij de Cyber Protect-console.
2. Klik op **Apparaten** > **Alle apparaten** > **Toevoegen**.
3. Blader omlaag naar **Registratietoken** en klik vervolgens op **Actieve tokens beheren**.
   Aan de rechterkant wordt een lijst geopend met de actieve tokens die zijn gegenereerd voor de tenant.

> **Opmerking**
> Om veiligheidsredenen worden in de kolom **Token** alleen de eerste twee tekens van de tokenwaarde weergegeven.

Een registratietoken verwijderen:

1. Meld u aan bij de Cyber Protect-console.
2. Klik op **Apparaten** > **Alle apparaten** > **Toevoegen**.
3. Blader omlaag naar **Registratietoken** en klik vervolgens op **Actieve tokens beheren**.
   Aan de rechterkant wordt een lijst geopend met de actieve tokens die zijn gegenereerd voor de tenant.

Opmerking
Om veiligheidsredenen worden in de kolom **Token** alleen de eerste twee tekens van de tokenwaarde weergegeven.

4. Selecteer het token en klik vervolgens op **Verwijderen**.

Workloads registreren en de registratie van workloads ongedaan maken via de opdrachtregelinterface

Wanneer u de opdrachtregelinterface gebruikt, kunt u de registratie uitvoeren als een zelfstandige procedure.

Als u een beveiligingsagent bijvoorbeeld wilt registreren voor een ander account, hoeft u de agent niet eerst te verwijderen.

Workloads registreren met gebruikersreferenties

Gebruik de gebruikersnaam en het wachtwoord voor het account waarvoor u de workload wilt registreren. Dit account moet een account zijn in een klanttenant. Als het wachtwoord speciale tekens of spaties bevat: zie "Wachtwoorden met speciale tekens of spaties gebruiken" (p. 130).

Het serviceadres is de URL die u gebruikt voor **aanmelding** bij de Cyber Protection-service.

Bijvoorbeeld: `https://cloud.company.com`.

Een workload registreren met een gebruikersnaam en wachtwoord

In Windows

- Voer de volgende opdracht uit op de opdrachtprompt:

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

Bijvoorbeeld:

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

In Linux

- Voer de volgende opdracht uit op de opdrachtprompt:

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

Bijvoorbeeld:

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

In macOS

Belangrijk
Als u macOS 10.14 of later gebruikt, moet u de beveiligingsagent volledige schijftoegang geven. Dit kunt u doen door naar **Toepassingen** >**Hulpprogramma's** te gaan en dan **Cyber Protect Agent Assistant** uit te voeren. Volg verder de instructies in het toepassingsvenster.

- Voer de volgende opdracht uit op de opdrachtprompt:

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

Bijvoorbeeld:

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

Wachtwoorden met speciale tekens of spaties gebruiken

Als uw wachtwoord speciale tekens of spaties bevat, moet u het tussen aanhalingstekens plaatsen wanneer u het invoert op de opdrachtregel.

Voer bijvoorbeeld in Windows de volgende opdracht uit:

Opdrachtsjabloon:

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

Opdrachtvoorbeeld:

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

Als deze opdracht niet werkt, codeert u uw wachtwoord in base64-indeling op https://www.base64encode.org/. Geef op de opdrachtregel het gecodeerde wachtwoord op met behulp van de parameter -b of --base64.

Voer bijvoorbeeld in Windows de volgende opdracht uit:

Opdrachtsjabloon:

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

Opdrachtvoorbeeld:

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

Workloads registreren met een registratietoken

Een registratietoken is een reeks van 12 tekens in drie segmenten, gescheiden door streepjes. Het registratietoken geeft de identiteit van een gebruiker door aan het installatieprogramma van de agent, zonder de gebruikersreferenties voor de Cyber Protect-console op te slaan. Zo kunnen gebruikers workloads registreren voor hun account of beschermingsplannen toepassen op workloads zonder zich aan te melden bij de console.

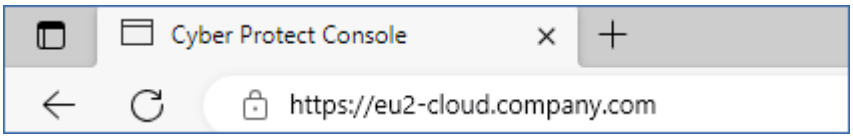
Zie "Een registratietoken genereren" (p. 126) voor meer informatie.

Opmerking
Beschermingsplannen worden niet automatisch toegepast tijdens de registratie van de workload. Het toepassen van een beschermingsplan is een afzonderlijke taak.

Voor meer informatie: zie dit Knowledge Base-artikel.

Wanneer u een registratietoken gebruikt, moet u het exacte adres van het datacenter opgeven. Dit is de URL die u ziet **na uw aanmelding** bij de Cyber Protection-service.

Bijvoorbeeld: `https://eu2-cloud.company.com`.



Een workload registreren met een registratietoken

In Windows

- Voer de volgende opdracht uit op de opdrachtprompt:

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

Bijvoorbeeld:

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

In Linux

- Voer de volgende opdracht uit op de opdrachtprompt:

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

Bijvoorbeeld:

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

In macOS

Belangrijk
Als u macOS 10.14 of later gebruikt, moet u de beveiligingsagent volledige schijftoegang geven. Dit kunt u doen door naar **Toepassingen** >**Hulpprogramma's** te gaan en dan **Cyber Protect Agent Assistant** uit te voeren. Volg verder de instructies in het toepassingsvenster.

- Voer de volgende opdracht uit op de opdrachtprompt:

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

Bijvoorbeeld:

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

Virtuele toepassing

1. Druk in de console van de virtuele toepassing op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
2. Voer de volgende opdracht uit op de opdrachtprompt:

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

   Bijvoorbeeld:

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

3. Druk op ALT+F1 om terug te gaan naar de grafische interface van de toepassing.

Registratie van workloads ongedaan maken

Vanuit de opdrachtregelinterface kunt u de registratie van een beveiligingsagent ongedaan maken zonder de agent te verwijderen.

Registratie van een workload ongedaan maken

In Windows

- Voer de volgende opdracht uit op de opdrachtprompt:

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

Bijvoorbeeld:

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

In Linux

- Voer de volgende opdracht uit op de opdrachtprompt:

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

In macOS

Voer de volgende opdracht uit op de opdrachtprompt:

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

Virtuele toepassing

1. Druk in de console van de virtuele toepassing op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
2. Voer de volgende opdracht uit op de opdrachtprompt:

```
register_agent -o unregister
```

3. Druk op ALT+F1 om terug te gaan naar de grafische interface van de toepassing.

De registratie van een workload wijzigen

U kunt de huidige registratie van een workload wijzigen door deze te registreren in een nieuwe tenant of voor een nieuw gebruikersaccount.

Belangrijk
Wanneer u de registratie van een workload wijzigt, worden alle beschermingsschema's voor die workload ingetrokken. U moet een nieuw beschermingsschema toepassen op de workload als u deze wilt blijven beschermen.

Als u de workload registreert in een nieuwe tenant, heeft de workload geen toegang meer tot de back-ups in de cloudopslag van de oorspronkelijke tenant. De back-ups in niet-cloudopslag blijven toegankelijk.

De registratie van een workload wijzigen:

Via de opdrachtregelinterface

1. Maak de registratie van de beveiligingsagent ongedaan, zoals beschreven in "Registratie van workloads ongedaan maken" (p. 132).
2. Registreer de beveiligingsagent in de nieuwe tenant of voor het nieuwe gebruikersaccount, zoals beschreven in "Workloads registreren met gebruikersreferenties" (p. 129) of "Workloads registreren met een registratietoken" (p. 131).

Via de grafische gebruikersinterface

1. Verwijder de beveiligingsagent.
2. Installeer de beveiligingsagent en registreer deze vervolgens in de nieuwe tenant of voor het nieuwe gebruikersaccount.

Voor meer informatie over hoe u een agent installeert en registreert: zie "Beveiligingsagents installeren via de grafische gebruikersinterface" (p. 81).

Workloads verplaatsen naar een andere tenant

Het verplaatsen van een workload naar een andere tenant wordt niet standaard ondersteund. Als tijdelijke oplossing kunt u de registratie van de workload ongedaan maken en deze vervolgens registreren in een andere tenant. Alle toegepaste beschermingsschema's worden ingetrokken voor die workload en de back-ups in de cloudopslag van de oorspronkelijke tenant zijn niet meer toegankelijk.

Zie "De registratie van een workload wijzigen" (p. 133) voor meer informatie over het registreren van een workload in een nieuwe tenant of voor een nieuw gebruikersaccount.

Beveiligingsagents bijwerken

U kunt alle agents handmatig bijwerken via de Cyber Protect-console of door het installatiebestand te downloaden en uit te voeren.

U kunt automatische updates configureren voor de volgende agenten:

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

Als u een agent automatisch wilt bijwerken, of handmatig via de Cyber Protect-console, hebt u 4,2 GB vrije schijfruimte nodig op de volgende locatie:

- Voor Linux: de hoofdmap (root directory)
- Voor Windows: het volume waarop de agent is geïnstalleerd

Als u een agent wilt bijwerken in macOS, hebt u 5 GB vrije schijfruimte nodig in de hoofdmap (root directory).

Opmerking
[Voor alle agents die worden geleverd in de vorm van een virtuele toepassing, inclusief Agent voor VMware, Agent voor Scale Computing, Agent voor Virtuozzo Hybrid Infrastructure, Agent voor RHV (oVirt)]

Als u automatische of handmatige updates wilt uitvoeren van een virtuele toepassing die zich achter een proxy bevindt, moet de proxyserver in elke toepassing als volgt worden geconfigureerd.

Voeg in het bestand `/opt/acronis/etc/va-updater/config.yaml` de volgende regel toe onderaan het bestand en voer de waarden in die specifiek zijn voor uw omgeving:

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

Beveiligingsagents handmatig bijwerken

U kunt agents bijwerken via de Cyber Protect-console of door het installatiebestand te downloaden en uit te voeren.

Virtuele toepassingen met de volgende versies mogen alleen worden bijgewerkt via de Cyber Protect-console:

- Agent voor VMware (Virtual Appliance): versie 12.5.23094 en later.
- Agent voor Virtuozzo Hybrid Infrastructure (Virtual Appliance): versie 12.5.23094 en later.

Agents met de volgende versies kunnen ook worden bijgewerkt via de Cyber Protect-console:

- Agent voor Windows, Agent voor VMware (Windows), Agent voor Hyper-V: versie 12.5.21670 en later.
- Agent voor Linux: versie 12.5.23094 en later.
- Andere agenten: versie 12.5.23094 en later.

Als u de versie van de agent wilt vinden, selecteert u de machine in de Cyber Protect-console en klikt u op **Details**.

Als u eerdere versies van die agenten wilt bijwerken, moet u de nieuwste versie handmatig downloaden en installeren. Voor de downloadlinks klikt u op **Alle apparaten** > **Toevoegen**.

Vereisten

Voor Cyber Protect-functies op Windows-machines is Microsoft Visual C++ 2017 Redistributable vereist. Controleer of dit pakket al op uw machine is geïnstalleerd of installeer het voordat u de agent bijwerkt. Na de installatie moet mogelijk opnieuw worden opgestart. U kunt het Microsoft Visual C++ Redistributable-pakket vinden op de Microsoft-website: https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Een agent bijwerken met de Cyber Protect-console:

1. Klik op **Instellingen** > **Agenten**.

   De software geeft de lijst met machines weer. De machines met verouderde agentversies herkent u aan een oranje uitroepteken.
2. Selecteer de machines waarop u de agenten wilt bijwerken. De machines moeten online zijn.
3. Klik op **Agent bijwerken**.

Opmerking
Tijdens de update mislukken alle back-ups die op dat moment worden uitgevoerd.

Agent voor VMware (Virtual Appliance) met een oudere versie dan 12.5.23094 bijwerken

1. Klik op **Instellingen** > **Agenten** > de agent die u wilt bijwerken > **Details** en bekijk dan het gedeelte **Toegewezen virtuele machines**. U moet deze instellingen na de update opnieuw invoeren.
   a. Noteer de stand van de schakelaar **Automatische toewijzing**.
   b. Als u wilt weten welke virtuele machines handmatig aan de agent worden toegewezen, klikt u op de link **Toegewezen:**. U krijgt dan automatisch de lijst met toegewezen virtuele machines te zien. Noteer de machines met `(M)` achter de naam van de agent in de kolom **Agent**.
2. Verwijder Agent voor VMware (Virtual Appliance), zoals beschreven in 'Agenten verwijderen'. Verwijder in stap 5 de agent uit **Instellingen** > **Agenten**, zelfs als u van plan bent de agent opnieuw te installeren.
3. Implementeer Agent voor VMware (Virtual Appliance), zoals beschreven in 'De OVF-sjabloon implementeren'.
4. Configureer Agent voor VMware (Virtual Appliance), zoals beschreven in 'De virtuele toepassing configureren'.

   Als u de lokaal gekoppelde opslag wilt herstellen, gaat u in stap 7 als volgt te werk:
   a. Voeg de schijf met de lokale opslag toe aan de virtuele toepassing.
   b. Klik op **Vernieuwen** > **Opslag maken** > **Koppelen**.
   c. In de software ziet u de oorspronkelijke **Letter** en **Label** van de schijf. Wijzig deze niet.
   d. Klik op **OK**.
5. Klik op **Instellingen** > **Agenten** > de agent die u wilt bijwerken > **Details** en herstel dan de instellingen die u hebt genoteerd bij stap 1. Als sommige virtuele machines handmatig aan de agent zijn toegewezen, wijs ze dan opnieuw toe zoals beschreven in 'Binding van virtuele machines'.

   Wanneer de configuratie van de agent is voltooid, worden de beschermingsschema's die zijn toegepast op de oude agent, automatisch opnieuw toegepast op de nieuwe agent.
6. In het geval van schema's met applicatiegerichte back-up moeten de referenties van het gastbesturingssysteem opnieuw worden ingevoerd. Bewerk deze schema's en voer de referenties opnieuw in.

7. Voor schema's waarmee een back-up van de ESXi-configuratie wordt gemaakt, moet het rootwachtwoord opnieuw worden ingevoerd. Bewerk deze schema's en voer het wachtwoord opnieuw in.

Definities van Cyber Protection op een machine bijwerken

1. Klik op **Instellingen** > **Agenten**.
2. Selecteer de machine waarop u de Cyber Protection-definities wilt bijwerken en klik op **Definities bijwerken**. De machine moet online zijn.

De rol Updater toewijzen aan een agent

1. Klik op **Instellingen** > **Agenten**.
2. Selecteer de machine waaraan u de Updater-rol wilt toewijzen, klik op **Details** en schakel in het gedeelte **Cyber Protection-definities** de optie **Deze agent gebruiken om patches en updates te downloaden en te distribueren** in.

   Opmerking
   Een agent met de Updater-rol kan alleen patches downloaden en distribueren voor Windows-producten van derden. De Updater-agent biedt geen ondersteuning voor de distributie van patches voor Microsoft-producten.

Gegevens over een agent in het cachegeheugen wissen

1. Klik op **Instellingen** > **Agenten**.
2. Selecteer de machine waarvan u de cachegegevens (verouderde updatebestanden en patchbeheergegevens) wilt wissen en klik op **Cache wissen**.

Beveiligingsagents automatisch bijwerken

U kunt het beheer van meerdere workloads vergemakkelijken door automatische updates te configureren voor Agent voor Windows, Agent voor Linux en Agent voor Mac. Automatische updates zijn beschikbaar voor agenten versie 15.0.26986 (uitgebracht in mei 2021) of later. Oudere agenten moeten eerst handmatig worden bijgewerkt naar de nieuwste versie.

Automatische updates worden ondersteund op machines met een van de volgende besturingssystemen:

- Windows XP SP 3 en later
- Red Hat Enterprise Linux 6 en later, CentOS 6 en later
- OS X 10.9 Mavericks en later

De instellingen voor automatische updates zijn vooraf geconfigureerd op datacenterniveau. Een bedrijfbeheerder kan deze instellingen aanpassen voor alle machines in een bedrijf of een eenheid, of voor afzonderlijke machines. Als er geen aangepaste instellingen worden toegepast, dan worden de instellingen van het bovenste niveau gebruikt, in deze volgorde:

1. Cyber Protection-datacenter
2. Bedrijf (klanttenant)
3. Eenheid
4. Machine

Een eenheidbeheerder kan bijvoorbeeld aangepaste instellingen voor automatisch bijwerken configureren voor alle machines in de eenheid. Dit verschilt dus van de instelling die wordt toegepast op de machines op bedrijfsniveau. De beheerder kan ook andere instellingen configureren voor een of meer afzonderlijke machines in de eenheid, waarop noch de eenheidinstellingen noch de bedrijfsinstellingen worden toegepast.

Na het inschakelen van de automatische updates kunt u de volgende opties configureren:

- **Updatekanaal**
  Het updatekanaal bepaalt welke versie van de agenten wordt gebruikt: de meest recente versie of de nieuwste versie van de vorige release.
- **Tijdvenster voor onderhoud**
  Het tijdvenster voor onderhoud bepaalt wanneer updates kunnen worden geïnstalleerd. Als het tijdvenster voor onderhoud is uitgeschakeld, kunnen updates op elk moment worden uitgevoerd.
  Zelfs binnen het ingeschakelde tijdvenster voor onderhoud worden updates niet geïnstalleerd wanneer de agent een van de volgende bewerkingen uitvoert:
  - Back-up
  - Herstel
  - Back-upreplicatie
  - Replicatie van virtuele machines
  - Replica testen
  - Een virtuele machine uitvoeren vanaf een back-up (inclusief voltooiing)
  - Failover voor noodherstel
  - Failback voor noodherstel
  - Een script uitvoeren (voor Cyber Scripting-functionaliteit)
  - Patchinstallatie
  - Back-up van ESXi-configuratie

Instellingen voor automatisch bijwerken aanpassen

1. Ga in de Cyber Protect-console naar **Instellingen** > **Agents**.
2. Selecteer het bereik voor de instellingen:
   - Als u de instellingen voor alle machines wilt wijzigen, klikt u op **Standaardinstellingen voor agentupdates bewerken**.
   - Als u de instellingen voor specifieke machines wilt wijzigen, selecteert u de gewenste machines en klikt u vervolgens op **Instellingen voor agentupdates**.

3. Configureer de instellingen volgens uw behoeften en klik vervolgens op **Toepassen**.

Aangepaste instellingen voor automatisch bijwerken verwijderen

1. Ga in de Cyber Protect-console naar **Instellingen** > **Agents**.
2. Selecteer het bereik voor de instellingen:
   - Als u de aangepaste instellingen voor alle machines wilt verwijderen, klikt u op **Standaardinstellingen voor agentupdates bewerken**.
   - Als u de aangepaste instellingen voor specifieke machines wilt verwijderen, selecteert u de gewenste machines en klikt u vervolgens op **Instellingen voor agentupdates**.
3. Klik op **Terugzetten naar standaardinstellingen** en klik vervolgens op **Toepassen**.

Status van automatisch bijwerken controleren

1. Ga in de Cyber Protect-console naar **Instellingen** > **Agents**.
2. Klik op het tandwielpictogram in de rechterbovenhoek van de tabel en controleer of het selectievakje voor **automatisch bijwerken** is ingeschakeld.
3. Controleer de status die wordt weergegeven in de kolom **Automatisch bijwerken**.

Beveiligingsagents bijwerken voor workloads met BitLocker-versleuteling

Als u een agent bijwerkt en Startup Recovery Manager hierdoor wordt gewijzigd, conflicteert dit met BitLocker voor workloads waarvoor zowel BitLocker als Startup Recovery Manager is ingeschakeld. Na opnieuw opstarten is in dit geval de BitLocker-herstelsleutel vereist. U kunt dit probleem verhelpen door BitLocker op te schorten of uit te schakelen voordat u de agent bijwerkt.

Betreffende agentversies:

- 23.12.36943, uitgebracht in december 2023

In de releaseopmerkingen van de beveiligingsagent kunt u ook controleren of een update wijzigingen veroorzaakt in Startup Recovery Manager.

De agent bijwerken voor een workload waarvoor zowel BitLocker als Startup Recovery Manager is ingeschakeld:

1. U kunt BitLocker opschorten of uitschakelen voor de workload waarvoor u de agent wilt bijwerken.
2. Werk de agent bij.
3. Start de workload opnieuw op.
4. Schakel BitLocker in.

Beveiligingsagents via Groepsbeleid implementeren

U kunt Windows-groepsbeleid gebruiken om Agent voor Windows centraal te installeren (of te implementeren) op machines die lid zijn van een Active Directory-domein.

In dit gedeelte wordt uitgelegd hoe u een groepsbeleidobject instelt om agenten te implementeren op alle machines in een domein of organisatie-eenheid.

Telkens wanneer een machine wordt aangemeld bij het domein, zorgt het groepsbeleidobject ervoor dat de agent wordt geïnstalleerd en geregistreerd.

Vereisten

- U hebt een Active Directory-domein met een domeincontroller waarop Microsoft Windows Server 2003 of later wordt uitgevoerd.
- U moet lid zijn van de groep **Domeinadministrators** in het domein.
- U hebt het installatieprogramma voor **Alle agenten voor Windows** gedownload.

  Als u het installatieprogramma wilt downloaden, klikt u in de Cyber Protect-console op het accountpictogram in de rechterbovenhoek en vervolgens op **Downloads**. De downloadlink is ook beschikbaar in het deelvenster **Apparaten toevoegen**.

Agenten implementeren via Groepsbeleid:

1. Genereer een registratietoken zoals beschreven in "Een registratietoken genereren" (p. 126).
2. Maak het MST-bestand, het MSI-bestand en de CAB-bestanden zoals beschreven in "Het transformatiebestand maken en de installatiepakketten uitpakken" (p. 140).
3. Stel het groepsbeleidobjecten in zoals beschreven in "Het groepsbeleidobject instellen" (p. 141).

Het transformatiebestand maken en de installatiepakketten uitpakken

Als u beveiligingsagents wilt implementeren via Windows-groepsbeleid, hebt u een transformatiebestand (.mst) en de installatiepakketten (.msi- en .cab-bestanden) nodig.

Opmerking
In de onderstaande procedure wordt de standaardregistratieoptie gebruikt, namelijk registratie per token. Zie "Een registratietoken genereren" (p. 126) voor meer informatie over het genereren van een registratietoken.

Het MST-bestand maken en de installatiepakketten (.msi- en .cab-bestanden) uitpakken

1. Meld u als beheerder aan bij een van de machines in het Active Directory-domein.

2. Maak een gedeelde map die de installatiepakketten bevat. Zorg dat de gedeelde map toegankelijk is voor de gebruikers van het domein, bijvoorbeeld door de standaardinstelling voor delen in te stellen op **Iedereen**.
3. Voer het installatieprogramma van de agent uit.
4. Klik op **MST- en MSI-bestanden maken voor installatie zonder toezicht**.
5. Ga naar **Installatie-items**, selecteer de onderdelen die u wilt opnemen in de installatie en klik op **Gereed**.
6. Ga naar **Registratie-instellingen** en klik op **Opgeven**, voer een registratietoken in en klik vervolgens op **Gereed**.

   U kunt de registratiemethode wijzigen van **Registratietoken gebruiken** (standaard) in **Referenties gebruiken** of **Registratie overslaan**. Als u **Registratie overslaan** kiest, wordt ervan uitgegaan dat u de workloads later handmatig wilt registreren.
7. Controleer of wijzig de installatie-instellingen die aan het MST-bestand worden toegevoegd en klik vervolgens op **Doorgaan**.
8. Ga naar **De bestanden opslaan in** en geef het pad op naar de gedeelde map die u hebt gemaakt.
9. Klik op **Genereren**.

Het MST-bestand, het MSI-bestand en de CAB-bestanden worden gemaakt en gekopieerd naar de gedeelde map die u hebt opgegeven.

Vervolgens stelt u het Windows-groepsbeleidobject in. Raadpleeg "Het groepsbeleidobject instellen" (p. 141) voor informatie over hoe u dit doet.

Het groepsbeleidobject instellen

In deze procedure gebruikt u de installatiepakketten die u in "Het transformatiebestand maken en de installatiepakketten uitpakken" (p. 140) hebt gemaakt, om ee groepsbeleidobject (GPO) in te stellen. Met het groepsbeleidobject worden de agents geïmplementeerd op de machines in uw domein.

Het groepsbeleidobject instellen:

1. Meld u als domeinbeheerder aan bij de domeincontroller.

   Als het domein meerdere domeincontrollers heeft, kunt u zich bij een van deze domeincontrollers aanmelden als domeinbeheerder.
2. [Als u agents in een organisatie-eenheid wilt implementeren]: controleer of de betreffende organisatie-eenheid bestaat in het domein.
3. Wijs in het menu **Start** van Windows de optie **Systeembeheer** aan en klik vervolgens op **Groepsbeleidsbeheer** (of **Active Directory: gebruikers en computers** voor Windows Server 2003).
4. [Voor Windows Server 2008 of later] Klik met de rechtermuisknop op de naam van het domein of de organisatie-eenheid en klik vervolgens op **Groepsbeleidobject in dit domein maken en hier een koppeling maken...**.

5. [Voor Windows Server 2003] Klik met de rechtermuisknop op de naam van het domein of de organisatie-eenheid en klik vervolgens op **Eigenschappen**. Klik in het dialoogvenster op het tabblad **Groepsbeleid** en klik vervolgens op **Nieuw**.
6. Geef **Agent voor Windows** als naam van het nieuwe groepsbeleidobject.
7. Open het groepsbeleidobject **Agent voor Windows** om het te bewerken:
   - [In Windows Server 2008 of later] Klik met de rechtermuisknop in het gedeelte **Groepsbeleidobjecten** op het betreffende groepsbeleidobject en klik vervolgens op **Bewerken**.
   - [In Windows Server 2003] Klik op het groepsbeleidobject en klik vervolgens op **Bewerken**.
8. Vouw in de module Groepsbeleidobjecteditor de optie **Computerconfiguratie** uit.
9. [Voor Windows Server 2012 of later] Vouw **Beleidsregels** > **Software-instellingen** uit.
10. [Voor Windows Server 2003 en Windows Server 2008] Vouw **Software-instellingen** uit.
11. Klik met de rechtermuisknop op **Software-installatie**, wijs **Nieuw** aan en klik vervolgens op **Pakket**.
12. Selecteer het MSI-installatiepakket van de agent in de gedeelde map die u eerder hebt gemaakt en klik vervolgens op **Openen**.
13. Klik in het dialoogvenster **Software distribueren** op **Geavanceerd** en klik vervolgens op **OK**.
14. Klik op het tabblad **Wijzigingen** op **Toevoegen** en selecteer vervolgens het MST-bestand in de gedeelde map die u hebt gemaakt.
15. Klik op **OK** om het dialoogvenster **Software distribueren** te sluiten.

Virtuele apparaten implementeren

Agent voor VMware (Virtual Appliance) implementeren

Voordat u start

Systeemvereisten voor de agent

Standaard krijgt de virtuele toepassing 4 GB RAM en 2 vCPU's toegewezen. Dit is optimaal en voldoende voor de meeste bewerkingen.

Als u de back-upprestaties wilt verbeteren en storingen als gevolg van onvoldoende RAM-geheugen wilt voorkomen, raden we aan om deze resources uit te breiden naar 16 GB RAM en 4 vCPU's voor veeleisende gevallen. U kunt de toegewezen resources bijvoorbeeld uitbreiden wanneer u verwacht dat het back-upverkeer meer dan 100 MB per seconde zal bedragen (bijvoorbeeld in netwerken van 10 gigabit) of als u tegelijkertijd een back-up maakt van meerdere virtuele machines met grote harde schijven (500 GB of meer).

De eigen virtuele schijven van de toepassing gebruiken niet meer dan 6 GB. De indeling van de schijf (thick of thin) heeft geen invloed op de prestaties van de toepassing.

Hoeveel agenten heb ik nodig?

Een virtuele toepassing kan een hele vSphere-omgeving beschermen, maar het wordt aanbevolen om één virtuele toepassing per vSphere-cluster (of per host, als er geen clusters zijn) te implementeren. Hierdoor kunnen back-ups sneller worden gemaakt, omdat de toepassing de schijven waarvan een back-up is gemaakt, kan koppelen via HotAdd-transport, zodat het back-upverkeer van de ene lokale schijf naar een andere wordt geleid.

Het is normaal om zowel de virtuele toepassing als Agent voor VMware (Windows) tegelijkertijd te gebruiken, op voorwaarde dat ze zijn verbonden met dezelfde vCenter Server *of* met verschillende ESXi-hosts. Vermijd gevallen waarbij één agent rechtstreeks is verbonden met een ESXi en een andere agent is verbonden met de vCenter Server die deze ESXi beheert.

Als u meer dan één agent hebt, raden we af om lokaal gekoppelde opslag te gebruiken (dat wil zeggen om back-ups op te slaan op virtuele schijven die aan de virtuele toepassing zijn toegevoegd). Zie "Een lokaal gekoppelde opslag gebruiken" (p. 729) voor meer informatie.

Automatische DRS voor de agent uitschakelen

Als de virtuele toepassing wordt geïmplementeerd in een vSphere-cluster, moet u de automatische vMotion hiervoor uitschakelen. Ga naar de DRS-instellingen van het cluster, schakel individuele automatiseringsniveaus voor virtuele machines in en stel vervolgens **Automatiseringsniveau** voor de virtuele toepassing in op **Uitgeschakeld**.

De OVF-sjabloon implementeren

1. Klik op **Alle apparaten** > **Toevoegen** > **VMware ESXi** > **Virtual Appliance (OVF)**.
   Het ZIP-archief wordt gedownload naar uw machine.
2. Pak het ZIP-archief uit. De map bevat één .ovf-bestand en twee .vmdk-bestanden.
3. Controleer of deze bestanden toegankelijk zijn vanaf de machine met vSphere Client.
4. Start vSphere Client en meld u aan bij vCenter Server.
5. Implementeer de OVF-sjabloon.
   - Als er een gedeelde gegevensopslag bestaat, selecteert u deze wanneer u opslag configureert. De indeling van de schijf (thick of thin) heeft geen invloed op de prestaties van de toepassing.
   - Bij het configureren van netwerkverbindingen moet u een netwerk selecteren dat een internetverbinding mogelijk maakt, zodat de agent zich correct in de cloud kan registreren.

De virtuele toepassing configureren

Na implementatie van de virtuele toepassing moet u deze configureren, zodat deze toegang heeft tot zowel vCenter Server of de ESXi-host en tot de Cyber Protection-service.

De virtuele toepassing configureren

1. Ga naar vSphere Client en open de console van de virtuele toepassing.
2. Controleer of de netwerkverbinding is geconfigureerd.

   De verbinding wordt automatisch geconfigureerd via Dynamic Host Configuration Protocol (DHCP).

   Als u de standaardconfiguratie wilt wijzigen, gaat u in **Agentopties** naar het veld **eth0** en vervolgens klikt u op **Wijzigen** en geeft u de gewenste netwerkinstellingen op.
3. Verbind de virtuele toepassing met vCenter Server of de ESXi-host.
   a. Ga in **Agentopties** naar het veld **vCenter/ESX(i)**, klik op **Wijzigen** en geef vervolgens het volgende op.
      - [Als u vCenter Server gebruikt] De naam of het IP-adres van vCenter Server.
      - [Als u vCenter Server niet gebruikt] De naam of het IP-adres van de ESXi-host waarop u een back-up wilt maken en virtuele machines wilt herstellen. Als u snellere back-ups wilt, implementeert u de virtuele toepassing op dezelfde host.
      - De referenties waarmee de toepassing verbinding kan maken met vCenter Server of de ESXi-host.

        We raden u aan een speciaal account te gebruiken voor toegang tot vCenter Server of de ESXi-host, in plaats van een bestaand account met de rol Beheerder. Voor meer informatie: zie "Vereiste bevoegdheden voor Agent voor VMware" (p. 735).

   b. Klik op **Verbinding controleren** om te controleren of de instellingen juist zijn.
   c. Klik op **OK**.
4. Registreer de toepassing in de Cyber Protection-service via een van de volgende methoden.
   - [Alleen voor tenants zonder tweeledige verificatie] Registreer de toepassing in de grafische interface.
     a. Ga naar **Agentopties** en klik in het veld **Beheerserver** op **Wijzigen**.
     b. Ga naar het veld **Servernaam/IP** en selecteer **Cloud**.

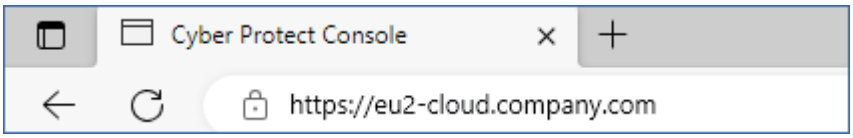
        Het serviceadres van Cyber Protection wordt weergegeven. Wijzig dit adres niet tenzij anders wordt aangegeven.
     c. Ga naar de velden **Gebruikersnaam** en **Wachtwoord** en geef de referenties op voor uw account in de Cyber Protection-service. De virtuele toepassing en de virtuele machines die met de toepassing worden beheerd, worden geregistreerd voor dit account.
     d. Klik op **OK**.
   - Registreer de toepassing in de opdrachtregelinterface.

     Opmerking
     Bij deze methode hebt u een registratietoken nodig. Voor meer informatie over hoe u er een kunt genereren: zie "Een registratietoken genereren" (p. 126).

     a. Druk op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
     b. Voer de volgende opdracht uit:

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

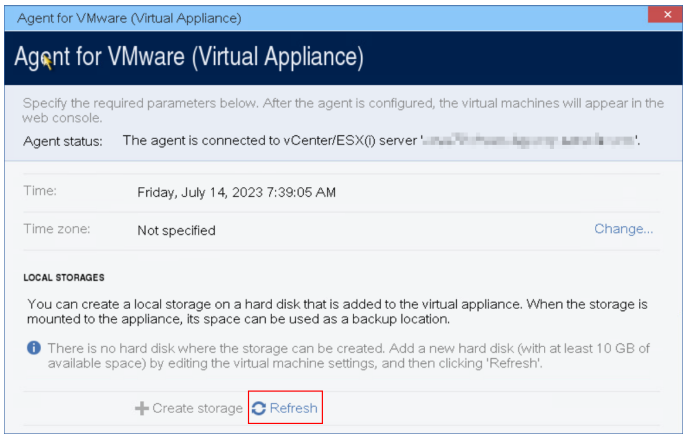
Opmerking
Wanneer u een registratietoken gebruikt, moet u het exacte adres van het datacenter opgeven. Dit is de URL die u ziet **nadat u zich hebt aangemeld** bij de Cyber Protect-console. Bijvoorbeeld: `https://eu2-cloud.company.com`.



In dit geval moet u niet `https://cloud.company.com` gebruiken.

c. Druk op ALT+F1 om terug te gaan naar de grafische interface van de toepassing.

5. [Optioneel] Voeg lokale opslag toe.
   a. Ga naar vSphere Client en koppel een virtuele schijf aan de virtuele toepassing. De virtuele schijf moet minimaal 10 GB vrije schijfruimte hebben.
   b. Klik in de grafische gebruikersinterface van de toepassing op **Vernieuwen**.



   De knop **Opslag maken** wordt actief.
   c. Klik op **Opslag maken.**
   d. Geef een label op voor de opslag en klik op **OK**.
   e. Bevestig uw keuze door te klikken op **Ja**.

6. [Als een proxyserver is ingeschakeld in uw netwerk] Configureer de proxyserver.
   a. Druk op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
   b. Open het bestand **/etc/Acronis/Global.config** in een teksteditor.
   c. Voer een van de volgende handelingen uit:
      - Als de proxyinstellingen zijn opgegeven tijdens de installatie van agenten, gaat u naar het volgende gedeelte:

```
<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>
```

- Kopieer anders de bovenstaande regels en plak deze in het bestand tussen de tags `<registry name="Global">...</registry>`.

d. Vervang `ADDRESS` door de nieuwe waarden voor de hostnaam/het IP-adres van de proxyserver en vervang `PORT` door de decimale waarde van het poortnummer.

e. Als uw proxyserver verificatie vereist, vervangt u `LOGIN` en `PASSWORD` door de referenties van de proxyserver. Zo niet, dan kunt u deze regels verwijderen uit het bestand.

f. Sla het bestand op.

g. Open het bestand **/opt/acronis/etc/aakore.yaml** in een teksteditor.

h. Zoek het gedeelte **env** of maak dit en voeg de volgende regels toe:

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

i. Vervang `proxy_login` en `proxy_password` door de referenties van de proxyserver en vervang `proxy_address:port` door het adres en poortnummer van de proxyserver.

j. Voer de opdracht `reboot` uit.

Opmerking

Als u een virtuele toepassing wilt bijwerken die achter een proxy is geïmplementeerd, bewerkt u het bestand `config.yaml` van de toepassing (`/opt/acronis/etc/va-updater/config.yaml`) door de volgende regel toe te voegen onderaan dat bestand en vervolgens de waarden in te voeren die specifiek zijn voor uw omgeving:

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

Bijvoorbeeld:

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

Agent voor Scale Computing HC3 (Virtual Appliance) implementeren ...

Voordat u start

Deze toepassing is een vooraf geconfigureerde virtuele machine die u implementeert in een Scale Computing HC3-cluster. Deze bevat een beveiligingsagent waarmee u cyberbescherming kunt beheren voor alle virtuele machines in het cluster.

Systeemvereisten voor de agent

Standaard gebruikt de virtuele machine met de agent 2 vCPU's en 4 GiB RAM. Deze instellingen zijn voldoende voor de meeste bewerkingen, maar u kunt ze wijzigen door de virtuele machine te bewerken in de Scale Computing HC3-webinterface.

Als u de back-upprestaties wilt verbeteren en storingen als gevolg van onvoldoende RAM-geheugen wilt voorkomen, raden we aan om deze resources uit te breiden naar 4 vCPU's en 8 GiB RAM voor veeleisende gevallen. U kunt de toegewezen resources bijvoorbeeld uitbreiden wanneer u verwacht dat het back-upverkeer meer dan 100 MB per seconde zal bedragen (bijvoorbeeld in netwerken van 10 gigabit) of als u tegelijkertijd een back-up maakt van meerdere virtuele machines met grote harde schijven (500 GB of meer).

De grootte van de virtuele schijf van de toepassing is ongeveer 9 GB.

Hoeveel agenten heb ik nodig?

Eén agent kan het hele cluster beschermen. U kunt echter meer dan één agent in het cluster hebben als u de bandbreedtebelasting voor back-upverkeer wilt verdelen.

Als u meer dan één agent in een cluster hebt, worden de virtuele machines automatisch gelijkmatig over de agenten verdeeld, zodat elke agent een vergelijkbaar aantal machines beheert.

Een automatische herdistributie wordt uitgevoerd telkens wanneer er een verschil van 20 procent is in de taakverdeling tussen agenten. Dit kan gebeuren nadat u een machine of een agent hebt toegevoegd of verwijderd. U beseft bijvoorbeeld dat u meer agenten nodig hebt om te helpen met de doorvoer en u implementeert een extra virtuele toepassing in het cluster. De beheerserver wijst de geschiktste machines toe aan de nieuwe agent. De belasting van de oude agents wordt minder. Wanneer u een agent verwijdert uit de beheerserver, worden de aan de agent toegewezen machines herverdeeld over de resterende agenten. Dit gebeurt echter niet als een agent beschadigd raakt of handmatig wordt verwijderd uit het Scale Computing HC3-cluster. De herdistributie begint pas nadat u die agent hebt verwijderd uit de Cyber Protect-console.

Controleren door welke agent een specifieke machine word beheerd

1. Klik in de Cyber Protect-console op **Apparaten** en selecteer vervolgens **Scale Computing**.
2. Klik op het tandwielpictogram in de rechterbovenhoek van de tabel en schakel onder **Systeem** het selectievakje **Agent** in.
3. Vink de naam van de agent aan in de kolom die wordt weergegeven.

De QCOW2-sjabloon implementeren

1. Meld u aan bij uw Cyber Protection-account.
2. Klik op **Apparaten** > **Alle apparaten** > **Toevoegen** > **Scale Computing HC3**.
   Het ZIP-archief wordt gedownload naar uw machine.

3. Pak het .zip-archief uit en sla het .qcow2-bestand en het .xml-bestand op in een map met de naam **ScaleAppliance**.
4. Upload de map **ScaleAppliance** naar een netwerkshare en controleer of het Scale Computing HC3-cluster hiertoe toegang heeft.
5. Meld u aan bij het Scale Computing HC3-cluster als beheerder met de rol **VM maken/bewerken**. Zie "Agent voor Scale Computing HC3 (Virtual Appliance) – vereiste rollen" (p. 151) voor meer informatie over de vereiste rollen voor bewerkingen met virtuele Scale Computing HC3-machines.
6. Importeer in de Scale Computing HC3-webinterface de sjabloon voor de virtuele machine uit de map **ScaleAppliance**.
   a. Klik op het pictogram **HC3 VM** importeren.
   b. Geef in het venster **HC3 VM importeren** het volgende op:
      - Een naam voor de nieuwe virtuele machine.
      - De netwerkshare waarop de map **ScaleAppliance** zich bevindt.
      - De gebruikersnaam en het wachtwoord voor toegang tot deze netwerkshare.
      - [Optioneel] Een domeintag voor de nieuwe virtuele machine.
      - Het pad naar de map **ScaleAppliance** op de netwerkshare.
   c. Klik op **Importeren**.

Wanneer de implementatie is voltooid, moet u de virtuele toepassing configureren. Zie "De virtuele toepassing configureren" (p. 148) voor meer informatie over het configureren hiervan.

Opmerking
Als u meer dan één virtuele toepassing nodig hebt in uw cluster, herhaalt u de bovenstaande stappen en implementeert u aanvullende virtuele toepassingen. Kloon geen bestaande virtuele toepassing met de optie voor **VM klonen** in de Scale Computing HC3-webinterface.

De virtuele toepassing configureren

Na implementatie van de virtuele toepassing moet u deze configureren, zodat deze verbinding kan maken zowel met het Scale Computing HC3-cluster dat u hiermee wilt beschermen, als met de Cyber Protection-service.

De virtuele toepassing configureren

1. Meld u aan bij uw Scale Computing HC3-account.
2. Selecteer de virtuele toepassing die u wilt configureren en klik vervolgens op het pictogram **Console**.
3. Configureer de netwerkinterfaces van de toepassing in het veld **eth0**.
   Controleer of automatisch toegewezen DHCP-adressen (indien aanwezig) geldig zijn binnen de netwerken die door uw virtuele machine worden gebruikt, of wijs ze handmatig toe. Afhankelijk van het aantal netwerken dat door het apparaat wordt gebruikt, moet u mogelijk één of meer interfaces configureren.

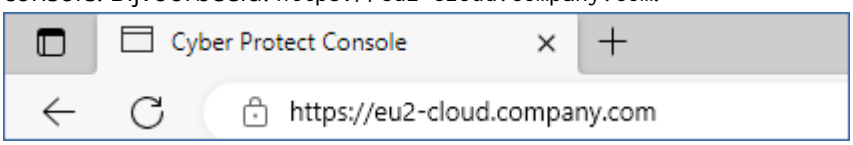
4. Klik in het veld **Scale Computing** op **Wijzigen** om het adres van het Scale Computing HC3-cluster en de referenties voor toegang daartoe op te geven.
   a. Voer in het veld **Servernaam/IP** de DNS-naam of het IP-adres van het cluster in.
   b. Voer in de velden **Gebruikersnaam** en **Wachtwoord** de referenties in voor het account van de Scale Computing HC3-beheerder.
      Controleer of dit account de vereiste rollen voor bewerkingen met virtuele Scale Computing HC3-machines. Zie "Agent voor Scale Computing HC3 (Virtual Appliance) – vereiste rollen" (p. 151) voor meer informatie over deze rollen.
   c. Klik op **Verbinding controleren** om te controleren of de instellingen juist zijn.
   d. Klik op **OK**.
5. Registreer de toepassing in de Cyber Protection-service via een van de volgende methoden.
   - [Alleen voor tenants zonder tweeledige verificatie] Registreer de toepassing in de grafische interface.
     a. Ga naar **Agentopties** en klik in het veld **Beheerserver** op **Wijzigen**.
     b. Ga naar het veld **Servernaam/IP** en selecteer **Cloud**.
        Het serviceadres van Cyber Protection wordt weergegeven. Wijzig dit adres niet tenzij anders wordt aangegeven.
     c. Ga naar de velden **Gebruikersnaam** en **Wachtwoord** en geef de referenties op voor uw account in de Cyber Protection-service. De virtuele toepassing en de virtuele machines die met de toepassing worden beheerd, worden geregistreerd voor dit account.
     d. Klik op **OK**.
   - Registreer de toepassing in de opdrachtregelinterface.

     Opmerking
     Bij deze methode hebt u een registratietoken nodig. Voor meer informatie over hoe u er een kunt genereren: zie "Een registratietoken genereren" (p. 126).

     a. Druk op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
     b. Voer de volgende opdracht uit:

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

     Opmerking
     Wanneer u een registratietoken gebruikt, moet u het exacte adres van het datacenter opgeven. Dit is de URL die u ziet **nadat u zich hebt aangemeld** bij de Cyber Protect-console. Bijvoorbeeld: `https://eu2-cloud.company.com`.

In dit geval moet u niet `https://cloud.company.com` gebruiken.

c. Druk op ALT+F1 om terug te gaan naar de grafische interface van de toepassing.

6. [Optioneel] Klik in het veld **Naam** op **Wijzigen** om de standaardnaam (**localhost**) voor de virtuele toepassing te bewerken. Deze naam wordt weergegeven in de Cyber Protect-console.
7. [Optioneel] Klik in het veld **Tijd** op **Wijzigen** en selecteer vervolgens de tijdzone van uw locatie om te waarborgen dat de geplande bewerkingen op de juiste tijd worden uitgevoerd.
8. [Als een proxyserver is ingeschakeld in uw netwerk] Configureer de proxyserver.
   a. Druk op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
   b. Open het bestand **/etc/Acronis/Global.config** in een teksteditor.
   c. Voer een van de volgende handelingen uit:
      - Als de proxyinstellingen zijn opgegeven tijdens de installatie van agenten, gaat u naar het volgende gedeelte:

        ```
        <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>
        ```

      - Kopieer anders de bovenstaande regels en plak deze in het bestand tussen de tags `<registry name="Global">...</registry>`.
   d. Vervang `ADDRESS` door de nieuwe waarden voor de hostnaam/het IP-adres van de proxyserver en vervang `PORT` door de decimale waarde van het poortnummer.
   e. Als uw proxyserver verificatie vereist, vervangt u `LOGIN` en `PASSWORD` door de referenties van de proxyserver. Zo niet, dan kunt u deze regels verwijderen uit het bestand.
   f. Sla het bestand op.
   g. Open het bestand **/opt/acronis/etc/aakore.yaml** in een teksteditor.
   h. Zoek het gedeelte **env** of maak dit en voeg de volgende regels toe:

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

   i. Vervang `proxy_login` en `proxy_password` door de referenties van de proxyserver en vervang `proxy_address:port` door het adres en poortnummer van de proxyserver.
   j. Voer de opdracht `reboot` uit.

Opmerking

Als u een virtuele toepassing wilt bijwerken die achter een proxy is geïmplementeerd, bewerkt u het bestand `config.yaml` van de toepassing (`/opt/acronis/etc/va-updater/config.yaml`) door de volgende regel toe te voegen onderaan dat bestand en vervolgens de waarden in te voeren die specifiek zijn voor uw omgeving:

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

Bijvoorbeeld:

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

Virtuele machines in het Scale Computing HC3-cluster beschermen

1. Meld u aan bij uw Cyber Protection-account.
2. Ga naar **Apparaten** > **Scale Computing HC3**> <uw cluster> of zoek uw machines in **Apparaten** > **Alle apparaten**.
3. Selecteer machines en pas een beschermingsschema toe op deze machines.

Agent voor Scale Computing HC3 (Virtual Appliance) – vereiste rollen

Dit gedeelte bevat een beschrijving van de vereiste rollen voor bewerkingen met virtuele Scale Computing HC3-machines.

Bewerking	Rol
Een back-up maken van een virtuele machine	Back-up VM maken/bewerken VM verwijderen
Herstellen naar een bestaande virtuele machine	Back-up VM maken/bewerken VM – energiebeheer VM verwijderen Clusterinstellingen
Herstellen naar een nieuwe virtuele machine	Back-up VM maken/bewerken VM – energiebeheer VM verwijderen Clusterinstellingen

Agent voor Virtuozzo Hybrid Infrastructure (Virtual Appliance) implementeren

Voordat u start

Deze toepassing is een vooraf geconfigureerde virtuele machine die u implementeert in Virtuozzo Hybrid Infrastructure. Deze bevat een beveiligingsagent waarmee u cyberbescherming kunt beheren voor alle virtuele machines in een Virtuozzo Hybrid Infrastructure-cluster.

Opmerking
Als u wilt dat back-ups waarvoor de back-upoptie **Volume Shadow Copy Service (VSS) voor virtuele machines** is ingeschakeld, goed worden uitgevoerd en gegevens in applicatieconsistente status worden vastgelegd, controleert u of Virtuozzo Guest Tools zijn geïnstalleerd en bijgewerkt op de beschermde virtuele machines.

Systeemvereisten voor de agent

Bij de implementatie van de virtuele toepassing kunt u kiezen tussen verschillende vooraf gedefinieerde combinaties van vCPU's en RAM (varianten). U kunt ook uw eigen varianten maken.

2 vCPU's en 4 GB RAM (gemiddelde variant) zijn optimaal en voldoende voor de meeste bewerkingen. Als u de back-upprestaties wilt verbeteren en storingen als gevolg van onvoldoende RAM-geheugen wilt voorkomen, raden we aan om deze resources uit te breiden naar 4 vCPU's en 8 GB RAM voor veeleisende gevallen. U kunt de toegewezen resources bijvoorbeeld uitbreiden wanneer u verwacht dat het back-upverkeer meer dan 100 MB per seconde zal bedragen (bijvoorbeeld in netwerken van 10 gigabit) of als u tegelijkertijd een back-up maakt van meerdere virtuele machines met grote harde schijven (500 GB of meer).

Hoeveel agenten heb ik nodig?

Eén agent kan het hele cluster beschermen. U kunt echter meer dan één agent in het cluster hebben als u de bandbreedtebelasting voor back-upverkeer wilt verdelen.

Als u meer dan één agent in een cluster hebt, worden de virtuele machines automatisch gelijkmatig over de agenten verdeeld, zodat elke agent een vergelijkbaar aantal machines beheert.

Een automatische herdistributie wordt uitgevoerd telkens wanneer er een verschil van 20 procent is in de taakverdeling tussen agenten. Dit kan gebeuren nadat u een machine of een agent hebt toegevoegd of verwijderd. U beseft bijvoorbeeld dat u meer agenten nodig hebt om te helpen met de doorvoer en u implementeert een extra virtuele toepassing in het cluster. De beheerserver wijst de geschiktste machines toe aan de nieuwe agent. De belasting van de oude agents wordt minder. Wanneer u een agent verwijdert uit de beheerserver, worden de aan de agent toegewezen machines herverdeeld over de resterende agenten. Dit gebeurt echter niet als een agent beschadigd raakt of handmatig wordt verwijderd uit het Virtuozzo Hybrid Infrastructure-knooppunt. De herdistributie begint pas nadat u die agent uit de Cyber Protection-webinterface hebt verwijderd.

Controleren door welke agent een specifieke machine word beheerd

1. Klik in de Cyber Protect-console op **Apparaten** en selecteer vervolgens **Virtuozzo Hybrid Infrastructure**.
2. Klik op het tandwielpictogram in de rechterbovenhoek van de tabel en schakel onder **Systeem** het selectievakje **Agent** in.
3. Vink de naam van de agent aan in de kolom die wordt weergegeven.

Beperkingen

- De Virtuozzo Hybrid Infrastructure-toepassing kan niet op afstand worden geïmplementeerd.
- Applicatiegerichte back-up van virtuele machines wordt niet ondersteund.

Netwerken configureren in Virtuozzo Hybrid Infrastructure

Voordat u de virtuele toepassing implementeert en configureert, moeten de netwerken in Virtuozzo Hybrid Infrastructure zijn geconfigureerd.

Netwerkvereisten voor de Agent voor Virtuozzo Hybrid Infrastructure (Virtual Appliance)

- Voor de virtuele toepassing zijn 2 netwerkadapters vereist.
- De virtuele toepassing moet worden verbonden met Virtuozzo-netwerken via de volgende typen netwerkverkeer:
  - Compute-API
  - VM-back-up
  - ABGW openbaar
  - VM openbaar

Zie Clustervereisten berekenen in de Virtuozzo-documentatie voor meer informatie over het configureren van de netwerken.

Gebruikersaccounts configureren in Virtuozzo Hybrid Infrastructure

Als u de virtuele toepassing wilt configureren, hebt u een gebruikersaccount voor Virtuozzo Hybrid Infrastructure nodig. Dit account moet de rol **Beheerder** hebben in het **Standaard**domein. Zie Gebruikers met beheerdersrechten beheren in de Virtuozzo Hybrid Infrastructure-documentatie voor meer informatie over gebruikers. Controleer of dit account toegang heeft tot alle projecten in het **Standaard**domein.

Toegang tot alle projecten verlenen in het Standaarddomein

1. Maak een omgevingsbestand voor de systeembeheerder. Gebruik hiervoor de OpenStack-opdrachtregelinterface om het volgende script uit te voeren in het Virtuozzo Hybrid Infrastructure-cluster. Zie Verbinding maken met de OpenStack-opdrachtregelinterface in de Virtuozzo Hybrid Infrastructure-documentatie voor meer informatie over de verbinding met deze interface.

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

2. Gebruik het omgevingsbestand om verdere OpenStack-opdrachten te autoriseren:

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

3. Voer de volgende opdrachten uit:

```
openstack --insecure user set --project admin --project-domain Default --domain
Default <username>
openstack --insecure role add --domain Default --user <username> --user-domain
Default compute --inherited
```

<gebruikersnaam> is het Virtuozzo Hybrid Infrastructure-account met de rol **Beheerder** in het **Standaard**domein. Dit account wordt door de virtuele toepassing gebruikt voor back-up en herstel van de virtuele machines in elk onderliggend project onder het **Standaard**domein.

Voorbeeld

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

Als u back-ups voor virtuele machines in een ander domein dan het **Standaard**domein wilt beheren, voert u ook de volgende opdracht uit.

Toegang tot alle projecten verlenen in een ander domein

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

<domeinnaam> is het domein met de projecten waartoe het account van <gebruikersnaam> toegang krijgt.

Voorbeeld

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

Controleer, wanneer toegang tot projecten is verleend, welke rollen aan het account zijn toegewezen.

Toegewezen rollen controleren

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

<gebruikersnaam> is het Virtuozzo Hybrid Infrastructure-account.

Voorbeeld

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | MyNewDomain |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

In dit voorbeeld worden de opties `-c Role`, `-c User`, `-c Project` en `-c Domain` gebruikt om de uitvoer van de opdracht in te korten zodat deze op de pagina past.

Als u wilt controleren welke effectieve rollen zijn toegewezen aan het account in alle projecten, voert u ook de volgende opdracht uit.

Effectieve rollen in alle projecten controleren

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

<gebruikersnaam> is het Virtuozzo Hybrid Infrastructure-account.

Voorbeeld

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

```
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

In dit voorbeeld worden de opties `-c Role`, `-c User`, `-c Project` en `-c Domain` gebruikt om de uitvoer van de opdracht in te korten zodat deze op de pagina past.

De QCOW2-sjabloon implementeren

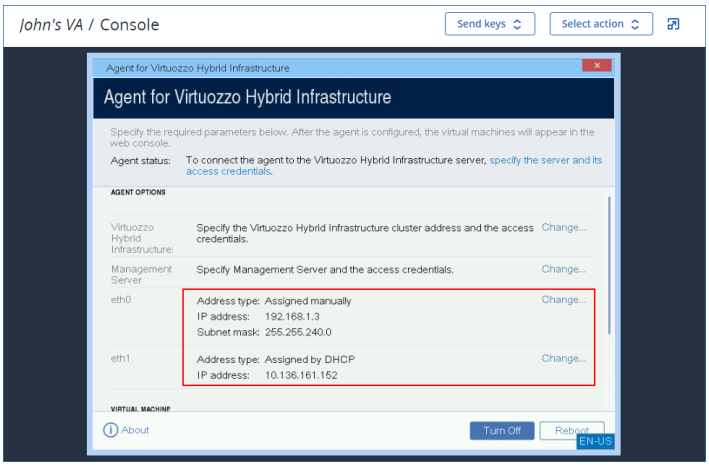
1. Meld u aan bij uw Cyber Protection-account.
2. Klik op **Apparaten** > **Alle apparaten** > **Toevoegen** > **Virtuozzo Hybrid Infrastructure**.
   Het ZIP-archief wordt gedownload naar uw machine.
3. Pak het ZIP-archief uit. Het bevat een .qcow2-imagebestand.
4. Meld u aan bij uw Virtuozzo Hybrid Infrastructure-account.
5. Voeg het imagebestand .qcow2 als volgt toe aan het compute-cluster van Virtuozzo Hybrid Infrastructure:
   - Ga naar **Compute** > **Virtuele machines** > tabblad **Images** en klik op **Image toevoegen**.
   - Klik in het venster **Image toevoegen** op **Bladeren** en selecteer vervolgens het .qcow2-bestand.
   - Geef de naam van de image op, selecteer het type **Algemeen Linux OS** en klik vervolgens op **Toevoegen**.
6. Ga naar **Compute** > **Virtuele machines** > tabblad **Virtuele machines** en klik op **Virtuele machine maken**. Er wordt een venster geopend waarin u de volgende parameters moet opgeven:
   - Een naam voor de nieuwe virtuele machine.
   - Kies in **Implementeren vanaf** de optie **Image**.
   - Selecteer in het venster **Images** het .qcow2-imagebestand van de toepassing en klik vervolgens op **Gereed**.
   - In het venster **Volumes** hoeft u geen volumes toe te voegen. Het volume dat automatisch wordt toegevoegd voor de systeemschijf, is voldoende.
   - Kies in het venster **Variant** de gewenste combinatie van vCPU's en RAM en klik vervolgens op **Gereed**. Doorgaans zijn 2 vCPU's en 4 GB RAM voldoende.
   - Klik in het venster **Netwerkinterfaces** op **Toevoegen**, selecteer het virtuele netwerk van het type *openbaar* en klik vervolgens op **Toevoegen**. Uw keuze wordt nu weergegeven in de lijst **Netwerkinterfaces**.
     Als u een installatie gebruikt met meer dan één fysiek netwerk (en dus met meer dan één virtueel netwerk van het type openbaar), herhaalt u deze stap en selecteert u de virtuele netwerken die u nodig hebt.
7. Klik op **Gereed**.
8. Wanneer u weer terug bent in het venster **Virtuele machine maken**, klikt u op **Implementeren** om de virtuele machine te maken en op te starten.

De virtuele toepassing configureren

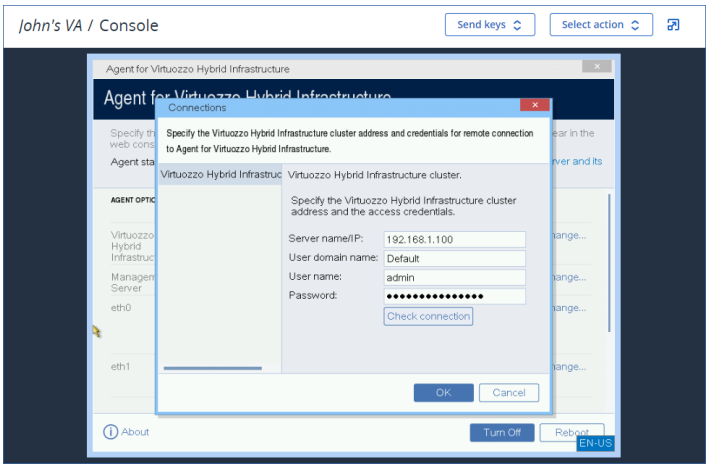
Na implementatie van de Agent voor Virtuozzo Hybrid Infrastructure (Virtual Appliance) moet u de virtuele toepassing configureren zodat deze verbinding kan maken zowel met het Virtuozzo Hybrid Infrastructure-cluster dat u hiermee wilt beschermen, als met de Cyber Protection-cloudservice.

De virtuele toepassing configureren

1. Meld u aan bij uw Virtuozzo Hybrid Infrastructure-account.
2. Ga naar **Compute** > **Virtuele machines** > tabblad **Virtuele machines** en selecteer de virtuele machine die u hebt gemaakt. Klik vervolgens op **Console**.
3. Configureer de netwerkinterfaces van de toepassing. Mogelijk moet u een of meer interfaces configureren, dit hangt af van het aantal virtuele netwerken dat door de toepassing worden gebruikt. Controleer of automatisch toegewezen DHCP-adressen (indien aanwezig) geldig zijn binnen de netwerken die door uw virtuele machine worden gebruikt, of wijs ze handmatig toe.



4. Geef het adres en de referenties van het Virtuozzo-cluster op:
   - DNS-naam of IP-adres van het Virtuozzo Hybrid Infrastructure-cluster (dit is het adres van het beheerknooppunt van het cluster). De standaardpoort 5000 wordt automatisch ingesteld. Als u een andere poort gebruikt, moet u deze handmatig opgeven.
   - Voer in het veld **Gebruikersdomeinnaam** uw domein in Virtuozzo Hybrid Infrastructure in. Bijvoorbeeld: **Standaard**.
     De domeinnaam is hoofdlettergevoelig.
   - Voer in de velden **Gebruikersnaam** en **Wachtwoord** de referenties in voor het Virtuozzo Hybrid Infrastructure-gebruikersaccount met de rol **Beheerder** in het opgegeven domein. Zie Gebruikersaccounts configureren in Virtuozzo Hybrid Infrastructure voor meer informatie over gebruikers, rollen en domeinen.



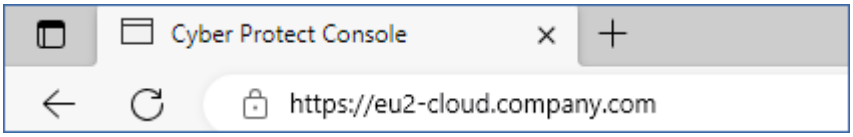
5. Registreer de toepassing in de Cyber Protection-service via een van de volgende methoden.
   - [Alleen voor tenants zonder tweeledige verificatie] Registreer de toepassing in de grafische interface.
     a. Ga naar **Agentopties** en klik in het veld **Beheerserver** op **Wijzigen**.
     b. Ga naar het veld **Servernaam/IP** en selecteer **Cloud**.
        Het serviceadres van Cyber Protection wordt weergegeven. Wijzig dit adres niet tenzij anders wordt aangegeven.
     c. Ga naar de velden **Gebruikersnaam** en **Wachtwoord** en geef de referenties op voor uw account in de Cyber Protection-service. De virtuele toepassing en de virtuele machines die met de toepassing worden beheerd, worden geregistreerd voor dit account.
     d. Klik op **OK**.
   - Registreer de toepassing in de opdrachtregelinterface.

     Opmerking
     Bij deze methode hebt u een registratietoken nodig. Voor meer informatie over hoe u er een kunt genereren: zie "Een registratietoken genereren" (p. 126).

     a. Druk op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
     b. Voer de volgende opdracht uit:

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

     Opmerking
     Wanneer u een registratietoken gebruikt, moet u het exacte adres van het datacenter opgeven. Dit is de URL die u ziet **nadat u zich hebt aangemeld** bij de Cyber Protect-console. Bijvoorbeeld: `https://eu2-cloud.company.com`.

In dit geval moet u niet `https://cloud.company.com` gebruiken.

c. Druk op ALT+F1 om terug te gaan naar de grafische interface van de toepassing.

6. [Als een proxyserver is ingeschakeld in uw netwerk] Configureer de proxyserver.
   a. Druk op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
   b. Open het bestand **/etc/Acronis/Global.config** in een teksteditor.
   c. Voer een van de volgende handelingen uit:
      - Als de proxyinstellingen zijn opgegeven tijdens de installatie van agenten, gaat u naar het volgende gedeelte:

        ```
        <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>
        ```

      - Kopieer anders de bovenstaande regels en plak deze in het bestand tussen de tags `<registry name="Global">...</registry>`.
   d. Vervang `ADDRESS` door de nieuwe waarden voor de hostnaam/het IP-adres van de proxyserver en vervang `PORT` door de decimale waarde van het poortnummer.
   e. Als uw proxyserver verificatie vereist, vervangt u `LOGIN` en `PASSWORD` door de referenties van de proxyserver. Zo niet, dan kunt u deze regels verwijderen uit het bestand.
   f. Sla het bestand op.
   g. Open het bestand **/opt/acronis/etc/aakore.yaml** in een teksteditor.
   h. Zoek het gedeelte **env** of maak dit en voeg de volgende regels toe:

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

   i. Vervang `proxy_login` en `proxy_password` door de referenties van de proxyserver en vervang `proxy_address:port` door het adres en poortnummer van de proxyserver.
   j. Voer de opdracht `reboot` uit.

Opmerking

Als u een virtuele toepassing wilt bijwerken die achter een proxy is geïmplementeerd, bewerkt u het bestand `config.yaml` van de toepassing (`/opt/acronis/etc/va-updater/config.yaml`) door de volgende regel toe te voegen onderaan dat bestand en vervolgens de waarden in te voeren die specifiek zijn voor uw omgeving:

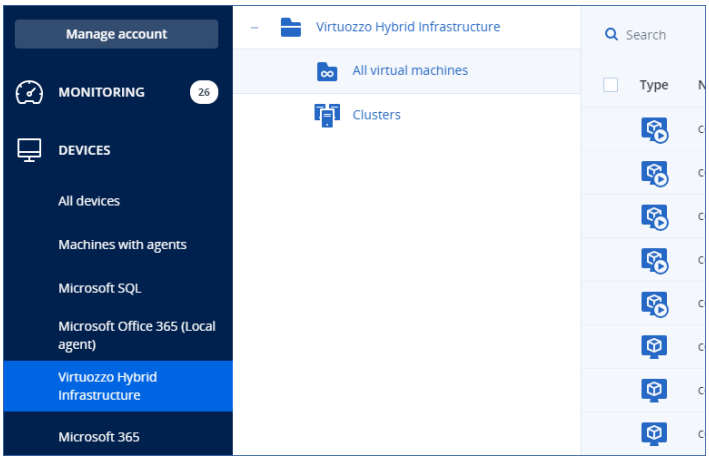
```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Bijvoorbeeld:

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

De virtuele machines in het Virtuozzo Hybrid Infrastructure-cluster beschermen

1. Meld u aan bij uw Cyber Protection-account.
2. Ga naar **Apparaten** > **Virtuozzo Hybrid Infrastructure**> <uw cluster> > **Standaardproject** > **admin** of zoek uw machines in **Apparaten** > **Alle apparaten**.
3. Selecteer machines en pas een beschermingsschema toe op deze machines.



Agent voor oVirt (Virtual Appliance) implementeren ...

Voordat u start

Deze toepassing is een vooraf geconfigureerde virtuele machine die u implementeert in een Red Hat Virtualization/oVirt-datacenter. De toepassing bevat een beveiligingsagent waarmee u cyberbescherming kunt beheren voor alle virtuele machines in het datacenter.

Systeemvereisten voor de agent

Standaard gebruikt de virtuele machine met de agent 2 vCPU's en 4 GiB RAM. Deze instellingen zijn voldoende voor de meeste bewerkingen, maar u kunt ze bewerken in de Red Hat Virtualization/oVirt-beheerportal.

Als u de back-upprestaties wilt verbeteren en storingen als gevolg van onvoldoende RAM-geheugen wilt voorkomen, raden we aan om deze resources uit te breiden naar 4 vCPU's en 8 GiB RAM voor veeleisende gevallen. U kunt de toegewezen resources bijvoorbeeld uitbreiden wanneer u verwacht dat het back-upverkeer meer dan 100 MB per seconde zal bedragen (bijvoorbeeld in netwerken van 10 gigabit) of als u tegelijkertijd een back-up maakt van meerdere virtuele machines met grote harde schijven (500 GB of meer).

De grootte van de virtuele schijf van de toepassing is 8 GiB.

Hoeveel agenten heb ik nodig?

Eén agent kan het hele datacenter beschermen. U kunt echter meer dan één agent in het datacenter hebben als u de bandbreedtebelasting van het back-upverkeer wilt verdelen.

Als u meer dan één agent in het datacenter hebt, worden de virtuele machines automatisch verdeeld over de agenten, zodat elke agent een vergelijkbaar aantal machines beheert.

Een automatische herdistributie wordt uitgevoerd telkens wanneer er een verschil van 20 procent is in de taakverdeling tussen agenten. Dit kan gebeuren nadat u een machine of een agent hebt toegevoegd of verwijderd. U beseft bijvoorbeeld dat u meer agenten nodig hebt om te helpen met de doorvoer en u implementeert een extra virtuele toepassing in het datacenter. De beheerserver wijst de geschiktste machines toe aan de nieuwe agent. De belasting van de oude agents wordt minder. Wanneer u een agent verwijdert, worden de machines die aan de agent zijn toegewezen, verdeeld onder de resterende agenten. Dit gebeurt echter niet als een agent beschadigd raakt of handmatig wordt verwijderd uit de Red Hat Virtualization/oVirt-beheerportal. De herdistributie begint pas nadat u die agent hebt verwijderd uit de Cyber Protect-console.

Controleren door welke agent een specifieke machine word beheerd

1. Klik in de Cyber Protect-console op **Apparaten** en selecteer vervolgens **oVirt**.
2. Klik op het tandwielpictogram in de rechterbovenhoek van de tabel en schakel onder **Systeem** het selectievakje **Agent** in.
3. Vink de naam van de agent aan in de kolom die wordt weergegeven.

Beperkingen

De volgende bewerkingen worden niet ondersteund voor virtuele Red Hat Virtualization/oVirt-machines:

- Applicatiegerichte back-up
- Een virtuele machine uitvoeren vanaf een back-up
- Replicatie van virtuele machines
- Gewijzigde blokken bijhouden

De OVA-sjabloon implementeren

1. Meld u aan bij uw Cyber Protection-account.
2. Klik op **Apparaten** > **Alle apparaten** > **Toevoegen** > **Red Hat Virtualization (oVirt)**.
   Het ZIP-archief wordt gedownload naar uw machine.
3. Pak het ZIP-archief uit. Het bevat één .ova-bestand.
4. Upload het .ova-bestand naar een host in het Red Hat Virtualization/oVirt-datacenter dat u wilt beschermen.
5. Meld u als beheerder aan bij de Red Hat Virtualization/oVirt-beheerportal. Zie "Agent voor oVirt – vereiste rollen en poorten" (p. 166) voor meer informatie over de vereiste rollen voor bewerkingen met virtuele machines.
6. Selecteer in het navigatiemenu **Compute** > **Virtuele machines**.
7. Klik op het pictogram van de verticale ellips  boven de hoofdtabel en klik vervolgens op **Importeren**.
8. Doe het volgende in het venster **Virtuele machine(s) importeren**:
   a. Selecteer in **Datacenter** het datacenter dat u wilt beschermen.
   b. Selecteer in **Bron** de optie **Virtual Appliance (OVA)**.
   c. Selecteer in **Host** de host waarop u het .ova-bestand hebt geüpload.
   d. Geef in **Bestandspad** het pad op naar de map die het .ova-bestand bevat.
   e. Klik op **Laden**.
      De sjabloon voor oVirt (Virtual Appliance) uit het .ova-bestand wordt weergegeven in het deelvenster **Virtuele machines in bron**.
      Als de sjabloon niet wordt weergegeven in dit deelvenster, controleert u of u het juiste pad naar het bestand hebt opgegeven, of het bestand niet is beschadigd en of de host kan worden bereikt.
   f. Selecteer in **Virtuele machines in bron** de sjabloon voor oVirt (Virtual Appliance) en klik vervolgens op de pijl-rechts.
      De sjabloon wordt weergegeven in het deelvenster **Virtuele machines om te importeren**.
   g. Klik op **Volgende**.
9. Klik in het nieuwe venster op de naam van de toepassing en configureer vervolgens de volgende instellingen:
   - Configureer de netwerkinterfaces op het tabblad **Netwerkinterfaces**.
   - [Optioneel] Wijzig op het tabblad **Algemeen** de standaardnaam van de virtuele machine met de agent.

De implementatie is nu voltooid. Vervolgens moet u de virtuele toepassing configureren. Zie "De virtuele toepassing configureren" (p. 163) voor meer informatie over het configureren hiervan.

Opmerking
Als u meer dan één virtuele toepassing nodig hebt in uw datacenter, herhaalt u de bovenstaande stappen en implementeert u aanvullende virtuele toepassingen. Kloon geen bestaande virtuele toepassing met de optie voor **VM klonen** in de Red Hat Virtualization/oVirt-beheerportal.

Als u de virtuele toepassing wilt uitsluiten van back-ups van de dynamische groep, moet u deze ook uitsluiten van de lijst met virtuele machines in de Cyber Protect-console. Als u deze wilt uitsluiten, selecteert u in de Red Hat Virtualization/oVirt-beheerportal de virtuele machine met de agent en wijst u hieraan vervolgens de tag `acronis_virtual_appliance` toe.

De virtuele toepassing configureren

Na implementatie van de virtuele toepassing moet u deze configureren, zodat deze verbinding kan maken zowel met de oVirt-engine als met de Cyber Protection-service.

De virtuele toepassing configureren

1. Meld u aan bij de Red Hat Virtualization/oVirt-beheerportal.
2. Selecteer de virtuele toepassing die u wilt configureren en klik vervolgens op het pictogram **Console**.
3. Configureer de netwerkinterfaces van de toepassing in het veld **eth0**.
   Controleer of automatisch toegewezen DHCP-adressen (indien aanwezig) geldig zijn binnen de netwerken die door uw virtuele machine worden gebruikt, of wijs ze handmatig toe. Afhankelijk van het aantal netwerken dat door het apparaat wordt gebruikt, moet u mogelijk één of meer interfaces configureren.
4. Klik in het veld **oVirt** op **Wijzigen** om het adres van de oVirt-engine en de referenties voor toegang op te geven:
   a. Voer in het veld **Servernaam/IP** de DNS-naam of het IP-adres van de engine in.
   b. Voer in de velden **Gebruikersnaam** en **Wachtwoord** de beheerdersreferenties voor deze engine in.
      Controleer of dit beheerdersaccount de vereiste rollen heeft voor bewerkingen met virtuele Red Hat Virtualization/oVirt-machines. Zie "Agent voor oVirt – vereiste rollen en poorten" (p. 166) voor meer informatie over deze rollen.
      Als Keycloak de Single-Sign-On (SSO)-provider is voor de oVirt-engine (standaard in oVirt 4.5.1), gebruikt u de Keycloak-indeling bij het opgeven van de gebruikersnaam. Geef bijvoorbeeld het standaard beheerdersaccount op als `admin@ovirt@internalsso` in plaats van `admin@internal`.
   c. [Optioneel] Klik op **Verbinding controleren** om te controleren of de verstrekte referenties juist zijn.
   d. Klik op **OK**.
5. Registreer de toepassing in de Cyber Protection-service via een van de volgende methoden.

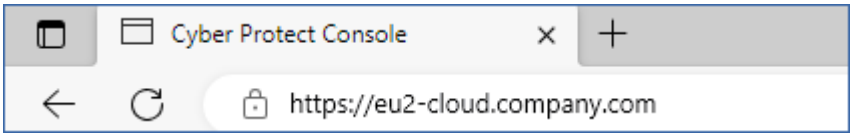
- [Alleen voor tenants zonder tweeledige verificatie] Registreer de toepassing in de grafische interface.
  a. Ga naar **Agentopties** en klik in het veld **Beheerserver** op **Wijzigen**.
  b. Ga naar het veld **Servernaam/IP** en selecteer **Cloud**.
     Het serviceadres van Cyber Protection wordt weergegeven. Wijzig dit adres niet tenzij anders wordt aangegeven.
  c. Ga naar de velden **Gebruikersnaam** en **Wachtwoord** en geef de referenties op voor uw account in de Cyber Protection-service. De virtuele toepassing en de virtuele machines die met de toepassing worden beheerd, worden geregistreerd voor dit account.
  d. Klik op **OK**.
- Registreer de toepassing in de opdrachtregelinterface.

  Opmerking
  Bij deze methode hebt u een registratietoken nodig. Voor meer informatie over hoe u er een kunt genereren: zie "Een registratietoken genereren" (p. 126).

  a. Druk op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
  b. Voer de volgende opdracht uit:

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

  Opmerking
  Wanneer u een registratietoken gebruikt, moet u het exacte adres van het datacenter opgeven. Dit is de URL die u ziet **nadat u zich hebt aangemeld** bij de Cyber Protect-console. Bijvoorbeeld: `https://eu2-cloud.company.com`.

  In dit geval moet u niet `https://cloud.company.com` gebruiken.

  c. Druk op ALT+F1 om terug te gaan naar de grafische interface van de toepassing.

6. [Optioneel] Klik in het veld **Naam** op **Wijzigen** om de standaardnaam (**localhost**) voor de virtuele toepassing te bewerken. Deze naam wordt weergegeven in de Cyber Protect-console.
7. [Optioneel] Klik in het veld **Tijd** op **Wijzigen** en selecteer vervolgens de tijdzone van uw locatie om te waarborgen dat de geplande bewerkingen op de juiste tijd worden uitgevoerd.
8. [Optioneel] [Als een proxyserver is ingeschakeld in uw netwerk] Configureer de proxyserver.
   a. Druk op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
   b. Open het bestand **/etc/Acronis/Global.config** in een teksteditor.

c. Voer een van de volgende handelingen uit:
   - Als de proxyinstellingen zijn opgegeven tijdens de installatie van agenten, gaat u naar het volgende gedeelte:

     ```
     <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>
     ```

   - Kopieer anders de bovenstaande regels en plak deze in het bestand tussen de tags `<registry name="Global">...</registry>`.

d. Vervang `ADDRESS` door de nieuwe waarden voor de hostnaam/het IP-adres van de proxyserver en vervang `PORT` door de decimale waarde van het poortnummer.

e. Als uw proxyserver verificatie vereist, vervangt u `LOGIN` en `PASSWORD` door de referenties van de proxyserver. Zo niet, dan kunt u deze regels verwijderen uit het bestand.

f. Sla het bestand op.

g. Open het bestand **/opt/acronis/etc/aakore.yaml** in een teksteditor.

h. Zoek het gedeelte **env** of maak dit en voeg de volgende regels toe:

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

i. Vervang `proxy_login` en `proxy_password` door de referenties van de proxyserver en vervang `proxy_address:port` door het adres en poortnummer van de proxyserver.

j. Voer de opdracht `reboot` uit.

Opmerking

Als u een virtuele toepassing wilt bijwerken die achter een proxy is geïmplementeerd, bewerkt u het bestand `config.yaml` van de toepassing (`/opt/acronis/etc/va-updater/config.yaml`) door de volgende regel toe te voegen onderaan dat bestand en vervolgens de waarden in te voeren die specifiek zijn voor uw omgeving:

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

Bijvoorbeeld:

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

Virtuele machines in het Red Hat Virtualization/oVirt-datacenter beschermen

1. Meld u aan bij uw Cyber Protection-account.
2. Ga naar **Apparaten** > **oVirt** > <uw cluster> of zoek uw machines in **Apparaten** > **Alle apparaten**.
3. Selecteer machines en pas een beschermingsschema toe op deze machines.

Agent voor oVirt – vereiste rollen en poorten

Vereiste rollen

Voor de implementatie en werking van Agent voor oVirt is een beheerdersaccount vereist met de volgende toegewezen rollen.

oVirt/Red Hat Virtualization 4.2 en 4.3/Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4, 4.5

- SuperUser

Vereiste poorten

Agent voor oVirt maakt verbinding met de oVirt-engine door de URL te gebruiken die u opgeeft wanneer u de virtuele toepassing configureert. Gewoonlijk heeft de URL van de engine de volgende indeling: `https://ovirt.company.com`. In dit geval worden het HTTPS-protocol en poort 443 gebruikt.

Voor andere dan de standaard oVirt-instellingen is mogelijk een andere poort vereist. U kunt de exacte poort vinden door de URL-indeling te analyseren. Bijvoorbeeld:

URL van oVirt-engine	Poort	Protocol
`https://ovirt.company.com/`	443	HTTPS
`http://ovirt.company.com/`	80	HTTP
`https://ovirt.company.com:1234/`	1234	HTTPS

Er zijn geen extra poorten vereist voor lees-/schrijfbewerkingen op de schijf, omdat de back-up wordt uitgevoerd in de HotAdd-modus.

Agent implementeren voor Synology

Voordat u start

Met Agent voor Synology kunt u back-ups maken van bestanden en mappen van en naar Synology NAS-apparaten. De specifieke NAS-eigenschappen en toegangsrechten voor shares, mappen en bestanden blijven behouden.

Agent voor Synology wordt uitgevoerd op het NAS-apparaat. Hierdoor kunt u de resources van het apparaat gebruiken voor gegevensbewerkingen buiten de host, zoals replicatie, validatie en opschoning van back-ups. Zie "Plannen voor gegevensbescherming buiten de host" (p. 224) voor meer informatie over deze bewerkingen.

Opmerking
Agent voor Synology ondersteunt alleen NAS-apparaten met x86_64-processors. ARM-processors worden niet ondersteund.

U kunt een back-up herstellen op de oorspronkelijke locatie of een nieuwe locatie op het NAS-apparaat en in een netwerkmap die toegankelijk is via dat apparaat. Back-ups in de cloudopslag kunnen ook worden hersteld op een NAS-apparaat met Agent voor Synology dat niet het oorspronkelijke NAS-apparaat is.

De onderstaande tabel geeft een overzicht van de beschikbare back-upbronnen en -bestemmingen.

Welke back-ups moeten worden uitgevoerd?	**Items voor back-up (Back-upbron)**	**Waar moeten de back-ups worden uitgevoerd? (Back-upbestemming)**
Bestanden/mappen	Lokale map*	Cloudopslag
		Lokale map*
	Netwerkmap (SMB)**	Netwerkmap (SMB)**
		NFS-map
		Openbare clouds***

* Inclusief USB-stations die op het NAS-apparaat zijn aangesloten.

Opmerking
Versleutelde mappen worden niet ondersteund. Deze mappen worden niet weergegeven in de grafische gebruikersinterface van Cyber Protection.

** Het gebruik van externe netwerkshares als back-upbron of back-upbestemming via het SMB-protocol is alleen beschikbaar voor agents die worden uitgevoerd met Synology DiskStation

Manager 6.2.3 en later. Er kunnen onbeperkte back-ups worden gemaakt van de gegevens die in Synology NAS zelf worden gehost, inclusief gehoste netwerkshares.

*** Back-up naar openbare clouds, zoals Microsoft Azure, Amazon, Wasabi of S3-compatibele opslag, wordt alleen ondersteund door Agent voor Synology 7.x. Agent voor Synology 6.x ondersteunt deze back-upbestemming niet vanwege beperkingen van de Linux-kernel van Synology DSM 6.x.

Beperkingen

- Agent voor Synology ondersteunt alleen NAS-apparaten met x86_64-processors. ARM-processors worden niet ondersteund.
- Back-ups van versleutelde shares worden hersteld als niet-versleuteld.
- Back-upshares waarvoor de optie **Bestandscompressie** is ingeschakeld, worden hersteld met deze optie uitgeschakeld.
- Op een Synology NAS-apparaat kunt u alleen back-ups herstellen die zijn gemaakt door Agent voor Synology.

Het installatieprogramma downloaden

Het installatieprogramma voor Agent voor Synology is beschikbaar als SPK-bestand.

Agent voor Synology 7.x

Het installatieprogramma downloaden:

1. Ga in de Cyber Protect-console, naar **Apparaten** > **Alle apparaten**.
2. Klik in de rechterbovenhoek op **Toevoegen**.
3. Klik onder **Network Attached Storage (NAS)** op **Synology**.
   Het installatieprogramma wordt gedownload naar uw machine.

Agent voor Synology 6.x

Het installatieprogramma downloaden:

1. Ga in de Cyber Protect-console, naar **Apparaten** > **Alle apparaten**.
2. Klik in de rechterbovenhoek op **Toevoegen**.
3. Klik onder **Network Attached Storage (NAS)** op **Synology**.
   Het installatieprogramma voor Agent voor Synology 7.x wordt gedownload naar uw machine.
   U kunt het downloadproces veilig stoppen of het gedownloade bestand negeren.
4. Klik op **Agent voor Synology 6.x downloaden**.
   Het installatieprogramma voor Agent voor Synology 6.x wordt gedownload naar uw machine.

Agent voor Synology installeren

Als u Agent voor Synology wilt installeren, voert u het SPK-bestand uit in Synology DiskStation Manager.

Opmerking
Agent voor Synology ondersteunt alleen NAS-apparaten met x86_64-processors. ARM-processors worden niet ondersteund.

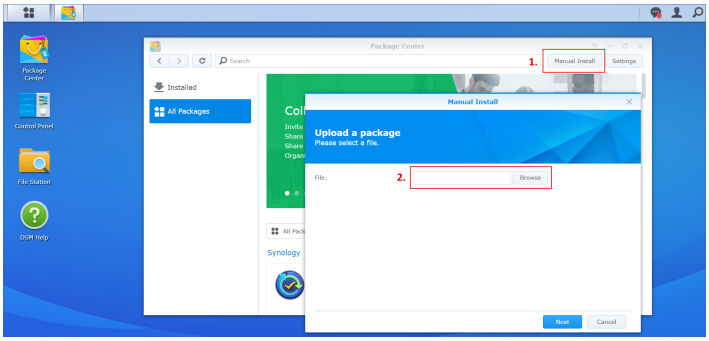
Agent voor Synology 7.x

Vereisten

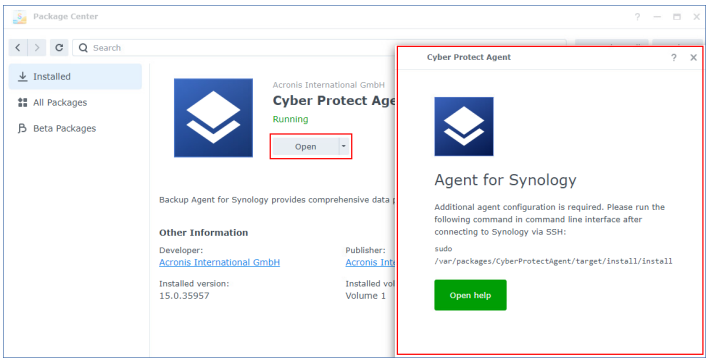
- Op het NAS-apparaat wordt DiskStation Manager 7.x uitgevoerd.
- U bent lid van de groep **administrators** op het NAS-apparaat.
- Er is ten minste 200 MB vrije schijfruimte op het NAS-volume waarop u de agent wilt installeren.
- Er is een SSH-client beschikbaar op uw machine. In dit document wordt Putty als voorbeeld gebruikt.

Agent voor Synology installeren:

1. Meld u aan bij Synology DiskStation Manager.
2. Open **Package Center**.
3. Klik op **Handmatige installatie** en klik vervolgens op **Bladeren**.



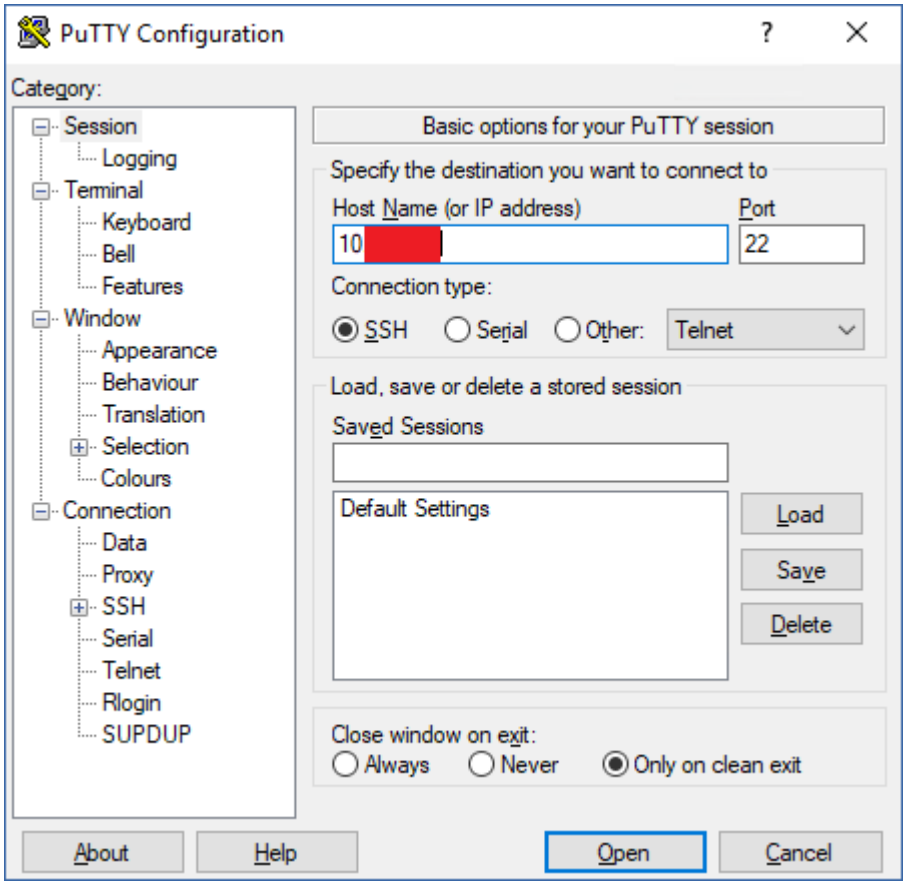
4. Selecteer het SPK-bestand dat u hebt gedownload van de Cyber Protect-console en klik vervolgens op **Volgende**.
   Er wordt een waarschuwing weergegeven dat u een softwarepakket van derden gaat installeren. Dit bericht maakt deel uit van de standaardinstallatieprocedure.
5. U kunt bevestigen dat u het pakket wilt installeren door te klikken op **Akkoord**.
6. Selecteer het volume waarop u de agent wilt installeren en klik op **Volgende**.
7. Controleer de instellingen en klik vervolgens op **Gereed**.
8. Ga naar het **Package Center** van Synology DiskStation Manager, open Cyber Protect Agent voor Synology en controleer vervolgens of u het volgende scherm ziet.



9. Ga naar het **Configuratiescherm** van Synology DiskStation Manager, open **Terminal & SNMP** en schakel vervolgens de SSH-toegang tot het NAS-apparaat in.
10. Voer het `install`-script uit op het NAS-apparaat met behulp van een SSH-client (in dit voorbeeld Putty).

    Het script maakt toegang tot de hoofdmap van DSM 7.0 of later mogelijk (dit is vereist om de agent te configureren).

    a. Start Putty en geef het IP-adres of de hostnaam op van het Synology NAS-apparaat.



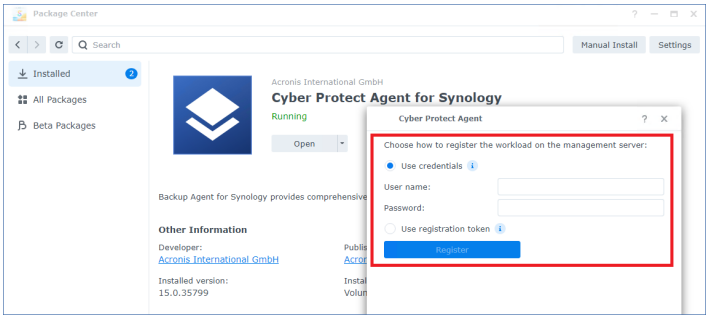
    b. Klik op **Openen** en meld u vervolgens aan als Synology DSM-beheerder.

    c. Voer de volgende opdracht uit.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

Nadat het script is gestart, wacht u 15 seconden totdat de Cyber Protection-services zijn geïnitialiseerd.

11. Ga naar het **Configuratiescherm** van Synology DiskStation Manager, open **Terminal & SNMP** en schakel vervolgens de SSH-toegang tot het NAS-apparaat uit. De SSH-toegang is dan niet meer vereist.
12. Ga naar het **Package Center** van Synology DiskStation Manager en open Cyber Protect Agent voor Synology.
13. Selecteer de registratiemethode.



- [De agent registreren met referenties]
  - In de velden **Gebruikersnaam** en **Wachtwoord** geeft u de referenties op voor het account waarvoor de agent wordt geregistreerd. Dit account kan geen partnerbeheerdersaccount zijn.
- [De agent registreren met een registratietoken]
  - Geef bij **Registratieadres** het exacte adres van het datacentrum op. Het exacte adres van het datacentrum is de URL die u ziet wanneer u zich aanmeldt bij de Cyber Protect-console. Bijvoorbeeld: `https://us5-cloud.acronis.com`.

    Opmerking
    Gebruik geen URL-indeling zonder het adres van het datacenter. Gebruik bijvoorbeeld niet `https://cloud.acronis.com`.

  - Geef in het veld **Token** het registratietoken op.

    Zie "Een registratietoken genereren" (p. 126) voor meer informatie over het genereren van een registratietoken.

14. Klik op **Registreren**.

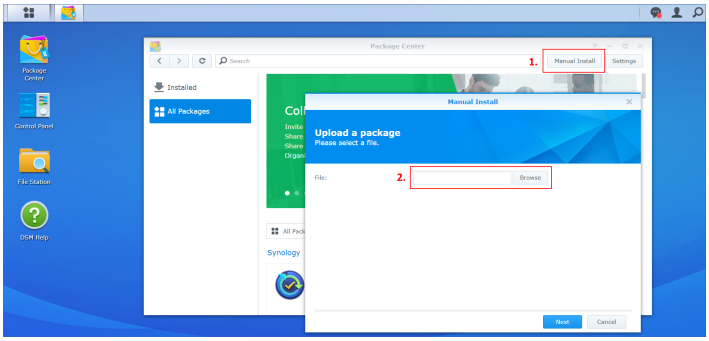
Agent voor Synology 6.x

Vereisten

- Op het NAS-apparaat wordt DiskStation Manager 6.2.x uitgevoerd.
- U bent lid van de groep **administrators** op het NAS-apparaat.
- Er is ten minste 200 MB vrije schijfruimte op het NAS-volume waarop u de agent wilt installeren.

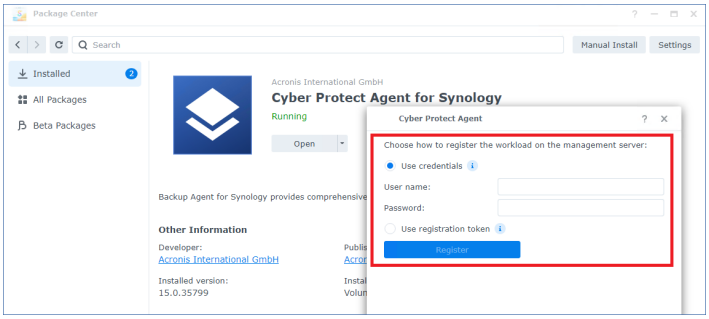
Agent voor Synology installeren:

1. Meld u aan bij Synology DiskStation Manager.
2. Open **Package Center**.
3. Klik op **Handmatige installatie** en klik vervolgens op **Bladeren**.



4. Selecteer het SPK-bestand dat u hebt gedownload van de Cyber Protect-console en klik vervolgens op **Volgende**.

   Er wordt een waarschuwing weergegeven dat u een pakket zonder digitale handtekening gaat installeren. Dit bericht maakt deel uit van de standaardinstallatieprocedure.
5. U kunt bevestigen dat u het pakket wilt installeren door te klikken op **Ja**.
6. Selecteer het volume waarop u de agent wilt installeren en klik op **Volgende**.
7. Controleer uw instellingen en klik vervolgens op **Toepassen**.
8. Ga naar het **Package Center** van Synology DiskStation Manager en open Cyber Protect Agent voor Synology.
9. Selecteer de registratiemethode.



- [De agent registreren met referenties]
  - In de velden **Gebruikersnaam** en **Wachtwoord** geeft u de referenties op voor het account waarvoor de agent wordt geregistreerd. Dit account kan geen partnerbeheerdersaccount zijn.
- [De agent registreren met een registratietoken]
  - Geef bij **Registratieadres** het exacte adres van het datacentrum op. Het exacte adres van het datacentrum is de URL die u ziet wanneer u zich aanmeldt bij de Cyber Protect-console. Bijvoorbeeld: `https://us5-cloud.acronis.com`.

Opmerking
Gebruik geen URL-indeling zonder het adres van het datacenter. Gebruik bijvoorbeeld niet `https://cloud.acronis.com`.

- Geef in het veld **Token** het registratietoken op.
  Zie "Een registratietoken genereren" (p. 126) voor meer informatie over het genereren van een registratietoken.

10. Klik op **Registreren**.

Wanneer de registratie is voltooid, wordt het Synology NAS-apparaat weergegeven in de Cyber Protect-console, op het tabblad **Apparaten** > **Network Attached Storage**.

Als u een back-up wilt maken van de gegevens op het NAS-apparaat, past u een beschermingsschema toe.

Agent voor Synology bijwerken

U kunt Agent voor Synology 6.x bijwerken naar een nieuwere versie van Agent voor Synology 6.x. En u kunt ook Agent voor Synology 7.x bijwerken naar een nieuwere versie van Agent voor Synology 7.x.

Als u de agent wilt bijwerken, voert u de nieuwere versie van het installatieprogramma uit in Synology DiskStation Manager. De oorspronkelijke registratie van de agent, en de instellingen en de schema's die zijn toegepast op de beschermde workloads, blijven behouden.

Opmerking
U kunt de agent niet bijwerken vanuit de Cyber Protect-console.

Een upgrade van Agent voor Synology 6.x naar Agent voor Synology 7.x wordt alleen ondersteund door de oudere agent te verwijderen en de nieuwere agent te installeren. In dit geval worden alle beschermingsschema's ingetrokken en moet u ze handmatig opnieuw toepassen.

Agent voor Synology 7.x

Vereisten

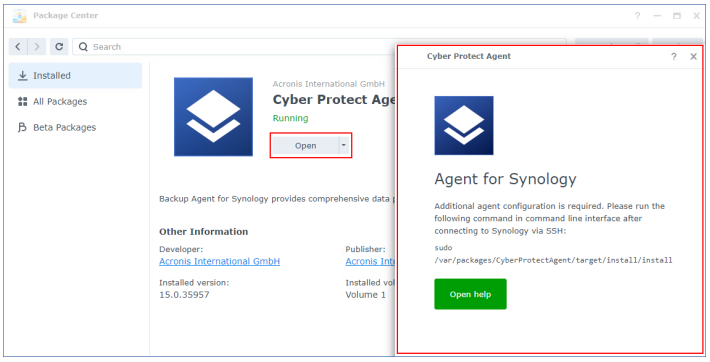
- U bent lid van de groep **administrators** op het NAS-apparaat.
- Er is ten minste 200 MB vrije schijfruimte op het NAS-volume waarop u de agent wilt installeren.
- Er is een SSH-client beschikbaar op uw machine. In dit document wordt Putty als voorbeeld gebruikt.

Agent voor Synology bijwerken:

1. Open **Package Center** in DiskStation Manager.
2. Klik op **Handmatige installatie** en klik vervolgens op **Bladeren**.

3. Selecteer het nieuwere SPK-bestand voor Agent voor Synology 7.x dat u hebt gedownload van de Cyber Protect-console en klik vervolgens op **Volgende**.

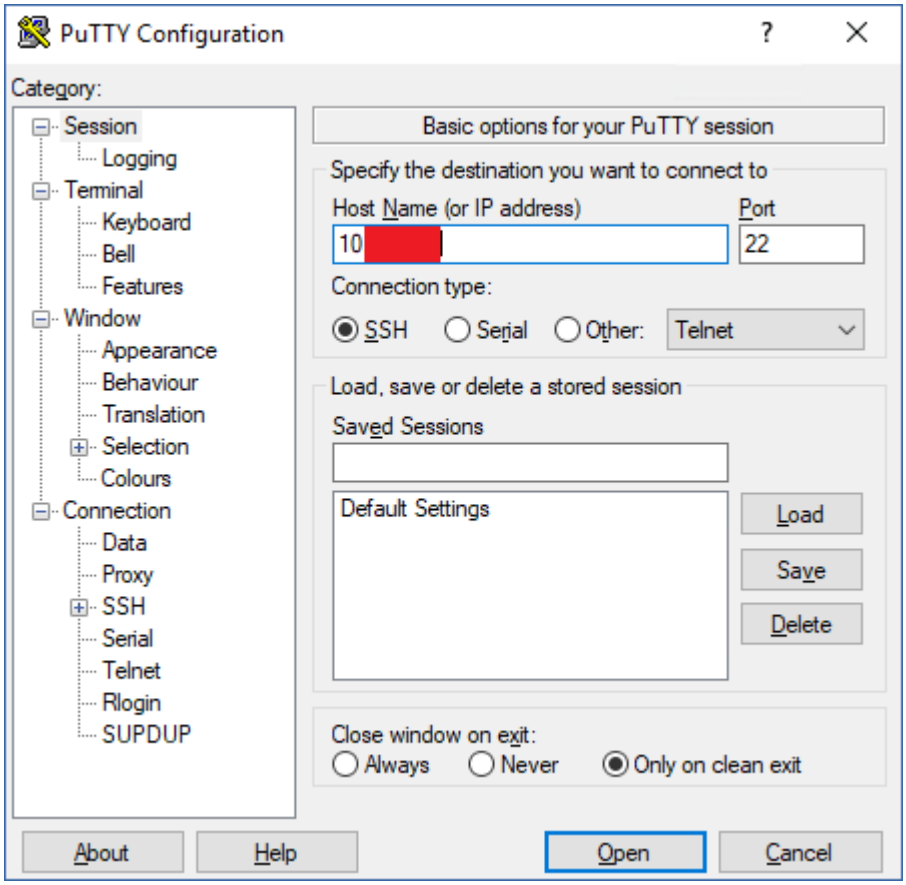
   Er wordt een waarschuwing weergegeven dat u een softwarepakket van derden gaat installeren. Dit bericht maakt deel uit van de standaardinstallatieprocedure.
4. U kunt bevestigen dat u het pakket wilt installeren door te klikken op **Akkoord**.
5. Controleer de instellingen en klik vervolgens op **Gereed**.
6. Ga naar het **Package Center** van Synology DiskStation Manager, open Cyber Protect Agent voor Synology en controleer vervolgens of u het volgende scherm ziet.



7. Ga naar het **Configuratiescherm** van Synology DiskStation Manager, open **Terminal & SNMP** en schakel vervolgens de SSH-toegang tot het NAS-apparaat in.
8. Voer het `install`-script uit op het NAS-apparaat met behulp van een SSH-client (in dit voorbeeld Putty).

   Het script maakt toegang tot de hoofdmap van DSM 7.0 of later mogelijk (dit is vereist om de agent te configureren).

a. Start Putty en geef het IP-adres of de hostnaam op van het Synology NAS-apparaat.



b. Klik op **Openen** en meld u vervolgens aan als Synology DSM-beheerder.

c. Voer de volgende opdracht uit.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

9. Ga naar het **Configuratiescherm** van Synology DiskStation Manager, open **Terminal & SNMP** en schakel vervolgens de SSH-toegang tot het NAS-apparaat uit. De SSH-toegang is dan niet meer vereist.

Agent voor Synology 6.x

Vereisten

- U bent lid van de groep **administrators** op het NAS-apparaat.
- Er is ten minste 200 MB vrije schijfruimte op het NAS-volume waarop u de agent wilt installeren.

Agent voor Synology bijwerken:

1. Open **Package Center** in DiskStation Manager.
2. Klik op **Handmatige installatie** en klik vervolgens op **Bladeren**.
3. Selecteer het nieuwere SPK-bestand voor Agent voor Synology 6.x dat u hebt gedownload van de Cyber Protect-console en klik vervolgens op **Volgende**.

Er wordt een waarschuwing weergegeven dat u een pakket zonder digitale handtekening gaat installeren. Dit bericht maakt deel uit van de standaardinstallatieprocedure.

4. U kunt bevestigen dat u het pakket wilt installeren door te klikken op **Ja**.
5. Controleer uw instellingen en klik vervolgens op **Toepassen**.

SSH-verbindingen met een virtueel apparaat

Gebruik een Secure Socket Shell (SSH)-verbinding wanneer u remote access gebruikt voor een virtueel apparaat waaraan u onderhoud wilt verrichten.

De Secure Shell-daemon starten

Als u SSH-verbindingen met een virtueel apparaat wilt toestaan, start u de Secure Shell-daemon (sshd) op het apparaat.

De Secure Shell-daemon starten:

1. Open de hypervisor-software en open de console van het virtuele apparaat.
2. Druk in de grafische gebruikersinterface van het apparaat op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
3. Voer de volgende opdracht uit:

   ```
   /bin/sshd
   ```

4. [Alleen tijdens de eerste verbinding met het apparaat] Stel het wachtwoord in voor de `root`gebruiker.

   Voor informatie over hoe je het wachtwoord instelt: zie "Het rootwachtwoord instellen op een virtueel apparaat" (p. 176).

Opmerking
We raden aan dat u de Secure Shell-daemon stopt wanneer u de SSH-verbinding niet gebruikt.

Het rootwachtwoord instellen op een virtueel apparaat

Voordat u voor de eerste keer een SSH-verbinding met een virtueel apparaat tot stand brengt, moet u het rootwachtwoord instellen op het apparaat.

Het rootwachtwoord instellen:

1. Open de hypervisor-software en open de console van het virtuele apparaat.
2. Druk in de grafische gebruikersinterface van het apparaat op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
3. Voer de volgende opdracht uit:

   ```
   passwd
   ```

4. Geef een wachtwoord op en druk op Enter.

Het wachtwoord moet minimaal negen tekens bevatten en moet een complexiteitsscore van drie of hoger hebben. De complexiteitsscore wordt automatisch berekend. Als u een hogere score wilt bereiken, gebruikt u een combinatie van speciale symbolen, hoofdletters en kleine letters en cijfers.

5. Bevestig het wachtwoord en druk vervolgens op Enter.

Toegang krijgen tot een virtueel apparaat via een SSH-client

Vereisten

- Een SSH-client moet beschikbaar zijn op de externe machine. De onderstaande procedure gebruikt de WinSCP-client als voorbeeld. U kunt elke SSH-client gebruiken door de stappen dienovereenkomstig aan te passen.
- De Secure Shell daemon (sshd) moet worden gestart op het virtuele apparaat. Voor meer informatie: zie "De Secure Shell-daemon starten" (p. 176).

Toegang krijgen tot een virtueel apparaat via WinSCP

1. Open WinSCP op de externe machine.
2. Klik op **Sessie** > **Nieuwe sessie**.
3. Ga naar **Bestandsprotocol** en selecteer **SCP**.
4. Geef bij **Hostnaam** het IP-adres van de virtuele toepassing op.
5. Ga naar **Gebruikersnaam** en **Wachtwoord**en geef `root` en het wachtwoord voor de `root`gebruiker op.
6. Klik op **Aanmelden**.

Een lijst met alle mappen op het virtuele apparaat wordt weergegeven.

Automatische detectie van machines

Wanneer u automatische detectie gebruikt, kunt u het volgende doen:

- De installatie van beveiligingsagents en de registratie van machines automatiseren door de machines in uw Active Directory-domein of het lokale netwerk te detecteren.
- Beveiligingsagents installeren en bijwerken op meerdere machines.
- Synchronisatie met Active Directory gebruiken om de inrichting van resources en het beheer van machines in een groot Active Directory-domein te vergemakkelijken.

Vereisten

- Er moet minstens één machine met een geïnstalleerde beveiligingsagent beschikbaar zijn in uw lokale netwerk of Active Directory-domein. Deze agent wordt gebruikt als detectieagent.
- U moet een van de volgende rollen hebben voor de Cyber Protection-service: Cyberbeheerder of Beheerder.

Belangrijk
Alleen agents die op Windows-machines zijn geïnstalleerd, kunnen detectieagents zijn. Als er geen detectieagents in uw omgeving zijn, kunt u de optie **Meerdere apparaten** in het deelvenster **Apparaten toevoegen** niet gebruiken.

Externe installatie van agents wordt alleen ondersteund voor machines met Windows (Windows XP wordt niet ondersteund). Voor een externe installatie op een machine met Windows Server 2012 R2 moet Windows-update KB2999226 zijn geïnstalleerd op deze machine.

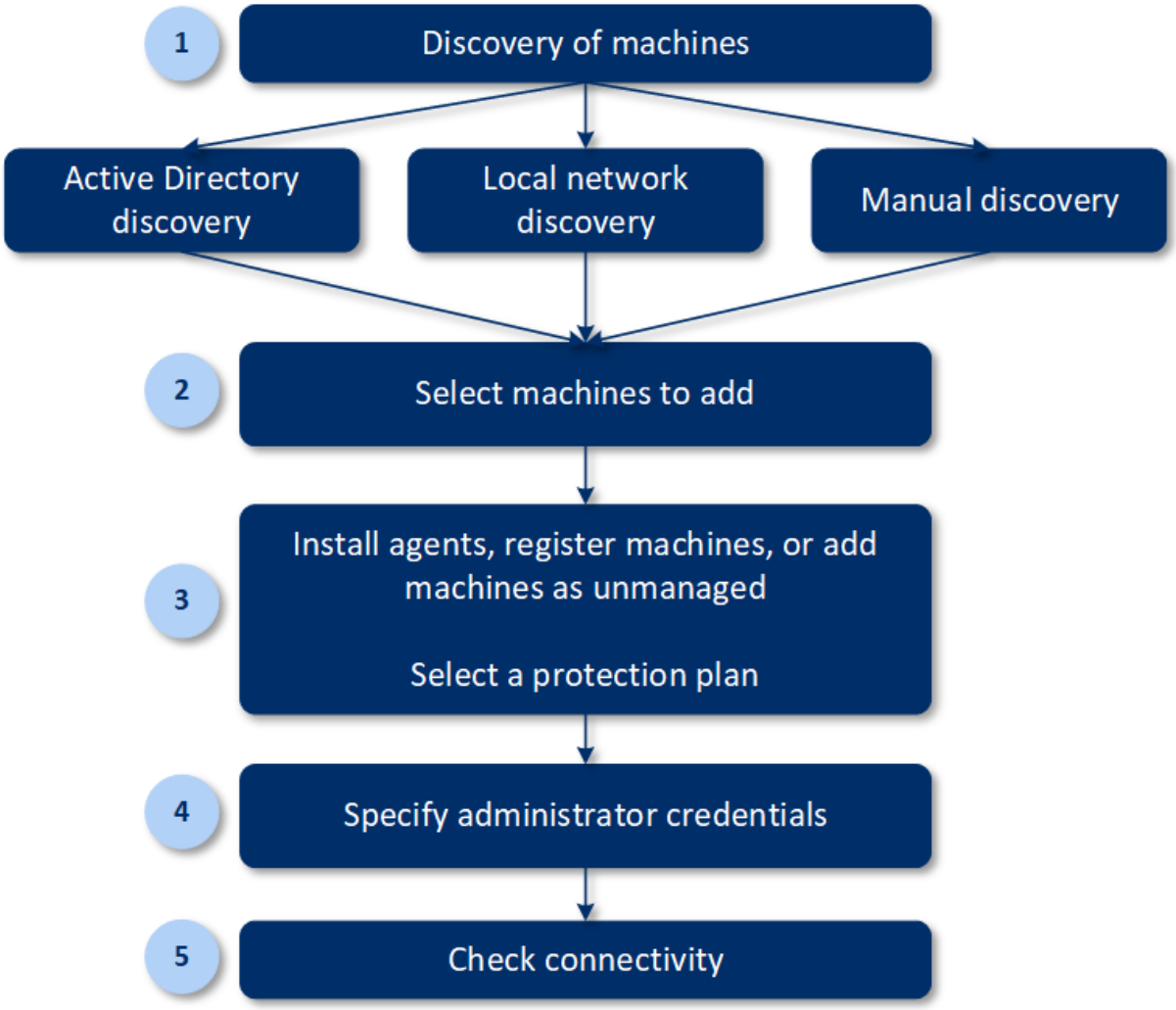
Hoe automatische detectie werkt

Tijdens een lokale-netwerkdetectie gebruikt de detectieagent NetBIOS-detectie, Web Service Discovery (WSD) en de tabel Address Resolution Protocol (ARP) om de volgende informatie voor elke machine in het netwerk te verzamelen:

- Naam (korte naam/NetBIOS-hostnaam)
- Fully qualified domain name (FQDN)
- Domein/werkgroep
- IPv4/IPv6-adressen
- MAC-adressen
- Besturingssysteem (naam/versie/familie)
- Machinecategorie (werkstation/server/domeincontroller)

Tijdens een Active Directory-detectie verzamelt de detectieagent, naast de bovengenoemde items, informatie over de organisatie-eenheid van de machines en meer gedetailleerde informatie over de namen en besturingssystemen van de machines. De IP- en MAC-adressen worden echter niet verzameld.

Het volgende diagram bevat een overzicht van het autodetectieproces.



1. Selecteer de detectiemethode:
   - Active Directory-detectie
   - Lokale-netwerkdetectie
   - Handmatige detectie – Door een IP-adres of hostnaam van een machine te gebruiken of door een lijst met machines te importeren uit een bestand

   Machines waarop beveiligingsagents zijn geïnstalleerd, worden uitgesloten in de resultaten van een Active Directory-detectie of een lokale-netwerkdetectie.

   Tijdens een handmatige detectie worden de bestaande beveiligingsagents bijgewerkt en opnieuw geregistreerd. Als u autodetectie uitvoert met hetzelfde account als waarmee een agent is geregistreerd, wordt de agent alleen bijgewerkt naar de nieuwste versie. Als u een ander account gebruikt, wordt de agent bijgewerkt naar de nieuwste versie en opnieuw geregistreerd onder de tenant waartoe het account behoort.
2. Selecteer de machines die u wilt toevoegen aan uw tenant.
3. Selecteer hoe u deze machines wilt toevoegen:
   - Een beveiligingsagent en aanvullende onderdelen installeren op de machines en deze registreren in de Cyber Protect-console.

- De machines registreren in de Cyber Protect-console (als er al een beveiligingsagent is geïnstalleerd).
- De machines toevoegen aan de Cyber Protect-console als **Onbeheerde machines**, zonder een beveiligingsagent te installeren.

U kunt ook een bestaand beschermingsschema toepassen op de machines waarop u een beveiligingsagent installeert of die u registreert in de Cyber Protect-console.

4. Geef beheerdersreferenties op voor de geselecteerde machines.
5. Controleer of u met de opgegeven referenties verbinding kunt maken met de machines.

De machines die in de Cyber Protect-console worden weergegeven, worden onderverdeeld in de volgende categorieën:

- **Gedetecteerd**: machines die zijn gedetecteerd, maar waarop geen beveiligingsagent is geïnstalleerd.
- **Beheerd**: machines waarop een beveiligingsagent is geïnstalleerd.
- **Onbeschermd**: machines waarop geen beschermingsschema wordt toegepast. Onbeschermde machines kunnen zowel gedetecteerde als beheerde machines zonder beschermingsschema zijn.
- **Beschermd**: machines waarop een beschermingsschema wordt toegepast.

Externe installatie van agents

1. De detectieagent maakt verbinding met de doelmachines met behulp van de hostnaam, het IP-adres en de beheerdersreferenties die zijn opgegeven in de detectiewizard, en uploadt het bestand `web_installer.exe` vervolgens naar deze machines.
2. Het bestand `web_installer.exe` wordt uitgevoerd op de doelmachines in de modus zonder toezicht.
3. Het webinstallatieprogramma haalt aanvullende installatiepakketten op uit de cloud en installeert deze vervolgens op de doelmachines via de opdracht `msiexec`.
4. Nadat de installatie is voltooid, worden de onderdelen geregistreerd in de cloud.

Opmerking
Externe installatie van agents wordt niet ondersteund voor domeincontrollers, vanwege de extra machtigingen die nodig zijn om de agentservice uit te voeren.

Automatische detectie en handmatige detectie uitvoeren

Voordat u met de detectie begint, moet u controleren of dat aan de voorwaarden is voldaan.

Opmerking
Automatische detectie wordt niet ondersteund voor het toevoegen van domeincontrollers, vanwege de extra machtigingen die nodig zijn om de agentservice uit te voeren.

Machines detecteren

1. Ga in de Cyber Protect-console naar **Apparaten** > **Alle apparaten**.
2. Klik op **Toevoegen**.
3. Klik onder **Meerdere apparaten** op **Alleen Windows**. De detectiewizard wordt geopend.
4. [Als er eenheden in uw organisatie zijn] Selecteer een eenheid. Vervolgens kunt u onder **Detectieagent** de agenten selecteren die zijn gekoppeld aan de geselecteerde eenheid en de onderliggende eenheden.
5. Selecteer de detectieagent die de scan uitvoert om machines te detecteren.
6. Selecteer de detectiemethode:
   - **Zoeken in Active Directory**. Controleer of de machine met de detectieagent het Active Directory-domeinlid is.
   - **Lokaal netwerk scannen**. Als de geselecteerde detectieagent geen machines kan vinden, selecteert u een andere detectieagent.
   - **Handmatig opgeven of importeren uit bestand**. Definieer handmatig de machines die u wilt toevoegen of importeer ze uit een tekstbestand.
7. [Als de detectiemethode met Active Directory is geselecteerd] Selecteer hoe u naar machines wilt zoeken:
   - **In de lijst met organisatie-eenheden**. Selecteer de groep machines die u wilt toevoegen.
   - **Met een query in LDAP-dialect**. Gebruik de query in LDAP-dialect om de machines te selecteren. **Zoekbasis**: hiermee bepaalt u waar moet worden gezocht; gebruik **Filter** om de criteria voor machineselectie op te geven.
8. Afhankelijk van de detectiemethode die u hebt geselecteerd, voert u een van de volgende acties uit:

Detectiemethode	Actie
Zoeken in Active Directory	Open de lijst met gedetecteerde machines en selecteer de machines die u wilt toevoegen.
Lokaal netwerk scannen	Open de lijst met gedetecteerde machines en selecteer de machines die u wilt toevoegen.

Handmatig opgeven of importeren uit bestand	Geef de machine-IP-adressen of hostnamen op of importeer de lijst met machines uit een tekstbestand. Het bestand moet IP-adressen/hostnamen bevatten, één per regel. Hier is een voorbeeld van een bestand:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Wanneer u machineadressen handmatig hebt toegevoegd of hebt geïmporteerd uit een bestand, probeert de agent de toegevoegde machines te pingen en hun beschikbaarheid te definiëren.

9. Selecteer de acties die moeten worden uitgevoerd na de detectie:

Optie	Beschrijving
Agents installeren en machines registreren	U kunt selecteren welke onderdelen u wilt installeren op de machines door te klikken op **Onderdelen selecteren**. Voor meer details: zie "Onderdelen selecteren voor installatie" (p. 185).
Aanmelden bij de agentservice	Deze instelling is beschikbaar op het scherm **Onderdelen selecteren**. Deze instelling bepaalt voor welk account de services worden uitgevoerd. U kunt een van de volgende opties selecteren: • **Servicegebruikeraccounts gebruiken** (standaard voor de agentservice) Servicegebruikeraccounts zijn Windows-systeemaccounts die worden gebruikt om services uit te voeren. Het voordeel van deze instelling is dat de beleidsregels voor domeinbeveiliging geen invloed hebben op de gebruikersrechten van deze accounts. De agent wordt standaard uitgevoerd onder het **Lokale systeemaccount**. • **Een nieuw account maken** De accountnaam is Agent User voor de agent. • **Het volgende account gebruiken** Als u de agent installeert op een domeincontroller, wordt u gevraagd om bestaande accounts (of hetzelfde account) op te geven voor de agent. Uit veiligheidsoverwegingen worden er niet automatisch nieuwe accounts op een domeincontroller. Als u de optie **Een nieuw account maken** of **Het volgende account gebruiken** kiest, controleer dan of het beveiligingsbeleid van het domein geen invloed heeft op de rechten van de gerelateerde accounts. Als de gebruikersrechten die tijdens de installatie zijn toegewezen, worden ingetrokken voor een account, werkt het onderdeel mogelijk onjuist of helemaal niet.
Machines registreren met geïnstalleerde agenten	Gebruik deze optie als de agent al op de machines is geïnstalleerd en u deze alleen hoeft te registreren in Cyber Protection. Als er geen agent op de machines wordt gevonden, worden ze toegevoegd als **Onbeheerde** machines.
Toevoegen als onbeheerde machines	Als u deze optie selecteert, wordt de agent niet op de machines geïnstalleerd. U kunt ze bekijken in de console en de agent later installeren of registreren.
Start de machine indien nodig opnieuw op	Deze optie wordt weergegeven wanneer **Agents installeren en machines registreren** is geselecteerd. Als u deze optie selecteert, wordt de machine zo vaak als nodig is opnieuw opgestart om de installatie te voltooien. De machine moet mogelijk opnieuw worden opgestart in een van de volgende gevallen: • De installatie van de vereiste voorbereidende items is voltooid en een herstart is vereist om de installatie voort te zetten. • De installatie is voltooid, maar een herstart is vereist, omdat sommige

Optie	Beschrijving
	bestanden tijdens de installatie zijn vergrendeld. • De installatie is voltooid, maar een herstart is vereist voor andere eerder geïnstalleerde software.
Niet opnieuw opstarten als de gebruiker is aangemeld	Deze optie wordt weergegeven wanneer **De machine indien nodig opnieuw opstarten** is geselecteerd. Als u deze optie selecteert, wordt de machine niet automatisch opnieuw opgestart als de gebruiker is aangemeld bij het systeem. Als een gebruiker bijvoorbeeld aan het werk is terwijl de installatie een herstart vereist, wordt het systeem niet opnieuw opgestart. Als de vereiste voorbereidende items zijn geïnstalleerd, maar de machine niet opnieuw is opgestart omdat een gebruiker was aangemeld, moet de machine opnieuw opstarten en vervolgens de installatie opnieuw starten om deze te kunnen voltooien. Als de agent is geïnstalleerd, maar de machine vervolgens niet opnieuw is opgestart, moet u de machine opnieuw opstarten.
Gebruiker waarvoor u de machines wilt registreren	[Als er eenheden in uw organisatie zijn] Selecteer het gebruikersaccount van de eenheid of ondergeschikte eenheden waarvoor u de machines wilt registreren. [Bij het uitvoeren van automatische detectie op partnertenantniveau] In de lijst met klanttenants die u beheert, vouwt u de boomstructuur uit en selecteert u vervolgens het gebruikersaccount waarvoor u de machines wilt registreren. [Bij het uitvoeren van automatische detectie als klantbeheerder] Als u **Agents installeren en machines registreren** of **Machines registreren met geïnstalleerde agenten** hebt geselecteerd, is er ook een optie om het beschermingsplan toe te passen op de machines. Als u meerdere beschermingsplannen hebt, kunt u selecteren welke u wilt gebruiken.

10. Geef de referenties op van de gebruiker met beheerdersrechten voor alle machines.

Belangrijk
De externe installatie van een agent zonder voorbereidingen werkt alleen als u de referenties van het ingebouwde beheerdersaccount opgeeft (het eerste account dat is gemaakt toen het besturingssysteem is geïnstalleerd). Als u aangepaste beheerdersreferenties wilt definiëren, moet u dit handmatig voorbereiden met enkele aanvullende acties, zoals beschreven in "Een machine voorbereiden voor externe installatie" (p. 184).

11. Het systeem controleert de connectiviteit voor alle machines. Als de verbinding met sommige machines mislukt, kunt u de referenties voor deze machines wijzigen.

Wanneer de detectie van machines wordt gestart, vindt u de bijbehorende taak in de activiteit **Controle** > **Activiteiten** > **Machines detecteren**.

Een machine voorbereiden voor externe installatie

- Als u de installatie wilt uitvoeren op een externe machine met Windows 7 of later, moet de optie **Configuratiescherm** > **Mapopties** > **Weergave** > **Wizard Delen gebruiken** zijn *uitgeschakeld* op die machine.
- Als u de installatie wilt uitvoeren op een externe machine die *geen* lid is van een Active Directory-domein, moet Gebruikersaccountbeheer (UAC) zijn *uitgeschakeld* op die machine. Meer informatie over het uitschakelen vindt u in 'Vereisten voor Gebruikersaccountbeheer (UAC)' > UAC uitschakelen.
- Standaard zijn de referenties van het ingebouwde beheerdersaccount vereist voor externe installatie op een Windows-computer. Als u de externe installatie wilt uitvoeren met de referenties van een ander beheerdersaccount, moeten de externe beperkingen voor Gebruikersaccountbeheer (UAC) zijn *uitgeschakeld*. Meer informatie over het uitschakelen hiervan vindt u in'Vereisten voor Gebruikersaccountbeheer (UAC)' > Externe beperkingen voor UAC uitschakelen.
- Bestands- en printerdeling moet zijn *ingeschakeld* op de externe machine. Zo krijgt u toegang tot deze optie:
  - Op een machine met Windows 2003 Server: ga naar **Configuratiescherm** > **Windows Firewall** > **Uitzonderingen** > **Bestands- en printerdeling**.
  - Op een machine met Windows Server 2008, Windows 7 of later: ga naar **Configuratiescherm** > **Windows Firewall** > **Netwerkcentrum** > **Geavanceerde instellingen voor delen wijzigen**.
- Voor een externe installatie van Cyber Protection worden de TCP-poorten 445, 25001 en 43234 gebruikt.

  Poort 445 wordt automatisch geopend wanneer u Bestands- en printerdeling inschakelt. De poorten 43234 en 25001 worden automatisch geopend via Windows Firewall. Als u een andere firewall gebruikt, controleert u of deze drie poorten zijn geopend (toegevoegd aan de uitzonderingen) voor zowel binnenkomende als uitgaande aanvragen.

  Wanneer de externe installatie is voltooid, wordt poort 25001 automatisch gesloten door Windows Firewall. De poorten 445 en 43234 moeten open blijven als u de agent later vanaf een externe locatie wilt kunnen bijwerken. Tijdens de updates wordt poort 25001 automatisch geopend en gesloten door Windows Firewall. Als u een andere firewall gebruikt, houdt u alle drie poorten open.

Vereisten voor Gebruikersaccountbeheer (UAC)

UAC en externe beperkingen voor UAC moeten zijn uitgeschakeld voor bewerkingen van het gecentraliseerd beheer (waaronder externe installatie) op een machine met Windows 7 of later die geen lid is van een Active Directory-domein.

UAC uitschakelen

Voer een van de volgende handelingen uit (afhankelijk van het besturingssysteem):

- **In een Windows-besturingssysteem ouder dan Windows 8:**
  Ga naar **Configuratiescherm > Weergave: Kleine pictogrammen > Gebruikersaccounts > Instellingen voor Gebruikersaccountbeheer wijzigen** en verplaats de schuifregelaar naar **Nooit een melding weergeven**. Start de machine vervolgens opnieuw op.
- **In elk Windows-besturingssysteem**:
  1. Open Register-editor.
  2. Zoek de volgende registersleutel: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. Stel de waarde van **EnableLUA** in op **0**.
  4. Start de machine opnieuw op.

Externe beperkingen voor UAC uitschakelen

1. Open Register-editor.
2. Zoek de volgende registersleutel: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Stel de waarde van **LocalAccountTokenFilterPolicy** in op **1**.
   Als de waarde van **LocalAccountTokenFilterPolicy** niet bestaat, maak deze dan aan als DWORD (32 bits). Zie de Microsoft-documentatie https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows voor meer informatie over deze waarde.

Opmerking
Vanwege de veiligheid raden we aan dat u na het beëindigen van de beheerbewerking (zoals externe installatie) beide instellingen terugzet naar de oorspronkelijke status: **EnableLUA**=**1** en **LocalAccountTokenFilterPolicy** = **0**

Onderdelen selecteren voor installatie

U vindt de beschrijving van verplichte en aanvullende onderdelen in de volgende tabel:

Onderdeel	Beschrijving
Verplicht onderdeel	
Agent voor Windows	Deze agent maakt een back-up van schijven, volumes en bestanden en wordt geïnstalleerd op Windows-machines. Wordt altijd geïnstalleerd en is niet selecteerbaar.
Aanvullende onderdelen	
Agent voor preventie van gegevensverlies	Met deze agent kunt u de gebruikerstoegang beperken tot lokale en omgeleide randapparatuur, poorten en het klembord op machines met beschermingsschema's. Dit wordt geïnstalleerd indien geselecteerd.
Antimalware en	Met dit onderdeel kunnen de modules Antivirus- en antimalwarebeveiliging en URL-

URL-filtering	filtering worden ingeschakeld in beschermingsschema's. Zelfs als u ervoor kiest om het niet te installeren, zal het later automatisch worden geïnstalleerd, als een van deze modules is ingeschakeld in een beschermingsschema voor de machine.
Agent voor Hyper-V	Deze agent maakt een back-up van virtuele Hyper-V-machines en wordt geïnstalleerd op Hyper-V-hosts. Deze wordt geïnstalleerd indien geselecteerd en als de Hyper-V-rol is gedetecteerd op een machine.
Agent voor SQL	Deze agent maakt een back-up van SQL Server-databases en wordt geïnstalleerd op machines met Microsoft SQL Server. Deze wordt geïnstalleerd indien geselecteerd en als de toepassing is gedetecteerd op een machine.
Agent voor Exchange	Deze agent maakt een back-up van Exchange-databases en -postvakken en wordt geïnstalleerd op machines waarop de postvakfunctie van Microsoft Exchange Server wordt uitgevoerd. Deze wordt geïnstalleerd indien geselecteerd en als de toepassing is gedetecteerd op een machine.
Agent voor Active Directory	Deze agent maakt een back-up van de gegevens van Active Directory Domain Services en wordt geïnstalleerd op domeincontrollers. Deze wordt geïnstalleerd indien geselecteerd en als de toepassing is gedetecteerd op een machine.
Agent voor VMware (Windows)	Deze agent maakt een back-up van virtuele VMware-machines en wordt geïnstalleerd op Windows-machines die netwerktoegang hebben tot vCenter Server. Deze wordt geïnstalleerd indien geselecteerd.
Agent voor Microsoft 365	Deze agent maakt een back-up van Microsoft 365-postvakken naar een lokale bestemming en wordt geïnstalleerd op Windows-machines. Dit wordt geïnstalleerd indien geselecteerd.
Agent voor Oracle	Deze agent maakt een back-up van Oracle-databases en wordt geïnstalleerd op machines met Oracle Database. Dit wordt geïnstalleerd indien geselecteerd.
Cyber Protection Monitor	Met dit onderdeel kan een gebruiker de uitvoering van actieve taken in het systeemvak controleren. Het onderdeel wordt geïnstalleerd op Windows-machines. Dit wordt geïnstalleerd indien geselecteerd. Ondersteund op Windows 7 Service Pack 1 en later, en Windows Server 2008 R2 Service Pack 1 en later.

Gedetecteerde machines beheren

Wanneer het detectieproces is uitgevoerd, kunt u alle gedetecteerde machines vinden in **Apparaten** > **Onbeheerde machines**.

Dit gedeelte is onderverdeeld in subsecties op basis van de gebruikte detectiemethode. De volledige lijst met machineparameters wordt hieronder weergegeven (deze kan variëren, afhankelijk van de detectiemethode):

Naam	Beschrijving
Naam	De naam van de machine. Het IP-adres wordt weergegeven als de naam van de

	machine niet kan worden gedetecteerd.
IP-adres	Het IP-adres van de machine.
Type detectie	De detectiemethode die is gebruikt om de machine te detecteren.
Organisatie-eenheid	De organisatie-eenheid in Active Directory waartoe de machine behoort. Deze kolom wordt weergegeven als u de lijst met machines bekijkt in **Onbeheerde machines** > **Active Directory**.
Besturingssysteem	Het besturingssysteem dat is geïnstalleerd op de machine.

Er is een gedeelte **Uitsluitingen**, waar u de machines kunt toevoegen die tijdens het detectieproces moeten worden overgeslagen. Als bijvoorbeeld de exacte machines niet hoeven te worden gedetecteerd, kunt u deze aan deze lijst toevoegen.

Als u een machine wilt toevoegen aan **Uitsluitingen**, selecteert u deze in de lijst en klikt u op **Toevoegen aan uitzonderingen**. Als u een machine wilt verwijderen uit **Uitsluitingen**, gaat u naar **Onbeheerde machines** > **Uitsluitingen**, selecteert u de machine en klikt u op **Verwijderen uit uitzonderingen**.

U kunt de beveiligingsagent installeren en meerdere gedetecteerde machines registreren in Cyber Protection door ze in de lijst te selecteren en op **Installeren en registreren** te klikken. Met de geopende wizard kunt u het beschermingsschema ook toewijzen aan meerdere machines.

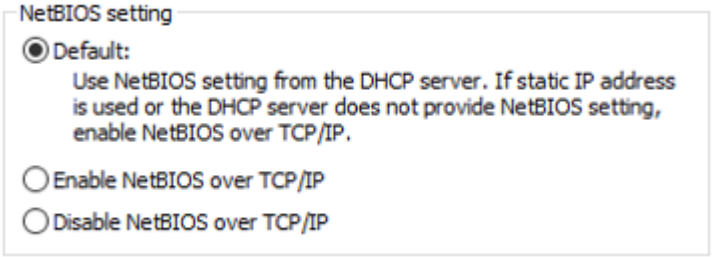
Wanneer de beveiligingsagent op machines is geïnstalleerd, worden deze machines weergegeven in het gedeelte **Apparaten** > **Machines met agenten**.

Als u de beveiligingsstatus wilt controleren, gaat u naar **Controle** > **Overzicht** en voegt u de widget **Beveiligingsstatus** of de widget **Gedetecteerde machine** toe.

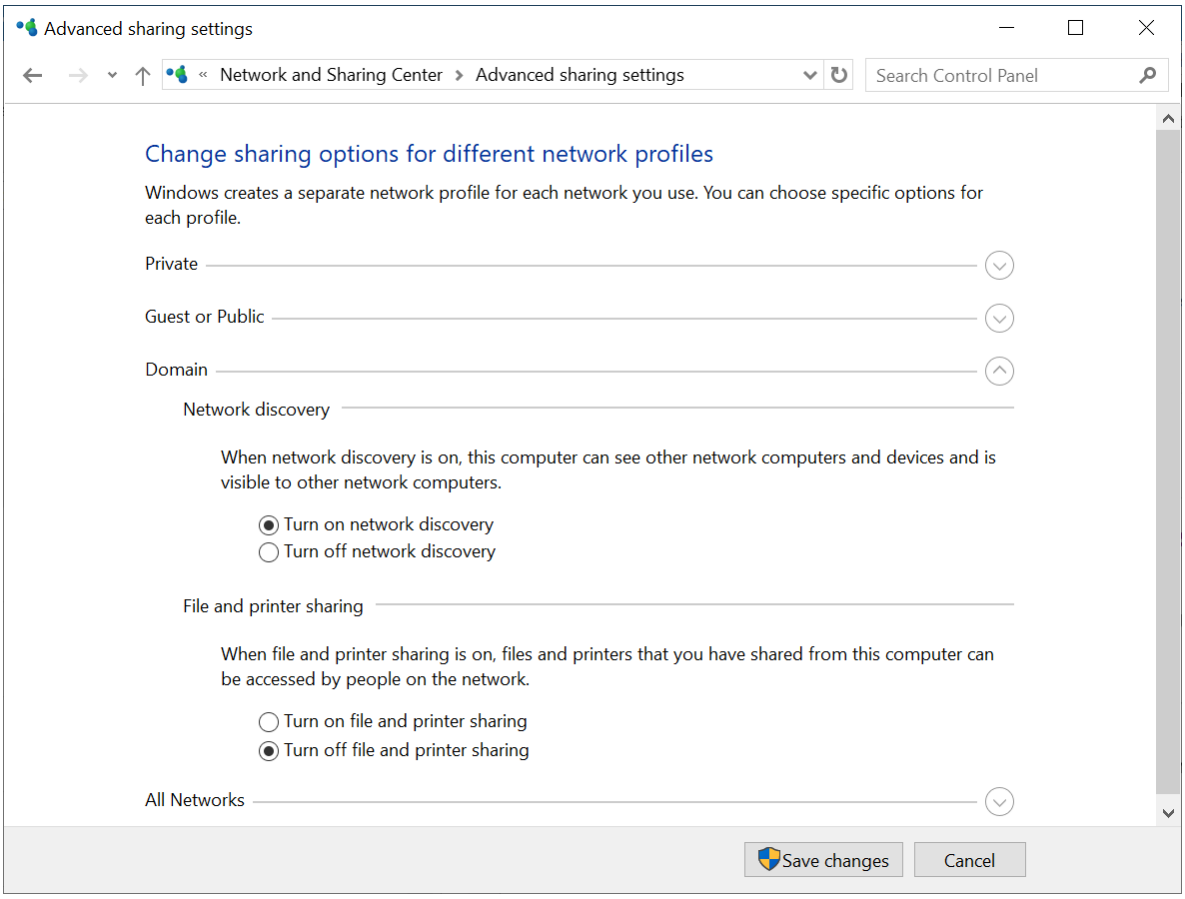
Problemen oplossen

Als u problemen ondervindt met de functie voor automatische detectie, probeer dan het volgende:

- Controleer of NetBIOS via TCP/IP is ingeschakeld of is ingesteld op standaard.



- Ga naar 'Configuratiescherm\Netwerkcentrum\Geavanceerde instellingen voor delen' en schakel netwerkdetectie in.



- Controleer of de Function Discovery Provider-hostservice wordt uitgevoerd op zowel de machine die detectie uitvoert als op de te detecteren machines.
- Controleer of de Function Discovery Resource Publication-service wordt uitgevoerd op de te detecteren machines.

Voorkomen van niet-geautoriseerde verwijdering of wijziging van agenten

U kunt Agent voor Windows beschermen tegen niet-geautoriseerde verwijdering of wijziging door de instelling **Wachtwoordbescherming** in te schakelen in een beschermingsschema. Deze instelling is alleen beschikbaar wanneer de instelling **Zelfbescherming** is ingeschakeld.

Wachtwoordbescherming inschakelen

1. Vouw in een beschermingsschema de module **Antivirus- en antimalwarebeveiliging** uit (module **Active Protection** voor Cyber Backup-edities).
2. Klik op **Zelfbescherming** en controleer of de schakelaar **Zelfbescherming** op 'Aan' staat.
3. Zet de schakelaar **Wachtwoordbescherming** op 'Aan'.
4. Klik in het venster dat wordt geopend en kopieer het wachtwoord dat u nodig hebt om de onderdelen van een beveiligde Agent voor Windows te verwijderen of te wijzigen.

Dit wachtwoord is uniek en u kunt het niet meer herstellen wanneer u dit venster sluit. Als u dit wachtwoord verliest of vergeet, kunt u het beschermingsschema bewerken en een nieuw wachtwoord maken.

5. Klik op **Sluiten**.
6. Klik in het deelvenster **Zelfbescherming** op **Gereed**.
7. Sla het beschermingsschema op.

Wachtwoordbescherming wordt ingeschakeld voor de machines waarop dit beschermingsschema wordt toegepast. Wachtwoordbescherming is alleen beschikbaar voor Agent voor Windows versie *15.0.25851* of nieuwer. De machines moeten online zijn.

Wanneer wachtwoordbescherming is ingeschakeld, kunt u een beschermingsschema toepassen op een machine met macOS, maar er wordt geen bescherming geboden. U kunt een dergelijk schema niet toepassen op een machine met Linux.

Wanneer wachtwoordbescherming is ingeschakeld, kunt u ook niet meer dan één beschermingsschema toepassen op dezelfde Windows-machine. Zie Conflicten tussen schema's oplossen voor meer informatie over het oplossen van een mogelijk conflict.

Het wachtwoord in een bestaand beschermingsschema wijzigen

1. Vouw in het beschermingsschema de module **Antivirus- en antimalwarebeveiliging** uit (module **Active Protection** voor Cyber Backup-editie).
2. Klik op **Zelfbescherming**.
3. Klik op **Nieuw wachtwoord maken**.
4. Klik in het venster dat wordt geopend en kopieer het wachtwoord dat u nodig hebt om de onderdelen van een beveiligde Agent voor Windows te verwijderen of te wijzigen.
   Dit wachtwoord is uniek en u kunt het niet meer herstellen wanneer u dit venster sluit. Als u dit wachtwoord verliest of vergeet, kunt u het beschermingsschema bewerken en een nieuw wachtwoord maken.
5. Klik op **Sluiten**.
6. Klik in het deelvenster **Zelfbescherming** op **Gereed**.
7. Sla het beschermingsschema op.

De servicequota van machines wijzigen

Een servicequota wordt automatisch toegewezen wanneer een beschermingsschema voor de eerste keer wordt toegepast op een machine.

De meest geschikte quota wordt toegewezen, afhankelijk van het type van de beschermde machine, het besturingssysteem, het vereiste beschermingsniveau en de beschikbaarheid van de quota. Als de meest geschikte quota niet beschikbaar is in uw organisatie, wordt de op één na beste quota toegewezen. Als de meest geschikte quota bijvoorbeeld **Webhostingserver** is, maar deze niet beschikbaar is, dan wordt de quota voor **Server** toegewezen.

Voorbeelden van toewijzing van quota's:

- Een fysieke machine waarop een besturingssysteem voor Windows Server of een Linux-server (zoals Ubuntu Server) wordt uitgevoerd, krijgt de quota voor **Server** toegewezen.
- Een fysieke machine waarop een besturingssysteem voor Windows of een Linux-desktop (zoals Ubuntu Desktop) wordt uitgevoerd, krijgt de quota voor **Werkstation** toegewezen.
- Een fysieke machine waarop Windows 10 met ingeschakelde Hyper-V-rol wordt uitgevoerd, krijgt de quota **Werkstation** toegewezen.
- Een desktopmachine die wordt uitgevoerd op een virtuele desktopinfrastructuur en waarvan de beveiligingsagent is geïnstalleerd in het gastbesturingssysteem (bijvoorbeeld Agent voor Windows), krijgt de quota voor **Virtuele machine** toegewezen. Voor dit type machine kan ook de quota voor **Werkstation** worden gebruikt als de quota voor **Virtuele machine** niet beschikbaar is.
- Een desktopmachine die wordt uitgevoerd op een virtuele desktopinfrastructuur en waarvan een back-up wordt gemaakt in de modus zonder back-up (bijvoorbeeld Agent voor VMware of Agent voor Hyper-V), krijgt de quota voor **Virtuele machine** toegewezen.
- Een Hyper-V- of vSphere-server krijgt de quota voor **Server** toegewezen.
- Een server met cPanel of Plesk krijgt de quota voor **Webhostingserver** toegewezen. Als de quota voor **Webhostingserver** niet beschikbaar is, kan ook de quota voor **Virtuele machine** of **Server** worden gebruikt, afhankelijk van het type machine waarop de webserver wordt uitgevoerd.
- Voor de applicatiegerichte back-up is de quota voor **Server** vereist, zelfs voor een werkstation.

U kunt de oorspronkelijke toewijzing later handmatig wijzigen. Als u bijvoorbeeld een geavanceerder beschermingsschema wilt toepassen op dezelfde machine, moet u de servicequota van de machine mogelijk upgraden. Als de door dit beschermingsschema vereiste functies niet worden ondersteund door de momenteel toegewezen servicequota, mislukt het beschermingsschema.

U kunt de servicequota ook wijzigen als u na de oorspronkelijke toewijzing een quota aanschaft die meer geschikt is. Stel bijvoorbeeld dat u een virtuele machine hebt waaraan een quota voor **Werkstation** is toegewezen. Wanneer u een quota voor **Virtuele machines** aanschaft, kunt u deze quota handmatig toewijzen aan de machine in plaats van de oorspronkelijke quota voor **Werkstation**.

U kunt de huidige toegewezen servicequota ook vrijgeven en deze aan een andere machine toewijzen.

U kunt de servicequota van een afzonderlijke machine of voor een groep machines wijzigen.

De servicequota van een afzonderlijke machine wijzigen

1. Ga in de Cyber Protect-console naar **Apparaten**.
2. Selecteer de gewenste machine en klik op **Details**.
3. Klik in het gedeelte **Servicequota** op **Wijzigen**.

4. Open het venster **Quota wijzigen**, selecteer de gewenste servicequota of **Geen quota** en klik vervolgens op **Wijzigen**.

De servicequota voor een groep machines wijzigen

1. Ga in de Cyber Protect-console naar **Apparaten**.
2. Selecteer meer dan één machine en klik vervolgens op **Quota toewijzen**.
3. Open het venster **Quota wijzigen**, selecteer de gewenste servicequota of **Geen quota** en klik vervolgens op **Wijzigen**.

Beveiligingsinstellingen

Als u de algemene beveiligingsinstellingen voor Cyber Protection wilt configureren, gaat u in de Cyber Protect-console naar **Instellingen** > **Bescherming**.

Automatische updates voor onderdelen

Standaard kunnen alle agenten verbinding maken met internet en updates downloaden.

Een beheerder kan de bandbreedte van het netwerkverkeer minimaliseren door één of meerdere agenten in de omgeving te selecteren en hieraan de rol Updater toe te wijzen. De speciale agenten maken dan verbinding met internet en zorgen ervoor dat de updates worden gedownload. Alle andere agenten gebruiken peer-to-peer-technologie om verbinding te maken met de speciale Updater-agenten en downloaden de updates van die agenten.

De agenten zonder Updater-rol maken verbinding met internet als er geen speciale Updater-agent aanwezig is in de omgeving of als er gedurende ongeveer vijf minuten geen verbinding met een speciale Updater-agent tot stand kan worden gebracht.

De Updater-agent distribueert updates en patches voor Antivirus- en antimalwarebeveiliging, Evaluatie van beveiligingsproblemen en Patchbeheer, maar bevat geen updates van de agentversie.

Opmerking
Een agent met de Updater-rol kan alleen patches downloaden en distribueren voor Windows-producten van derden. De Updater-agent biedt geen ondersteuning voor de distributie van patches voor Microsoft-producten.

Voordat u de Updater-rol toewijst aan een agent, moet u controleren of de machine waarop de agent wordt uitgevoerd, krachtig genoeg is en een stabiele, snelle internetverbinding en voldoende schijfruimte heeft.

Een machine voorbereiden voor de Updater-rol

1. Pas op de machine van de agent waar u de Updater-rol wilt inschakelen, de volgende firewallregels toe:
   - Inbound (inkomend) "updater_incoming_tcp_ports": verbinding toestaan met TCP-poorten 18018 en 6888 voor alle firewallprofielen (openbaar, privé en domein).

- Inbound (inkomend) "updater_incoming_udp_ports": verbinding toestaan met UDP-poort 6888 voor alle firewallprofielen (openbaar, privé en domein).

2. Start de Acronis Agent Core Service opnieuw op.
3. Start de Firewall-service opnieuw op.

Als u deze regels niet toepast en de firewall is ingeschakeld, dan worden de updates uit de cloud gedownload door peer-agenten.

De rol Updater toewijzen aan een beveiligingsagent

1. Ga in de Cyber Protect-console naar **Instellingen** > **Agents**.
2. Selecteer de machine met de agent waaraan u de rol Updater wilt toewijzen.
3. Klik op **Details** en schakel vervolgens de optie **Deze agent gebruiken om patches en updates te downloaden en te distribueren** in.

De peer-to-peer-update werkt als volgt.

1. De agent met de rol Updater controleert, volgens een schema, het indexbestand van de serviceprovider om de kernonderdelen bij te werken.
2. De agent met de rol Updater begint updates te downloaden en te distribueren naar alle agenten.

U kunt de Updater-rol toewijzen aan meerdere agenten in de omgeving. Dus als een agent met de Updater-rol offline is, kunnen andere agenten met deze rol worden gebruikt als bron voor definitie-updates.

De Cyber Protection-definities bijwerken volgens een schema

Op het tabblad **Planning** kunt u het schema instellen voor automatische update van de Cyber Protection-definities voor elk van de volgende onderdelen:

- Antimalware
- Evaluatie van beveiligingsproblemen
- Patchbeheer

U kunt de instelling van de definitie-updates wijzigen via **Instellingen** > **Bescherming** > **Update van beveiligingsdefinities** > **Planning**.

Type schema:

- **Dagelijks:** definieer op welke dagen van de week de definities moeten worden bijgewerkt.
  Starten om: selecteer hoe laat de definities worden bijgewerkt.
- **Elk uur**: definieer een meer gedetailleerd uurschema voor updates.
  Uitvoeren om de: definieer de periodiciteit voor updates.
  Van ... **Tot**: definieer een specifiek tijdbereik voor de updates.

De Cyber Protection-definities op aanvraag bijwerken

De Cyber Protection-definities op aanvraag bijwerken voor een bepaalde machine

1. Ga in de Cyber Protect-console naar **Instellingen** > **Agents**.
2. Selecteer de machines waarop u de beveiligingsdefinities wilt bijwerken en klik vervolgens op **Definities bijwerken**.

Cacheopslag

De locatie van de gegevens in de cache is als volgt:

- Op Windows-machines: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Op Linux-machines: `/opt/acronis/var/atp-downloader/Cache`
- Op macOS-machines: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

U kunt de instelling van de cacheopslag wijzigen via **Instellingen** > **Bescherming** > **Update van beveiligingsdefinities** > **Cacheopslag**.

Geef in **Verouderde updatebestanden en patchbeheergegevens** op na welke periode de gegevens in de cache moeten worden verwijderd.

Maximale grootte van de cacheopslag (GB) voor agenten:

- **Rol Updater**: definieer de opslaggrootte voor de cache op machines met de rol Updater.
- **Andere rollen**: definieer de opslaggrootte voor de cache op andere machines.

Opmerking
Cyber Protection verzamelt voorbeelden van gedetecteerde malware voor aanvullende analyse, zodat we onze software kunnen verbeteren. U kunt deze instelling op elk gewenst moment wijzigen op het tabblad **Bescherming** door de wisselknop **Voorbeelden van malware verzamelen en uploaden naar CPOC** uit te zetten.

Cyber Protection-services geïnstalleerd in uw omgeving

Cyber Protection installeert enkele of alle van de volgende services, afhankelijk van de Cyber Protection-opties die u gebruikt.

Services geïnstalleerd in Windows

Servicenaam	Doel
Acronis Managed Machine Service	Biedt functionaliteit voor back-up, herstel, replicatie, retentie en validatie
Acronis Scheduler2 Service	Voert geplande taken uit voor bepaalde gebeurtenissen
Acronis Active Protection Service	Biedt bescherming tegen ransomware
Acronis Cyber Protection Service	Biedt antimalwarebeveiliging

Services geïnstalleerd in macOS

Servicenaam en locatie	Doel
`/Library/LaunchDaemons/com.acronis.aakore.plist`	Zorgt voor de communicatie tussen de agent en beheeronderdelen
`/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist`	Zorgt voor de detectie van malware
`/Library/LaunchDaemons/com.acronis.mms.plist`	Biedt back-up- en herstelfuncties
`/Library/LaunchDaemons/com.acronis.schedule.plist`	Voert geplande taken uit

Een agentlogbestand opslaan

U kunt het logboek van een agent opslaan in een zipbestand. Als een back-up om een onbekende reden mislukt, biedt dit bestand informatie die de technische ondersteuning kan helpen om het probleem vast te stellen.

Standaard is de informatie in het logboek geoptimaliseerd voor de laatste drie dagen, maar je kunt deze periode wijzigen.

Logboeken van agents verzamelen

1. Voer een van de volgende handelingen uit:
   - Ga naar **Apparaten** en selecteer de machine waarvan u de logboeken wilt verzamelen. Klik vervolgens op **Activiteiten**.
   - Ga naar **Instellingen** > **Agents** en selecteer de machine waarvan u de logboeken wilt verzamelen. Klik vervolgens op **Details**.
2. [Optioneel] Als u de standaardperiode wilt wijzigen waarvoor systeeminformatie wordt geregistreerd, klikt u op de pijl naast de knop **Systeeminformatie verzamelen** en selecteert u vervolgens de periode.
3. Klik op **Systeeminformatie verzamelen**.
4. Wanneer u via uw webbrowser wordt gevraagd waar u het bestand wilt opslaan, geeft u de locatie op waar u het bestand wilt opslaan.

Site-to-site Open VPN - Aanvullende informatie

Wanneer u een herstelserver maakt, configureert u het **IP-adres in het productienetwerk** en het **Test-IP-adres** van deze server.

Nadat u een failover hebt uitgevoerd (de virtuele machine in de cloud hebt uitgevoerd) en u aanmeldt op de virtuele machine om het IP-adres van de server te controleren, ziet u het **IP-adres in het productienetwerk**.

Wanneer u een testfailover uitvoert, kunt u de testserver alleen bereiken via het **Test-IP-adres**, dat alleen zichtbaar is in de configuratie van de herstelserver.

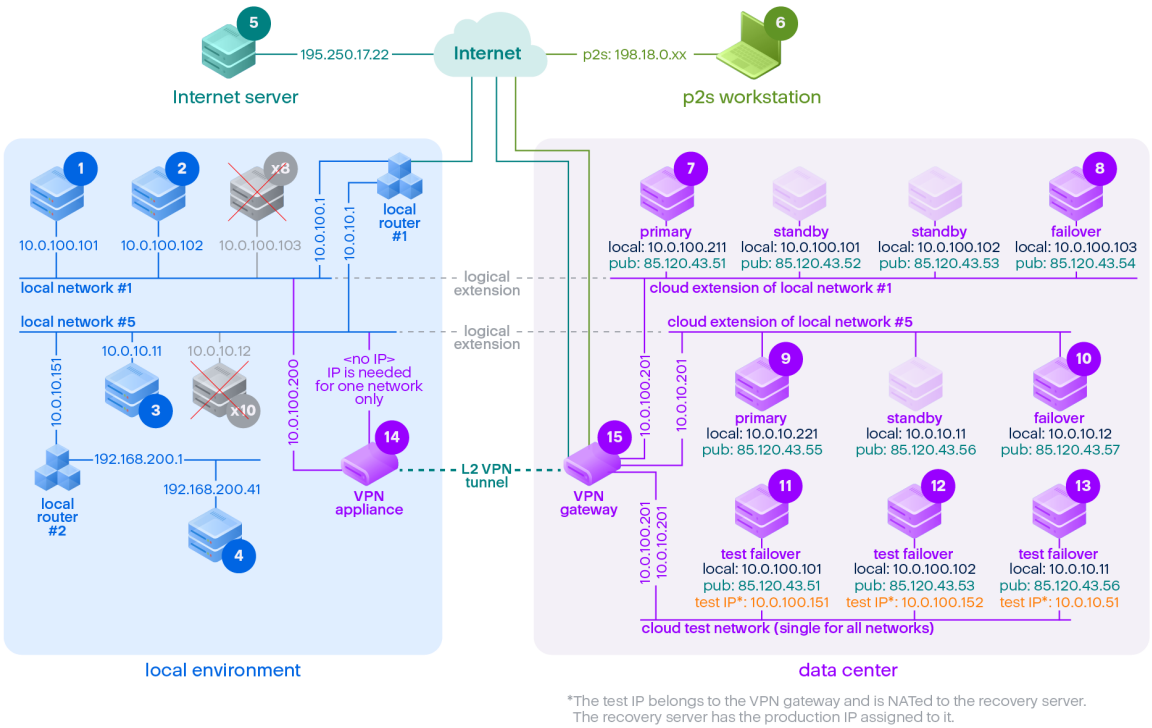
Als u een testserver wilt bereiken vanaf uw lokale site, moet u het **Test-IP-adres** gebruiken.

Opmerking
De netwerkconfiguratie van de server toont altijd het **IP-adres in het productienetwerk** (want de testserver geeft een spiegelbeeld van de productieserver). Dit gebeurt omdat het test-IP-adres niet bij de testserver hoort, maar bij de VPN-gateway, en via NAT wordt vertaald naar het productie-IP-adres.

Het onderstaande diagram bevat een voorbeeld van de site-to-site Open VPN-configuratie. Sommige servers in de lokale omgeving worden hersteld naar de cloud via failover (wanneer de netwerkinfrastructuur in orde is).

1. De klant heeft Noodherstel ingeschakeld door:
   a. de VPN-toepassing te configureren (14) en te verbinden met de speciale VPN-server in de cloud (15)
   b. sommige lokale servers te beschermen met Noodherstel (1, 2, 3, x8 en x10)

      Sommige servers op de lokale site (zoals 4) zijn verbonden met netwerken die niet zijn verbonden met de VPN-toepassing. Dergelijke servers worden niet beschermd met Noodherstel.
2. Een deel van de servers (verbonden met verschillende netwerken) werkt op de lokale site: (1, 2, 3 en 4)
3. De beveiligde servers (1, 2 en 3) worden getest met testfailover (11, 12 en 13)
4. Sommige servers op de lokale site zijn niet beschikbaar (x8, x10). Na het uitvoeren van een failover zijn ze beschikbaar in de cloud (8 en 10)
5. Sommige primaire servers (7 en 9), verbonden met verschillende netwerken, zijn beschikbaar in de cloudomgeving
6. (5) is een server op internet met een openbaar IP-adres
7. (6) is een werkstation dat is verbonden met de cloud via een point-to-site VPN-verbinding (p2s)



In dit voorbeeld is de volgende verbindingsconfiguratie beschikbaar (bijvoorbeeld 'ping') van een server in de rij **Van:** naar een server in de kolom **Aan:**.

	Tot:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Van:		lokaal	lokaal	lokaal	lokaal	internet	p2s	primair	failover	primair	failover	testfailover	testfailover	testfailover	VPN-toepassing	VPN-server
1	lokaal		direct	via lokale router 1	via lokale router 2	via lokale router 1 en internet	nee	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: NAT (VPN-server) via lokale router 1 en internet: pub	via tunnel: NAT (VPN-server) via lokale router 1 en internet: pub	via lokale router 1 en tunnel: NAT (VPN-server) via lokale rout	direct	nee

	Tot:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														er 1 en internet: pub		
2	lokaal	direct		via lokale router 1	via lokale router 2	via lokale router 1 en internet	nee	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: NAT (VPN-server) via lokale router 1 en internet: pub	via tunnel: NAT (VPN-server) via lokale router 1 en internet: pub	via lokale router 1 en tunnel: NAT (VPN-server) via lokale router 1 en internet: pub	direct	nee
3	lokaal	via lokale router 1	via lokale router 1		via lokale router 2	via lokale router 1 en internet	nee	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: lokaal via lokale router 1 en internet: pub	via tunnel: NAT (VPN-server) via lokale router 1 en internet: pub	via tunnel: NAT (VPN-server) via lokale router 1 en internet: pub	via lokale router 1 en tunnel: NAT (VPN-server) via lokale router 1	via lokale router	nee

	Tot:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														en internet: pub		
4	lokaal	via lokale router 2 en router 1	via lokale router 2 en router 1	via lokale router 2		via lokale router 2 en router 1 en internet	nee	via lokale router 2 en tunnel: lokaal via lokale router 2 en lokale router 1 en internet: pub	via lokale router 2 en tunnel: lokaal via lokale router 2 en lokale router 1 en internet: pub	via lokale router 2 en tunnel: lokaal via lokale router 2 en lokale router 1 en internet: pub	via lokale router 2 en tunnel: lokaal via lokale router 2 en lokale router 1 en internet: pub	via tunnel: NAT (VPN-server) via lokale router 2 en router 1 en internet: pub	via tunnel: NAT (VPN-server) via lokale router 2 en router 1 en internet: pub	via tunnel: NAT (VPN-server) via lokale router 2 en router 1 en internet: pub	via lokale router 2	nee
5	internet	nee	nee	nee	nee		N.v.t.	via internet: pub	via internet: pub	via internet: pub	via internet: pub	via internet: pub	via internet: pub	via internet: pub	nee	nee
6	p2s	nee	nee	nee	nee	via internet		via p2s VPN (VPN-ser	via p2s VPN (VPN-ser	via p2s VPN (VPN-ser	via p2s VPN (VPN-ser	via p2s VPN - NAT (VPN-serv	via p2s VPN - NAT (VPN-serv	via p2s VPN - NAT (VPN-serv	nee	nee

	Tot:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								ver): lokaal via internet: pub	ver): lokaal via internet: pub	ver): lokaal via internet: pub	ver): lokaal via internet: pub	er) via internet: pub	er) via internet: pub	er) via internet: pub		
7	primair	via tunnel	via tunnel	via tunnel en lokale router 1	via tunnel en lokale router 1 en 2	via internet (via VPN-server)	nee		direct in de cloud: lokaal	via tunnel en lokale router 1: lokaal	via tunnel en lokale router 1: lokaal	via VPN-server: NAT	via VPN-server: NAT	via tunnel en lokale router 1: NAT	nee	alle en DHCP- en DNS-protocol
8	failover	via tunnel	via tunnel	via tunnel en lokale router 1	via tunnel en lokale router 1 en 2	via internet (via VPN-server)	nee	direct in de cloud: lokaal		via tunnel en lokale router 1: lokaal	via tunnel en lokale router 1: lokaal	via VPN-server: NAT	via VPN-server: NAT	via tunnel en lokale router 1: NAT	nee	alle en DHCP- en DNS-protocol
9	primair	via tunnel en lokale ro	via tunnel en lokale ro	via tunnel	via tunnel	via internet (via VPN-ser	nee	via tunnel en lokale router	via tunnel en lokale router		direct in de cloud: lokaal	via tunnel en lokale router 1: NAT	via tunnel en lokale router 1: NAT	via VPN-server: NAT	nee	alle en DHCP- en DNS-pro

	Tot:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		uter 1	uter 1			ver)		1: lokaal	1: lokaal							tocol
10	failover	via tunnel en lokale router 1	via tunnel en lokale router 1	via tunnel	via tunnel	via internet (via VPN-server)	nee	via tunnel en lokale router 1: lokaal	via tunnel en lokale router 1: lokaal	direct in de cloud: lokaal		via tunnel en lokale router 1: NAT	via tunnel en lokale router 1: NAT	via VPN-server: NAT	nee	alle en DHCP-en DNS-protocol
11	testfailover	nee	nee	nee	nee	via internet (via VPN-server)	nee	nee	nee	nee	nee		direct in de cloud: lokaal	via VPN-server: lokaal (routering)	nee	alle en DHCP-en DNS-protocol
12	testfailover	nee	nee	nee	nee	via internet (via VPN-server)	nee	nee	nee	nee	nee	direct in de cloud: lokaal		via VPN-server: lokaal (routering)	nee	alle en DHCP-en DNS-protocol
13	testfailover	nee	nee	nee	nee	via internet (via VPN-server)	nee	nee	nee	nee	nee	via VPN-server: lokaal (routering)	via VPN-server: lokaal (routering)		nee	alle en DHCP-en DNS-protoc

	Tot:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
																ol
14	VPN-toepassing	direct	direct	via lokale router 1	via lokale router 2	via internet (lokale router 1)	nee	nee	nee	nee	nee	nee	nee	nee		nee
15	VPN-server	nee	nee	nee	nee	nee	nee	nee	nee	nee	nee	nee	nee	nee	nee	

Licentiebeheer voor on-premises beheerservers

Voor gedetailleerde informatie over hoe u een on-premises beheerserver activeert of hoe u hieraan licenties toewijst, raadpleegt u het gedeelte Licenties in de Cyber Protect-gebruikershandleiding.

Werken met plannen

Inzicht in plannen

Opmerking
De beschikbaarheid van sommige functies hangt af van de opties die zijn ingeschakeld voor uw account.

Een plan is een set van configuraties en regels die u kunt toepassen op één of meerdere workloads voor verschillende doelen, zoals een back-up maken van een workload, een workload beschermen tegen malware, prestaties van de workload monitoren, enz.

Een plan bestaat uit modules die u kunt inschakelen of uitschakelen. Elke module bevat instellingen die gerelateerd zijn aan een specifieke functionaliteit.

Alle plannen die u hebt gemaakt, zijn zichtbaar op het tabblad **Beheer**.

Schema	Beschrijving
Beschermingsschema	Beschermt de gegevens van de workload. Het beschermingsplan bestaat uit de volgende modules: • Back-up • "Noodherstel implementeren" (p. 775) • Antivirus- en antimalwarebeveiliging • Eindpuntdetectie en -respons (EDR) • URL-filtering • Windows Defender Antivirus • Microsoft Security Essentials • Evaluatie van beveiligingsproblemen • Patchbeheer • Overzicht van gegevensbescherming • Apparaatbeheer • Advanced Data Loss Prevention Voor meer informatie over de beschermingsplannen: zie "Beschermingsschema's en -modules" (p. 216).
Plan voor extern beheer	Maakt de functionaliteit voor extern bureaublad en hulp op afstand mogelijk voor uw beheerde workloads. Voor meer informatie: zie "Schema's voor extern beheer" (p. 1065).
Scripting-schema	Maakt scriptuitvoering voor meerdere workloads, geplande scriptuitvoering en configuratie van extra scriptinstellingen mogelijk. Voor meer informatie: zie "Scripting-schema's" (p. 410).
Controleschema	Monitort de performance, hardware, software, systeem- en

Schema	Beschrijving
	beveiligingsparameters van uw beheerde workloads. Voor meer informatie: zie "Bewakingsschema" (p. 1140).
Back-up van cloudtoepassingen	Maakt back-ups van applicaties in de cloud door middel van agents in de cloud, waarbij de cloudopslag wordt gebruikt als back-uplocatie. Voor meer informatie: zie "Back-upschema's voor cloudtoepassingen" (p. 241)
Schema voor back-upscans	Scant back-ups op malware (inclusief ransomware).
VM-replicatie	Scant back-ups op malware (inclusief ransomware). Voor meer informatie: zie "Replicatie van virtuele machines" (p. 720).
Validatie	Valideert een back-up en verifieert of de gegevens uit de back-up kunnen worden hersteld. Voor meer informatie: zie "Validatie" (p. 228).
Opschonen	Verwijdert verouderde back-ups volgens de retentieregels. Dit plan is alleen van toepassing op agents en workloads, en niet op cloud-naar-cloud back-ups. Voor meer informatie: zie "Opschonen" (p. 235).
Conversie naar VM	Dit plan is alleen van toepassing op back-ups op schijfniveau. Controleert of een back-up het systeemvolume en alle informatie bevat die nodig is om het besturingssysteem te starten, zodat de resulterende virtuele machine zelfstandig kan starten. Voor meer informatie: zie "Conversie naar een virtuele machine" (p. 236).
Back-upreplicatie	Repliceert een back-up naar een andere locatie. Voor meer informatie: zie "Back-upreplicatie" (p. 225).

Ingebouwde plannen

Ingebouwde plannen zijn plannen die vooraf zijn geconfigureerd met enkele van de meest gebruikte of aanbevolen instellingen. Ingebouwde plannen zijn direct beschikbaar voor selectie. U kunt ingebouwde plannen niet wijzigen, maar nadat u een ingebouwd plan hebt toegepast op een workload, kunt u de instellingen bewerken.

Ingebouwde plannen zijn beschikbaar voor de volgende typen plannen: beschermingsplannen, monitoringplannen en plannen voor extern beheer.

Ingebouwde beschermingsplannen

De volgende tabel bevat meer informatie over de ingebouwde beschermingsplannen.

Modules en instellingen	Ingebouwde beschermingsplannen		
	Essentiële bescherming	**Uitgebreide bescherming**	**Volledige bescherming**
	Minimale downtime en gegevensverlies, moeiteloos herstel met kort RPO en eenvoudig onderhoud	**Tweede niveau van bescherming: bedrijfscontinuïteit, proactieve beperking van beveiligingsrisico's en naleving**	**Derde niveau van bescherming: bedrijfscontinuïteit, bijna nul RTO, proactieve beperking van beveiligingsrisico's, preventie van gegevenslekken en naleving**
Back-up	Aan	Aan	Aan
BACK-UP VAN Items waarvan een back-up moet worden gemaakt	Volledige machine	Volledige machine	Volledige machine
Continue gegevensbescherming (CDP)	Uitgeschakeld	Uitgeschakeld	Ingeschakeld
Waar back-up maken	Cloudopslag	Cloudopslag	Cloudopslag
Planning	Maandag t/m vrijdag om 12:00 uur Aanvullende ingeschakelde opties en startvoorwaarden: • Als de machine is uitgeschakeld, gemiste taken uitvoeren wanneer de machine wordt opgestart • De slaapstand of stand-bymodus beëindigen om een geplande back-up te starten • Batterijstroom	Maandag t/m vrijdag om 00:00 uur Aanvullende ingeschakelde opties en startvoorwaarden: • Als de machine is uitgeschakeld, gemiste taken uitvoeren wanneer de machine wordt opgestart • De slaapstand of stand-bymodus beëindigen om een geplande back-up te starten • Batterijstroom besparen: Niet starten bij gebruik van batterijstroom	Maandag t/m vrijdag om 00:00 uur Aanvullende ingeschakelde opties en startvoorwaarden: • Als de machine is uitgeschakeld, gemiste taken uitvoeren wanneer de machine wordt opgestart • De slaapstand of stand-bymodus beëindigen om een geplande back-up te starten • Batterijstroom besparen: Niet starten bij gebruik van batterijstroom

Modules en instellingen	Ingebouwde beschermingsplannen		
	Essentiële bescherming	**Uitgebreide bescherming**	**Volledige bescherming**
	Minimale downtime en gegevensverlies, moeiteloos herstel met kort RPO en eenvoudig onderhoud	**Tweede niveau van bescherming: bedrijfscontinuïteit, proactieve beperking van beveiligingsrisico's en naleving**	**Derde niveau van bescherming: bedrijfscontinuïteit, bijna nul RTO, proactieve beperking van beveiligingsrisico's, preventie van gegevenslekken en naleving**
	besparen: Niet starten bij gebruik van batterijstroom • Niet starten bij verbinding met een datalimiet	• Niet starten bij verbinding met een datalimiet	• Niet starten bij verbinding met een datalimiet
Back-upschema	Altijd incrementeel	Altijd incrementeel	Altijd incrementeel
Bewaartijd	Alle back-ups 90 dagen bewaren	Alle back-ups 90 dagen bewaren	Alle back-ups 90 dagen bewaren
Back-upopties	Standaardopties	Standaardopties, plus: • Prestatie- en back-upvenster (de groene set): CPU-prioriteit: Laag Uitvoersnelheid: 50%	Standaardopties, plus: • Prestatie- en back-upvenster (de groene set): CPU-prioriteit: Laag Uitvoersnelheid: 50%
EDR	Uit	Uit	Aan
Antivirus- en antimalwarebeveiliging	Aan	Aan	Aan
Active Protection	Aan	Aan	Aan
Geavanceerde antimalware	Aan	Aan	Aan
Netwerkmapbescherming	Aan	Aan	Aan
Bescherming op server	Uit	Uit	Uit

Modules en instellingen	Ingebouwde beschermingsplannen		
	Essentiële bescherming	**Uitgebreide bescherming**	**Volledige bescherming**
	Minimale downtime en gegevensverlies, moeiteloos herstel met kort RPO en eenvoudig onderhoud	**Tweede niveau van bescherming: bedrijfscontinuïteit, proactieve beperking van beveiligingsrisico's en naleving**	**Derde niveau van bescherming: bedrijfscontinuïteit, bijna nul RTO, proactieve beperking van beveiligingsrisico's, preventie van gegevenslekken en naleving**
Zelfbescherming	Aan	Aan	Aan
Detectie van cryptomining-processen	Aan	Aan	Aan
Quarantaine	Bestanden in quarantaine verwijderen na 30 dagen	Bestanden in quarantaine verwijderen na 30 dagen	Bestanden in quarantaine verwijderen na 30 dagen
Gedragengine	Quarantaine	Quarantaine	Quarantaine
Preventie tegen aanvallen	Melden en het proces stoppen	Melden en het proces stoppen	Melden en het proces stoppen
Realtime bescherming	Quarantaine	Quarantaine	Quarantaine
Scan plannen	Snelle scan: Quarantaine Om 20:00 uur, zondag t/m zaterdag Volledige scan: Quarantaine Om 21:00 uur, woensdag en vrijdag Aanvullende ingeschakelde opties en startvoorwaarden: De slaapstand of stand-bymodus beëindigen om een	Snelle scan: Quarantaine Om 20:00 uur, zondag t/m zaterdag Volledige scan: Quarantaine Om 21:00 uur, woensdag en vrijdag Aanvullende ingeschakelde opties en startvoorwaarden: De slaapstand of stand-bymodus beëindigen om een geplande back-up te starten	Snelle scan: Quarantaine Om 20:00 uur, zondag t/m zaterdag Volledige scan: Quarantaine Om 21:00 uur, woensdag en vrijdag Aanvullende ingeschakelde opties en startvoorwaarden: De slaapstand of stand-bymodus beëindigen om een geplande back-up te starten

Modules en instellingen	Ingebouwde beschermingsplannen		
	Essentiële bescherming	**Uitgebreide bescherming**	**Volledige bescherming**
	Minimale downtime en gegevensverlies, moeiteloos herstel met kort RPO en eenvoudig onderhoud	**Tweede niveau van bescherming: bedrijfscontinuïteit, proactieve beperking van beveiligingsrisico's en naleving**	**Derde niveau van bescherming: bedrijfscontinuïteit, bijna nul RTO, proactieve beperking van beveiligingsrisico's, preventie van gegevenslekken en naleving**
	geplande back-up te starten		
Uitsluitingen	Geen	Geen	Geen
URL-filtering	Uit	Aan	Aan
Toegang via schadelijke website	Blokkeren	Blokkeren	Blokkeren
Categorieën om te filteren	Standaardopties	Standaardopties	Standaardopties
Uitsluitingen	Geen	Geen	Geen
Microsoft Defender Antivirus	Uit	Uit	Uit
Firewallbeheer	Uit	Aan	Aan
Microsoft Security Essentials	Uit	Uit	Uit
Evaluatie van beveiligingsproblemen	Aan	Aan	Aan
Bereik van evaluatie van beveiligingsproblemen	Microsoft-producten, Windows-producten van derden, Apple-producten, macOS-producten van derden, Scan Linux-pakket	Microsoft-producten, Windows-producten van derden, Apple-producten, macOS-producten van derden, Scan Linux-pakket	Microsoft-producten, Windows-producten van derden, Apple-producten, macOS-producten van derden, Scan Linux-pakket
Planning	Om 11:00 uur, alleen op woensdag en vrijdag	Om 11:00 uur, alleen op woensdag en vrijdag	Om 11:00 uur, alleen op woensdag en vrijdag

Modules en instellingen	Ingebouwde beschermingsplannen		
	Essentiële bescherming	**Uitgebreide bescherming**	**Volledige bescherming**
	Minimale downtime en gegevensverlies, moeiteloos herstel met kort RPO en eenvoudig onderhoud	**Tweede niveau van bescherming: bedrijfscontinuïteit, proactieve beperking van beveiligingsrisico's en naleving**	**Derde niveau van bescherming: bedrijfscontinuïteit, bijna nul RTO, proactieve beperking van beveiligingsrisico's, preventie van gegevenslekken en naleving**
Patchbeheer	Aan	Aan	Aan
Microsoft-producten	Alle updates	Alle updates	Alle updates
Windows-producten van derden	Alle updates	Alle updates	Alle updates
Planning	Om 12:30 uur, alleen op woensdag en vrijdag	Om 12:30 uur, alleen op woensdag en vrijdag	Om 12:30 uur, alleen op woensdag en vrijdag
Back-up vóór update	Aan	Aan	Aan
Overzicht van gegevensbescherming	Uit	Uit	Aan
Extensies en uitzonderingsregels	–	–	Standaardopties (66 extensies die moeten worden gedetecteerd)
Planning	–	–	Om 15:40 uur, maandag t/m vrijdag
Apparaatbesturing	Uit	Uit	Uit
Toegangsinstellingen	Toegestaan: Alles	Toegestaan: Alles	Toegestaan: Alles
Acceptatielijst voor apparaattypen	1 toegestaan (USD HID (muis, toetsenbord, enz.)	1 toegestaan (USD HID (muis, toetsenbord, enz.)	1 toegestaan (USD HID (muis, toetsenbord, enz.)
Acceptatielijst voor USB-apparaten	Leeg	Leeg	Leeg
Uitsluiting	Geen	Geen	Geen

Modules en instellingen	Ingebouwde beschermingsplannen		
	Essentiële bescherming	**Uitgebreide bescherming**	**Volledige bescherming**
	Minimale downtime en gegevensverlies, moeiteloos herstel met kort RPO en eenvoudig onderhoud	**Tweede niveau van bescherming: bedrijfscontinuïteit, proactieve beperking van beveiligingsrisico's en naleving**	**Derde niveau van bescherming: bedrijfscontinuïteit, bijna nul RTO, proactieve beperking van beveiligingsrisico's, preventie van gegevenslekken en naleving**
Preventie van gegevensverlies	Uit	Uit	Uit
Modus	–	–	–
Geavanceerde instellingen	–	–	–
Disaster Recovery	Uit	Uit	Uit

Voor meer informatie over beschermingsplannen: zie "Beschermingsschema's en -modules" (p. 216).

Ingebouwde monitoringplannen

De volgende tabel bevat meer informatie over de ingebouwde monitoringplannen.

Naam	Beschrijving	Ingeschakelde monitors
Aanbevolen voor Windows	Controleert de status en prestaties van Windows-machines	De volgende 13 monitors zijn ingeschakeld in dit plan: • Status van antimalwaresoftware • Status van de Autorun-functie • CPU-temperatuur • CPU-gebruik • Schijfruimte • Schijfoverdrachtssnelheid • Mislukte aanmeldingen • Firewallstatus • GPU-temperatuur • Laatste herstart van systeem • Geheugengebruik • Netwerkgebruik

Naam	Beschrijving	Ingeschakelde monitors
		• Windows Update-status
Aanbevolen voor macOS	Monitort de gezondheid en performance van macOS-machines	De volgende 10 monitors zijn ingeschakeld in dit plan: • Status van antimalwaresoftware • CPU-temperatuur • CPU-gebruik • Schijfruimte • Schijfoverdrachtssnelheid • Firewallstatus • GPU-temperatuur • Laatste herstart van systeem • Geheugengebruik • Netwerkgebruik
Aanbevolen voor servers	Monitort de gezondheid en performance van Windows-servers	De volgende 20 monitors zijn ingeschakeld in dit plan: • Status van antimalwaresoftware • CPU-temperatuur, 2 monitors: 80 graden, 10 min., waarschuwing 90 graden, 10 min., kritiek • CPU-gebruik, 3 monitors: Minder dan 20%, 10 min., informatie Meer dan 80%, 10 min., waarschuwing Meer dan 90%, 10 min., kritiek • Schijfruimte, 2 monitors: Minder dan 20%, 30 min., waarschuwing Minder dan 10%, 30 min., kritiek • Schijfoverdrachtssnelheid • Mislukte aanmeldingspogingen, 3 monitors: 5 pogingen, 1 uur, informatie 10 pogingen, 1 uur, waarschuwing 20 pogingen, 1 uur, kritiek • Firewallstatus • Hardwarewijzigingen • Geïnstalleerde software • Geheugengebruik, 3 monitors: Minder dan 20%, 10 min.,

Naam	Beschrijving	Ingeschakelde monitors
		informatie Meer dan 80%, 10 min., waarschuwing Meer dan 90%, 10 min., kritiek • Netwerkgebruik • Windows Update-status

Voor meer informatie over monitoringsplannen: zie "Bewakingsschema" (p. 1140).

Ingebouwde plannen voor extern beheer

De volgende tabel bevat meer informatie over het ingebouwde plan voor extern beheer.

Naam	Beschrijving	Instellingen
Essentieel extern bureaublad	Schakelt de mogelijkheden voor extern bureaublad en bestandsoverdracht in	Verbindingsprotocollen **Verbindingen toestaan via NEAR**: Aan NEAR-beveiligingsinstellingen • **Workload vergrendelen wanneer de gebruiker de verbinding met de consolesessie verbreekt**: Uit • **Slechts één gebruiker tegelijk toestaan om verbinding te maken met NEAR of bestanden over te dragen**: Uit • **Workloadbeheerder toestaan om verbinding te maken met elke sessie**: Aan • **Het maken van systeemsessies toestaan**: Uit • **Klembordsynchronisatie toestaan**: Aan **Verbindingen via RDP toestaan**: Aan **Verbindingen toestaan via schermdeling van Apple**: Uit Beveiligingsinstellingen • **Weergeven of de workload op afstand wordt beheerd**: Aan • **De gebruiker toestemming vragen om momentopnamen van de workload te maken**: Aan Workloadbeheer • **Bestandsoverdracht**: Aan • **Overdracht van momentopnamen**: Uit

Naam	Beschrijving	Instellingen
		Weergave-instellingen • **Bureaubladdeduplicatie gebruiken voor het vastleggen van bureaubladen**: Aan • **OpenCL-versnelling gebruiken**: Aan • **H.264-hardwarecodering gebruiken**: Aan Toolbox **Laatst aangemelde gebruikers weergeven**: Uit

Voor meer informatie over plannen voor extern beheer: zie "Schema's voor extern beheer" (p. 1065).

Standaardplannen

Het standaardplan is een plan dat vooraf geselecteerd is in de lijst met plannen in de velden voor planselectie. U kunt slechts één standaardplan per tenant hebben voor elk ondersteund plantype op een gegeven moment. U kunt een standaardplan niet verwijderen totdat u een ander plan als standaard instelt.

Standaardplannen worden ondersteund voor de volgende plantypen: beschermingsplannen, monitoringplannen en plannen voor extern beheer.

Plannen instellen als standaard

U kunt één plan van de ondersteunde plantypen (beschermingsplan, monitoringplan of plan voor extern beheer) als standaard instellen.

Opmerking
De functie is niet beschikbaar voor gebruikers aan wie de rol van alleen-lezen beheerder is toegewezen voor de beschermingsservice.

Beschermingsschema's

Vereisten

Er is ten minste één beschermingsplan gemaakt voor uw tenant. Voor meer informatie: zie "Een beschermingsschema maken" (p. 217).

Een beschermingsplan instellen als standaard

1. Open het scherm **Beschermingsplannen**, zoek het plan dat u wilt instellen als standaard en klik op dat plan.
2. Klik op **Instellen als standaard**.
3. Klik in het bevestigingsvenster op **Instellen**.

In het scherm **Beschermingsplannen** wordt de tag **Standaard** weergegeven naast de naam van het plan.

Schema's voor extern beheer

Vereisten

- 2FA is ingeschakeld voor uw gebruikersaccount.
- Er is ten minste één plan voor extern beheer gemaakt voor uw tenant. Voor meer informatie: zie "Een schema voor extern beheer maken" (p. 1065).

Een plan voor extern beheer instellen als standaard:

1. Open het scherm **Plannen voor extern beheer** en zoek het plan dat u wilt instellen als standaard.
2. Klik in dezelfde rij op het pictogram **Meer acties**
3. Klik op **Instellen als standaard**.
4. Klik in het bevestigingsvenster op **Instellen**.
   In het scherm **Plannen voor extern beheer** wordt de tag **Standaard** weergegeven naast de naam van het plan.

Bewakingsschema

Vereisten

- 2FA is ingeschakeld voor uw gebruikersaccount.
- Er is ten minste één monitoringplan gemaakt voor uw tenant. Voor meer informatie: zie "Een controleschema maken" (p. 1140).

Een monitoringplan instellen als extern

1. Open het scherm **Montoringplannen** en zoek het plan dat u wilt instellen als standaard.
2. Klik in dezelfde rij op het pictogram **Meer acties**.
3. Klik op **Toevoegen aan favorieten**.
4. Klik in het bevestigingsvenster op **Instellen**.
   In het scherm **Monitoringplannen** wordt de tag **Standaard** weergegeven naast de naam van het plan.

Favoriete plannen

Favoriete plannen worden bovenaan de lijst met plannen weergegeven. Wanneer u een plan als favoriet instelt, is dit plan zichtbaar en gemakkelijk te vinden, zelfs wanneer uw organisatie een lange lijst met veel plannen heeft.

Favoriete plannen worden ondersteund voor de volgende typen plannen: beschermingsplannen, monitoringplannen en plannen voor extern beheer.

Plannen instellen als favoriet

U kunt tot 10 favoriete plannen instellen per ondersteund plantype (beschermingsplan, monitoringplan of plan voor extern beheer) per tenant.

Opmerking
De functie is niet beschikbaar voor gebruikers aan wie de rol van alleen-lezen beheerder is toegewezen voor de beschermingsservice.

Beschermingsschema's

Vereisten

Er is ten minste één beschermingsplan gemaakt voor uw tenant. Voor meer informatie: zie "Een beschermingsschema maken" (p. 217).

Een beschermingsplan instellen als favoriet

1. Klik in het scherm **Beschermingsplannen** op het plan dat u wilt instellen als favoriet.
2. Klik op **Instellen als favoriet**.
   In het scherm **Beschermingsplannen** wordt een pictogram van een ster weergegeven naast de naam van het plan.

Schema's voor extern beheer

Vereisten

- 2FA is ingeschakeld voor uw gebruikersaccount.
- Er is ten minste één plan voor extern beheer gemaakt voor uw tenant. Voor meer informatie: zie "Een controleschema maken" (p. 1140).

Een plan voor extern beheer instellen als favoriet

1. Open het scherm **Plannen voor extern beheer** en zoek het plan dat u wilt toevoegen als favoriet.
2. Klik in de rij van het plan op het pictogram **Meer acties**.
3. Klik op **Toevoegen aan favorieten**.
   In het scherm **Plannen voor extern beheer** wordt een pictogram van een ster weergegeven naast de naam van het plan.

Bewakingsschema

Vereisten

- 2FA is ingeschakeld voor uw gebruikersaccount.
- Er is ten minste één beheerplan gemaakt voor uw tenant. Voor meer informatie: zie "Een controleschema maken" (p. 1140).

Monitoringplan instellen als favoriet:

1. Open het scherm **Montoringplannen** en zoek het plan dat u wilt instellen als favoriet.
2. Klik in de rij van het plan op het pictogram **Meer acties**.
3. Klik op **Toevoegen aan favorieten**.
   In het scherm **Monitoringplannen** wordt een pictogram van een ster weergegeven naast de naam van het plan.

Plannen verwijderen uit favorieten

U kunt favoriete beschermingsplannen, monitoringplannen en plannen voor extern beheer verwijderen uit de lijst met favorieten.

Opmerking
De functie is niet beschikbaar voor gebruikers aan wie de rol van alleen-lezen beheerder is toegewezen voor de beschermingsservice.

Beschermingsschema's

Vereisten

Er is ten minste één beschermingsplan ingesteld als favoriet voor uw tenant.

Een beschermingsplan verwijderen uit de favorieten:

1. Klik in het scherm **Beschermingsplannen** op het plan dat u wilt verwijderen uit favorieten.
2. Klik op **Verwijderen uit favorieten**.

Schema's voor extern beheer

Vereisten

- 2FA is ingeschakeld voor uw gebruikersaccount.
- Er is ten minste één plan voor extern beheer ingesteld als favoriet voor uw tenant.

Een plan voor extern beheer verwijderen uit de favorieten:

1. Open het scherm **Plannen voor extern beheer** en zoek het plan dat u wilt verwijderen uit favorieten.
2. Klik in de rij van het plan op het pictogram **Meer acties**.
3. Klik op **Verwijderen uit favorieten**.

Bewakingsschema

Vereisten

- 2FA is ingeschakeld voor uw gebruikersaccount.
- Er is ten minste één monitoringplan ingesteld als favoriet voor uw tenant.

Een monitoringplan verwijderen uit de favorieten:

1. Open het scherm **Monitoringplannen** en zoek het plan dat u wilt verwijderen uit favorieten.
2. Klik in de rij van het plan op het pictogram **Meer acties**.
3. Klik op **Verwijderen uit favorieten**.

Beschermingsschema's en -modules

Als u uw gegevens wilt beschermen, moet u beschermingsschema's maken en deze vervolgens toepassen op uw workloads.

Een beschermingsschema bestaat uit verschillende beschermingsmodules. Schakel de modules in die u nodig hebt en configureer de instellingen om beschermingsschema's te maken die aan uw specifieke behoeften voldoen.

De volgende modules zijn beschikbaar:

- Back-up. Maakt een back-up van uw gegevensbronnen naar een lokale of cloudopslag.
- "Noodherstel implementeren" (p. 775). Start exacte kopieën van uw machines op de cloudsite en verplaatst de workload van beschadigde oorspronkelijke machines naar de herstelservers in de cloud.
- Antivirus- en antimalwarebeveiliging. Controleert uw workloads via een ingebouwde antimalwareoplossing.
- Eindpuntdetectie en -respons (EDR). Detecteert verdachte activiteiten voor de workload, waaronder onopgemerkte aanvallen, en genereert incidenten die u inzicht geven in de manier van uitvoering van een aanval en hoe u deze in de toekomst kunt voorkomen.
- URL-filtering. Beschermt uw machines tegen bedreigingen vanuit internet. Hierbij wordt de toegang tot schadelijke URL's en downloadbare inhoud geblokkeerd.
- Windows Defender Antivirus. Beheert de instellingen van Windows Defender Antivirus om uw omgeving te beschermen.
- Microsoft Security Essentials. Beheert de instellingen van Microsoft Security Essentials om uw omgeving te beschermen.
- Evaluatie van beveiligingsproblemen. Controleert Windows, Linux, macOS, Microsoft-producten van derden en macOS-producten van derden die op uw machines zijn geïnstalleerd en stelt u op de hoogte van beveiligingsproblemen.
- Patchbeheer. Installeert patches en updates voor Windows, Linux, macOS, Microsoft-producten van derden en macOS-producten van derden op uw machines om de gedetecteerde beveiligingsproblemen op te lossen.
- Overzicht van gegevensbescherming. Detecteert gegevens om de beschermingsstatus van belangrijke bestanden te bewaken.
- Apparaatbeheer. Geef apparaten aan die gebruikers wel of niet mogen gebruiken op uw machines.

- Advanced Data Loss Prevention. Voorkomt het lekken van gevoelige gegevens via randapparatuur (zoals printers of verwisselbare opslag), of via interne en externe netwerkoverdrachten, op basis van een datastroombeleid.

Een beschermingsschema maken

U kunt een beschermingsschema op de volgende manieren maken:

- Op het tabblad **Apparaten**. Selecteer een of meer workloads die u wilt beschermen en maak vervolgens een beschermingsschema voor deze workloads.
- Op het tabblad **Beheer** > **Beschermingsschema's**. Maak een beschermingsschema en selecteer vervolgens een of meer workloads waarop u het schema wilt toepassen.

Wanneer u een beschermingsschema maakt, worden alleen de modules weergegeven die van toepassing zijn op uw type workload.

U kunt een beschermingsschema toepassen op meer dan één workload. U kunt ook meerdere beschermingsschema's toepassen op dezelfde workload. Voor meer informatie over mogelijke conflicten: zie "Conflicten tussen schema's oplossen" (p. 223).

Een beschermingsschema maken

Apparaten

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de workloads die u wilt beschermen en klik vervolgens op **Beschermen**.
3. [Indien er reeds toegepaste schema's zijn] Klik op **Schema toevoegen**.
4. Klik op **Schema maken** > **Bescherming**.
   Het deelvenster van het beschermingsschema wordt geopend.
5. [Optioneel] Als u de naam van het beschermingsplan wilt wijzigen, klikt u op het potloodpictogram en voert u vervolgens de nieuwe naam in.
6. [Optioneel] Gebruik de schakelaar naast de modulenaam om een module in het schema in of uit te schakelen.
7. [Optioneel] Als u een module wilt configureren, klikt u erop om deze uit te vouwen. Vervolgens kunt u de instellingen naar wens wijzigen.
8. Wanneer u klaar bent, klikt u op **Maken**.

> **Opmerking**
> Als u een beschermingsschema met versleuteling wilt maken, geeft u een versleutelingswachtwoord op. Voor meer informatie: zie "Versleuteling" (p. 469).

Beheer > Beschermingsschema's

1. Ga in de Cyber Protect-console naar **Beheer** > **Beschermingsschema's**.
2. Klik op **Schema maken**.
   De sjabloon voor een beschermingsschema wordt geopend.

3. [Optioneel] Als u de naam van het beschermingsplan wilt wijzigen, klikt u op het potloodpictogram en voert u vervolgens de nieuwe naam in.
4. [Optioneel] Gebruik de schakelaar naast de modulenaam om een module in het schema in of uit te schakelen.
5. [Optioneel] Als u een module wilt configureren, klikt u erop om deze uit te vouwen. Vervolgens kunt u de instellingen naar wens wijzigen.
6. [Optioneel] Klik op **Apparaten toevoegen** om de workloads te selecteren waarop u het schema wilt toepassen.

   Opmerking
   U kunt een schema maken zonder het toe te passen op workloads. U kunt later workloads toevoegen door het schema te bewerken. Voor meer informatie over hoe u een workload aan een schema toevoegt: zie "Een beschermingsschema toepassen op een workload" (p. 219).

7. Wanneer u klaar bent, klikt u op **Maken**.

   Opmerking
   Als u een beschermingsschema met versleuteling wilt maken, geeft u een versleutelingswachtwoord op. Voor meer informatie: zie "Versleuteling" (p. 469).

Als u een module op aanvraag wilt uitvoeren (zoals **Back-up**, **Antivirus- en antimalwarebeveiliging**, **Evaluatie van beveiligingsproblemen**, **Patchbeheer** of **Overzicht van gegevensbescherming**), klikt u op **Nu uitvoeren**.

Bekijk de instructievideo Het eerste beschermingsschema maken.

Voor meer informatie over de module voor noodherstel: zie "Een beschermingsschema voor noodherstel maken" (p. 781).

Voor meer informatie over de module voor apparaatbeheer: zie "Werken met de module Apparaatbeheer" (p. 353).

Acties met beschermingsschema's

Wanneer u een beschermingsschema hebt gemaakt, kunt u hiermee de volgende acties uitvoeren:

- Een schema toepassen op een workload of een apparaatgroep.
- Naam van een schema wijzigen.
- Een schema bewerken.
  U kunt de modules in een schema in- en uitschakelen en de instellingen wijzigen.
- Een schema in- of uitschakelen.
  Een uitgeschakeld schema wordt niet uitgevoerd in de workloads waarop het wordt toegepast.
  Deze actie is handig voor beheerders die dezelfde workload later met hetzelfde schema willen beschermen. Het schema wordt niet ingetrokken van de workload en u kunt de bescherming snel herstellen door het schema opnieuw in te schakelen.

- Een schema intrekken van een workload.

  Een ingetrokken schema wordt niet meer toegepast op de workload.

  Deze actie is handig voor beheerders die niet opnieuw een snelle bescherming nodig hebben voor dezelfde workload met hetzelfde schema. Als u de bescherming van een ingetrokken schema wilt herstellen, moet u de naam van dit schema weten, het selecteren in de lijst met beschikbare schema's en het vervolgens opnieuw toepassen op de betreffende workload.
- Een schema stoppen.
  Deze actie stopt alle actieve back-upbewerkingen voor alle workloads waarop het schema wordt toegepast. Back-ups beginnen opnieuw volgens de planning van het schema.

  Antimalwarescans worden niet beïnvloed door deze actie en worden uitgevoerd zoals geconfigureerd in het schema.
- Een schema klonen.

  U kunt een exacte kopie maken van een bestaand schema. Het nieuwe schema wordt niet toegewezen aan workloads.
- Een schema exporteren en importeren.

  U kunt een schema exporteren als een JSON-bestand, dat u later weer kunt importeren. U hoeft dus niet handmatig een nieuw schema te maken en de instellingen ervan te configureren.

  Opmerking
  U kunt beschermingsschema's importeren die zijn gemaakt in Cyber Protection 9.0 (uitgebracht in maart 2020) en later. Schema's die in eerdere versies zijn gemaakt, zijn niet compatibel met Cyber Protection 9.0 en hoger.

- De details van een schema controleren.
- De activiteiten en waarschuwingen voor een schema controleren.
- Een schema verwijderen.

Een beschermingsschema toepassen op een workload

Als u een workload wilt beschermen, moet u hierop een beschermingsschema toepassen.

U kunt een schema toepassen vanuit het tabblad **Apparaten** en vanuit het tabblad **Beheer** > **Beschermingsschema's**.

Apparaten

1. Selecteer een of meer workloads die u wilt beschermen.
2. Klik op **Beschermen**.
3. [Als er al een ander beschermingsschema is toegepast op de geselecteerde workloads] Klik op **Schema toevoegen**.
4. Er wordt een lijst met beschikbare beschermingsschema's weergegeven.
5. Selecteer het beschermingsschema dat u wilt toepassen en klik vervolgens op **Toepassen**.

Beheer > Beschermingsschema's

1. Ga in de Cyber Protect-console naar **Beheer** > **Beschermingsschema's**.
2. Selecteer het beschermingsschema dat u wilt toepassen.
3. Klik op **Bewerken**.
4. Klik op **Apparaten beheren**.
5. Klik in het venster **Apparaten** op **Toevoegen**.
6. Selecteer de workloads waarop u het schema wilt toepassen en klik vervolgens op **Toevoegen**.
7. Klik in het venster **Apparaten** op **Gereed**.
8. Open het deelvenster van het beschermingsschema en klik op **Opslaan**.

Voor informatie over het toepassen van een beschermingsschema voor een apparaatgroep: zie "Een schema toepassen op een groep" (p. 351).

Een beschermingsschema bewerken

Wanneer u een schema bewerkt, kunt u de modules in het schema in- en uitschakelen en de instellingen wijzigen.

U kunt een beschermingsschema bewerken voor alle workloads waarop het wordt toegepast of alleen voor geselecteerde workloads.

U kunt een schema bewerken vanuit het tabblad **Apparaten** en vanuit het tabblad **Beheer** > **Beschermingsschema's**.

Apparaten

1. Selecteer een of meer workloads waarop het schema wordt toegepast.
2. Klik op **Beschermen**.
3. Selecteer het beschermingsschema dat u wilt bewerken.
4. Klik op het ellipspictogram naast de naam van het schema en klik vervolgens op **Bewerken**.
5. Klik op een module die u wilt bewerken en configureer de instellingen zoals u wilt.
6. Klik op **Opslaan**.
7. [Als u niet alle workloads hebt geselecteerd waarop het schema van toepassing is] Selecteer het bereik van de bewerking:
   - Als u het schema wilt bewerken voor alle workloads waarop het wordt toegepast, klikt u op **De wijzigingen toepassen op dit beschermingsschema (dit heeft gevolgen voor andere apparaten)**.
   - Als u het schema alleen voor geselecteerde workloads wilt wijzigen, klikt u op **Alleen een nieuw beschermingsschema maken voor de geselecteerde apparaten**.
     Hierdoor wordt het bestaande schema ingetrokken voor de geselecteerde workloads. Er wordt een nieuw beschermingsschema gemaakt met de instellingen die u hebt geconfigureerd en dit wordt toegepast op deze workloads.

Beheer > Beschermingsschema's

1. Ga in de Cyber Protect-console naar **Beheer** > **Beschermingsschema's**.
2. Selecteer het beschermingsschema dat u wilt bewerken.
3. Klik op **Bewerken**.
4. Klik op de modules die u wilt bewerken en configureer vervolgens de instellingen zoals u wilt.
5. Klik op **Opslaan**.

Opmerking
Als u een schema bewerkt vanuit het tabblad **Beheer** > **Beschermingsschema's**, heeft dit gevolgen voor alle workloads waarop dat schema wordt toegepast.

Een beschermingsschema intrekken

Wanneer u een schema intrekt, verwijdert u het uit een of meer workloads. Het schema beschermt nog wel de andere workloads waarop het wordt toegepast.

U kunt een schema intrekken vanuit het tabblad **Apparaten** en het tabblad **Beheer** > **Beschermingsschema's**.

Apparaten

1. Selecteer de workloads waarvan u het schema wilt intrekken.
2. Klik op **Beschermen**.
3. Selecteer het beschermingsschema dat u wilt intrekken.
4. Klik op het ellipspictogram naast de naam van het schema en klik vervolgens op **Intrekken**.

Beheer > Beschermingsschema's

1. Ga in de Cyber Protect-console naar **Beheer** > **Beschermingsschema's**.
2. Selecteer het beschermingsschema dat u wilt intrekken.
3. Klik op **Bewerken**.
4. Klik op **Apparaten beheren**.
5. Selecteer in het venster **Apparaten** de workloads waarvan u het schema wilt intrekken.
6. Klik op **Verwijderen**.
7. Klik in het venster **Apparaten** op **Gereed**.
8. Klik in de sjabloon voor het beschermingsschema op **Opslaan**.

Een beschermingsschema in- of uitschakelen

Een ingeschakeld schema is actief en wordt uitgevoerd in de workloads waarop het wordt toegepast. Een uitgeschakeld schema is inactief: het wordt nog wel toegepast op workloads, maar wordt niet uitgevoerd in die workloads.

Wanneer u een beschermingsschema in- of uitschakelt vanaf het tabblad **Apparaten**, heeft uw actie alleen gevolgen voor de geselecteerde workloads.

Wanneer u een beschermingsschema in- of uitschakelt via het tabblad **Beheer** > **Beschermingsschema's**, heeft uw actie gevolgen voor alle workloads waarop dit schema wordt toegepast. U kunt ook meerdere beschermingsschema's in- of uitschakelen.

Apparaten

1. Selecteer de workload waarvan u het schema wilt uitschakelen.
2. Klik op **Beschermen**.
3. Selecteer het beschermingsschema dat u wilt uitschakelen.
4. Klik op het ellipspictogram naast de naam van het schema en klik vervolgens op **Inschakelen** of **Uitschakelen**.

Beheer > Beschermingsschema's

1. Ga in de Cyber Protect-console naar **Beheer** > **Beschermingsschema's**.
2. Selecteer een of meer beschermingsschema's die u wilt in- of uitschakelen.
3. Klik op **Bewerken**.
4. Klik op **Inschakelen** of **Uitschakelen**.

Opmerking
Deze actie heeft geen gevolgen voor beschermingsschema's die zich al in de doelstatus bevinden. Als uw selectie bijvoorbeeld zowel ingeschakelde als uitgeschakelde schema's bevat en u op **Inschakelen** klikt, worden alle geselecteerde schema's ingeschakeld.

Een beschermingsschema verwijderen

Wanneer u een schema verwijdert, wordt het ingetrokken van alle workloads en verwijderd uit de Cyber Protect-console.

U kunt een schema verwijderen vanuit het tabblad **Apparaten** en het tabblad **Beheer** > **Beschermingsschema's**.

Apparaten

1. Selecteer een workload waarop het beschermingsschema wordt toegepast dat u wilt verwijderen.
2. Klik op **Beschermen**.
3. Selecteer het beschermingsschema dat u wilt verwijderen.
4. Klik op het ellipspictogram naast de naam van het schema en klik vervolgens op **Verwijderen**.

Beheer > Beschermingsschema's

1. Ga in de Cyber Protect-console naar **Beheer** > **Beschermingsschema's**.
2. Selecteer het beschermingsschema dat u wilt verwijderen.
3. Klik op **Verwijderen**.
4. Bevestig uw keuze door het selectievakje **Ik bevestig dat ik het volgende schema wil verwijderen** in te schakelen en klik vervolgens op **Verwijderen**.

Conflicten tussen schema's oplossen

U kunt meerdere beschermingsschema's toepassen op dezelfde workload. U kunt bijvoorbeeld één beschermingsschema toepassen waarin u alleen de module **Antivirus en antimalware** hebt ingeschakeld en geconfigureerd, en een ander beschermingsschema waarin u alleen de module **Back-up** hebt ingeschakeld en geconfigureerd.

U kunt beschermingsschema's combineren waarin verschillende modules zijn ingeschakeld. U kunt ook meerdere beschermingsschema's combineren waarin alleen de module **Back-up** is ingeschakeld. Als er echter een andere module in meer dan één schema is ingeschakeld, treedt er een conflict op. Als u het schema wilt toepassen, moet u eerst het conflict oplossen.

Conflict tussen een nieuw en bestaand schema

Als een nieuw schema in strijd is met een bestaand schema, kunt u het conflict op een van de volgende manieren oplossen:

- Maak een nieuw schema, pas het toe en schakel vervolgens het bestaande schema (dat in strijd is met het nieuwe) uit.
- Maak een nieuw schema en schakel het vervolgens uit.

Conflict tussen een individueel schema en een groepsschema

Als een individueel beschermingsschema in strijd is met een groepsschema dat wordt toegepast op een apparaatgroep, kunt u het conflict op een van de volgende manieren oplossen:

- Verwijder de workload uit de apparaatgroep en pas het individuele beschermingsschema erop toe.
- Bewerk het bestaande groepsschema of pas een nieuw groepsschema toe op de apparaatgroep.

Licentieprobleem

Een beschermingsschemamodule vereist mogelijk dat een specifieke servicequota wordt toegewezen aan de beschermde workload. Als de toegewezen servicequota niet geschikt is, zult u het beschermingsschema waarin de betreffende module is ingeschakeld, niet kunnen uitvoeren, bijwerken of toepassen.

Voer een van de volgende handelingen uit om een licentieprobleem op te lossen:

- Schakel de module uit die niet wordt ondersteund door de momenteel toegewezen servicequota en ga door met het beschermingsschema.
- Wijzig het toegewezen servicequotum handmatig. Voor meer informatie: zie "De servicequota van machines wijzigen" (p. 189).

Individuele beschermingsschema's voor integraties van hosting-besturingspanelen

Wanneer u integraties voor hosting-besturingspanelen inschakelt op uw webhostingservers waarop DirectAdmin, cPanel of Plesk wordt gebruikt, wordt er door de Cyber Protection-service automatisch een individueel beschermingsschema voor uw gebruikersaccount gemaakt voor elke workload. Dit beschermingsschema is gekoppeld aan de specifieke workload waardoor het beschermingsschema is geïnitieerd, en kan niet worden ingetrokken of aan andere workloads worden toegewezen.

Als u dit beschermingsschema niet meer wilt gebruiken, verwijdert u het uit de Cyber Protect-console. U kunt afzonderlijke beschermingsschema's herkennen aan het -teken naast de naam van het schema.

Als u een beschermingsschema wilt toepassen voor de bescherming van meerdere webhostingservers waarop integraties van hosting-besturingspanelen worden uitgevoerd, kunt u een regulier beschermingsschema maken in de Cyber Protect-console en deze workloads hieraan toewijzen. Wijzigingen in een beschermingsschema dat wordt gedeeld door meerdere besturingspanelen voor webhosting, kunnen echter alleen worden aangebracht in de Cyber Protect-console en niet vanuit de integraties.

Plannen voor gegevensbescherming buiten de host

Opmerking
Deze functionaliteit is beschikbaar in klanttenants voor wie het quotum **Advanced Backup - Servers** of **Advanced Backup - NAS** is ingeschakeld als onderdeel van het Advanced Backup-pakket.

Replicatie, validatie en opschoning worden meestal uitgevoerd door de beveiligingsagent die de back-up uitvoert. Dit betekent een extra belasting voor de machine waarop de agent wordt uitgevoerd, zelfs nadat het back-upproces is voltooid. U kunt de machine ontlasten door off-host gegevensbeschermingsschema's te maken, dat wil zeggen afzonderlijke schema's voor replicatie, validatie, opschoning en conversie naar een virtuele machine.

Met de off-host gegevensbeschermingsschema's kunt u het volgende doen:

- Verschillende agents kiezen voor back-up- en off-host gegevensbeschermingsbewerkingen
- De off-host gegevensverwerkingsbewerkingen inplannen tijdens daluren om het verbruik van de netwerkbandbreedte te minimaliseren

- De off-host gegevensverwerkingsbewerkingen inplannen buiten kantooruren (als u geen speciale agent wilt installeren voor off-host gegevensverwerking)

Opmerking
De off-host gegevensverwerkingsschema's worden uitgevoerd volgens de tijdinstellingen (inclusief de tijdzone) van de machine waarop de beveiligingsagent is geïnstalleerd. Voor een virtueel apparaat (bijvoorbeeld Agent voor VMware of Agent voor Scale Computing HC3) kunt u de tijdzone configureren in de grafische gebruikersinterface van de agent.

Back-upreplicatie

Opmerking
Deze functionaliteit is beschikbaar in klanttenants voor wie het quotum **Advanced Backup - Servers** of **Advanced Backup - NAS** is ingeschakeld als onderdeel van het Advanced Backup-pakket.

Bij back-upreplicatie wordt een back-up gekopieerd naar een andere locatie. Dit is een gegevensbewerking buiten de host en deze wordt geconfigureerd in een back-upreplicatieschema.

Back-upreplicatie kan ook deel uitmaken van een beschermingsschema. Zie "Replicatie" (p. 467) voor meer informatie over deze optie.

Een back-up maken van een replicatieschema

Als u back-ups wilt repliceren als gegevensbewerking buiten de host, moet u een back-upreplicatieschema maken.

Een back-upreplicatieschema maken

1. Klik in de Cyber Protect-console op **Beheer** > **Back-upreplicatie**.
2. Klik op **Schema maken**.
3. Ga naar **Agent** en selecteer de agent die de replicatie gaat uitvoeren.
   U kunt elke agent selecteren die toegang heeft tot zowel de bronlocatie als de replicatielocaties.
4. Ga naar **Items om te repliceren** en selecteer de archieven of back-uplocaties die u wilt repliceren.
   Met de schakelaar **Locaties** / **Back-ups** in de rechterbovenhoek kunt u schakelen tussen archieven en locaties.
   Als u meerdere versleutelde archieven selecteert, moeten deze hetzelfde versleutelingswachtwoord hebben. Als archieven verschillende versleutelingswachtwoorden hebben, moet u afzonderlijke schema's maken.
5. Ga naar **Bestemming** en geef de replicatielocatie op.
6. Selecteer in **Hoe replicatie functioneert** welke back-ups (ook wel herstelpunten genoemd) u wilt repliceren.
   De volgende opties zijn beschikbaar:

- **Alle back-ups**
- **Alleen volledige back-ups**
- **Alleen laatste back-up**

Zie "Wat wilt u repliceren" (p. 226) voor meer informatie over deze opties.

7. Ga naar **Schema** en configureer het replicatieschema.

   Wanneer u het back-upreplicatieschema configureert, moet u controleren of de laatste gerepliceerde back-up nog steeds beschikbaar is op de oorspronkelijke locatie wanneer de back-upreplicatie start. Als deze back-up niet beschikbaar is op de oorspronkelijke locatie, bijvoorbeeld omdat deze is verwijderd vanwege een bewaarregel, wordt het hele archief gerepliceerd als een volledige back-up. Dit kan erg tijdrovend zijn en zal extra opslagruimte in beslag nemen.
8. Ga naar **Bewaarregels** en geef de bewaarregels op voor de doellocatie.

   De volgende opties zijn beschikbaar:

   - **Op aantal back-ups**
   - **Op leeftijd van de back-up** (afzonderlijke instellingen voor maandelijkse, wekelijkse, dagelijkse en uurlijkse back-ups)
   - **Op totale grootte van de back-ups**
   - **Back-ups voor onbepaalde tijd bewaren**

   Opmerking
   Als u deze optie selecteert, resulteert dit in een hoger opslaggebruik. U moet de onnodige back-ups handmatig verwijderen.
9. [Als u versleutelde archieven hebt geselecteerd in **Items om te repliceren**] Activeer de schakelaar **Back-upwachtwoord** en geef het versleutelingswachtwoord op.
10. [Optioneel] Als u de schemaopties wilt wijzigen, klikt u op het tandwielpictogram en vervolgens configureert u de opties zoals gewenst.
11. Klik op **Maken**.

Wat wilt u repliceren

Opmerking
Sommige replicatiebewerkingen, zoals het repliceren van een hele locatie of het repliceren van alle back-ups in een back-upset, kunnen erg tijdrovend zijn.

U kunt afzonderlijke back-upsets of hele back-uplocaties repliceren. Wanneer u een back-uplocatie repliceert, worden alle daar aanwezige back-upsets gerepliceerd.

Back-upsets bestaan uit back-ups (ook wel herstelpunten genoemd). U moet selecteren welke back-ups u wilt repliceren.

De volgende opties zijn beschikbaar:

- **Alle back-ups**
  Alle back-ups in de back-upset worden gerepliceerd telkens wanneer het replicatieschema wordt uitgevoerd.
- **Alleen volledige back-ups**
  Alleen de volledige back-ups in de back-upset worden gerepliceerd.
- **Alleen laatste back-up**
  Alleen de nieuwste back-up in de back-upset wordt gerepliceerd, ongeacht het type (volledig, differentieel of incrementeel).

Selecteer de gewenste optie en het back-upschema dat u gebruikt. Als u bijvoorbeeld het back-upschema **Altijd incrementeel (één bestand)** gebruikt en alleen de nieuwste incrementele back-up wilt repliceren, selecteert u in het back-upreplicatieschema de optie **Alleen laatste back-up**.

De volgende tabel bevat een overzicht van de back-ups die worden gerepliceerd met verschillende back-upschema's.

	Altijd incrementeel (één bestand)	**Altijd volledig**	**Wekelijks volledig, Dagelijks incrementeel**	**Maandelijks volledig, Wekelijks differentieel, Dagelijks incrementeel (GFS)**
Alle back-ups	Alle back-ups in de back-upset	Alle back-ups in de back-upset	Alle back-ups in de back-upset	Alle back-ups in de back-upset
Alleen volledige back-ups	Alleen de eerste back-up (volledige back-up)	Alle back-ups	Elke week één back-up*	Elke maand één back-up*
Alleen laatste back-up	Alleen de nieuwste back-up in de back-upset*	Alleen de nieuwste back-up in de back-upset*	Alleen het nieuwste in de back-upset, ongeacht het type*	Alleen het nieuwste in de back-upset, ongeacht het type*

*Wanneer u het back-upreplicatieschema configureert, moet u controleren of de laatste gerepliceerde back-up nog steeds beschikbaar is op de oorspronkelijke locatie wanneer de back-upreplicatie start. Als deze back-up niet beschikbaar is op de oorspronkelijke locatie, bijvoorbeeld omdat deze is verwijderd vanwege een bewaarregel, wordt het hele archief gerepliceerd als een volledige back-up. Dit kan erg tijdrovend zijn en zal extra opslagruimte in beslag nemen.

Ondersteunde locaties

De volgende tabel bevat een overzicht van back-uplocaties die door back-upreplicatieschema's worden ondersteund.

Back-uplocatie	Ondersteund als bron	Ondersteund als doel
Cloudopslag	+	+
Lokale map	+	+
Netwerkmap	+	+
Openbare cloud	+	+
NFS-map	–	–
Secure Zone	–	–

Validatie

Opmerking
Deze functionaliteit is beschikbaar in klanttenants voor wie het quotum **Advanced Backup - Servers** of **Advanced Backup - NAS** is ingeschakeld als onderdeel van het Advanced Backup-pakket.

Door een back-up te valideren verifieert u dat u de gegevens ervan kunt herstellen.

U maakt een validatieschema als u een back-up wilt valideren als gegevensbewerking buiten de host. Zie "Een validatieschema maken" (p. 229) voor meer informatie over hoe u dit kunt maken.

De volgende validatiemethoden zijn beschikbaar:

- Controlesomverificatie
- Uitvoeren als virtuele machine
  - Heartbeat van VM
  - Momentopnamevalidatie

U kunt een of meer van deze methoden selecteren. Wanneer meer dan één methode is geselecteerd, worden de bewerkingen voor elke validatiemethode achter elkaar uitgevoerd. Zie "Validatiemethoden" (p. 231) voor meer informatie over de methoden.

U kunt back-upsets of back-uplocaties valideren. Bij validatie van een back-uplocatie worden alle back-upsets op die locatie gevalideerd.

Ondersteunde locaties

De volgende tabel toont de ondersteunde back-uplocaties en validatiemethoden.

Opmerking
De validatieoptie is niet beschikbaar voor back-ups in de openbare cloud vanwege de hoge kosten voor het lezen van een volledig archief uit een openbare cloud.

Back-uplocatie	Controlesomverificatie	Uitvoeren als virtuele machine	
		Heartbeat van VM	Momentopnamevalidatie
Cloudopslag	+	+	+
Lokale map	+	+	+
Netwerkmap	+	+	+
NFS-map	–	–	–
Secure Zone	–	–	–

Validatiestatus

Wanneer een validatie is uitgevoerd, wordt de back-up gemarkeerd met een groene stip en het label **Gevalideerd**.

Als de validatie mislukt, wordt de back-up gemarkeerd met een rode stip. De validatie mislukt zelfs wanneer slechts één van de gebruikte validatiemethoden mislukt. In sommige gevallen kan dit het gevolg zijn van een verkeerde configuratie van het validatieschema, bijvoorbeeld het gebruik van de methode **Heartbeat van VM** voor virtuele machines op een verkeerde host.

De validatiestatus van een back-up wordt bijgewerkt bij elke nieuwe validatiebewerking. De status voor elke validatiemethode wordt afzonderlijk bijgewerkt. Daarom wordt de validatie van een back-up waarbij één methode is mislukt, weergegeven als mislukt totdat de betreffende validatiemethode kan worden uitgevoerd, zelfs als de mislukte methode niet wordt gebruikt door de meest recente validatiebewerkingen en deze bewerkingen gewoon kunnen worden uitgevoerd.

Zie "De validatiestatus van een back-up controleren" (p. 235) voor meer informatie over het controleren van de validatiestatus.

Een validatieschema maken

Als u een back-upset wilt valideren als een gegevensbewerking buiten de host, maakt u een validatieschema.

Een validatieschema maken:

1. Klik in de Cyber Protect-console op **Beheer** > **Validatie**.
2. Klik op **Schema maken**.
   De sjabloon voor een nieuw validatieschema wordt geopend.
3. [Optioneel] Klik op de standaardnaam om de naam van het schema te wijzigen.
4. Selecteer bij **Agent** de agent die de validatie gaat uitvoeren en klik vervolgens op **OK**.

Als u wilt valideren door een virtuele machine uit te voeren vanaf een back-up, selecteert u een machine met Agent voor VMware of Agent voor Hyper-V. Selecteer anders een machine die toegang heeft tot de back-uplocatie.

5. Selecteer bij **Items om te valideren** de back-upsets die u wilt valideren.
   a. Selecteer het bereik voor het schema (afzonderlijke back-upsets of volledige locaties), door te klikken op **Locaties** of **Back-ups** in de rechterbovenhoek.
      Als de geselecteerde back-ups zijn versleuteld, moeten ze allemaal hetzelfde versleutelingswachtwoord gebruiken. Voor back-ups met verschillende versleutelingswachtwoorden maakt u afzonderlijke schema's.
   b. Klik op **Toevoegen**.
   c. Selecteer, afhankelijk van het bereik van het validatieschema, meerdere locaties of een locatie en back-upsets en klik vervolgens op **Gereed**.
   d. Klik op **Gereed**.
6. Selecteer bij **Validatie-items** de back-ups (ook wel herstelpunten genoemd) binnen de geselecteerde back-upsets die moeten worden gevalideerd. De volgende opties zijn beschikbaar:
   - **Alle back-ups**
   - **Alleen laatste back-up**
7. Selecteer bij **Hoe validatie functioneert** de gewenste validatiemethode.
   U kunt een of beide van de volgende opties selecteren:
   - **Controlesomverificatie**
   - **Uitvoeren als virtuele machine**

   Zie "Validatiemethoden" (p. 231) voor meer informatie over de methoden.
8. [Als u **Controlesomverificatie** hebt geselecteerd] Klik op **Gereed**.
9. [Als u **Uitvoeren als virtuele machine** hebt geselecteerd]. Configureer de instellingen voor deze methode.
   a. Selecteer bij **Doelmachine** het type virtuele machine (ESXi of Hyper-V), de host en de sjabloon voor de machinenaam en klik vervolgens op **OK**.
      De standaardnaam is **[Machinenaam]_validate**.
   b. Selecteer bij **Gegevensopslag** (voor ESXi) of **Pad** (voor Hyper-V) de gegevensopslag voor de virtuele machine.
   c. Selecteer een of beide validatiemethoden voor **Uitvoeren als virtuele machine**:
      - **Heartbeat van VM**
      - **Momentopnamevalidatie**
   d. [Optioneel] Klik op **VM-instellingen** om de geheugengrootte en de netwerkverbindingen van de virtuele machine te wijzigen.
      De virtuele machine is standaard niet verbonden met een netwerk het geheugen van de virtuele machine is net zo groot als dat van de oorspronkelijke machine.
   e. Klik op **Gereed**.

10. [Optioneel] Klik in de sjabloon voor het validatieschema op **Planning** en configureer het vervolgens.
11. [Als de geselecteerde back-upsets in **Items om te valideren** zijn versleuteld] Activeer de schakelaar **Back-upwachtwoord** en geef het versleutelingswachtwoord op.
12. [Optioneel] Klik op het tandwielpictogram om de schemaopties te wijzigen.
13. Klik op **Maken**.

Nu is uw validatieschema gereed en het wordt uitgevoerd volgens de configuratie die u hebt ingesteld. Als u het schema onmiddellijk wilt uitvoeren, selecteert u het in **Beheer** > **Validatie** en vervolgens klikt u op **Nu uitvoeren**.

Wanneer het schema is gestart, kunt u de lopende activiteiten controleren en de details bekijken in de Cyber Protect-console, onder **Monitoring** > **Activiteiten**.

Een validatieschema kan meerdere back-ups bevatten en één back-up kan worden gevalideerd door meerdere validatieschema's.

Opmerking
Alle back-ups worden sequentieel verwerkt, één voor één, door een enkele validatietaak.

Er kan slechts één validatietaak tegelijk worden uitgevoerd door een agent. Meerdere validatietaken kunnen parallel worden uitgevoerd door verschillende agents: voor twee gelijktijdige taken zijn twee agents vereist, voor drie taken drie agents, enzovoort.

De volgende tabel geeft een overzicht van de mogelijke statussen van de validatieactiviteit.

Resultaat van de activiteit	Schema met één back-up	Schema met meerdere back-ups
Voltooid	Alle validatiemethoden zijn uitgevoerd	Alle validatiemethoden zijn uitgevoerd in alle back-ups
Uitgevoerd met waarschuwingen	N.v.t.	Ten minste één validatiemethode is mislukt in ten minste één back-up
Fout	Ten minste één validatiemethode is mislukt	Ten minste één validatiemethode is mislukt in alle back-ups

Validatiemethoden

In een validatieschema zijn de volgende validatiemethoden beschikbaar:

- Controlesomverificatie
- Uitvoeren als virtuele machine
  - Heartbeat van VM
  - Momentopnamevalidatie

Controlesomverificatie

Bij validatie via controlesomverificatie wordt een controlesom berekend voor elk gegevensblok dat kan worden hersteld vanuit de back-up. Deze controlesom wordt vervolgens vergeleken met de oorspronkelijke controlesom voor dat gegevensblok, die is geschreven tijdens het back-upproces. De enige uitzondering is validatie van back-ups op bestandsniveau in de cloudopslag. Deze back-ups worden gevalideerd door de consistentie van de metagegevens in de back-up te controleren.

Validatie via controlesomverificatie is een tijdrovend proces, zelfs voor een relatief kleine incrementele of een differentiële back-up. De reden is dat de validatiebewerking niet alleen de gegevens controleert die zich fysiek in een bepaalde back-up bevinden, maar alle gegevens die moeten worden hersteld. Dat wil zeggen dat eerdere back-ups mogelijk ook moeten worden gevalideerd.

Als validatie via controlesomverificatie lukt, betekent dit dat er een grote kans is op gegevensherstel. Bij validatie via deze methode worden echter niet alle factoren gecontroleerd die van invloed zijn op het herstelproces.

Als u een back-up maakt van een besturingssysteem, raden we u aan enkele van de volgende aanvullende bewerkingen uit te voeren:

- Het herstel testen via de opstartmedia naar een reserveschijf.
- Een virtuele machine uitvoeren vanaf de back-up in een ESXi- of Hyper-V-omgeving.
- Een validatieschema uitvoeren waarin de validatiemethode **Uitvoeren als virtuele machine** is ingeschakeld.

Uitvoeren als virtuele machine

Deze methode werkt alleen bij back-ups op schijfniveau die een besturingssysteem bevatten. Als u deze methode wilt gebruiken, hebt u een ESXi- of Hyper-V-host nodig en een beveiligingsagent (Agent voor VMware of Agent voor Hyper-V) die deze host beheert.

De validatiemethode **Uitvoeren als virtuele machine** is beschikbaar in de volgende varianten:

- Heartbeat van VM
- Momentopnamevalidatie

U moet er ten minste één selecteren.

Heartbeat van VM

Met deze validatiemethode voert de agent een virtuele machine uit vanaf de back-up, maakt verbinding met VMware Tools of Hyper-V Integration Services en controleert vervolgens de heartbeat-respons om te controleren of het besturingssysteem zonder problemen is opgestart. Als de verbinding niet tot stand kan worden gebracht, probeert de agent elke twee minuten verbinding te maken. In totaal worden vijf pogingen ondernomen. Als geen van de pogingen resultaat heeft, mislukt de validatie.

De virtuele machines worden een voor een door de agent gevalideerd, ongeacht het aantal validatieschema's en gevalideerde back-ups. Wanneer het resultaat van de validatie duidelijk is, verwijdert de agent de virtuele machine en gaat verder met de volgende machine.

Opmerking
Gebruik deze methode alleen wanneer u back-ups van virtuele VMware-machines valideert door deze back-ups als virtuele machines op een ESXi-host uit te voeren, en back-ups van virtuele Hyper-V-machines door ze als virtuele machines op een Hyper-V-host uit te voeren.

Momentopnamevalidatie

Bij deze validatiemethode voert de agent een virtuele machine uit vanaf de back-up en worden er momentopnamen gemaakt terwijl de virtuele machine opstart. Een MI-module (Machine Intelligence) controleert de momentopnamen en als er een aanmeldingsscherm wordt gevonden, wordt de back-up gemarkeerd als gevalideerd.

De momentopname is gekoppeld aan het herstelpunt en u kunt dit binnen een jaar na validatie downloaden in de Cyber Protect-console. Zie "De validatiestatus van een back-up controleren" (p. 235) voor meer informatie over het controleren van de momentopname.

Als meldingen zijn ingeschakeld voor uw gebruikersaccount, ontvangt u een e-mail over de validatiestatus van de back-up, met de momentopname bijgevoegd als bijlage. Zie De instellingen voor de meldingen voor een gebruiker wijzigen voor meer informatie over de meldingen.

Momentopnamevalidatie wordt ondersteund door agentversie 15.0.30971 (uitgebracht in november 2022) en later.

Opmerking
Momentopnamevalidatie werkt het beste met back-ups van Windows- en Linux-systemen met een aanmeldingsscherm van een gebruikersinterface. Deze methode is niet geoptimaliseerd voor Linux-systemen met een aanmeldingsscherm van een console.

De time-out wijzigen voor heartbeat van VM en validatie van momentopnamen

Wanneer u een back-up valideert door deze uit te voeren als virtuele machine, kunt u de time-out configureren die u wilt gebruiken tussen het opstarten van de virtuele machine en het verzenden van het heartbeat-verzoek of het maken van een momentopname.

De standaardperiode is als volgt:

- Eén minuut: voor back-ups die zijn opgeslagen in een lokale map of een netwerkshare
- Vijf minuten: voor back-ups die zijn opgeslagen in de cloud

U kunt deze waarden wijzigen door het configuratiebestand voor Agent voor VMware of Agent voor Hyper-V te bewerken.

De time-out wijzigen:

1. Open het configuratiebestand om dit te bewerken. U vindt het bestand op de volgende locaties:
   - Voor Agent voor VMware of Agent voor Hyper-V in Windows: `C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - Voor Agent voor VMware (Virtual appliance): `/bin/mms_settings.config`

     Voor meer informatie over hoe u toegang krijgt tot het configuratiebestand op een virtueel apparaat: zie "SSH-verbindingen met een virtueel apparaat" (p. 176).
2. Ga naar `<validation>` en wijzig waar nodig de waarden voor lokale back-ups en cloudback-ups:

   ```
   <validation>
   <run_vm>
   <initial_timeout_minutes>
   <local_backups>1</local_backups>
   <cloud_backups>5</cloud_backups>
   </initial_timeout_minutes>
   </run_vm>
   </validation>
   ```
3. Sla het configuratiebestand op.
4. Start de agent opnieuw op.
   - [Voor Agent voor VMware of Agent voor Hyper-V in Windows] Voer de volgende opdrachten uit op de opdrachtprompt:

     ```
     net stop mms
     ```

     ```
     net start mms
     ```
   - [Voor Agent voor VMware (Virtual appliance)] Start de virtuele machine opnieuw op met de agent.

Het aantal nieuwe pogingen configureren in geval van een fout

Als u het aantal uitgevoerde validaties wilt maximaliseren, kunt u automatische nieuwe pogingen configureren voor validatiebewerkingen die worden beëindigd met een fout.

Automatische nieuwe pogingen configureren:

1. Klik op het tandwielpictogram wanneer u een validatieschema maakt.
2. Ga naar het deelvenster **Opties** en selecteer **Foutafhandeling**.
3. Klik bij **Opnieuw proberen als er een fout optreedt** op **Ja**.
4. Configureer in **Aantal pogingen** het maximale aantal nieuwe pogingen als er een fout optreedt. De validatiebewerking wordt opnieuw geprobeerd totdat deze wordt voltooid of totdat het maximale aantal nieuwe pogingen is bereikt.
5. Configureer in **Interval tussen pogingen** de time-out tussen twee opeenvolgende nieuwe pogingen.
6. Klik op **Gereed**.

De validatiestatus van een back-up controleren

U kunt de validatiestatus van een back-up controleren op het tabblad **Apparaten** of op het tabblad **Back-upopslag**.

U kunt ook de status voor elke validatiemethode bekijken en de momentopname downloaden die is gemaakt met de momentopnamevalidatiemethode.

Zie "Validatiestatus" (p. 229) voor meer informatie over hoe de statussen werken.

De validatiestatus van een back-up controleren:

Apparaten

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de workload waarvoor u de validatiestatus van de back-up wilt controleren en klik vervolgens op **Herstel**.
3. [Als er meerdere back-uplocaties beschikbaar zijn] Selecteer de back-uplocatie.
4. Selecteer de back-up waarvan u de status wilt controleren.

Back-upopslag

1. Ga in de Cyber Protect-console naar **Back-upopslag**.
2. Selecteer de locatie waar de back-upset is opgeslagen.
3. Selecteer de back-upset en klik vervolgens op **Back-ups weergeven**.
4. Selecteer de back-up waarvan u de validatiestatus wilt controleren.

Opschonen

Opschonen is een bewerking voor het verwijderen van back-ups die verouderd zijn volgens de bewaarregels. Deze bewerking is alleen van toepassing op agents en workloads, en niet op cloud-to-cloud back-ups (die alleen handmatig kunnen worden verwijderd).

Opmerking
Deze functionaliteit is beschikbaar in klanttenants voor wie het quotum **Advanced Backup - Servers** of **Advanced Backup - NAS** is ingeschakeld als onderdeel van het Advanced Backup-pakket.

Ondersteunde locaties

Bij opschoonschema's worden alle back-uplocaties ondersteund, behalve NFS-mappen en Secure Zone.

Een opschoonschema maken:

1. Klik in de Cyber Protect-console op **Beheer** > **Opschonen**.
2. Klik op **Schema maken**.
3. Ga naar **Agent** en selecteer de agent die de opschoning gaat uitvoeren.
   U kunt elke agent selecteren die toegang heeft tot de back-uplocatie.
4. Ga naar **Items om op te schonen** en selecteer de archieven of back-uplocaties die u wilt opschonen.
   Met de schakelaar **Locaties** / **Back-ups** in de rechterbovenhoek kunt u schakelen tussen archieven en locaties.
   Als u meerdere versleutelde archieven selecteert, moeten deze hetzelfde versleutelingswachtwoord hebben. Als archieven verschillende versleutelingswachtwoorden hebben, moet u afzonderlijke schema's maken.
5. Ga naar **Schema** en configureer het opschoonschema.
6. Ga naar **Bewaarregels** en geef de bewaarregels op.
   De volgende opties zijn beschikbaar:
   - **Op aantal back-ups**
   - **Op leeftijd van de back-up** (afzonderlijke instellingen voor maandelijkse, wekelijkse, dagelijkse en uurlijkse back-ups)
   - **Op totale grootte van de back-ups**
7. [Als u versleutelde archieven hebt geselecteerd in **Items om te repliceren**] Activeer de schakelaar **Back-upwachtwoord** en geef het versleutelingswachtwoord op.
8. [Optioneel] Als u de schemaopties wilt wijzigen, klikt u op het tandwielpictogram en vervolgens configureert u de opties zoals gewenst.
9. Klik op **Maken**.

Conversie naar een virtuele machine

Conversie naar een virtuele machine is alleen beschikbaar voor back-ups op schijfniveau. Als een back-up het systeemvolume en alle nodige informatie voor het opstarten van het besturingssysteem bevat, kan de resulterende virtuele machine zelf opstarten. Zo niet, dan kunt u de virtuele schijven daarvan toevoegen aan een andere virtuele machine.

Opmerking
Er kan geen back-up worden gemaakt van VM's die zijn gerepliceerd via de native replicatiefunctie van Scale Computing VM.

U kunt een afzonderlijk schema maken voor de conversie naar een virtuele machine en dit schema handmatig of volgens schema uitvoeren.

Zie "Wat u moet weten over conversie" (p. 238) voor informatie over vereisten en beperkingen.

Opmerking
Deze functionaliteit is beschikbaar in klanttenants voor wie het quotum **Advanced Backup - Servers** of **Advanced Backup - NAS** is ingeschakeld als onderdeel van het Advanced Backup-pakket.

Een schema voor conversie naar een virtuele machine maken

1. Klik op **Beheer** > **Conversie naar VM**.
2. Klik op **Schema maken**.
   Er wordt een sjabloon voor een nieuw schema weergegeven.
3. [Optioneel] Klik op de standaardnaam om de naam van het schema te wijzigen.
4. Selecteer bij **Converteren naar** het beoogde type virtuele machine. **U kunt een van de volgende opties selecteren**:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **VHDX-bestanden**

   Opmerking
   Bij een conversie naar VHDX-bestanden of VMware Workstation worden de VHDX/VMDK-bestanden in de doellocatie die tijdens de vorige conversie zijn gemaakt, overschreven zodat opslagruimte wordt bespaard.
5. Voer een van de volgende handelingen uit:
   - [Voor VMware ESXi, Hyper-V en Scale Computing HC3] Klik op **Host**, selecteer de doelhost en geef de nieuwe sjabloon voor de machinenaam op.
   - [Voor andere typen virtuele machines] Geef in **Pad** op waar u de bestanden van de virtuele machines en de sjabloon voor de bestandsnaam wilt opslaan.

   De standaardnaam is **[Machinenaam]_converted**.
6. Klik op **Agent** en selecteer vervolgens de agent die de conversie uitvoert.
7. Klik op **Items om te converteren** en selecteer de back-ups die in dit schema worden geconverteerd naar virtuele machines.
   Met de schakelaar **Locaties** / **Back-ups** in de rechterbovenhoek kunt u schakelen tussen het selecteren van back-ups en het selecteren van hele locaties.
   Als de geselecteerde back-ups zijn versleuteld, moeten ze allemaal hetzelfde versleutelingswachtwoord gebruiken. Voor back-ups met verschillende versleutelingswachtwoorden maakt u afzonderlijke schema's.
8. [Alleen voor VMware ESXi en Hyper-V] Klik op **Gegevensopslag** voor ESXi of **Pad** voor Hyper-V en selecteer vervolgens de gegevensopslag voor de virtuele machine.

9. [Alleen voor VMware ESXi en Hyper-V] Selecteer de schijfinrichtingsmodus. De standaardinstelling is **Thin** voor VMware ESXi en **Dynamisch uitbreidbaar** voor Hyper-V.
10. [Optioneel] [Voor VMware ESXi, Hyper-V en Scale Computing HC3] Klik op **VM-instellingen** om de geheugengrootte, het aantal processors of de netwerkverbindingen van de virtuele machine te wijzigen.
11. [Optioneel] Klik op **Planning** en wijzig het schema.
12. Als de back-ups die u hebt geselecteerd in **Items om te converteren**, zijn versleuteld, activeert u de schakelaar **Back-upwachtwoord** en geeft u het versleutelingswachtwoord op. Anders kunt u deze stap overslaan.
13. [Optioneel] Klik op het tandwielpictogram om de schemaopties te wijzigen.
14. Klik op **Maken**.

Wat u moet weten over conversie

Ondersteunde typen virtuele machines

Conversie van een back-up naar een virtuele machine kan worden uitgevoerd door dezelfde agent die de back-up heeft gemaakt of door een andere agent.

Als u een conversie wilt uitvoeren naar VMware ESXi, Hyper-V of Scale Computing HC3, hebt u respectievelijk een ESXi-, Hyper-V- of Scale Computing HC3-host en een beveiligingsagent (Agent voor VMware, Agent voor Hyper-V of Agent voor Scale Computing HC3) voor het beheer van deze host nodig.

Bij conversie naar VHDX-bestanden wordt ervan uitgegaan dat de bestanden als virtuele schijven worden verbonden met een virtuele Hyper-V-machine.

De volgende tabel bevat een overzicht van de typen virtuele machines die u kunt maken met de bewerking **Converteren naar VM**. De rijen in de tabel geven het type geconverteerde virtuele machines weer. De kolommen geven de agenten weer die de conversie uitvoeren.

Type VM	Agent voor VMware	Agent voor Hyper-V	Agent voor Windows	Agent voor Linux	Agent voor Mac	Agent voor Scale Computing HC3	Agent voor oVirt (KVM)	Agent voor Virtuozzo Hybrid Infrastructure	Agent voor Virtuozzo
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–

VMware Workstation	+	+	+	+	–	–	–	–	–
VHDX-bestanden	+	+	+	+	–	–	–	–	–
Scale Computing HC3	–	–	–	–	–	+	–	–	–

Beperkingen

- Back-ups die zijn opgeslagen op NFS, kunnen niet worden geconverteerd.
- Back-ups die zijn opgeslagen in Secure Zone, kunnen alleen worden geconverteerd door de agent die op dezelfde machine wordt uitgevoerd.
- Back-ups die logische volumes van Linux (LVM) bevatten, kunnen alleen worden geconverteerd als ze zijn gemaakt met Agent voor VMware, Agent voor Hyper-V of Agent voor Scale Computing HC3 en als ze naar dezelfde hypervisor worden gestuurd. Conversie tussen verschillende hypervisors wordt niet ondersteund.
- Wanneer back-ups van een Windows-machine worden geconverteerd naar VMware Workstation of VHDX-bestanden, krijgt de resulterende virtuele machine hetzelfde CPU-type als dat van de machine die de conversie uitvoert. Hierdoor worden de bijbehorende CPU-stuurprogramma's geïnstalleerd in het gastbesturingssysteem. Indien gestart op een host met een ander CPU-type, geeft het gastsysteem een stuurprogrammafout weer. Werk dit stuurprogramma handmatig bij.

Regelmatige conversie naar een virtuele machine, vergeleken met het uitvoeren van een virtuele machine vanaf een back-up

Beide bewerkingen resulteren in een virtuele machine die in enkele seconden kan worden opgestart als de oorspronkelijke machine niet werkt.

Bij een regelmatige conversie naar een virtuele machine wordt gebruikgemaakt van het CPU en geheugenresources. Bestanden van de virtuele machine nemen constant ruimte in beslag in de (gegevens)opslag. Dit is mogelijk niet erg praktisch als een productiehost wordt gebruikt voor de conversie. De prestaties van de virtuele machine worden echter alleen beperkt door de resources van de host.

Bij het uitvoeren van een virtuele machine vanaf een back-up worden er alleen resources verbruikt wanneer de virtuele machine wordt uitgevoerd. De opslagruimte is alleen vereist om wijzigingen van de virtuele schijven te bewaren. Het kan echter wel voorkomen dat de virtuele machine langzamer werkt, omdat de host geen directe toegang heeft tot de virtuele schijven, maar communiceert met de agent die de gegevens leest vanaf de back-up. Bovendien is de virtuele machine tijdelijk.

Regelmatige conversie naar een virtuele machine

De werking van regelmatige conversies hangt af van de plek waar u de virtuele machine wilt maken.

- **Als u de virtuele machine wilt opslaan als een set bestanden:** bij elke conversie wordt de virtuele machine helemaal opnieuw gemaakt.
- **Als u de virtuele machine wilt maken op een virtualisatieserver:** bij de conversie van een incrementele of differentiële back-up wordt de bestaande virtuele machine bijgewerkt in plaats van deze helemaal opnieuw te maken. Een dergelijke conversie is doorgaans sneller. U bespaart er ook netwerkverkeer en CPU-resources mee van de host die de conversie uitvoert. Als het bijwerken van de virtuele machine niet mogelijk is, wordt de machine helemaal opnieuw gemaakt.

Hieronder volgt een gedetailleerde beschrijving van beide gevallen.

Als u de virtuele machine wilt opslaan als een set bestanden

Als resultaat van de eerste conversie wordt een nieuwe virtuele machine gemaakt. Bij elke volgende conversie wordt deze machine helemaal opnieuw gemaakt. Eerst krijgt de oude machine tijdelijk een andere naam. Vervolgens wordt een nieuwe virtuele machine gemaakt die de vorige naam van de oude machine heeft. Als deze bewerking goed is uitgevoerd, wordt de oude machine verwijderd. Als deze bewerking mislukt, wordt de nieuwe machine verwijderd en krijgt de oude machine weer haar vorige naam. Op deze manier resulteert de conversie altijd in één enkele machine. Tijdens de conversie is echter wel extra opslagruimte nodig om de oude machine op te slaan.

Als u de virtuele machine wilt maken op een virtualisatieserver

Bij de eerste conversie wordt een nieuwe virtuele machine gemaakt. Volgende conversies werken als volgt:

- Als er een *volledige back-up* is uitgevoerd sinds de laatste conversie, wordt de virtuele machine helemaal opnieuw gemaakt, zoals eerder beschreven.
- Anders wordt de bestaande virtuele machine bijgewerkt met de wijzigingen sinds de laatste conversie. Als de update niet mogelijk is (bijvoorbeeld als u de tussentijdse momentopnamen hebt verwijderd, zie hieronder), wordt de virtuele machine helemaal opnieuw gemaakt.

Tussentijdse momentopnamen

Er wordt er een tussentijdse momentopname van de hypervisor van de virtuele machine opgeslagen, zodat de geconverteerde virtuele machine veilig kan worden bijgewerkt. De momentopname krijgt de naam **Replica...** en deze moet worden bewaard.

De momentopname **Replica...** komt overeen met het resultaat van de meest recente conversie. U kunt naar deze momentopname gaan als u de machine wilt terugzetten naar die status, bijvoorbeeld als u met de machine hebt gewerkt en eventuele wijzigingen wilt verwijderen.

Voor geconverteerde virtuele Scale Computing HC3-machines wordt een extra **specifieke momentopname** gemaakt. Deze wordt alleen gebruikt door de Cyber Protection-service.

Schema's voor back-upscans

Als u back-ups wilt scannen op malware (inclusief ransomware), maakt u een back-upscanschema.

Belangrijk
Schema's voor back-upscans worden niet ondersteund voor alle workloads en back-upopslaglocaties. Zie "Beperkingen" (p. 912) voor meer informatie.

Een back-upscanschema maken

1. Ga in de Cyber Protect-console naar **Beheer** > **Back-upscans**.
2. Klik op **Schema maken**.
3. Geef de naam van het schema en de volgende parameters op:
   - **Type scan**:
     - **Cloud**: Deze optie kan niet worden gewijzigd. Een automatisch geselecteerde cloudagent voert de back-upscan uit.
   - **Back-ups om te scannen**:
     - **Locaties**: Selecteer locaties met de back-upsets die u wilt scannen.
     - **Back-ups**: Selecteer de back-upsets die u wilt scannen.
   - **Scannen op**:
     - **Malware**: Deze optie kan niet worden gewijzigd. De scan controleert de geselecteerde back-upsets op malware (inclusief ransomware).
   - **Versleuteling**: Als u versleutelde back-upsets wilt scannen, geeft u het versleutelingswachtwoord op. Als u een locatie of meerdere back-upsets selecteert en het opgegeven wachtwoord komt niet overeen met een back-upset, wordt er een waarschuwing gegenereerd.
   - **Planning**: Deze optie kan niet worden gewijzigd. In de cloudopslag begint de scan automatisch.
4. Klik op **Maken**.

Er wordt een schema voor de back-upscans gemaakt en de locaties of de back-upsets die u hebt opgegeven, worden door een cloudagent gescand op malware.

Back-upschema's voor cloudtoepassingen

Op het tabblad **Beheer** > **Back-up van cloudtoepassingen** worden cloud-to-cloud back-upschema's weergegeven. Met deze schema's worden back-ups gemaakt van toepassingen in de cloud door middel van agenten die in de cloud worden uitgevoerd en de cloudopslag gebruiken als back-uplocatie.

In dit gedeelte kunt u de volgende bewerkingen uitvoeren:

- Een back-upschema maken, bekijken, uitvoeren, stoppen, bewerken en verwijderen
- Activiteiten voor elk back-upschema bekijken
- Waarschuwingen voor elk back-upschema bekijken

Ga voor meer informatie over back-ups van cloudtoepassingen naar:

- Microsoft 365-gegevens beschermen
- Google Workspace-gegevens beveiligen

Cloud-to-cloud back-ups handmatig uitvoeren

Er kunnen slechts 10 handmatige cloud-to-cloud back-ups per Microsoft 365- of Google Workspace-organisatie per uur worden uitgevoerd om verstoring van de Cyber Protection-service te voorkomen. Wanneer dit aantal is bereikt, wordt het aantal toegestane uitvoeringen teruggezet naar één per uur, en daarna komt er elk uur een extra uitvoering beschikbaar (bijv. uur 1: 10, uur 2: 1 uitvoering, uur 3: 2 uitvoeringen) tot een totaal van 10 runs per uur is bereikt.

Back-upschema's die worden toegepast op groepen apparaten (postvakken, stations, locaties) of die meer dan 10 apparaten bevatten, kunnen niet handmatig worden uitgevoerd.

Bescherming van samenwerkings- en communicatietoepassingen

Zoom, Cisco Webex Meetings, Citrix Workspace en Microsoft Teams worden nu veel gebruikt voor video-/webvergaderingen en communicatie. Met de Cyber Protection-service kunt u uw samenwerkingsprogramma's beschermen.

Voor Zoom, Cisco Webex Meetings, Citrix Workspace en Microsoft Teams kan in grote lijnen dezelfde beveiligingsconfiguratie worden gebruikt. In het onderstaande voorbeeld bespreken we de configuratie voor Zoom.

Bescherming voor Zoom instellen

1. De beveiligingsagent installeren: installeer de beveiligingsagent op de machine waarop de samenwerkingstoepassing is geïnstalleerd.
2. Meld u aan bij de Cyber Protect-console en pas een beschermingsschema toe waarvoor een van de volgende modules is ingeschakeld:
   - **Antivirus- en antimalwarebeveiliging** met zowel de instelling **Zelfbescherming** als **Active Protection** ingeschakeld (als u een van de Cyber Protect-edities gebruikt).
   - **Active Protection** met de instelling **Zelfbescherming** ingeschakeld (als u een van de <ATP_NAME>-edities gebruikt).
3. [Optioneel] Voor de automatische installatie van updates configureert u de module **Patchbeheer** in het beschermingsschema.

Uw Zoom-toepassing wordt dan beschermd door onder meer de volgende activiteiten:

- Clientupdates van Zoom worden automatisch geïnstalleerd
- Zoom-processen worden beschermd tegen code-injecties
- Verdachte bewerkingen van Zoom-processen worden voorkomen
- Het 'hosts'-bestand wordt beschermd tegen het toevoegen van Zoom-gerelateerde domeinen

Inzicht krijgen in uw huidige beschermingsniveau

Controle

Het tabblad **Controle** biedt belangrijke informatie over uw huidige beschermingsniveau en bevat de volgende dashboards:

- **Overzicht**
- **Activiteiten**
- **Waarschuwingen**
- **Bedreigingsfeed** (zie "Bedreigingsfeed" (p. 291) voor meer informatie)

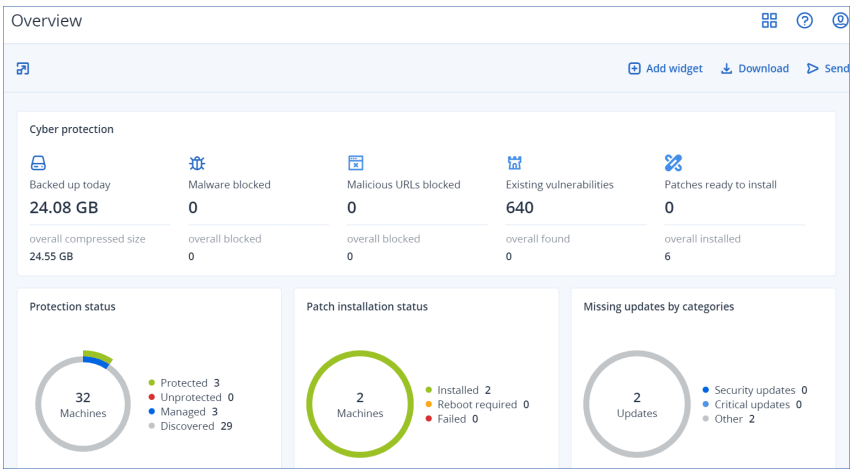
Het dashboard Overzicht

Het dashboard **Overzicht** bevat enkele aanpasbare widgets die een overzicht bieden van de bewerkingen voor de Cyber Protection-service. Widgets voor andere services worden in toekomstige releases beschikbaar gesteld.

De widgets worden elke vijf minuten bijgewerkt. De widgets hebben klikbare elementen waarmee u problemen kunt onderzoeken en oplossen. U kunt de huidige status van het dashboard downloaden of in PDF- en/of XLSX-indeling via e-mail verzenden.

U kunt kiezen uit verschillende widgets in de vorm van tabellen, cirkeldiagrammen, staafdiagrammen, lijsten en structuurkaarten. U kunt meerdere widgets van hetzelfde type toevoegen met verschillende filters.

De knoppen **Downloaden** en **Verzenden** in **Controle** > **Overzicht** zijn niet beschikbaar in de Standard-edities van de Cyber Protection-service.



De widgets op het dashboard opnieuw indelen

Versleep de widgets door op de betreffende namen te klikken.

Een widget bewerken

Klik op het potloodpictogram naast de naam van de widget. Wanneer u een widget bewerkt, kunt u de naam ervan wijzigen, het tijdsbereik wijzigen, filters instellen en rijen groeperen.

Een widget toevoegen

Klik op **Widget toevoegen** en voer vervolgens een van de volgende acties uit:

- Klik op de widget die u wilt toevoegen. De widget wordt toegevoegd met de standaardinstellingen.
- Als u de widget wilt bewerken voordat u deze toevoegt, klikt u op het Aanpassen wanneer de widget is geselecteerd. Wanneer u de widget hebt bewerkt, klikt u op **Gereed**.

Een widget verwijderen

Klik op de X naast de naam van de widget.

Het dashboard Activiteiten

Het dashboard **Activiteiten** geeft een overzicht van de huidige en eerdere activiteiten. De retentieperiode is standaard 90 dagen.

Als u de weergave van het dashboard **Activiteiten** wilt aanpassen, klikt u op het tandwielpictogram en selecteert u de kolommen die u wilt zien.

Als u de voortgang van de activiteit in real time wilt zien, schakelt u het selectievakje **Automatisch vernieuwen** in. Door frequente updates van meerdere activiteiten worden de prestaties van de beheerserver echter verminderd.

U kunt de vermelde activiteiten zoeken met de volgende criteria:

- **Apparaatnaam**
  Dit is de machine waarop de activiteit wordt uitgevoerd.
- **Gestart door**
  Dit is het account waarmee de activiteit is gestart.

U kunt de activiteiten ook filteren op de volgende eigenschappen:

- **Status**
  Bijvoorbeeld voltooid, mislukt, wordt uitgevoerd, geannuleerd.
- **Type**
  Bijvoorbeeld schema toepassen, back-ups verwijderen, software-updates installeren.
- **Tijd**
  Bijvoorbeeld de meest recente activiteiten, de activiteiten van de afgelopen 24 uur, of de activiteiten gedurende een bepaalde periode binnen de standaard retentieperiode.

Als u meer details over een activiteit wilt zien, selecteert u deze activiteit in de lijst en klikt u vervolgens in het deelvenster **Activiteitgegevens** op **Alle eigenschappen**. Zie de API-referenties

voor Activiteit en Taak in de Developer Network Portal voor meer informatie over de beschikbare eigenschappen.

Het dashboard Waarschuwingen

Het dashboard **Waarschuwingen** bevat al uw huidige waarschuwingen. De vermelde waarschuwingen zijn kritieke waarschuwingen of waarschuwingen voor fouten en zijn meestal gerelateerd aan taken zoals back-ups die om de een of andere reden zijn mislukt.

Waarschuwingen op het dashboard filteren:

1. Ga naar de vervolgkeuzelijst **Weergave** en selecteer een van de volgende criteria:
   - **Ernstgraad van de waarschuwing**
   - **Categorie Waarschuwing**
   - **Type waarschuwing**
   - **Type controle**
   - **Datumbereik: van ... tot ...**
   - **Workload**
   - **Schema**
   - **Klant**
2. Als u de **Categorie waarschuwing** hebt geselecteerd, gaat u naar de vervolgkeuzelijst **Categorie** en selecteert u de categorie waarschuwingen die u wilt bekijken.
3. Als u alle waarschuwingen wilt bekijken zonder ze te filteren, klikt u op **Alle typen waarschuwingen**.

Voor elke waarschuwing kunt u het volgende doen:

- Klik op de link **Apparaten** om naar het apparaat te gaan waarop de waarschuwing betrekking heeft.
- Lees het advies in het gedeelte **Problemen oplossen** van de waarschuwing en probeer dit op te volgen.
- Klik op **Zoeken naar een oplossing** om naar de betreffende documentatie en het artikel in de Knowledge Base te gaan. Met de functie **Zoeken naar een oplossing** worden de gegevens van de huidige waarschuwing vooraf ingevuld in uw zoekaanvraag om u zo effectief mogelijk te helpen.

Waarschuwingen op het dashboard sorteren:

Klik in de tabel met waarschuwingen op de pijlknop naast een van de volgende kolomnamen:

- **Ernstgraad van de waarschuwing**
- **Type waarschuwing**
- **Gemaakt**
- **Categorie Waarschuwing**

- **Workload**
- **Schema**

Als de Advanced Automation-service is ingeschakeld voor uw account, kunt u ook rechtstreeks vanuit de waarschuwing een nieuw servicedeskticket maken.

Een servicedeskticket maken

1. Klik in de betreffende waarschuwing op **Een nieuwe ticket maken**.
   Wanneer u in de tabelweergavemodus werkt, kunt u ook een waarschuwing selecteren en vervolgens **Een nieuwe ticket maken** selecteren in het rechterdeelvenster.
2. Definieer het volgende:
   - Schakel in het gedeelte voor de koptekst het selectievakje **Factureerbaar** in als u de op de ticket geregistreerde tijd wilt factureren aan de klant. Schakel ook het selectievakje **E-mail naar klant verzenden** in als u ticketupdates naar de klant wilt sturen.
   - Definieer een titel voor de ticket in het gedeelte **Algemene informatie**. In dit veld is vooraf een samenvatting van de waarschuwing ingevuld, maar u kunt deze bewerken.
   - In de velden van het gedeelte **Klantgegevens** is vooraf al de relevante informatie uit de waarschuwing ingevuld.
   - In de velden van het gedeelte **Configuratie-item of service** zijn vooraf al de gegevens ingevuld van het apparaat dat aan de waarschuwing is gekoppeld. U kunt desgewenst een apparaat opnieuw toewijzen.
   - In de velden van het gedeelte **Ondersteuningsagent** zijn vooraf al de gegevens van de standaard ondersteuningsagent, de categorie en de ondersteuningsgroep ingevuld. U kunt desgewenst een andere agent toewijzen.
   - In de velden van het gedeelte **Ticketupdate** zijn vooraf al de beschrijving en details van de waarschuwing ingevuld. Het veld **Status** is standaard ingesteld op **Nieuw** en kan worden gewijzigd.
   - In de gedeelten **Bijlagen**, **Factureerbare items** en **Interne opmerkingen** voegt u desgewenst de relevante items toe.
3. Klik op **Gereed**. Wanneer de ticket is gemaakt, wordt een link naar de ticket toegevoegd aan de waarschuwing.
   Als een waarschuwing wordt gesloten, wordt de gerelateerde ticket ook automatisch gesloten.

Opmerking
U kunt slechts één ticket per waarschuwing maken.

Typen waarschuwingen

Er worden waarschuwingen van de volgende typen gegenereerd:

- Waarschuwingen over back-ups
- Waarschuwingen over noodherstel
- Waarschuwingen over antimalwarebeveiliging

- Waarschuwingen over licenties
- Waarschuwingen over URL-filtering
- Waarschuwingen over EDR
- Waarschuwingen over apparaatbeheer
- Systeemwaarschuwingen

Waarschuwingen over back-ups

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Back-up mislukt	De waarschuwing wordt gegenereerd wanneer een back-up is mislukt vanwege een herstelbare fout of als de back-up is onderbroken omdat het systeem werd uitgeschakeld.	Controleer het logboek van de back-upbewerking: klik op de workload om deze te selecteren, klik op **Activiteiten** en zoek de waarschuwing in het logboek. Het bericht bevat informatie over de oorzaak van het probleem.
Back-up voltooid met waarschuwingen	De waarschuwing wordt gegenereerd wanneer een back-up is uitgevoerd met waarschuwingen.	Controleer de logboeken van conversie naar VM-, replicatie- of validatieschema's. Bij problemen tijdens deze bewerkingen wordt een waarschuwing gegenereerd zoals 'Activiteit mislukt' of 'Activiteit is voltooid met waarschuwing'.
Back-up is geannuleerd	De waarschuwing wordt gegenereerd telkens wanneer een back-up handmatig wordt geannuleerd door de gebruiker.	U kunt de back-up handmatig starten door op **Nu uitvoeren** te klikken of u kunt wachten tot de back-up op het volgende geplande tijdstip wordt uitgevoerd.
Back-up geannuleerd omdat back-upvenster is gesloten	De waarschuwing wordt gegenereerd wanneer de back-upactiviteit is gemist omdat deze niet in het tijdvenster past dat is opgegeven in de back-upopties.	Configureer het schema opnieuw of bewerk de opties van het back-upplan in het venster **Prestatie en back-up**. Vouw het gedeelte over uw product uit voor instructies.
Back-up wacht	De waarschuwing wordt gegenereerd wanneer er een conflict in de planning is en er tegelijkertijd twee back-uptaken worden gestart. In dit geval wordt de tweede back-uptaak in de wachtrij	Controleer of uw back-ups worden uitgevoerd binnen de verwachte tijdvensters en volgens het schema om conflicten in de planning te voorkomen.

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
	geplaatst totdat de eerste taak is voltooid of gestopt.	
Back-up reageert niet	De waarschuwing wordt gegenereerd wanneer een back-up al enige tijd geen voortgang toont en mogelijk is vastgelopen.	Het probleem kan worden veroorzaakt door een blokkering. Voor meer informatie: zie dit Knowledge Base-artikel.
Back-up is niet gestart	De waarschuwing wordt gegenereerd wanneer de geplande back-up niet is gestart om een onbekende reden.	Controleer of u de nieuwste versie van uw Acronis Backup-product gebruikt. • Als de agentmachine beschikbaar was tijdens de start van de back-up: 1. Bewerk de begintijd van de back-uptaak. 2. Als de waarschuwing opnieuw wordt weergegeven, moet u de back-uptaak opnieuw maken. 3. Als de waarschuwing ook wordt gegenereerd voor de nieuw gemaakte back-uptaak, neemt u contact op met het ondersteuningsteam voor hulp. • Als de agent offline was: 1. Schakel de machine niet uit tijdens de back-up. 2. Als de machine niet is uitgeschakeld, controleert u of de Acronis Managed Machine Service actief is: Start -> Zoeken -> services.msc -> zoek Acronis Managed Machine Service. Als u hulp nodig hebt, neem dan contact op met het ondersteuningsteam.
Back-upstatus is onbekend	De waarschuwing wordt gegenereerd wanneer de back-upagent offline was op een gepland tijdstip voor de back-up. De status van de resourceback-ups blijft	1. Controleer of er verwacht kon worden dat de agent offline is (het gaat bijvoorbeeld om een notebook buiten het Management Server-netwerk). 2. Als de agent niet offline had

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
	onbekend totdat de back-upagent weer online is.	moeten zijn, controleer dan of Acronis Managed Machine Service actief is: Start -> Zoeken -> services.msc -> zoek Acronis Managed Machine Service en controleer de status. Start de service als deze is gestopt.
Back-up ontbreekt	De waarschuwing wordt gegenereerd wanneer er gedurende meer dan [dagen na de laatste back-up] dagen geen back-up is gemaakt.	
Back-up is beschadigd	De waarschuwing wordt gegenereerd wanneer de validatieactiviteit is voltooid en aangeeft dat de back-up beschadigd is.	Volg de stappen in het artikel Problemen met beschadigde back-ups oplossen. Als u hulp nodig hebt om de oorzaak van een beschadigd archief vast te stellen, neemt u contact op met het ondersteuningsteam.
Continue gegevensbescherming mislukt	De waarschuwing wordt gegenereerd als de continue bescherming van de back-up is mislukt.	Controleer de volgende beperkingen: 1. Momenteel wordt Continue gegevensbescherming alleen ondersteund voor het NTFS-bestandssysteem en de volgende besturingssystemen: • Desktop: Windows 7 en later • Server: Windows Server 2008 R2 en later 2. CDP biedt geen ondersteuning voor **Acronis Secure Zone** als doel. 3. NFS-mappen die aan Windows zijn gekoppeld, worden niet ondersteund. 4. Continue replicatie wordt niet ondersteund: als er twee locaties in het beschermingsschema zijn, worden CDP-segmenten alleen op de eerste doellocatie gemaakt en worden de

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
		wijzigingen vervolgens naar de tweede locatie gerepliceerd tijdens de volgende back-up. 5. Wijzigingen die in een lokaal beschermde map worden toegepast vanaf een netwerkbron (bijvoorbeeld wanneer gebruikers de map via het netwerk openen), worden niet gedetecteerd door CDP. 6. Als een bestand wordt gebruikt (bijvoorbeeld als er enkele wijzigingen worden aangebracht in een Excel-bestand), worden de wijzigingen niet gedetecteerd door CDP. Als u wilt dat de wijzigingen door CDP worden gedetecteerd, slaat u ze op en sluit u het bestand.
Configuratie van Hyper-V-hosts is niet geldig	De waarschuwing wordt gegenereerd wanneer er twee of meer Agents voor Hyper-V zijn geïnstalleerd op Hyper-V-hosts met dezelfde hostnaam. Dit wordt niet ondersteund op hetzelfde accountniveau.	Registreer deze Agents voor Hyper-V onder verschillende onderliggende eenheden van het account, zodat er geen conflicten worden veroorzaakt.
Validatie mislukt	De waarschuwing wordt gegenereerd wanneer het validatieproces van de back-up niet kan worden voltooid.	Controleer het logboek van de bewerking met fouten: klik op de machine om deze te selecteren, klik op **Activiteiten**, en zoek de waarschuwing in het logboek. Deze moet informatie bevatten over de oorzaak van het probleem.
Kan de back-ups in de cloudopslag niet migreren naar de nieuwe indeling	De waarschuwing wordt gegenereerd wanneer de back-upmigratie naar de nieuwe indeling in de cloudopslag mislukt.	Voor meer informatie over de migratie van Acronis Cyber Backup Advanced-archieven: zie dit Knowledge Base-artikel. Voor meer informatie over de migratie van Acronis Cyber Backup-archieven: zie dit Knowledge Base-artikel.

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
		Voordat u contact opneemt met het ondersteuningsteam, gebruikt u migrate_archives om de volgende rapporten te verzamelen: **migrate_archives.exe --account=<Acronis-account> --password=<wachtwoord> --subaccounts=All > report1.txt** **migrate_archives.exe --cmd=finishUpgrade --account=<Acronis-account> --password=<wachtwoord> > report2.txt**
Versleutelingswachtwoord ontbreekt	De waarschuwing wordt gegenereerd wanneer de versleutelingssleutel van de database onjuist of beschadigd is of ontbreekt.	Er is geen manier om versleutelde back-ups te herstellen als u het wachtwoord verliest of vergeet. U moet het versleutelingswachtwoord lokaal instellen op het beschermde apparaat. U kunt het versleutelingswachtwoord niet instellen in het beschermingsschema. Zie Het versleutelingswachtwoord instellen voor meer informatie.
Upload is in behandeling	De waarschuwing wordt gegenereerd als uit een geplande controle blijkt dat Physical Data Shipping naar cloudarchief voor dit back-upplan niet wordt geüpload naar de opslag.	
Back-up kan niet worden hersteld	De waarschuwing wordt gegenereerd wanneer de herstelbewerking mislukt wanneer u bestanden of systeemback-ups probeert te herstellen.	Bepaal de exacte datum waarop de back-up is mislukt en probeer de back-up te herstellen met de laatst uitgevoerde back-up.

Waarschuwingen over noodherstel

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Opslagquota overschreden	De waarschuwing wordt gegenereerd wanneer de soft quota voor Disaster Recovery-opslag wordt overschreden.	Verhoog de quota of verwijder enkele back-ups uit de cloudopslag.
Quota is bereikt	De waarschuwing wordt gegenereerd wanneer de soft quota wordt overschreden voor de volgende opties: • Cloudserver. • Compute-punten. • Openbare IP-adressen.	
Opslagquota is overschreden	De waarschuwing wordt gegenereerd wanneer de hard quota voor Disaster Recovery-opslag wordt overschreden. Deze opslag wordt gebruikt door primaire en herstelservers. Als de maximale uitbreiding voor deze quota wordt bereikt, kunt u geen primaire en herstelservers maken, en geen schijven van de bestaande primaire servers toevoegen of uitbreiden. Als de maximale uitbreiding voor deze quota wordt overschreden, kunt u geen failover starten en ook geen gestopte server starten. Actieve servers blijven actief.	
Quota is overschreden	De waarschuwing wordt gegenereerd wanneer de hard quota voor de volgende opties wordt overschreden: • Cloudservers. • Compute-punten. • Openbare IP-adressen.	U kunt overwegen om extra apparaatquota's aan te schaffen of back-uptaken uit te schakelen voor de apparaten die u niet meer hoeft te beschermen.
Fout bij failover	De waarschuwing wordt gegenereerd wanneer er een	1. Selecteer de herstelserver en klik vervolgens op **Bewerken**.

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
	systeemprobleem optreedt nadat de failback is gestart.	2. Verlaag de CPU/RAM van de herstelserver. 3. Probeer opnieuw een failover uit te voeren.
Fout bij failovertest	De waarschuwing wordt gegenereerd wanneer er een systeemprobleem optreedt nadat een testfailover is gestart.	1. Selecteer de herstelserver en klik vervolgens op **Bewerken**. 2. Verlaag de CPU/RAM van de herstelserver. 3. Probeer opnieuw een testfailover uit te voeren. **Opmerking** Controleer of het IP-adres in het productienetwerk hetzelfde is als het IP-adres dat is geconfigureerd op de DHCP-server.
Fout bij failback	De waarschuwing wordt gegenereerd wanneer er een systeemprobleem optreedt nadat een failback is gestart.	U kunt de locatie met de fout zien in de lijst met back-upopslaglocaties: deze heeft een nummer in plaats van een naam (een locatienaam komt meestal overeen met een van de bestaande namen van eindgebruikers) en het is niet een locatie die u hebt gemaakt. Verwijder de locatie met de fout: 1. Ga in de Cyber Protect-console naar **Back-upopslag**. 2. Zoek de locatie en klik op het kruisje (x) om deze te verwijderen. 3. Bevestig uw keuze door te klikken op **Verwijderen**. 4. Probeer de failover opnieuw uit te voeren.
Failback is geannuleerd	De waarschuwing wordt gegenereerd wanneer een failback is geannuleerd door een gebruiker.	Verwijder de waarschuwing handmatig uit de console.
VPN-verbindingsfout	De waarschuwing wordt	Als u een probleem ondervindt

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
	gegenereerd wanneer een VPN-verbinding mislukt vanwege redenen die niet zijn gerelateerd aan de acties van de gebruiker. Het statusrapport van het VPN-apparaat is verouderd.	tijdens het implementeren of verbinden van het Acronis VPN-apparaat, neem dan contact op met het ondersteuningsteam. Neem de volgende informatie op in uw e-mail: • Screenshots van de foutmeldingen (indien aanwezig) • Screenshot van de CLI-interface van het Acronis VPN-apparaat • Uw Acronis Backup Cloud-datacenter en groepsnaam.
(Vpn onbereikbaar) Connectiviteitsgateway is niet bereikbaar	De waarschuwing wordt gegenereerd wanneer de Disaster Recovery-service de connectiviteitsgateway niet kan bereiken. Het statusrapport van de connectiviteitsgateway is verouderd.	Als u een probleem hebt ondervonden bij het implementeren of verbinden van het Acronis VPN-apparaat, neemt u contact op met het ondersteuningsteam. Neem de volgende informatie op in uw e-mail: • Screenshots van de foutmeldingen (indien aanwezig) • Screenshot van de CLI-interface van het Acronis VPN-apparaat • Uw Acronis Backup Cloud-datacenter en groepsnaam
IP van DR moet opnieuw worden toegewezen	De waarschuwing wordt gegenereerd wanneer het VPN-apparaat netwerkwijzigingen detecteert.	Wijs het IP-adres opnieuw toe. Zie IP-adressen opnieuw toewijzen voor meer informatie.
Fout van de connectiviteitsgateway	De waarschuwing wordt gegenereerd wanneer de implementatie van de VPN-server in de cloud mislukt.	Gebruik de verificatietool voor cloudverbinding en controleer de uitvoer op fouten. Sta toe dat Acronis-software wordt beheerd door het toepassingsbeheer van uw firewalls en antlmalwareprogramma's.

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Fout bij het maken van de primaire server	De waarschuwing wordt gegenereerd wanneer de primaire server niet is gemaakt vanwege een fout.	
Fout bij het maken van de herstelserver	De waarschuwing wordt gegenereerd wanneer de herstelserver niet is gemaakt vanwege een fout.	Controleer of de herstelserver voldoet aan de softwarevereisten. Voor meer informatie: zie "Softwarevereisten" (p. 776).
Primaire server verwijderen	De waarschuwing wordt gegenereerd wanneer een primaire server wordt verwijderd.	
Fout bij het herstellen van de server	De waarschuwing wordt gegenereerd wanneer het herstel van de primaire server of de herstelserver is mislukt.	Bekijk de details. Als de foutmelding algemeen of onduidelijk is (bijvoorbeeld 'Interne fout'), gaat u als volgt te werk: navigeer naar **Disaster Recovery** → **Servers**, klik om de betreffende machine te selecteren en klik op **Activiteiten**. Klik op een activiteit, houd Ctrl ingedrukt en klik met de linkermuisknop op de activiteit. Nu kunt u bij elke activiteit de drie puntjes (...) zien. Klik en selecteer **Informatie over taakactiviteit**.
Back-up mislukt	De waarschuwing wordt gegenereerd wanneer een back-up van de cloudserver (primaire server of server met de status productiefailover) is mislukt.	1. Controleer de verbinding met de back-uplocatie. 2. Controleer het opslagapparaat voor back-ups (lokale back-ups).
Netwerklimiet overschreden	De waarschuwing wordt gegenereerd wanneer het maximum aantal cloudnetwerken is bereikt (5 netwerken).	
Runbook-fout	De waarschuwing wordt gegenereerd wanneer de uitvoering van een runbook is mislukt.	Dit heeft geen invloed op de functionaliteit van het product en kan veilig worden genegeerd. Voor meer informatie: zie "Runbook maken" (p. 856).

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Runbook-waarschuwing	De waarschuwing wordt gegenereerd wanneer de uitvoering van het runbook is voltooid met waarschuwingen.	Dit heeft geen invloed op de functionaliteit van het product en kan veilig worden genegeerd. Voor meer informatie: zie "Runbook maken" (p. 856).
Interactie van de runbook-gebruiker vereist	De waarschuwing wordt gegenereerd wanneer het runbook wacht op actie van de gebruiker.	Dit heeft geen invloed op de functionaliteit van het product en kan veilig worden genegeerd. Voor meer informatie: zie "Runbook maken" (p. 856).
Internetverkeer geblokkeerd	De waarschuwing wordt gegenereerd wanneer het internetverkeer is geblokkeerd door de beheerder.	
Internetverkeer gedeblokkeerd	De waarschuwing wordt gegenereerd wanneer het internetverkeer is gedeblokkeerd door de beheerder.	
Lokale netwerken overlappen elkaar	De waarschuwing wordt gegenereerd wanneer identieke of overlappende lokale netwerken worden gedetecteerd.	
Onvoldoende serverquota voor licentiewijziging	De waarschuwing wordt gegenereerd wanneer de quota van de cloudservers onvoldoende is.	• Als de waarschuwing wordt gegenereerd voor een fysieke server, controleert u of de tenant en gebruiker voldoende quota hebben voor de optie **Webhostingservers** of **Servers**. • Als de waarschuwing wordt gegenereerd voor een virtuele server, controleert u of de tenant en gebruiker voldoende quota hebben voor de optie **Webhostingservers** of **Virtuele machines**. Een virtuele server kan geen gebruik maken van de quota voor de optie **Servers**.
Onvoldoende opties voor licentiewijziging	De waarschuwing wordt gegenereerd wanneer de optie **Disaster Recovery-opslag** wordt	

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
	uitgeschakeld.	
Fout bij licentiewijziging	De waarschuwing wordt gegenereerd wanneer er een fout is opgetreden bij de upgrade voor noodherstel.	
Onvoldoende compute-punten voor licentiewijziging	De waarschuwing wordt gegenereerd wanneer er geen compute-punten beschikbaar zijn.	Verhoog de hard quota voor de optie **Compute-punten**.
Onvoldoende serveropties voor licentiewijziging	De waarschuwing wordt gegenereerd wanneer de optie **Cloudservers** wordt uitgeschakeld.	
Herstelserver kan niet worden gemaakt door beleid	De waarschuwing wordt gegenereerd wanneer er een fout optreedt tijdens het instellen van de infrastructuur voor noodherstel.	Maak handmatig een herstelserver aan, zonder de eigenschap **Internettoegang**. Voor meer informatie: zie "Herstelserver maken" (p. 823).
Automatische testfailover van back-upprocessor opnieuw gepland	De waarschuwing wordt gegenereerd wanneer de automatische testfailover opnieuw is gepland.	
Time-out bereikt voor automatische testfailover van back-upprocessor	De waarschuwing wordt gegenereerd wanneer de automatische testfailover is verlopen. **Opmerking** Er worden compute-punten verbruikt voor elke automatische testfailover.	
Algemene fout bij automatische testfailover van back-upprocessor	De waarschuwing wordt gegenereerd wanneer de laatste geplande automatische testfailover van de herstelserver is mislukt.	• Start handmatig een testfailover van de herstelserver. Voor meer informatie: zie "Een testfailover uitvoeren" (p. 828). • Wacht tot de volgende geplande datum waarop de automatische testfailover wordt uitgevoerd.
Fout bij gegevensoverdracht via	De waarschuwing wordt	

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
failback	gegenereerd wanneer de gegevensoverdrachtfase van de failback mislukt.	
Failback mislukt	De waarschuwing wordt gegenereerd wanneer er een fout optreedt bij de failback.	U kunt de locatie met de fout zien in de lijst met back-upopslaglocaties: deze heeft een nummer in plaats van een naam (een locatienaam komt meestal overeen met een van de bestaande namen van eindgebruikers) en het is niet een locatie die u hebt gemaakt. Verwijder de locatie met de fout: 1. Ga in Cyber Protection naar **Back-upopslag**. 2. Zoek de locatie en klik vervolgens op het kruisje (x) om de locatie te verwijderen. 3. Bevestig uw keuze door te klikken op **Verwijderen**. 4. Start de failover opnieuw.
Bevestiging van failback mislukt	De waarschuwing wordt gegenereerd wanneer de bevestiging van de failback mislukt.	
Failbackmachine is klaar voor switchover	De waarschuwing wordt gegenereerd wanneer de machine klaar is voor switchover.	
Failback-switchover voltooid	De waarschuwing wordt gegenereerd wanneer de switchover is uitgevoerd.	Verwijder de waarschuwing handmatig uit de console.
Agent voor failbackdoel offline	De waarschuwing wordt gegenereerd wanneer de agent offline is.	

Waarschuwingen over antimalwarebeveiliging

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Er is verdachte activiteit	De waarschuwing wordt	Verwijder de waarschuwing handmatig uit

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
gedetecteerd op de externe verbinding	gegenereerd wanneer ransomware wordt gedetecteerd die afkomstig is van een externe verbinding.	de console.
Er is verdachte activiteit gedetecteerd	De waarschuwing wordt gegenereerd wanneer ransomware wordt gedetecteerd in de workload.	Verwijder de waarschuwing handmatig uit de console. om de waarschuwing te deactiveren. Afhankelijk van de optie die u hebt opgegeven in het Active Protection-schema, kan het volgende gebeuren: het schadelijke proces wordt gestopt, de tijdens het proces aangebrachte wijzigingen worden ongedaan gemaakt, of er zijn nog geen acties ondernomen en u moet dit probleem handmatig oplossen. Lees de details van de waarschuwing om te weten door welk proces de bestanden worden versleuteld en op welke bestanden dit van toepassing is. Als u besluit dat het proces voor versleuteling van de bestanden kan worden toegelaten (waarschuwing is vals-positief), kunt u dit proces toevoegen aan Vertrouwde processen: 1. Open het Active Protection-schema. 2. Klik op **bewerken** om de instellingen te wijzigen. 3. Ga naar **Vertrouwde processen** en geef de vertrouwde processen op die nooit als ransomware moeten worden beschouwd. Geef het volledige pad naar het uitvoerbare bestand voor het proces op. Het pad begint met de stationsletter. Bijvoorbeeld: `C:\Windows\Temp\er76s7sdkh.exe`
Cryptominingactiviteit is gedetecteerd	De waarschuwing wordt gegenereerd wanneer illegale cryptominers worden gedetecteerd in de workload.	Verwijder de waarschuwing handmatig uit de console.

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
MBR-verdediging: Verdachte activiteit gedetecteerd en opgeschort	De waarschuwing wordt gegenereerd wanneer ransomware wordt gedetecteerd in de workload (met name de MBR/GPT-partitie wordt gewijzigd door ransomware).	Verwijder de waarschuwing handmatig uit de console.
Niet-ondersteund netwerkpad opgegeven	De waarschuwing wordt gegenereerd wanneer het door de beheerder opgegeven herstelpad geen pad naar een lokale map is.	Geef het lokale pad op voor de bescherming van netwerkmappen (herstelpad). Verwijder de waarschuwing handmatig uit de console.
Kritiek proces is toegevoegd als schadelijk aan het Active Protection-schema	De waarschuwing wordt gegenereerd wanneer een kritiek proces wordt toegevoegd als geblokkeerd proces aan de lijst met uitsluitingen voor bescherming.	Verwijder de waarschuwing handmatig uit de console.
Kan Active Protection-beleid niet toepassen	De waarschuwing wordt gegenereerd wanneer het Active Protection-beleid niet kan worden toegepast.	Bekijk de foutmelding om te zien waarom het Active Protection-beleid niet kan worden toegepast.
Secure Zone: Ongeautoriseerde bewerking wordt gedetecteerd en geblokkeerd	De waarschuwing wordt gegenereerd wanneer ransomware wordt gedetecteerd in de workload (de ASZ-partitie wordt gewijzigd door ransomware).	Verwijder de waarschuwing handmatig uit de console.
Service Active Protection is niet actief	De waarschuwing wordt gegenereerd wanneer de Active Protection-service is vastgelopen of niet actief is.	Bekijk de foutmelding om te zien waarom de Active Protection-service niet actief is.
Active Protection-service is niet beschikbaar	De waarschuwing wordt gegenereerd wanneer de Active Protection-service niet beschikbaar is omdat een stuurprogramma niet compatibel is of ontbreekt.	Bekijk de Windows-gebeurtenislogboeken op crashes van de Acronis Active Protection-service (acronis_protection_service.exe).

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Conflict met een andere beveiligingsoplossing	Er wordt een waarschuwing gegenereerd als Active Protection niet beschikbaar is voor machine '{{resourceName}}' omdat er een conflict met een andere beveiligingsoplossing is gedetecteerd. Als u Active Protection wilt inschakelen, schakelt u de conflicterende beveiligingsoplossing uit of verwijdert u deze.	**Oplossing 1**: Als u realtime bescherming van Acronis wilt gebruiken, verwijdert u de third-party software voor antivirus uit de workload. **Oplossing 2**: Als u de third-party antivirus wilt gebruiken, opent u het beschermingsplan dat op de workload wordt toegepast en schakelt u vervolgens de realtime bescherming van Acronis, URL-filtering en Windows Defender antivirus uit.
Quarantaineactie mislukt	De waarschuwing wordt gegenereerd wanneer antimalware een gedetecteerde malware niet in quarantaine heeft geplaatst.	Bekijk de foutmelding om te zien waarom de quarantaine is mislukt.
Er is een schadelijk proces gedetecteerd	De waarschuwing wordt gegenereerd wanneer een malware (type proces) wordt gedetecteerd door de gedragengine. De gedetecteerde malware wordt in quarantaine geplaatst.	Verwijder de waarschuwing handmatig uit de console.
Er is een schadelijk proces gedetecteerd, maar niet in quarantaine geplaatst	De waarschuwing wordt gegenereerd wanneer een malware (type proces) wordt gedetecteerd door de gedragengine. De gedetecteerde malware wordt niet in quarantaine geplaatst.	Verwijder de waarschuwing handmatig uit de console.
Malware is gedetecteerd en geblokkeerd (ODS)	De waarschuwing wordt gegenereerd wanneer er malware wordt gedetecteerd tijdens een geplande scan. De gedetecteerde malware wordt in quarantaine geplaatst.	Verwijder de waarschuwing handmatig uit de console.

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Malware is gedetecteerd en geblokkeerd (RTP)	De waarschuwing wordt gegenereerd wanneer malware wordt gedetecteerd door Realtime bescherming. De gedetecteerde malware wordt in quarantaine geplaatst.	Verwijder de waarschuwing handmatig uit de console.
Er is malware gedetecteerd in een back-up	De waarschuwing wordt gegenereerd wanneer er malware wordt gedetecteerd tijdens een back-upscan.	Verwijder de waarschuwing handmatig uit de console.
Conflict gedetecteerd tussen Realtime antimalwarebeveiliging en een ander beveiligingsproduct	De waarschuwing wordt gegenereerd wanneer antimalware niet kan worden geregistreerd bij Windows Security Center.	Deactiveer of verwijder beveiligingsproducten van derden, of schakel Realtime antimalwarebeveiliging uit in het beschermingsplan.
Kan de Microsoft Security Essentials-module niet uitvoeren	De waarschuwing wordt gegenereerd wanneer de Microsoft Security Essentials-module niet kan worden uitgevoerd.	Bekijk de foutmelding om te zien waarom de Microsoft Security Essentials-module niet kon worden uitgevoerd.
Realtime bescherming is niet beschikbaar omdat antivirussoftware van derden is geïnstalleerd	De waarschuwing wordt gegenereerd wanneer Realtime bescherming niet kan worden ingeschakeld, omdat er nog realtime bescherming van een antivirusprogramma van derden is ingeschakeld.	Deactiveer of verwijder beveiligingsproducten van derden, of schakel Realtime antimalwarebeveiliging uit in het beschermingsplan.
Realtime bescherming is niet beschikbaar vanwege een incompatibel of ontbrekend stuurprogramma	De waarschuwing wordt gegenereerd als er geen realtime bescherming beschikbaar is vanwege een incompatibel of ontbrekend stuurprogramma.	Bekijk de foutmelding om te zien waarom de installatie van het stuurprogramma voor de workload is mislukt.
De Cyber Protection-service (of Active Protection-service) reageert niet	De waarschuwing wordt gegenereerd wanneer de Cyber Protection-service reageert op een ping van de	Verwijder de waarschuwing handmatig uit de console.

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
	statuscontrole vanuit de console.	
Kan beveiligingsdefinitie niet bijwerken	De waarschuwing wordt gegenereerd wanneer een update van de beveiligingsdefinitie is mislukt.	Bekijk de foutmelding om te zien waarom de update van de beveiligingsdefinitie is mislukt.
Tamper Protection is ingeschakeld	De waarschuwing wordt gegenereerd wanneer de instellingen van Microsoft Defender niet kunnen worden gewijzigd omdat Tamper Protection is ingeschakeld.	Schakel de instellingen voor Tamper Protection uit voor de Windows-workload.
Kan de Windows Defender-module niet uitvoeren	De waarschuwing wordt gegenereerd wanneer de uitvoering van de Windows Defender-module is mislukt.	Bekijk de foutmelding om te zien waarom de Windows Defender-module niet kon worden uitgevoerd.
Windows Defender is geblokkeerd door antivirussoftware van derden	De waarschuwing wordt gegenereerd wanneer Windows Defender wordt geblokkeerd omdat een antivirusprogramma van derden op de machine is geïnstalleerd.	Deactiveer of verwijder het beveiligingsproduct van derden.
Conflict met groepsbeleid	De waarschuwing wordt gegenereerd wanneer de instellingen van Microsoft Defender niet kunnen worden gewijzigd omdat deze worden beheerd door een groepsbeleid.	Schakel de instellingen van het groepsbeleid voor de Windows-workload uit.
Microsoft Security Essentials heeft actie ondernomen om deze machine te beschermen tegen malware	De waarschuwing wordt gegenereerd wanneer Microsoft Security Essentials een malware heeft verwijdert of in quarantaine heeft geplaatst.	Verwijder de waarschuwing handmatig uit de console.
Microsoft Security Essentials heeft malware gedetecteerd	De waarschuwing wordt gegenereerd wanneer Microsoft Security Essentials	Verwijder de waarschuwing handmatig uit de console.

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
	malware of andere mogelijk ongewenste software heeft gedetecteerd.	

Waarschuwingen over licenties

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Opslagquota is bijna bereikt	De waarschuwing wordt gegenereerd wanneer het gebruik onder de 80% daalt (na opschoning of quota-upgrade).	Koop extra opslagruimte of maak schijfruimte vrij in uw cloudopslag.
Opslagquota is overschreden	De waarschuwing wordt gegenereerd wanneer de hele 100% van de opslagquota is gebruikt.	Koop meer opslagruimte. Voor meer informatie: zie dit Knowledge Base-artikel.
Workloadquota bereikt	De waarschuwing wordt gegenereerd wanneer: gebruik voor optie > 0 en gebruik > quota, maar gebruik <= quota + uitbreiding.	
Workloadquota is overschreden	De waarschuwing wordt gegenereerd wanneer: gebruik voor optie > quota + uitbreiding.	
De workload heeft geen quota om een back-upschema toe te passen (resource heeft geen servicequota)	De waarschuwing wordt gegenereerd wanneer: • De quota is handmatig verwijderd: **Apparaat** > **Details** > **Servicequota**, klik vervolgens op **Wijzigen** en selecteer de optie **Geen quota**. • De optie voor de **beheerconsole** is uitgeschakeld. • De waarde van quota + uitbreiding voor de optie in de **beheerconsole** lager wordt dan het huidige gebruik.	

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Kan een workload met toegewezen quota niet beschermen	De waarschuwing wordt gegenereerd wanneer de optie niet voldoende is en u moet beschikken over: • een dynamische groep. • een back-upschema dat aan die groep is toegewezen. • een resource die tot die dynamische groep behoort, maar bepaalde eigenschappen heeft waardoor het niet mogelijk is om hierop hetzelfde back-upplan toe te passen.	
Abonnementslicentie verlopen	De waarschuwing wordt gegenereerd wanneer een licentie verloopt.	Wanneer een abonnement is verlopen, worden alle functies van het product, behalve herstel, geblokkeerd totdat het abonnement wordt verlengd. De gegevens waarvan een back-up is gemaakt, zijn nog wel toegankelijk voor herstel. Koop een nieuwe licentie. **Opmerking** Als u onlangs een nieuw abonnement hebt gekocht maar nog steeds het bericht krijgt dat het abonnement is verlopen, moet u het nieuwe abonnement importeren vanuit het Acronis-account: ga in de beheerconsole naar **Instellingen** -> **Licenties** en klik op **Synchroniseren** in de rechterbovenhoek. Abonnementen worden gesynchroniseerd.
Abonnementslicentie verloopt binnenkort	De waarschuwing wordt gegenereerd als een licentie binnen minder dan 30 dagen verloopt.	Koop een nieuw abonnement.

Waarschuwingen over URL-filtering

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Schadelijke URL is geblokkeerd	De waarschuwing wordt gegenereerd wanneer een schadelijke URL wordt geblokkeerd door URL-filtering.	Controleer de instellingen voor URL-filtering. URL-filtering blokkeert pagina's die volgens de instellingen voor URL-filtering moeten worden geblokkeerd. Voor meer informatie: zie "URL-filtering" (p. 893).
Een waarschuwing voor een schadelijke URL is genegeerd	De waarschuwing wordt gegenereerd wanneer u toch naar de schadelijke URL gaat die door URL-filtering wordt geblokkeerd.	Controleer de instellingen voor URL-filtering.
Conflict gedetecteerd tussen URL-filtering en een beveiligingsproduct	De waarschuwing wordt gegenereerd wanneer URL-filtering niet kan worden ingeschakeld vanwege een conflict met een ander beveiligingsproduct.	Controleer de instellingen voor URL-filtering.
Website-URL is geblokkeerd	De waarschuwing wordt gegenereerd wanneer een URL voldoet aan alle criteria die zijn opgegeven in de geblokkeerde categorie voor URL-filtering.	Controleer de instellingen voor URL-filtering.

Waarschuwingen over EDR

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Incident gedetecteerd	De waarschuwing wordt gegenereerd wanneer er een incident wordt gemaakt of wanneer de status van een bestaand incident wordt bijgewerkt.	Deze waarschuwing informeert u over een nieuw incident of een oud incident dat is bijgewerkt. U kunt de waarschuwing bekijken en sluiten. U kunt ervoor kiezen om het incident te openen voor verder onderzoek.
Inbreukindicator (IOC) gedetecteerd	De waarschuwing wordt gegenereerd wanneer een nieuwe inbreukindicator is gedetecteerd door de	Deze waarschuwing is bedoeld om u te informeren dat er een IOC is gedetecteerd voor een of meer workloads. U ziet de

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
	zoekservice voor IOC-bedreigingen in EDR.	waarschuwing en vervolgens kunt u op de link in de waarschuwing klikken om details over de IOC te bekijken.
Kan de workload niet isoleren van het netwerk	De waarschuwing wordt gegenereerd wanneer de gebruiker actie onderneemt om de machine van het netwerk te isoleren, maar de isolatieactie mislukt.	Onderneem de nodige acties.
Kan de workload niet opnieuw verbinden met het netwerk	De waarschuwing wordt gegenereerd wanneer de gebruiker actie onderneemt om de machine weer met het netwerk te verbinden, maar de actie mislukt.	Onderneem de nodige acties.
Windows Defender Firewall-instellingen zijn gewijzigd	De waarschuwing wordt gegenereerd wanneer de instellingen voor de firewall zijn gewijzigd op een geïsoleerde machine.	Deze waarschuwing is bedoeld om u te informeren dat de firewallgegevens op de geïsoleerde computer zijn gewijzigd. Dit is alleen ter informatie en u kunt de waarschuwing sluiten nadat u deze hebt bekeken.

Waarschuwingen over apparaatbeheer

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Apparaatbeheer en Preventie van gegevensverlies worden uitgevoerd met beperkte functionaliteit (incompatibele CPU gedetecteerd)	De waarschuwing wordt gegenereerd wanneer de DeviceLock-agent is gestart op een fysieke machine met een CPU die ondersteuning biedt voor CET-technologie.	Schakel de optie op de betreffende machines uit om deze waarschuwingen te voorkomen.
De functie voor apparaatbeheer wordt nog niet ondersteund in macOS Ventura	De waarschuwing wordt gegenereerd wanneer DeviceLock-agent wordt gestart op een fysieke macOS Ventura-machine en het beschermingsplan met	

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
	Apparaatbeheer wordt toegepast op de agent. Alleen van toepassing op versies waarbij er een kernel panic-probleem is vanwege het besturingsprogramma van DeviceLock.	
Toegestane doorgifte van gevoelige gegevens	De waarschuwing wordt gegenereerd wanneer doorgifte van gevoelige inhoud is toegestaan.	
Gemotiveerde doorgifte van gevoelige gegevens	De waarschuwing wordt gegenereerd wanneer de doorgifte van gevoelige inhoud is gemotiveerd.	
Geweigerde doorgifte van gevoelige gegevens	De waarschuwing wordt gegenereerd wanneer doorgifte van gevoelige inhoud is geblokkeerd.	
De resultaten van de observatiemodus van preventie van gegevensverlies bekijken	De waarschuwing wordt gegenereerd wanneer het tijd is om de observatieresultaten te bekijken: • De Advanced DLP Pack-licentie wordt niet toegepast. • Er is een maand verstreken sinds de observatiemodus is ingeschakeld in een beschermingsplan dat is toegepast op ten minste één workload. • Er is een maand verstreken sinds de laatste vergelijkbare waarschuwing is gegenereerd en er gebruik van DLP in de observatiemodus is gedetecteerd.	
Beveiligings-id is gewijzigd voor de gebruiker	De waarschuwing wordt gegenereerd wanneer een SID wordt bijgewerkt voor een bekende gebruikersnaam. Dit kan gebeuren wanneer het besturingssysteem opnieuw wordt geïnstalleerd op een workload buiten het domein.	

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Randapparaat is geblokkeerd	De waarschuwing wordt gegenereerd wanneer bepaalde acties (lees-/schrijfbewerkingen) voor ondersteunde apparaten worden geblokkeerd.	
Kan geen verbinding maken met een externe SSL-resource.	De waarschuwing wordt gegenereerd wanneer de toegang tot een externe SSL-resource wordt geblokkeerd door extra handshakepreventie bij de resource.	Voeg de resource toe aan de acceptatielijst voor externe hosts.

Systeemwaarschuwingen

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
Agent is verouderd	De waarschuwing wordt gegenereerd wanneer de versie van de agent verouderd is.	Ga naar de lijst met agents en werk de agent bij.
Automatische update is mislukt	De waarschuwing wordt gegenereerd wanneer de automatische update van de agent mislukt.	Probeer een handmatige update uit te voeren.
U moet het apparaat opnieuw opstarten na de installatie van een nieuwe agent	De waarschuwing wordt gegenereerd wanneer een herstart is vereist na een installatie op afstand.	Start de workload opnieuw op.
Activiteit mislukt	De waarschuwing wordt gegenereerd wanneer een activiteit is mislukt.	Start alle Acronis-services voor de workload opnieuw op.
Activiteit voltooid met waarschuwingen	De waarschuwing wordt gegenereerd wanneer een activiteit is uitgevoerd, maar er enkele waarschuwingen zijn gegenereerd.	
Activiteit reageert niet	De waarschuwing wordt gegenereerd wanneer een activiteit die wordt uitgevoerd, niet meer reageert.	
Kan schema niet implementeren	De waarschuwing wordt	

Waarschuwing	Beschrijving	Oplossing voor de waarschuwing
	gegenereerd wanneer de implementatie van het beschermingsplan is mislukt.	
Kan gebruikersnaam niet converteren naar SID	De waarschuwing wordt gegenereerd wanneer de conversie van de SID van het schema is mislukt.	

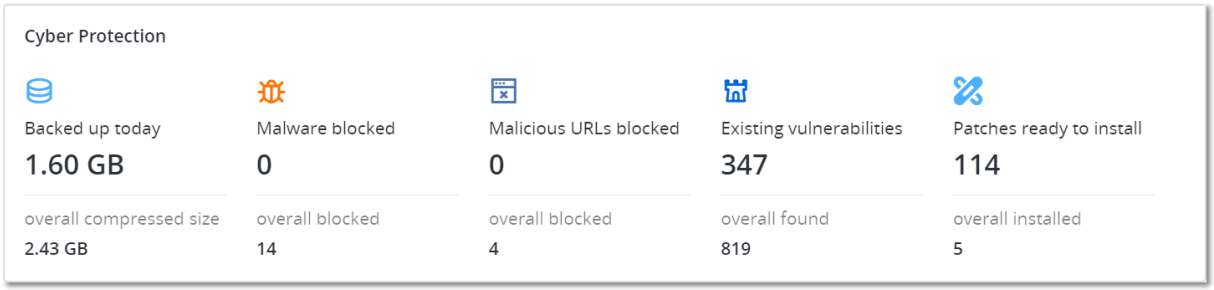
Waarschuwingswidgets

In de waarschuwingswidgets ziet u de volgende details van waarschuwingen in verband met uw workload:

Veld	Beschrijving
Widget 5 meest recente waarschuwingen	Een lijst met de vijf meest recente waarschuwingen.
Overzicht van historische waarschuwingen	Een grafische widget met waarschuwingen, met de ernst van de waarschuwing, het type waarschuwing en het tijdbereik.
Overzicht van waarschuwingen activeren	Een grafische widget met actieve waarschuwingen, met de ernst van de waarschuwing, het type waarschuwing en het totale aantal actieve waarschuwingen.
Geschiedenis van waarschuwingen	Een tabelweergave van historische waarschuwingen.
Gegevens van actieve waarschuwingen	Een tabelweergave van actieve waarschuwingen.

Cyberbescherming

Deze widget geeft algemene informatie over de grootte van back-ups, geblokkeerde malware, geblokkeerde URL's, gevonden beveiligingsproblemen en geïnstalleerde patches weer.



In de bovenste rij worden de huidige statistieken weergegeven:

- **Back-up vandaag gemaakt**: de som van de grootten van herstelpunten gedurende de afgelopen 24 uur
- **Malware geblokkeerd**: het aantal momenteel actieve waarschuwingen over geblokkeerde malware
- **URL's geblokkeerd**: het aantal momenteel actieve meldingen over geblokkeerde URL's
- **Bestaande kwetsbaarheden**: het aantal momenteel bestaande kwetsbaarheden
- **Patches klaar om te installeren**: het aantal momenteel beschikbare patches die moeten worden geïnstalleerd

In de onderste rij worden de algemene statistieken weergegeven:

- De gecomprimeerde grootte van alle back-ups
- Het totale aantal geblokkeerde malware op alle machines
- Het totale aantal geblokkeerde URL's op alle machines
- Het totale aantal gedetecteerde beveiligingsproblemen op alle machines
- Het totale aantal geïnstalleerde updates/patches op alle machines

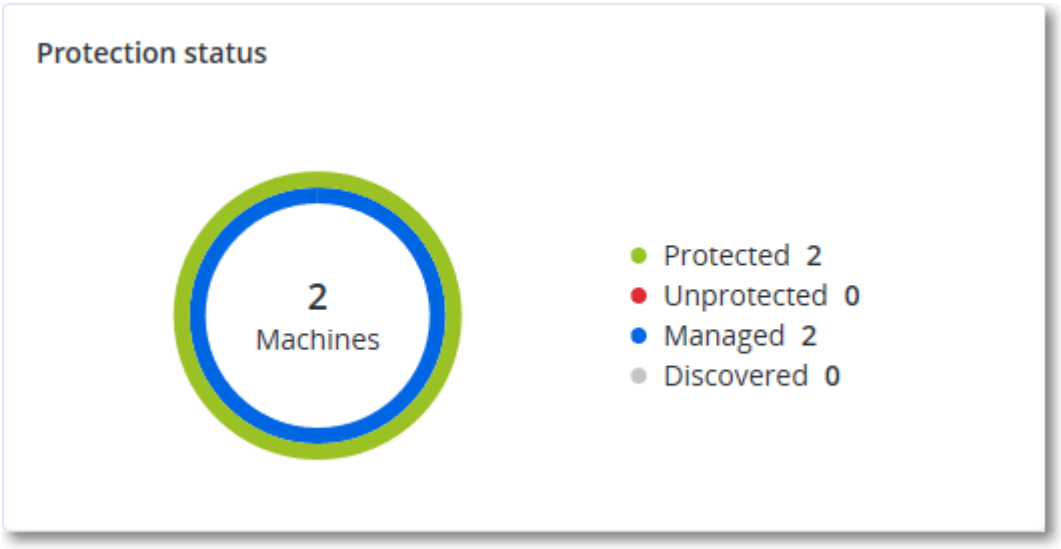
Beveiligingsstatus

Deze widget geeft de huidige beveiligingsstatus voor alle machines weer.

Een machine kan een van de volgende statussen hebben:

- **Beschermd**: machines met toegepast beschermingsschema.
- **Onbeschermd**: machines zonder toegepast beschermingsschema. Dit kunnen zowel gedetecteerde als beheerde machines zonder beschermingsschema zijn.
- **Beheerd**: machines met geïnstalleerde beveiligingsagent.
- **Gedetecteerd**: machines waarop geen beveiligingsagent is geïnstalleerd.

Als u op de machinestatus klikt, wordt u voor meer informatie omgeleid naar de lijst met machines die deze status hebben.



Gedetecteerde machines

Deze widget geeft de lijst met gedetecteerde machines tijdens het opgegeven tijdbereik weer.

Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

Widgets voor Eindpuntdetectie en -respons (EDR)

Eindpuntdetectie en -respons (EDR) bevat zeven widgets, die allemaal toegankelijk zijn via het dashboard **Overzicht**. Drie van deze widgets worden ook standaard weergegeven binnen de EDR-functionaliteit (zie "Incidenten bekijken" (p. 951)).

De zeven beschikbare widgets zijn:

- Verdeling van de belangrijkste incidenten per workload
- Bedreigingsstatus (weergegeven in EDR)
- Geschiedenis van de ernst van incidenten (weergegeven in EDR)

- Gemiddelde reparatietijd voor beveiligingsincidenten
- Burndown van beveiligingsincidenten
- Detectie door tactieken (weergegeven in EDR)
- Netwerkstatus van workloads

Verdeling van de belangrijkste incidenten per workload

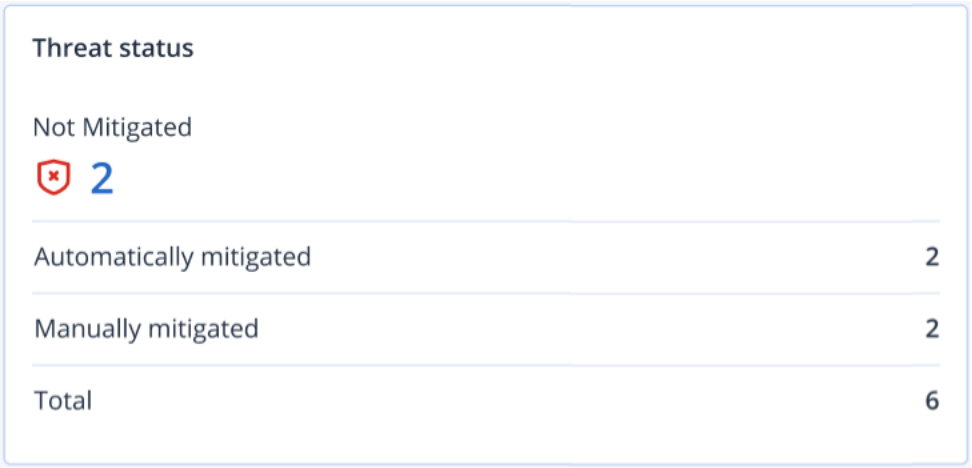
Deze widget toont de vijf belangrijkste workloads met de meeste incidenten (klik op **Alles weergeven** om naar de lijst met incidenten te gaan, gefilterd volgens de instellingen van de widget).

Beweeg de muis boven een rij met een workload om een uitsplitsing te zien van de huidige onderzoeksstatus voor de incidenten. Onderzoeksstatussen zijn **Niet gestart**, **Wordt onderzocht**, **Gesloten** en **Fout-positief**. Klik vervolgens op de workload die u verder wilt analyseren. De lijst met incidenten wordt vernieuwd volgens de instellingen van de widget.

Bedreigingsstatus

Deze widget geeft de huidige bedreigingsstatus weer voor alle workloads. U ziet ook hoeveel incidenten nog niet zijn verholpen en nog moeten worden onderzocht. De widget geeft ook het aantal incidenten aan dat is verholpen (zowel handmatig als automatisch).

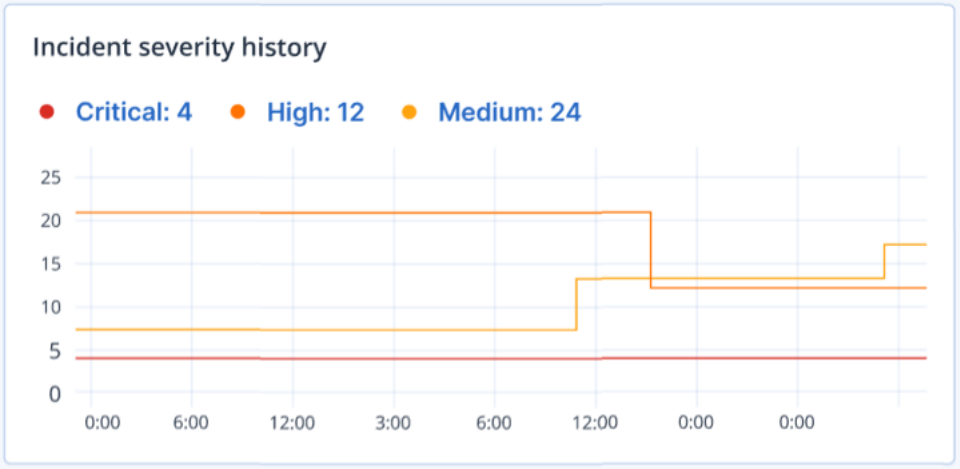
Klik op het aantal **Niet verholpen** incidenten om de lijst met incidenten weer te geven, gefilterd op niet-verholpen incidenten.



Geschiedenis van de ernst van incidenten

Deze widget geeft de voortgang van aanvallen naar ernstgraad weer en bevat aanwijzingen voor mogelijke aanvalscampagnes. Wanneer pieken zichtbaar zijn, kan dit erop wijzen dat de organisatie wordt aangevallen.

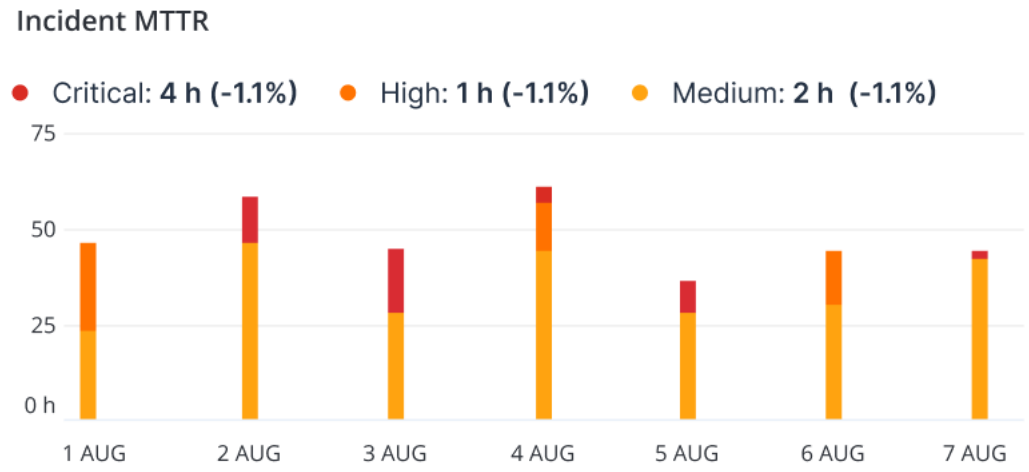
Plaats de muisaanwijzer op de grafiek om een uitsplitsing van de incidentgeschiedenis op een specifiek punt in de afgelopen 24 uur (de standaardperiode) te bekijken. Klik op de ernstgraad (**Kritiek**, **Hoog** of **Matig**) om de lijst met de betreffende incidenten te bekijken. U wordt omgeleid naar de lijst met incidenten die vooraf is gefilterd op incidenten met de geselecteerde ernstgraad.



Gemiddelde reparatietijd voor beveiligingsincidenten

Deze widget toont de gemiddelde tijd die nodig is voor het oplossen van beveiligingsincidenten. Hiermee wordt aangegeven hoe snel incidenten worden onderzocht en opgelost.

Klik op een kolom voor een uitsplitsing van de incidenten naar ernstgraad (**Kritiek**, **Hoog** en **Matig**), en hoeveel tijd nodig was om de incidenten per ernstgraad op te lossen. De tussen haakjes vermelde waarde in % geeft de toe- of afname aan ten opzichte van de vorige periode.

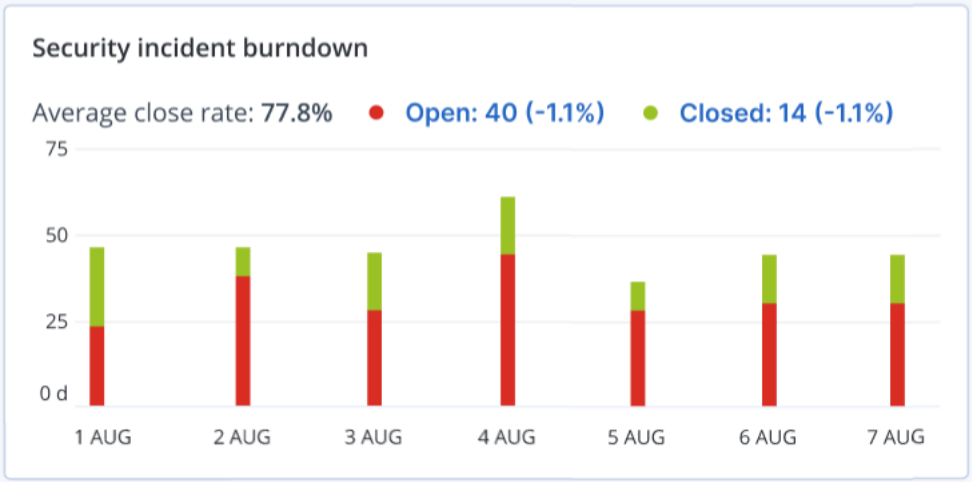


Burndown van beveiligingsincidenten

Deze widget toont de efficiëntiegraad bij het sluiten van incidenten. Het aantal openstaande incidenten wordt bepaald aan de hand van het aantal gesloten incidenten gedurende een bepaalde periode.

Beweeg de muis boven een kolom om een uitsplitsing te zien van de gesloten en openstaande incidenten voor de geselecteerde dag. Als u op de waarde Openstaand klikt, wordt de lijst met incidenten weergegeven, gefilterd op incidenten die momenteel nog openstaan (status **Wordt onderzocht** of **Niet gestart**). Als u op de waarde Gesloten klikt, wordt de lijst met incidenten weergegeven, gefilterd op incidenten die niet meer openstaan (status **Gesloten** of **Fout-positief**).

De tussen haakjes vermelde waarde in % geeft de toe- of afname aan ten opzichte van de vorige periode.



Detectie door tactieken

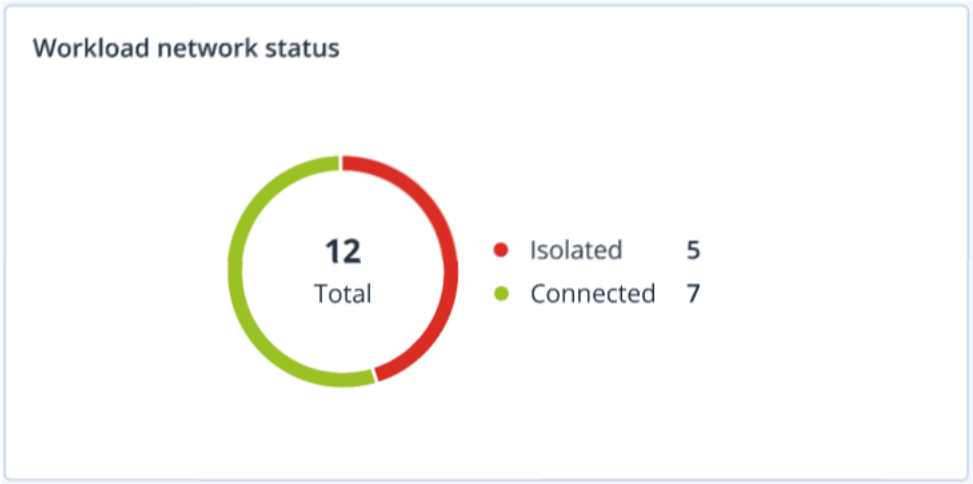
Deze widget geeft het aantal keren weer dat specifieke aanvalstechnieken zijn gevonden in incidenten gedurende de geselecteerde periode.

De waarden in groen en rood geven aan of er een toename of afname is geweest in de voorgaande periode. In het onderstaande voorbeeld zijn escalaties van bevoegdheden en Command and control-aanvallen de afgelopen periode toegenomen. Dit kan erop duiden dat uw referentiebeheer moet worden geanalyseerd en dat de beveiliging moet worden verbeterd.

Netwerkstatus van workloads

Deze widget toont de huidige netwerkstatus van uw workloads en geeft aan hoeveel workloads geïsoleerd zijn en hoeveel er verbonden zijn.

Klik op de waarde Geïsoleerd om de lijst Workload met agents weer te geven (onder het menu **Workloads** in de Cyber Protect-console), gefilterd op geïsoleerde workloads. Klik op de waarde Verbonden om de lijst Workloads met agents weer te geven, gefilterd op verbonden workloads.



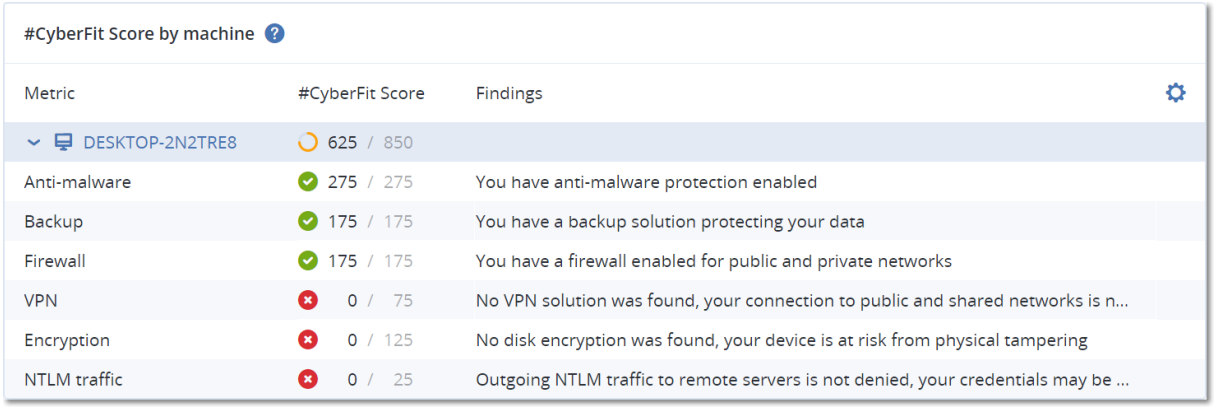
#CyberFit-score per machine

In deze widget ziet u voor elke machine de totale #CyberFit-score, de samengestelde scores en de bevindingen voor elk van de beoordeelde metrieken:

- Antimalware
- Back-up
- Firewall
- VPN
- Versleuteling
- NTLM-verkeer

Als u de score voor de verschillende metrieken wilt verbeteren, kunt u de aanbevelingen in het rapport bekijken.

Raadpleeg '#CyberFit-score voor machines' voor meer informatie over de #CyberFit-score.



Schijfintegriteitscontrole

Schijfintegriteitscontrole geeft informatie over de huidige status van de schijfintegriteit en een prognose daarover, zodat u gegevensverlies door een eventuele schijffout kunt voorkomen. Zowel HDD- als SSD-schijven worden ondersteund.

Beperkingen

- Prognose van schijfintegriteit wordt alleen ondersteund voor machines met Windows.
- Alleen schijven van fysieke machines worden gecontroleerd. De schijven van virtuele machines kunnen niet worden gecontroleerd en weergegeven in de widgets voor schijfintegriteit.
- RAID-configuraties worden niet ondersteund. De widgets voor schijfintegriteit bevatten geen informatie over machines met RAID-implementatie.
- NVMe SSD's worden niet ondersteund.

Schijfintegriteit kan een van de volgende statussen hebben:

- **OK**
  De schijfintegriteit is tussen de 70 en 100%.
- **Waarschuwing**
  De schijfintegriteit is tussen de 30 en 70%.

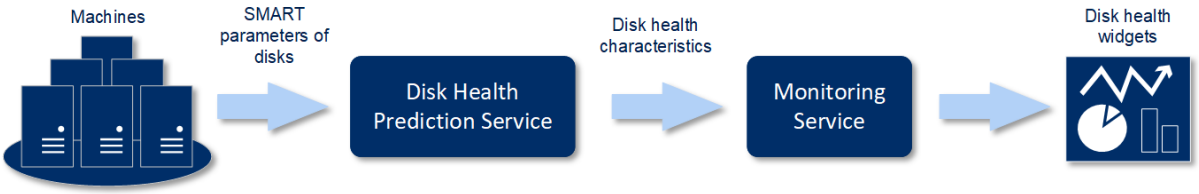
- **Kritiek**
  De schijfintegriteit is tussen de 0 en 30%.
- **Schijfgegevens berekenen**
  : de huidige schijfstatus en -prognose worden berekend.

Zo werkt het

De service Voorspelling van schijfintegriteit maakt gebruik van een op kunstmatige intelligentie gebaseerd voorspellingsmodel.

1. De agent verzamelt de SMART-parameters van de schijven en geeft deze gegevens door aan de service Voorspelling van schijfintegriteit:
   - SMART 5: aantal opnieuw toegewezen sectoren.
   - SMART 9: uren ingeschakeld.
   - SMART 187: gerapporteerde niet-corrigeerbare fouten.
   - SMART 188: time-out van opdrachten.
   - SMART 197: huidig aantal sectoren in behandeling.
   - SMART 198: aantal offline niet-corrigeerbare sectoren.
   - SMART 200: percentage schrijffouten.
2. De service Voorspelling van schijfintegriteit verwerkt de ontvangen SMART-parameters, maakt prognoses en genereert de volgende kenmerken van de schijfintegriteit:
   - Huidige status van schijfintegriteit: OK, Waarschuwing, Kritiek.
   - Prognose van schijfintegriteit: negatief, stabiel, positief.
   - Prognose van schijfintegriteit, waarschijnlijkheid uitgedrukt als percentage.

   De periode van de voorspelling is één maand.
3. De controleservice ontvangt deze kenmerken en toont vervolgens de relevante informatie in de widgets voor schijfintegriteit in de Cyber Protect-console.



Widgets voor schijfintegriteit

De resultaten van de schijfintegriteitscontrole worden weergegeven in de volgende widgets die beschikbaar zijn in de Cyber Protect-console.

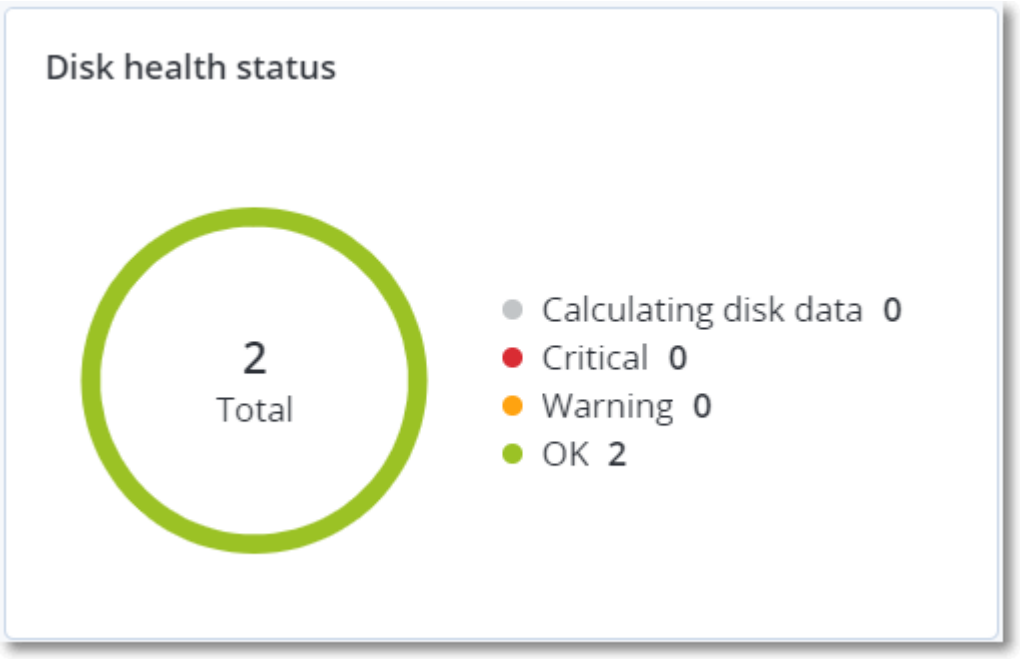
- **Overzicht van schijfintegriteit**: een widget met een structuurkaart op twee detailniveaus waartussen kan worden geschakeld.
  - Machineniveau
    Geeft samengevatte informatie weer over de status van de schijfintegriteit van de

geselecteerde klantmachines. Alleen de meest kritieke schijfstatus wordt weergegeven. De andere statussen worden in een knopinfo weergegeven wanneer u het betreffende blok aanwijst met de muis. Hoe groot het blok van de machine is, hangt af van de totale grootte van alle schijven van de machine. Welke kleur het blok van de machine heeft, hangt af van de meest kritieke schijfstatus die is gevonden.

- Schijfniveau
  Geeft de huidige status van de schijfintegriteit weer van alle schijven voor de geselecteerde machine. Elk schijfblok toont een van de volgende prognoses van schijfintegriteit en de waarschijnlijkheid ervan in procenten:
  - Zal minder worden
  - Zal stabiel blijven

- Zal beter worden

- **Status van schijfintegriteit**: Een widget met een cirkeldiagram met het aantal schijven voor elke status.



Waarschuwingen over de status van de schijfintegriteit

De controle van de schijfintegriteit wordt elke 30 minuten uitgevoerd en de bijbehorende waarschuwing wordt een keer per dag gegenereerd. Wanneer de status van de schijfintegriteit verandert van **Waarschuwing** in **Kritiek**, wordt er altijd een waarschuwing gegenereerd.

Naam van de waarschuwing	Ernstgraad	Status van schijfintegriteit	Beschrijving
Schijffout is mogelijk	Waarschuwing	(30 – 70)	De schijf <schijfnaam> op deze machine zal waarschijnlijk defect raken in de toekomst. Voer zo snel mogelijk een volledige systeemkopieback-up van deze schijf uit, vervang deze en herstel de systeemkopie vervolgens op de nieuwe schijf.
Schijf zal binnenkort defect raken	Kritiek	(0 – 30)	De status van de schijf <schijfnaam> op deze machine is kritiek en de schijf zal waarschijnlijk binnenkort defect raken. We raden niet aan om op dit moment een imageback-up van deze schijf te maken, omdat de schijf defect kan raken door de extra belasting. Maak nu meteen een back-up van de belangrijkste bestanden op deze schijf en vervang de schijf.

Overzicht van gegevensbescherming

Opmerking
Deze functie is alleen beschikbaar met het Advanced Backup-pakket.

Met de functie Overzicht van gegevensbescherming kunt u alle gegevens vinden die belangrijk voor u zijn en gedetailleerde informatie krijgen over het aantal, de grootte, de locatie en de beveiligingsstatus van alle belangrijke bestanden in een schaalbare weergave met structuurkaart.

De grootte van elke blok hangt af van het totale aantal/de grootte van alle belangrijke bestanden die bij een klant/machine horen.

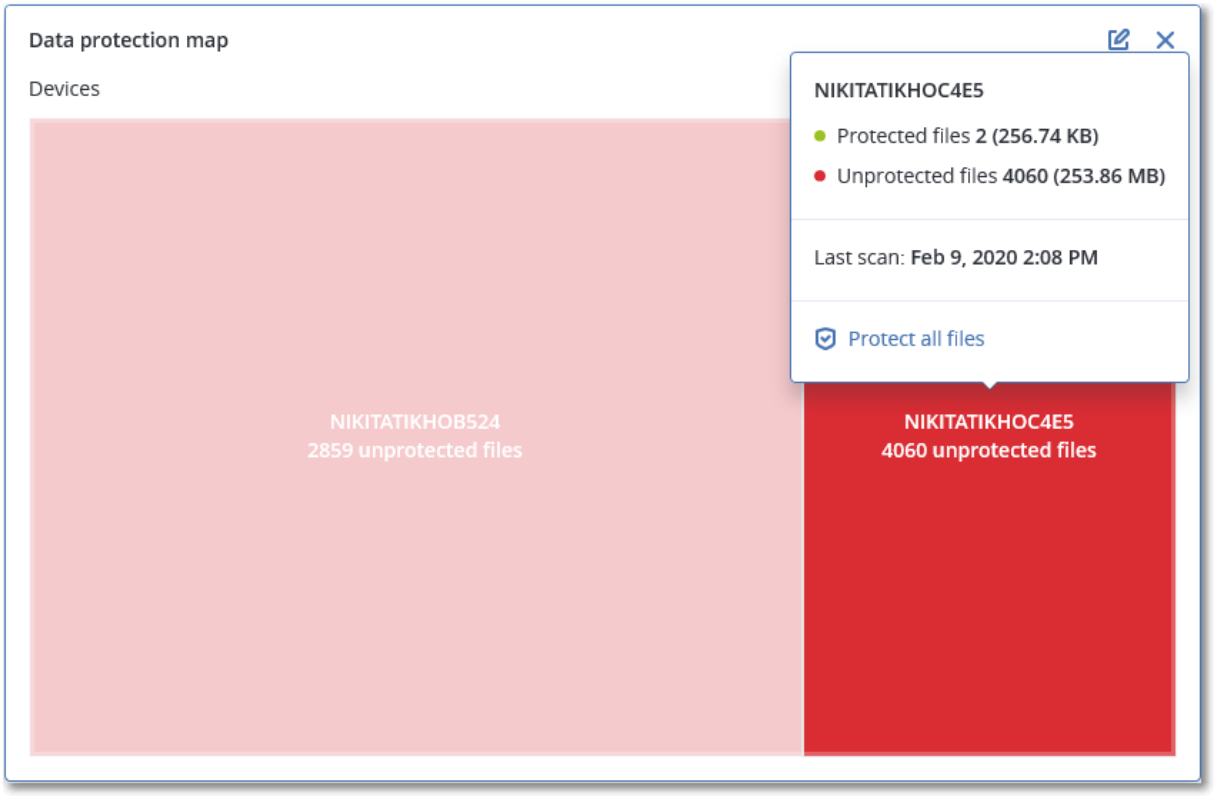
Bestanden kunnen een van de volgende beveiligingsstatussen hebben:

- **Kritiek** – er zijn 51-100% onbeschermde bestanden met de door u opgegeven extensies waarvan geen back-up wordt gemaakt met de bestaande back-upinstellingen voor de geselecteerde machine/locatie.
- **Laag** – er zijn 21-50% onbeschermde bestanden met de door u opgegeven extensies waarvan geen back-up wordt gemaakt met de bestaande back-upinstellingen voor de geselecteerde machine/locatie.

- **Medium**: er zijn 1-20% onbeschermde bestanden met de door u opgegeven extensies waarvan geen back-up wordt gemaakt met de bestaande back-upinstellingen voor de geselecteerde machine/locatie.
- **Hoog** – alle bestanden met de door u opgegeven extensies worden beschermd (er wordt een back-up van gemaakt) voor de geselecteerde machine/locatie.

De resultaten van het gegevensbeschermingsonderzoek zijn te vinden op het controledashboard in de widget Overzicht van gegevensbescherming. Deze widget bevat een structuurkaart waarin de details op machineniveau worden weergegeven:

- Machineniveau: geeft samengevatte informatie weer over de beveiligingsstatus van belangrijke bestanden per geselecteerde klant.



Als u onbeschermde bestanden wilt beschermen, wijst u het blok aan en klikt u op **Alle bestanden beschermen**. In het dialoogvenster vindt u informatie over het aantal onbeschermde bestanden en de locatie hiervan. Klik op **Alle bestanden beschermen** om ze te beschermen.

U kunt ook een gedetailleerd rapport in CSV-indeling downloaden.

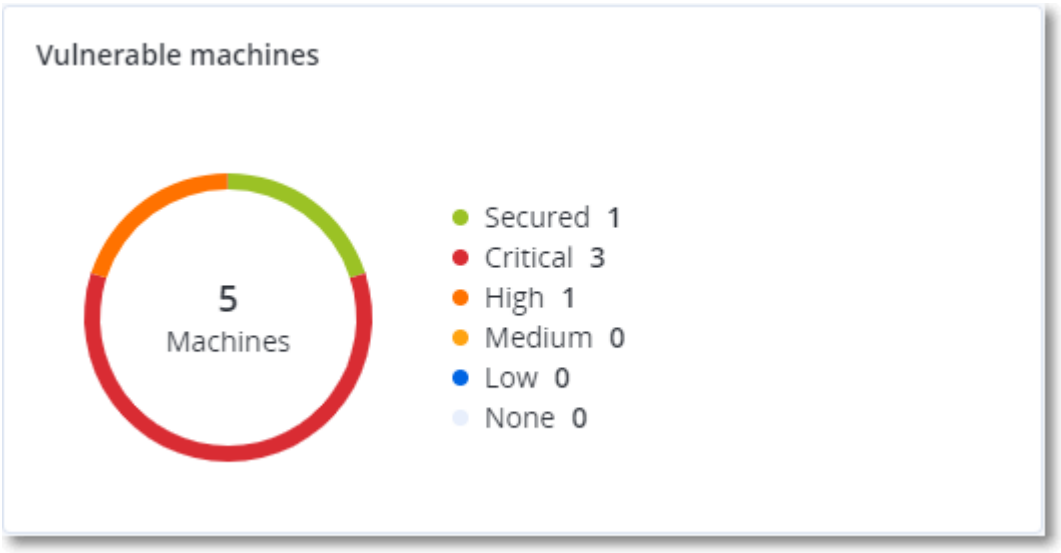
Widgets voor evaluatie van beveiligingsproblemen

Machines met beveiligingsproblemen

Deze widget geeft de machines met beveiligingsproblemen weer per ernstgraad.

Het gevonden beveiligingsprobleem kan een van de volgende ernstgraden hebben volgens het Common Vulnerability Scoring System (CVSS) v3.0:

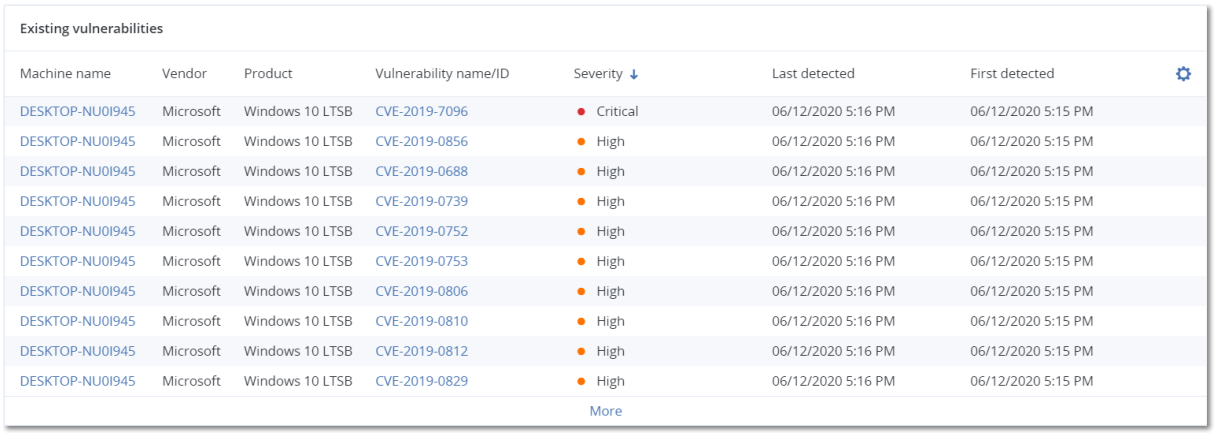
- Beveiligd: geen beveiligingsproblemen gevonden
- Kritiek: 9,0 – 10,0 CVSS
- Hoog: 7,0 – 8,9 CVSS
- Medium: 4,0 – 6,9 CVSS
- Laag: 0,1 – 3,9 CVSS
- Geen: 0,0 CVSS



Bestaande kwetsbaarheden

Deze widget geeft de momenteel bestaande beveiligingsproblemen op machines weer. De widget **Bestaande kwetsbaarheden** bevat twee kolommen met tijdstempels:

- **Eerst gedetecteerd**: datum en tijd waarop een beveiligingsprobleem voor het eerst is gedetecteerd op de machine.
- **Laatst gedetecteerd**: datum en tijd waarop een beveiligingsprobleem voor het laatst is gedetecteerd op de machine.


Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

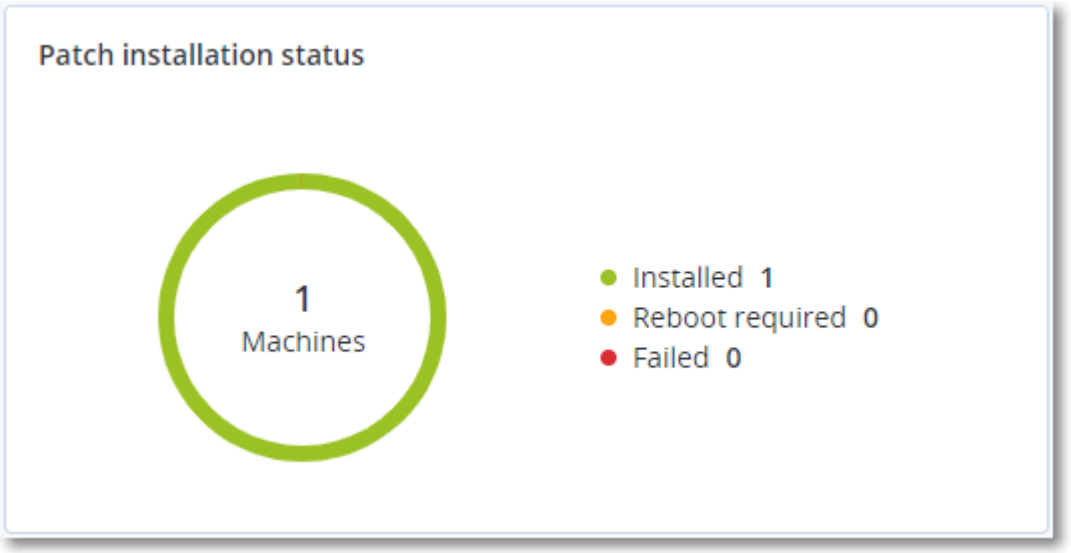
Widgets voor patchinstallatie

Er zijn vier widgets gerelateerd aan de functionaliteit voor patchbeheer.

Status van patchinstallatie

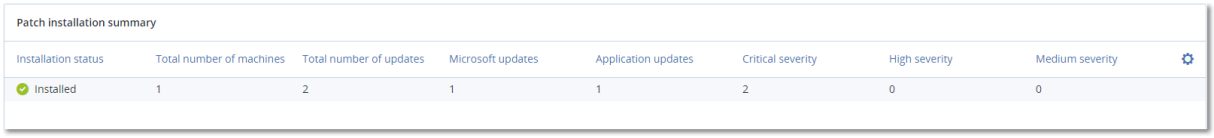
Deze widget geeft het aantal machines weer, gegroepeerd op status van de patchinstallatie.

- **Geïnstalleerd**: alle beschikbare patches zijn geïnstalleerd op een machine
- **Opnieuw opstarten vereist**: opnieuw opstarten is vereist voor een machine na de patchinstallatie
- **Mislukt**: patchinstallatie is mislukt op een machine



Overzicht van patchinstallatie

Deze widget geeft een overzicht van de patches op machines weer, gesorteerd op de status van de patchinstallatie.



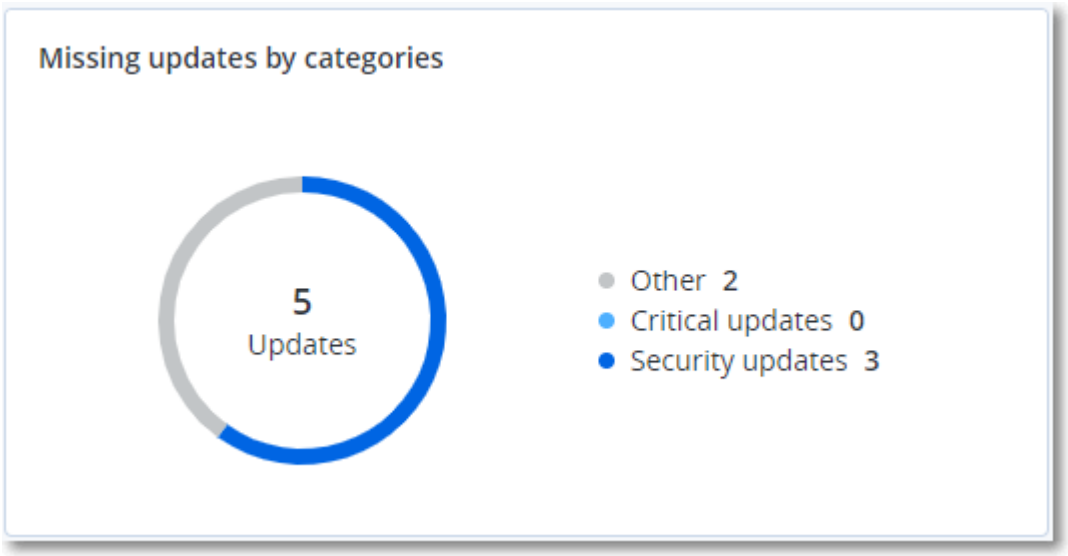
Geschiedenis van patchinstallatie

Deze widget geeft gedetailleerde informatie over patches op machines weer.

Ontbrekende updates per categorie

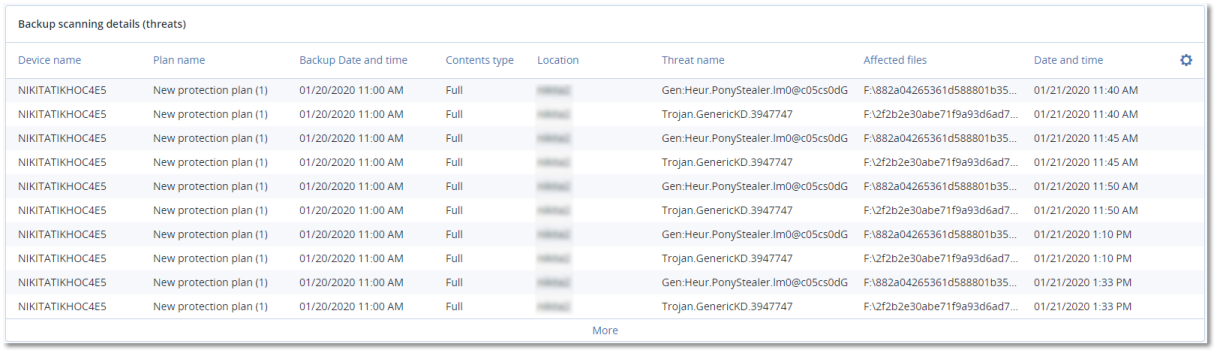
Deze widget geeft het aantal ontbrekende updates per categorie weer. De volgende categorieën worden weergegeven:

- Beveiligingsupdates
- Kritieke updates
- Anders



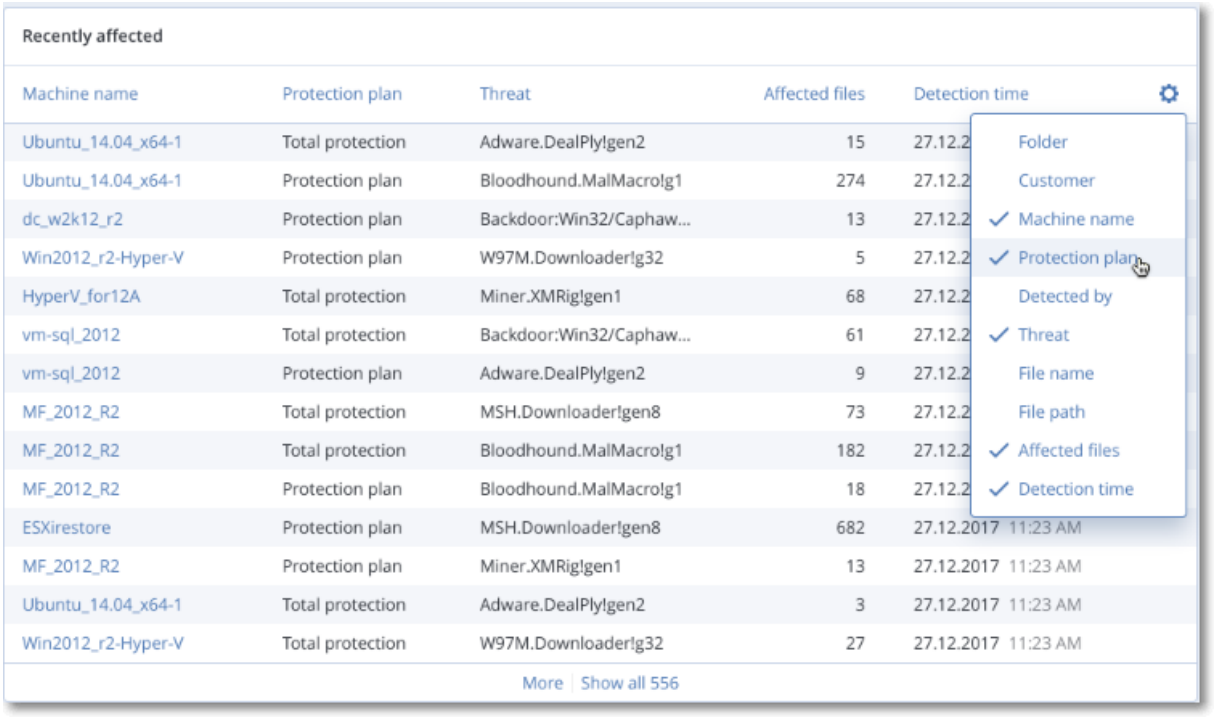
Gegevens van back-upscan

Deze widget geeft gedetailleerde informatie over de gedetecteerde bedreigingen in back-ups weer.



Onlangs beïnvloed

Deze widget toont gedetailleerde informatie over workloads die zijn beïnvloed door bedreigingen, zoals virussen, malware en ransomeware. U vindt hier informatie over de gedetecteerde bedreigingen, het tijdstip waarop de bedreigingen zijn gedetecteerd, en hoeveel bestanden zijn beïnvloed.



Gegevens voor de onlangs beïnvloede workloads downloaden

U kunt de gegevens voor de onlangs beïnvloede workloads downloaden, een CSV-bestand genereren en dit verzenden naar de ontvangers die u opgeeft.

De gegevens voor de onlangs beïnvloed workloads downloaden

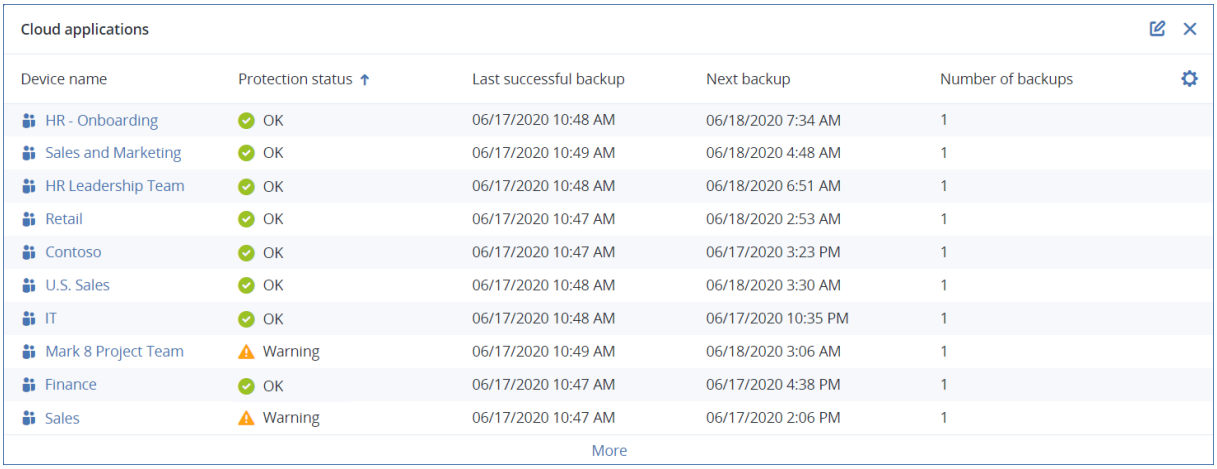
1. Klik in de widget **Onlangs beïnvloed** op **Gegevens downloaden**.
2. Geef in het veld **Periode** het aantal dagen op waarvoor u gegevens wilt downloaden. De maximale waarde die u kunt invoeren, is 200 dagen.
3. Geef in het veld **Ontvangers** de e-mailadressen op van alle personen die een e-mail zullen ontvangen met een link om het CSV-bestand te downloaden.
4. Klik op **Downloaden**.

   Het CSV-bestand met de gegevens voor de workloads die zijn beïnvloed in de opgegeven periode, wordt automatisch gegenereerd. Wanneer het CSV-bestand gereed is, krijgen de ontvangers automatisch een e-mailmelding. Vervolgens kan elke ontvanger het CSV-bestand downloaden.

Cloudtoepassingen

Deze widget geeft gedetailleerde informatie over cloud-to-cloud-resources weer:

- Microsoft 365-gebruikers (postvak, OneDrive)
- Microsoft 365-groepen (postvak, groepssite)
- Openbare Microsoft 365-mappen
- Microsoft 365-siteverzamelingen
- Microsoft 365 Teams
- Google Workspace-gebruikers (Gmail, Google Drive)
- Gedeelde Drives in Google Workspace

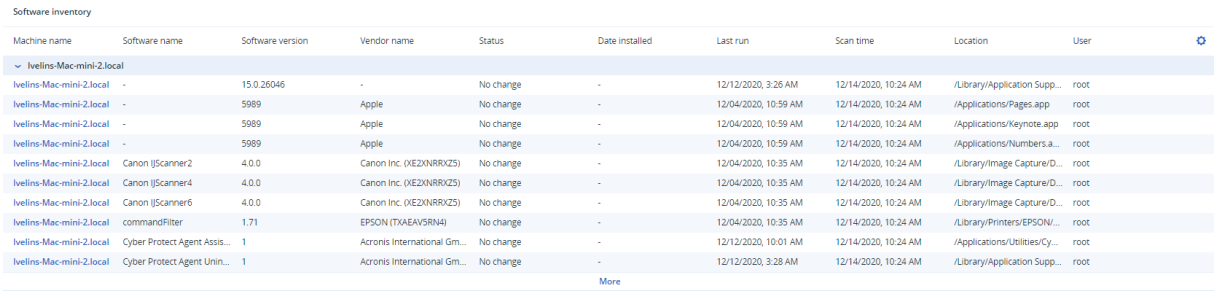


Aanvullende informatie over cloud-to-cloud-resources is ook beschikbaar in de volgende widgets:

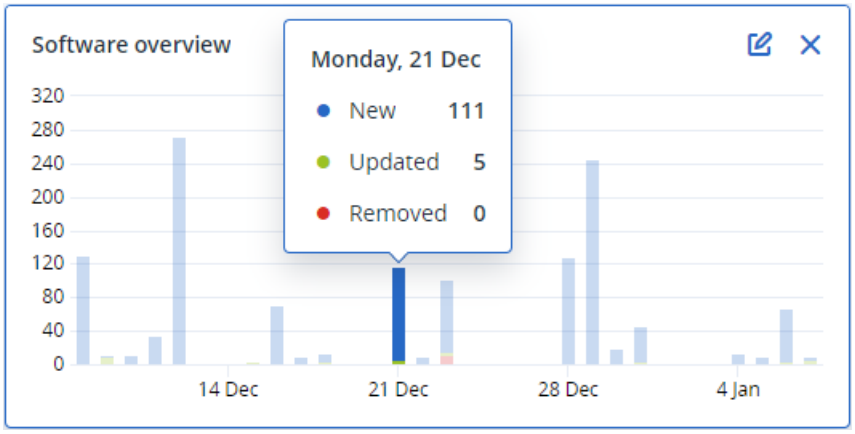
- Activiteiten
- Activiteitenlijst
- 5 meest recente waarschuwingen
- Geschiedenis van waarschuwingen
- Overzicht van waarschuwingen activeren
- Overzicht van historische waarschuwingen
- Gegevens van actieve waarschuwingen
- Locatieoverzicht

Widgets voor software-inventaris

De widget voor de tabel **Software-inventaris** geeft gedetailleerde informatie weer over alle software die is geïnstalleerd op Windows- en macOS-apparaten in uw organisatie.



De widget **Softwareoverzicht** geeft het aantal nieuwe, bijgewerkte en verwijderde toepassingen weer gedurende een bepaalde periode (7 dagen, 30 dagen of de huidige maand) op Windows- en macOS-apparaten in uw organisatie.



Wanneer u met de muis een bepaalde balk in het diagram aanwijst, wordt er knopinfo weergegeven met de volgende informatie:

Nieuw: het aantal nieuw geïnstalleerde toepassingen.

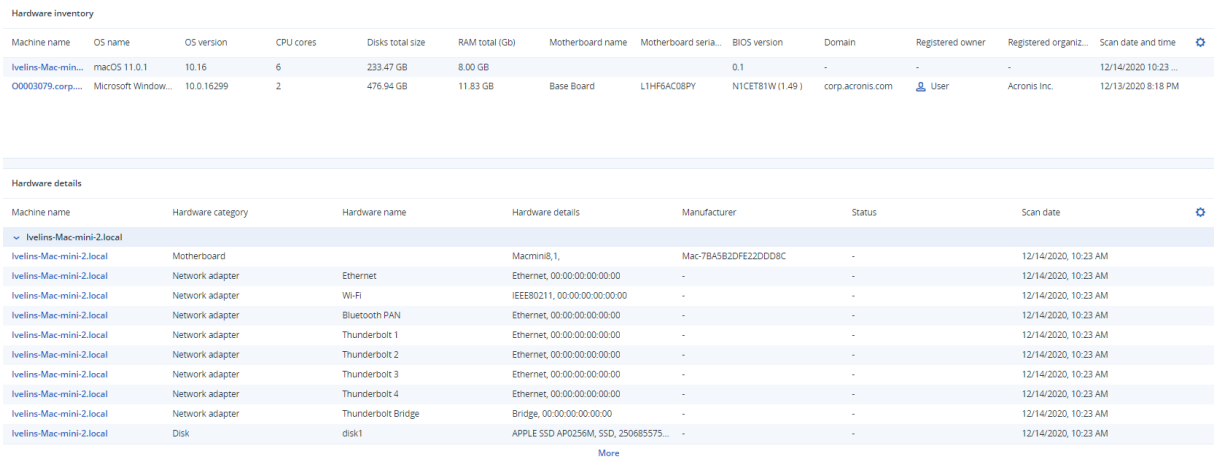
Bijgewerkt: het aantal bijgewerkte toepassingen.

Verwijderd: het aantal verwijderde toepassingen.

Wanneer u op het gedeelte van de balk klikt voor een bepaalde status, wordt u omgeleid naar de pagina **Softwarebeheer** -> **Software-inventaris**. De informatie op de pagina wordt gefilterd op de betreffende datum en status.

Widgets voor hardware-inventaris

De widgets voor de tabel **Hardware-inventaris** en **Hardwaregegevens** geven informatie weer over alle hardware die is geïnstalleerd op fysieke en virtuele Windows- en macOS-apparaten in uw organisatie.



Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-min...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp....	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1,	Mac-7BA5B2DFE22DDD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

More

De widget voor de tabel **Hardwarewijzigingen** geeft informatie weer over de hardware die gedurende een bepaalde periode (7 dagen, 30 dagen of de huidige maand) is toegevoegd, verwijderd of gewijzigd op fysieke en virtuele Windows- en macOS-apparaten in uw organisatie.

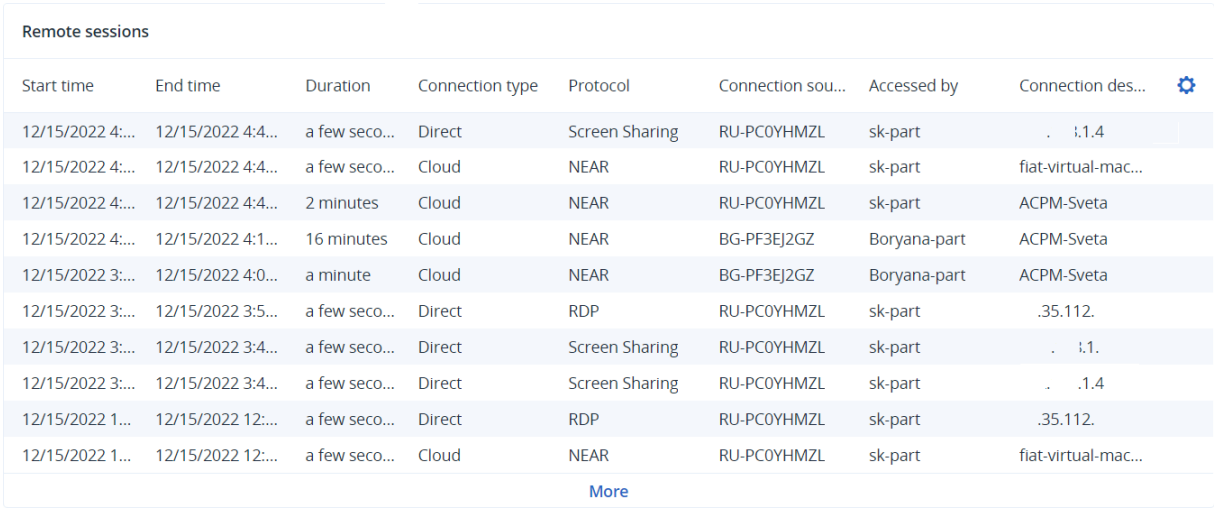
Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

Widget voor externe sessies

Deze widget geeft de gedetailleerde informatie over de sessies voor extern bureaublad en bestandsoverdracht weer.



Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

Slimme bescherming

Bedreigingsfeed

Acronis Cyber Protection Operations Center (CPOC) genereert beveiligingsmeldingen die alleen naar de gerelateerde geografische regio's worden verzonden. Deze beveiligingswaarschuwingen bieden informatie over malware, beveiligingsproblemen, natuurrampen, volksgezondheid en andere soorten wereldwijde gebeurtenissen die van invloed kunnen zijn op uw gegevensbescherming. De bedreigingsfeed informeert u over alle mogelijke bedreigingen en stelt u in staat deze te voorkomen.

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

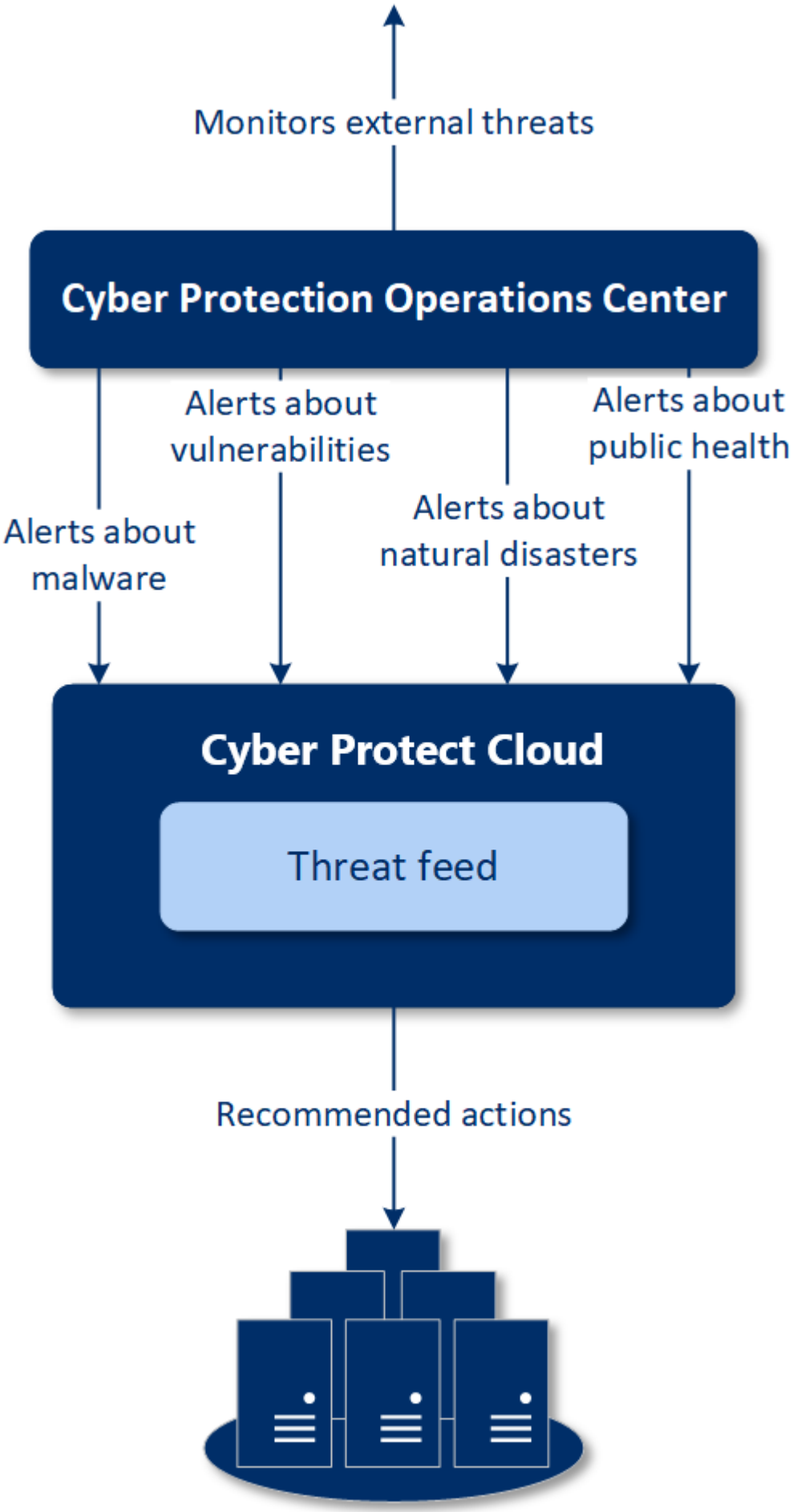
Sommige beveiligingswaarschuwingen kunnen worden opgelost met een set specifieke acties die worden opgegeven door de beveiligingsexperts. Andere beveiligingswaarschuwingen geven u alleen informatie over komende bedreigingen, maar er zijn geen aanbevolen acties beschikbaar.

Opmerking
Malwarewaarschuwingen worden alleen gegenereerd voor machines waarop de agent voor Antimalwarebeveiliging is geïnstalleerd.

Zo werkt het

Acronis Cyber Protection Operations Center bewaakt externe bedreigingen en genereert waarschuwingen over malware, beveiligingsproblemen, natuurrampen en bedreigingen voor de volksgezondheid. U kunt al deze waarschuwingen zien in de Cyber Protect-console, in het gedeelte **Bedreigingsfeed**. Afhankelijk van het type waarschuwing kunt u de betreffende aanbevolen acties uitvoeren.

De belangrijkste workflow van de bedreigingsfeed wordt weergegeven in het onderstaande diagram.



Als u de aanbevolen acties wilt starten voor ontvangen waarschuwingen van Acronis Cyber Protection Operations Center, gaat u als volgt te werk:

1. Ga in de Cyber Protect-console naar **Controle** > **Bedreigingsfeed** om te controleren of er bestaande beveiligingswaarschuwingen zijn.
2. Selecteer een waarschuwing in de lijst en bekijk de opgegeven details.
3. Klik op **Starten** om de wizard te starten.
4. Schakel de acties in die u wilt uitvoeren en de machines waarop deze acties moeten worden toegepast. De volgende acties kunnen worden voorgesteld:
   - **Evaluatie van beveiligingsproblemen**: machines scannen op beveiligingsproblemen
   - **Patchbeheer**: patches installeren op de geselecteerde machines
   - **Antimalwarebeveiliging**: volledige scan van de geselecteerde machines uitvoeren

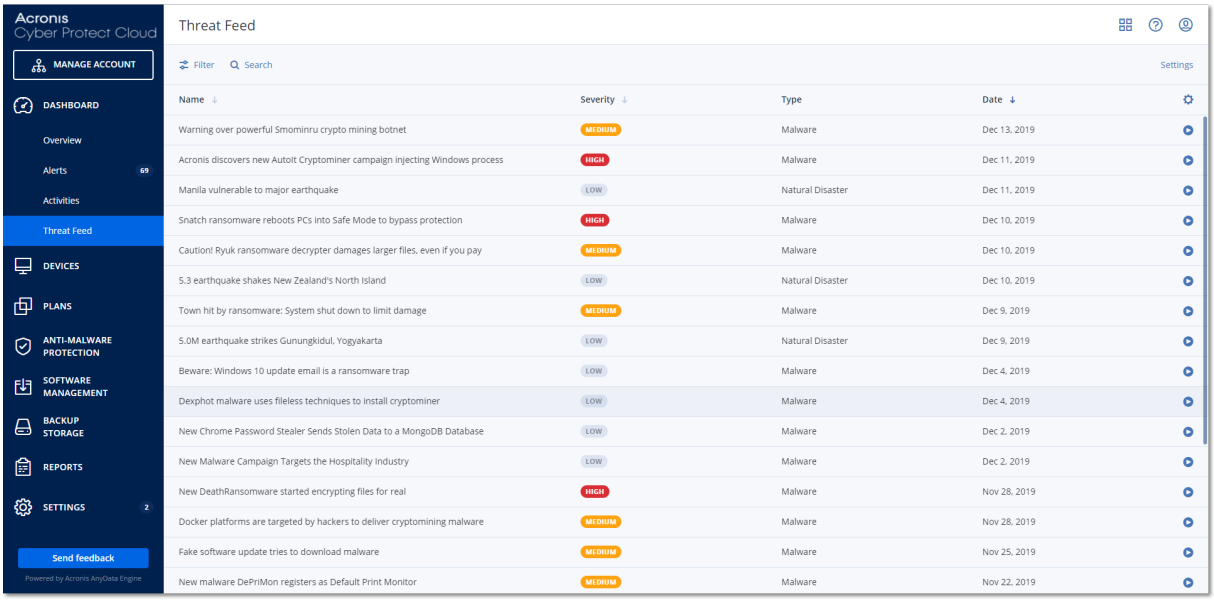
     Opmerking
     Deze actie is alleen beschikbaar voor machines waarop de agent voor antimalwarebeveiliging is geïnstalleerd.

   - **Back-up van beschermde of onbeschermde machines** – om een back-up te maken van beschermde en onbeschermde workloads.
     Als er nog geen back-ups zijn voor de workload (op alle toegankelijke locaties, zowel in de cloud als lokaal), of als de bestaande back-ups zijn versleuteld, wordt automatisch een volledige back-up gemaakt met de volgende naamnotatie:

     `%workload_name%-Remediation`

     Cyber Protect Cloud-opslag is de standaardbestemming voor de back-up, maar u kunt een andere locatie configureren voordat u de bewerking start.

     Als er al een niet-versleutelde back-up bestaat, wordt automatisch een incrementele back-up gemaakt in het bestaande archief.
5. Klik op **Starten**.
6. Controleer op de pagina **Activiteiten** of de activiteit is uitgevoerd.



Alle waarschuwingen verwijderen

Automatische opschoning van de bedreigingsfeed wordt uitgevoerd na de volgende tijdsperioden:

- Natuurramp: 1 week
- Beveiligingsprobleem: 1 maand
- Malware: 1 maand
- Volksgezondheid: 1 week

Overzicht van gegevensbescherming

Met de functie Overzicht van gegevensbescherming kunt u het volgende doen

- Gedetailleerde informatie ophalen over opgeslagen gegevens (classificatie, locaties, beveiligingsstatus en aanvullende informatie) op uw machines.
- Detecteren of gegevens beschermd zijn of niet. De gegevens worden beschouwd als beschermd als ze zijn beschermd met een back-up (een beschermingsschema waarin de back-upmodule is ingeschakeld).
- Acties uitvoeren voor gegevensbescherming.

Zo werkt het

1. Eerst maakt u een beschermingsschema terwijl de module Overzicht van gegevensbescherming is ingeschakeld.
2. Wanneer het schema is uitgevoerd en uw gegevens zijn gedetecteerd en geanalyseerd, ziet u de visuele weergave van gegevensbescherming in de widget Overzicht van gegevensbescherming.
3. U kunt ook naar **Apparaten** > **Overzicht van gegevensbescherming** gaan en daar informatie vinden over onbeschermde bestanden per apparaat.

4. U kunt acties ondernemen om de gedetecteerde onbeschermde bestanden op apparaten te beschermen.

Gedetecteerde onbeschermde bestanden beheren

Ga als volgt te werk om de belangrijke bestanden te beschermen die zijn gedetecteerd als onbeschermd:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Overzicht van gegevensbescherming**.
   In de lijst met apparaten vindt u algemene informatie over het aantal onbeschermde bestanden, de grootte van dergelijke bestanden per apparaat en de laatste gegevensdetectie.
   Als u bestanden op een bepaalde machine wilt beschermen, klikt u op het ellipspictogram en vervolgens op **Alle bestanden beschermen**. U wordt omgeleid naar de lijst met schema's waar u een beschermingsschema kunt maken terwijl de back-upmodule is ingeschakeld.
   Als u het specifieke apparaat met onbeschermde bestanden wilt verwijderen uit de lijst, klikt u op **Verbergen tot de volgende gegevensdetectie**.
2. Klik op de naam van een apparaat voor meer informatie over de onbeschermde bestanden op dat apparaat.
   U ziet het aantal onbeschermde bestanden per extensie en per locatie. Definieer in het zoekveld de extensies waarvoor u informatie over onbeschermde bestanden wilt verkrijgen.
3. Als u alle onbeschermde bestanden wilt beschermen, klikt u op **Alle bestanden beschermen**. U wordt omgeleid naar de lijst met schema's waar u een beschermingsschema kunt maken terwijl de back-upmodule is ingeschakeld.

Klik op **Gedetailleerd rapport in CSV** voor een rapport met informatie over de onbeschermde bestanden.

Instellingen voor Overzicht van gegevensbescherming

Raadpleeg 'Een beschermingsschema maken' voor meer informatie over het maken van een beschermingsschema met de module Overzicht van gegevensbescherming.

De volgende instellingen kunnen worden opgegeven voor de module Overzicht van gegevensbescherming.

Planning

U kunt verschillende instellingen definiëren om het schema te maken op basis waarvan de taak voor Overzicht van gegevensbescherming wordt uitgevoerd.

Veld	Beschrijving
De taakuitvoering plannen met de volgende gebeurtenissen	Met deze instelling definieert u wanneer de taak wordt uitgevoerd. De volgende waarden zijn beschikbaar: • **Schema op tijd**: dit is de standaardinstelling. De taak wordt uitgevoerd volgens de opgegeven tijd.

Veld	Beschrijving
	• **Wanneer de gebruiker zich aanmeldt bij het systeem**: standaard wordt de taak geactiveerd wanneer een gebruiker zich aanmeldt. U kunt deze instelling ook wijzigen, zodat alleen een specifiek gebruikersaccount de taak kan activeren. • **Wanneer de gebruiker zich afmeldt bij het systeem**: standaard wordt de taak geactiveerd wanneer een gebruiker zich afmeldt. U kunt deze instelling ook wijzigen, zodat alleen een specifiek gebruikersaccount de taak kan activeren. **Opmerking** De taak wordt niet uitgevoerd bij het afsluiten van het systeem. Afsluiten en afmelden zijn verschillende gebeurtenissen in de planningsconfiguratie. • **Wanneer het systeem wordt opgestart**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt gestart. • **Wanneer het systeem wordt afgesloten**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt afgesloten.
Type schema	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd. De volgende waarden zijn beschikbaar: • **Maandelijks**: selecteer de maanden en de weken of dagen van de maand wanneer de taak zal worden uitgevoerd. • **Dagelijks**: dit is de standaardinstelling. Selecteer de dagen van de week waarop de taak wordt uitgevoerd. • **Elk uur**: selecteer de dagen van de week, het aantal herhalingen en het tijdinterval waarin de taak wordt uitgevoerd.
Starten om	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd. Selecteer het exacte tijdstip waarop de taak wordt uitgevoerd.
Uitvoeren binnen een datumbereik	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd. Stel een bereik in waarin het geconfigureerde schema van kracht is.
Geef een gebruikersaccount op waarvoor een taak	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Wanneer de gebruiker zich aanmeldt bij het systeem** hebt geselecteerd.

Veld	Beschrijving
wordt geïnitieerd zodra het account wordt aangemeld bij het besturingssysteem	De volgende waarden zijn beschikbaar: • **Elke gebruiker**: gebruik deze optie als u wilt dat de taak wordt geactiveerd wanneer een willekeurige gebruiker zich aanmeldt. • **De volgende gebruiker**: gebruik deze optie als u wilt dat de taak alleen wordt geactiveerd wanneer een specifiek gebruikersaccount zich aanmeldt.
Geef een gebruikersaccount op waarvoor een taak wordt geïnitieerd zodra het account wordt afgemeld bij het besturingssysteem	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Wanneer de gebruiker zich afmeldt bij het systeem** hebt geselecteerd. De volgende waarden zijn beschikbaar: • **Elke gebruiker**: gebruik deze optie als u wilt dat de taak wordt geactiveerd wanneer een willekeurige gebruiker zich afmeldt. • **De volgende gebruiker**: gebruik deze optie als u wilt dat de taak alleen wordt geactiveerd wanneer een specifiek gebruikersaccount zich afmeldt.
Startvoorwaarden	Hiermee definieert u alle voorwaarden waaraan tegelijkertijd moet worden voldaan om de taak uit te voeren. De startvoorwaarden voor antimalwarescans zijn vergelijkbaar met de startvoorwaarden voor de **module Back-up** die worden beschreven in 'Startvoorwaarden'. U kunt de volgende aanvullende startvoorwaarden definiëren: • **Starttijd van taak binnen een tijdvenster distribueren**: met deze optie kunt u het tijdsbestek instellen voor de taak om knelpunten in het netwerk te voorkomen. U kunt de vertraging opgeven in uren of minuten. Als de standaardstarttijd bijvoorbeeld 10:00 uur en de vertraging 60 minuten is, dan zal de taak beginnen tussen 10:00 uur en 11:00 uur. • **Als de machine is uitgeschakeld, gemiste taken uitvoeren wanneer de machine wordt opgestart** • **De slaap- of sluimerstand voorkomen tijdens het uitvoeren van taken**: deze optie is alleen van toepassing op machines met Windows. • **Voer de taak na de start uit, zelfs als niet aan de startvoorwaarden wordt voldaan**: geef aan na hoeveel tijd de taak wordt uitgevoerd, ongeacht de andere startvoorwaarden. **Opmerking** Startvoorwaarden worden niet ondersteund voor Linux.

Extensies en uitzonderingsregels

Op het tabblad **Extensies** kunt u de lijst met bestandsextensies definiëren die als belangrijk worden beschouwd tijdens gegevensdetectie en waarvan de bescherming wordt gecontroleerd. Gebruik de volgende indeling voor het definiëren van extensies:

```
.html, .7z, .docx, .zip, .pptx, .xml
```

Op het tabblad **Uitzonderingsregels** kunt u bepalen van welke bestanden en mappen de beveiligingsstatus niet wordt gecontroleerd tijdens gegevensdetectie.

- **Verborgen bestanden en mappen**: indien geselecteerd, worden verborgen bestanden en mappen overgeslagen tijdens gegevensonderzoek.
- **Systeembestanden en mappen**: indien geselecteerd, worden systeembestanden en -mappen overgeslagen tijdens gegevensonderzoek.

Het tabblad Activiteiten

Het tabblad **Activiteiten** biedt een overzicht van activiteiten van de afgelopen 90 dagen.

Activiteiten op het dashboard filteren:

1. Geef in het veld **Apparaatnaam** de machine op waarop de activiteit wordt uitgevoerd.
2. Ga naar de vervolgkeuzelijst **Status** en selecteer de status. Bijvoorbeeld voltooid, mislukt, wordt uitgevoerd, geannuleerd.
3. Ga naar de vervolgkeuzelijst **Acties op afstand** en selecteer de actie. Bijvoorbeeld schema toepassen, back-ups verwijderen, software-updates installeren.
4. Stel in het veld **Nieuwste** de periode voor de activiteiten in. Bijvoorbeeld: de meest recente activiteiten, de activiteiten van de afgelopen 24 uur, of de activiteiten gedurende een bepaalde periode binnen de afgelopen 90 dagen.
5. Als u het tabblad **Activiteiten** opent als partnerbeheerder, kunt u de activiteiten filteren voor een specifieke klant die u beheert.

Als u de weergave van het tabblad **Activiteiten** wilt aanpassen, klikt u op het tandwielpictogram en selecteert u de kolommen die u wilt zien. Als u de voortgang van de activiteit in real time wilt zien, schakelt u het selectievakje **Automatisch vernieuwen** in.

Als u een huidige activiteit wilt annuleren, klikt u op de naam en vervolgens in het scherm **Details** op **Annuleren**.

U kunt de vermelde activiteiten zoeken met de volgende criteria:

- Apparaatnaam
  Dit is de machine waarop de activiteit wordt uitgevoerd.
- Gestart door
  Dit is het account waarmee de activiteit is gestart.

Activiteiten van het externe bureaublad kunnen worden gefilterd op de volgende eigenschappen:

- Schema maken
- Schema toepassen
- Schema intrekken
- Schema verwijderen
- Externe verbinding
  - Verbinding met extern bureaublad in de cloud via RDP
  - Verbinding met extern bureaublad in de cloud via NEAR
  - Verbinding met extern bureaublad in de cloud via Apple Schermdeling
  - Verbinding met extern bureaublad via webclient
  - Verbinding met extern bureaublad via Quick Assist
  - Directe verbinding met extern bureaublad via RDP
  - Directe verbinding met extern bureaublad via Apple Schermdeling
  - Bestandsoverdracht
  - Bestandsoverdracht via Quick Assist
- Actie op afstand
  - Een workload afsluiten...
  - Een workload opnieuw opstarten...
  - Externe gebruiker afmelden bij de workload...
  - Prullenbak leegmaken voor gebruiker van de workload...
  - Een workload in de slaapstand zetten...

Cyber Protect Monitor

Cyber Protect Monitor toont informatie over de beschermingsstatus van de machine waarop Agent voor Windows of Agent voor Mac is geïnstalleerd en stelt gebruikers in staat om de instellingen voor back-upversleuteling en de proxyserver te configureren.

Wanneer Agent voor File Sync & Share is geïnstalleerd op de machine, biedt Cyber Protect Monitor toegang tot de File Sync & Share-service. De File Sync & Share-functionaliteit is toegankelijk na een verplichte onboarding waarbij de gebruikers zich aanmelden op hun eigen File Sync & Share-account en een persoonlijke synchronisatiemap selecteren. Voor meer informatie over Agent voor File Sync & Share raadpleegt u de Cyber Files Cloud gebruikersgids.

Belangrijk
Cyber Protect Monitor is toegankelijk voor gebruikers die mogelijk geen beheerdersrechten hebben voor de Cyber Protection- of de File Sync & Share-service.

De onderstaande tabel bevat een samenvatting van de bewerkingen die beschikbaar zijn voor gebruikers zonder beheerdersrechten.

Geïnstalleerde agenten	Gebruikers kunnen	Gebruikers kunnen niet
Agent voor Windows of Agent voor Mac	• Het standaardbeschermingsplan toepassen op hun machines • De beschermingsstatus van hun machines controleren • Active Protection-meldingen ontvangen • De back-ups van hun machines tijdelijk onderbreken • De proxyserver-instellingen configureren • De instellingen voor back-upversleuteling wijzigen **Waarschuwing!** Als u de versleutelingsinstellingen in Cyber Protect Monitor wijzigt, overschrijft u de instellingen in het beschermingsplan en dit heeft gevolgen voor alle back-ups van de machine. Sommige beschermingsplannen kunnen mislukken door deze bewerking. Zie "Versleuteling" (p. 469) voor meer informatie. Er is geen manier om versleutelde back-ups te herstellen als u het wachtwoord verliest of vergeet.	• Aangepaste beschermingsplannen toepassen • Beschermingsplannen beheren die al zijn toegepast
Agent voor Windows en Agent voor Sync & Share Agent voor Mac en Agent voor Sync & Share	• Inhoud synchroniseren tussen hun lokale synchronisatiemap en hun File Sync & Share-account • De synchronisatiebewerkingen onderbreken • De synchronisatiemap wijzigen • De bestandstypen controleren die niet kunnen worden gesynchroniseerd	• De bestandstypen bewerken die niet kunnen worden gesynchroniseerd

Proxyserverinstellingen configureren in Cyber Protect Monitor

U kunt de proxyserverinstellingen configureren in Cyber Protect Monitor. De configuratie heeft gevolgen voor alle agents die op dezelfde machine zijn geïnstalleerd.

De proxyserverinstellingen configureren

1. Open Cyber Protect Monitor en klik vervolgens op het tandwielpictogram in de rechterbovenhoek.
2. Klik op **Instellingen** en vervolgens op **Proxy**.
3. Schakel de schakelaar **Een proxyserver gebruiken** in en geef vervolgens het adres en de poort van de proxyserver op.
4. [Als de toegang tot de proxyserver met een wachtwoord is beveiligd] Schakel de schakelaar **Wachtwoord vereist** in en geef vervolgens de gebruikersnaam en het wachtwoord op voor toegang tot de proxyserver.
5. Klik op **Opslaan**.
   De proxyserverinstellingen worden opgeslagen in het bestand `http-proxy.yaml`.

Rapporten

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Een rapport over bewerkingen kan elke set dashboard-widgets bevatten. Alle widgets tonen samenvattende informatie voor het hele bedrijf.

Afhankelijk van het widgettype bevat het rapport gegevens voor een tijdbereik of voor het moment van browsen of het genereren van rapporten. Zie "Gerapporteerde gegevens per type widget" (p. 304).

Alle historische widgets tonen gegevens voor hetzelfde tijdbereik. U kunt dit bereik wijzigen in de rapportinstellingen.

U kunt standaardrapporten gebruiken of een aangepast rapport maken.

U kunt een rapport downloaden of per e-mail verzenden in XLSX- (Excel) of PDF-indeling.

De set standaardrapporten hangt af van de Cyber Protection-service-editie die u gebruikt. De standaardrapporten worden hieronder weergegeven:

Naam van rapport	Beschrijving
#CyberFit-score per machine	Geeft de #CyberFit-score weer, gebaseerd op de evaluatie van de beveiligingsmetrieken en -configuraties voor elke machine, en geeft aanbevelingen voor verbeteringen.
Waarschuwingen	Geeft de waarschuwingen weer die zijn gegenereerd tijdens een bepaalde periode.
Gegevens van back-upscan	Geeft gedetailleerde informatie weer over gedetecteerde bedreigingen in de back-ups.
Dagelijkse activiteiten	Geeft de overzichtsinformatie weer over activiteiten die zijn uitgevoerd tijdens een bepaalde periode.

Overzicht van gegevensbescherming	Geeft gedetailleerde informatie weer over het aantal, de grootte, de locatie en de beveiligingsstatus van alle belangrijke bestanden op machines.
Gedetecteerde bedreigingen	Geeft details weer over de betroffen machines en het aantal geblokkeerde bedreigingen, en over de machines die in orde zijn en de machines met beveiligingsproblemen.
Gedetecteerde machines	Geeft alle gevonden machines in het organisatienetwerk weer.
Voorspelling van schijfintegriteit	Geeft voorspellingen weer over wanneer uw HDD/SSD zal uitvallen en de huidige schijfstatus.
Bestaande kwetsbaarheden	Geeft de bestaande beveiligingsproblemen voor het besturingssysteem en de toepassingen in uw organisatie weer. Het rapport geeft ook de details van de betroffen machines in uw netwerk weer voor elk product dat wordt vermeld.
Software-inventaris	Geeft informatie weer over de software die is geïnstalleerd op de apparaten van uw bedrijf.
Hardware-inventaris	Geeft informatie weer over de hardware die beschikbaar is op de apparaten van uw bedrijf.
Overzicht van patchbeheer	Geeft het aantal ontbrekende patches, geïnstalleerde patches en toepasselijke patches weer. U kunt de rapporten analyseren om de gegevens over ontbrekende/geïnstalleerde patches en de details van alle systemen te krijgen.
Overzicht	Geeft de overzichtsinformatie over de beschermde apparaten tijdens een bepaalde periode weer.
Wekelijkse activiteiten	Geeft de overzichtsinformatie weer over activiteiten die zijn uitgevoerd tijdens een bepaalde periode.
Externe sessies	Geeft informatie weer over de sessies voor extern bureaublad en bestandsoverdracht.

Acties met rapporten

Als u een rapport wilt bekijken, klikt u op de naam ervan.

Een nieuw rapport toevoegen:

1. Ga in de Cyber Protect-console naar **Rapporten**.
2. Klik onder de lijst met beschikbare rapporten op **Rapport toevoegen**.
3. [Een vooraf gedefinieerd rapport toevoegen] Klik op de naam van het vooraf gedefinieerde rapport.
4. [Een aangepast rapport toevoegen] Klik op **Aangepast** en voeg vervolgens widgets toe aan het rapport.
5. [Optioneel] Versleep de widgets om ze opnieuw te rangschikken.

Een rapport bewerken

1. Ga in de Cyber Protect-console naar **Rapporten**.
2. Ga naar de lijst met rapporten en selecteer het rapport dat u wilt bewerken.
   U kunt het volgende doen:
   - De naam van het rapport wijzigen.
   - Het tijdbereik voor alle widgets in het rapport wijzigen.
   - De ontvangers van het rapport opgeven, samen met de tijd waarop het rapport naar hen wordt verzonden. De beschikbare indelingen zijn PDF en XLSX.

Een rapport verwijderen:

1. Ga in de Cyber Protect-console naar **Rapporten**.
2. Ga naar de lijst met rapporten en selecteer het rapport dat u wilt verwijderen.
3. Klik op het ellipspictogram (...) en klik vervolgens op **Verwijderen**.
4. Bevestig uw keuze door te klikken op **Verwijderen**.

Een rapport plannen

1. Ga in de Cyber Protect-console naar **Rapporten**.
2. Ga naar de lijst met rapporten en selecteer het rapport dat u wilt plannen. Klik vervolgens op **Instellingen**.
3. Schakel de switch **Gepland** in.
   - Geef de e-mailadressen van de ontvangers op.
   - Selecteer de indeling van het rapport.

     Opmerking
     U kunt maximaal 1000 items exporteren in een PDF-bestand en 10.000 in een XLSX-bestand. De lokale tijd van uw machine wordt gebruikt voor de tijdstempels in de PDF- en XLSX-bestanden.

   - Selecteer de taal van het rapport.
   - Configureer het schema.
4. Klik op **Opslaan**.

Een rapport downloaden:

1. Ga in de Cyber Protect-console naar **Rapporten**.
2. Ga naar de lijst met rapporten, selecteer het rapport en klik vervolgens op **Downloaden**.
3. Selecteer de indeling van het rapport.

Een rapport verzenden:

1. Ga in de Cyber Protect-console naar **Rapporten**.
2. Ga naar de lijst met rapporten, selecteer het rapport en klik vervolgens op **Verzenden**.

3. Geef de e-mailadressen van de ontvangers op.
4. Selecteer de indeling van het rapport.
5. Klik op **Verzenden**.

De rapportstructuur exporteren:

1. Ga in de Cyber Protect-console naar **Rapporten**.
2. Ga naar de lijst met rapporten en selecteer het rapport.
3. Klik op het ellipspictogram (...) en klik vervolgens op **Exporteren**.

Hierdoor wordt de rapportstructuur op uw machine opgeslagen als JSON-bestand.

Een dump maken van de rapportgegevens

Met deze optie kunt u alle gegevens voor een aangepaste periode, zonder deze te filteren, exporteren naar een CSV-bestand en het CSV-bestand per e-mail verzenden naar een ontvanger.

Opmerking
U kunt maximaal 150.000 items exporteren in een CSV-bestand. De Coordinated Universal Time (UTC) wordt gebruikt voor de tijdstempels in het CSV-bestand.

1. Ga in de Cyber Protect-console naar **Rapporten**.
2. Ga naar de lijst met rapporten en selecteer het rapport waarvan u een dump wilt maken.
3. Klik op het ellipspictogram (...) en klik vervolgens op **Dumpgegevens**.
4. Geef de e-mailadressen van de ontvangers op.
5. Ga naar **Tijdbereik** en geef de aangepaste periode op waarvoor u een gegevensdump wilt maken.

   Opmerking
   De voorbereiding van CSV-bestanden voor langere perioden kost meer tijd.

6. Klik op **Verzenden**.

Gerapporteerde gegevens per type widget

Er zijn twee typen widgets op het dashboard, afhankelijk van het gegevensbereik dat ze weergeven:

- Widgets die actuele gegevens weergeven op het moment van browsen of het genereren van rapporten.
- Widgets die historische gegevens weergeven.

Wanneer u een datumbereik in de rapportinstellingen configureert om gegevens voor een bepaalde periode te dumpen, is het geselecteerde tijdbereik alleen van toepassing op widgets die historische gegevens weergeven. Voor widgets die actuele gegevens weergeven op het moment van browsen, is de parameter tijdbereik niet van toepassing.

In de volgende tabel worden de beschikbare widgets weergegeven, met de respectievelijke gegevensbereiken.

Naam van widget	Gegevens weergegeven in widget en rapporten
#CyberFit-score per machine	Actueel
5 meest recente waarschuwingen	Actueel
Gegevens van actieve waarschuwingen	Actueel
Overzicht van waarschuwingen activeren	Actueel
Activiteiten	Historisch
Activiteitenlijst	Historisch
Geschiedenis van waarschuwingen	Historisch
Statistieken van aanvalstactieken	Historisch
Back-upscangegevens (bedreigingen)	Historisch
Back-upstatus	Historisch: in de kolommen **Totaal aantal uitgevoerde bewerkingen** en **Aantal voltooide bewerkingen** Actueel: in alle andere kolommen
Geblokkeerde URL's	Actueel
Cloudtoepassingen	Actueel
Cyber protection	Actueel
Overzicht van gegevensbescherming	Historisch
Apparaten	Actueel
Gedetecteerde machines	Actueel
Overzicht van schijfintegriteit	Actueel
Status van schijfintegriteit per fysiek apparaat	Actueel
Bestaande kwetsbaarheden	Historisch
Hardwarewijzigingen	Historisch
Hardwaredetails	Actueel

Hardware-inventaris	Actueel
Overzicht van historische waarschuwingen	Historisch
Geschiedenis van de ernst van incidenten	Historisch
Locatieoverzicht	Actueel
Ontbrekende updates per categorie	Actueel
Niet beschermd	Actueel
Geschiedenis van patchinstallatie	Historisch
Status van patchinstallatie	Historisch
Overzicht van patchinstallatie	Historisch
Beveiligingsstatus	Actueel
Onlangs beïnvloed	Historisch
Externe sessies	Historisch
Burndown van beveiligingsincidenten	Historisch
Gemiddelde reparatietijd voor beveiligingsincidenten	Historisch
Software-inventaris	Actueel
Softwareoverzicht	Historisch
Bedreigingsstatus	Actueel
Machines met beveiligingsproblemen	Actueel
Netwerkstatus van workloads	Actueel

Workloads beheren in de Cyber Protect-console

In dit gedeelte wordt beschreven hoe u uw workloads kunt beheren in de Cyber Protect-console.

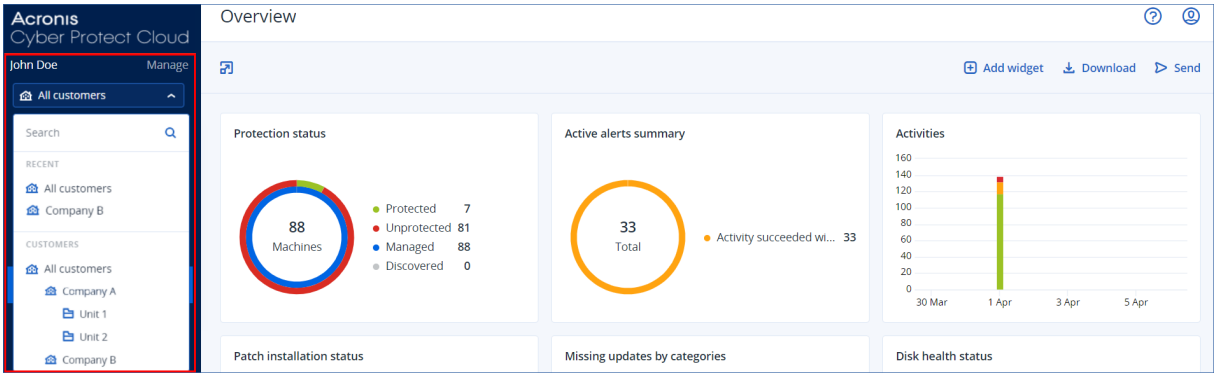
De Cyber Protect-console

In de Cyber Protect-console kunt u workloads en schema's beheren, de beveiligingsinstellingen wijzigen, rapporten configureren en de back-upopslag controleren.

Via de Cyber Protect-console hebt u ook toegang tot extra services en functies, zoals File Sync & Share, Antivirus- en antimalwarebeveiliging, Patchbeheer, Apparaatbeheer en Evaluatie van beveiligingsproblemen. Het type service en het aantal services kunnen variëren, afhankelijk van uw Cyber Protection-licentie.

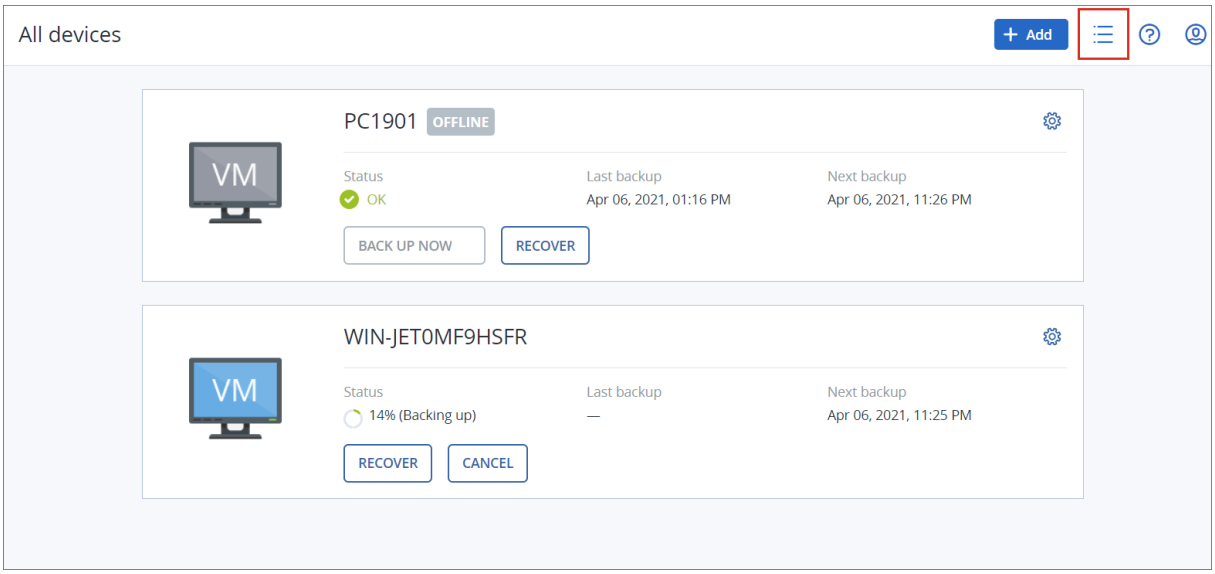
Ga naar **Controle** > **Overzicht** om het dashboard met de belangrijkste informatie over uw bescherming te bekijken.

Afhankelijk van uw toegangsmachtigingen kunt u de bescherming beheren voor één of meerdere klanttenants of eenheden in een tenant. Gebruik de vervolgkeuzelijst in het navigatiemenu om het hiërarchieniveau te wijzigen. Alleen de niveaus waartoe u toegang hebt, worden weergegeven. Klik op **Beheren** om naar de beheerportal te gaan.

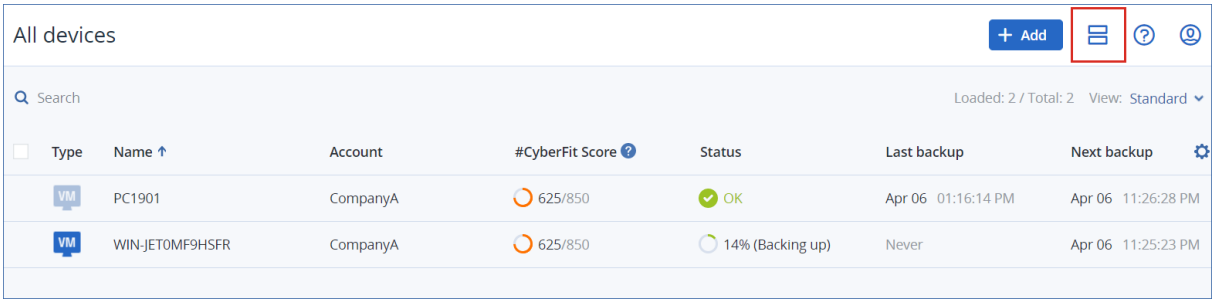


Het gedeelte **Apparaten** is beschikbaar in eenvoudige en tabelweergave. U kunt tussen de weergaven schakelen door te klikken op het betreffende pictogram in de rechterbovenhoek.

In de eenvoudige weergave ziet u slechts enkele workloads.



De tabelweergave wordt automatisch ingeschakeld wanneer er meer workloads bijkomen.



Beide weergaven bieden toegang tot dezelfde functies en bewerkingen. In dit document wordt beschreven hoe u de bewerkingen uitvoert vanuit de tabelweergave.

Wanneer een workload online of offline gaat, duurt het even voordat de status wordt gewijzigd in de Cyber Protect-console. De status van de workload wordt elke minuut gecontroleerd. Als de agent die op de betreffende machine is geïnstalleerd, geen gegevens overdraagt en er geen antwoord is na vijf opeenvolgende controles, wordt de workload weergegeven als offline. De machine wordt weer weergegeven als online wanneer deze reageert op een statuscontrole of begint gegevens over te dragen.

Wat is er nieuw in de Cyber Protect-console

Wanneer nieuwe functies van Cyber Protect Cloud beschikbaar zijn, ziet u een pop-upvenster met een korte beschrijving van deze functies wanneer u zich aanmeldt bij de Cyber Protect-console.

U kunt de beschrijving van de nieuwe functies ook bekijken door te klikken op de link **Wat is er nieuw** in de linkeronderhoek van het hoofdvenster van de Cyber Protect-console.

Als er geen nieuwe functies zijn, wordt de link **Wat is er nieuw** niet weergegeven.

De Cyber Protect-console gebruiken als partnerbeheerder

Als partnerbeheerder kunt u de Cyber Protect-console gebruiken op partnertenantniveau (**Alle klanten**) of op klanttenantniveau.

Partnertenantniveau (**Alle klanten**)

Op partnertenantniveau (**Alle klanten**) kunt u de volgende acties uitvoeren:

- Scripting-plannen beheren voor workloads van al uw beheerde klanttenants.
  U kunt hetzelfde scripting-plan toepassen op workloads van verschillende klanten en apparaatgroepen maken met workloads van verschillende klanten. Als u wilt weten hoe u een statische of een dynamische apparaatgroep op partnerniveau maakt, raadpleegt u "Een statische apparaatgroep maken op partnerniveau" (p. 312) en "Een dynamische apparaatgroep maken op partnerniveau" (p. 312). Voor meer informatie over de scripts en scripting-plannen: zie "Cyber Scripting" (p. 396).
- Maak monitoringplannen voor wokloads van al uw beheerde klanttenants.
- Maak plannen voor extern beheer van workloads van al uw beheerde klanttenants.
- Bekijk en beheer Eindpuntdetectie en -respons (EDR)-incidenten voor alle klanttenants in één interface voor incidentenbeheer, in plaats van dat u het incidentenscherm van elke afzonderlijke klant hoeft te openen.
- Voer automatische detectie uit van machines voor al uw beheerde klanttenants.

Klanttenantniveau

Op dit niveau hebt u dezelfde rechten als de bedrijfbeheerder namens wie u optreedt.

Een tenantniveau selecteren

U kunt het tenantniveau selecteren waarop u wilt werken in de Cyber Protect-console.

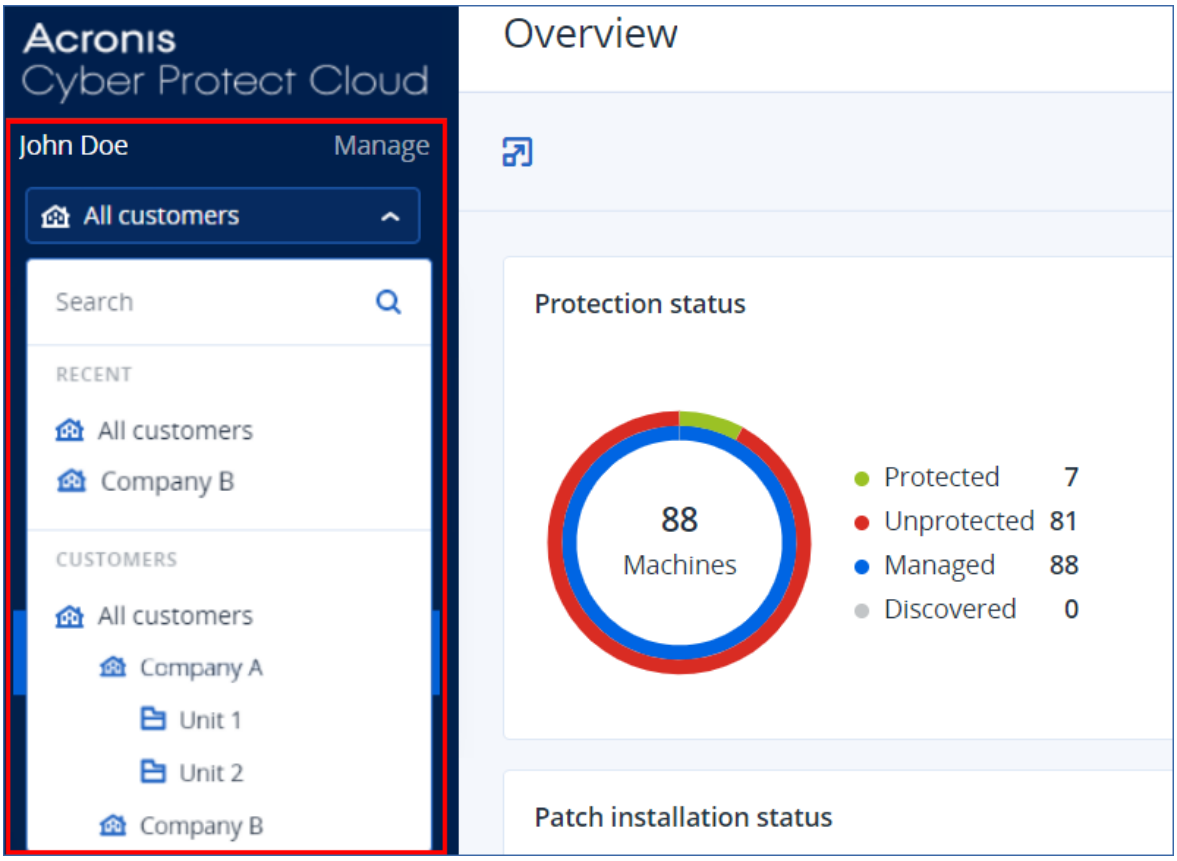
Vereisten

- U hebt toegangsrechten tot zowel de Cyber Protect-console als de beheerportal.
- U kunt meer dan één tenant of eenheid beheren.

Een tenantniveau selecteren in de Cyber Protect-console

1. Ga naar het navigatiemenu aan de linkerkant en klik op de pijl naast de naam van de klantentenant.
2. Selecteer een van de volgende opties:
   - Als u op partnerniveau wilt werken, selecteert u **Alle klanten**.

- Als u op klant- of eenheidniveau wilt werken, selecteert u de naam van die klant of eenheid.



Partnertenantniveau in de Cyber Protect-console

Wanneer u de Cyber Protect-console gebruikt op het partnertenantniveau (**Alle klanten**), is er een aangepaste weergave beschikbaar.

De tabbladen **Waarschuwingen** en **Activiteiten** bieden extra filters voor partners. De tabbladen **Apparaten** en **Beheer** bieden alleen toegang tot de functies of objecten die toegankelijk zijn voor partnerbeheerders.

Tabblad Waarschuwingen

Hier kunt U de waarschuwingen van al uw beheerde klanten zien, en u kunt ze zoeken en filteren volgens de volgende criteria:

- Apparaat
- Klant
- Schema

U kunt meerdere items selecteren voor elk van deze criteria.

Tabblad Activiteiten

Hier kunt u de activiteiten zien van alle tenants die u beheert of de activiteiten in een specifieke klanttenant.

U kunt de activiteiten filteren op klant, status, tijd en type.

De volgende typen activiteiten worden op dit niveau automatisch vooraf geselecteerd:

- Schema toepassen
- Beschermingsschema maken
- Beschermingsschema
- Schema intrekken
- Scripting

Tabblad Apparaten

Op het tabblad **Machines met agents** ziet u alle workloads van de door u beheerde klanttenants en kunt u workloads van een of meerdere tenants selecteren. U kunt ook apparaatgroepen maken die workloads van verschillende klanten bevatten.

Belangrijk
Wanneer u werkt op het partnerniveau (**Alle klanten**), kunt u een beperkt aantal bewerkingen uitvoeren met apparaten. U kunt bijvoorbeeld geen van de volgende bewerkingen uitvoeren:

- Bestaande beschermingsplannen bekijken en beheren op klantapparaten.
- Nieuwe beschermingsplannen maken.
- Back-ups herstellen.
- Disaster Recovery gebruiken.
- Toegang tot de Cyber Protection Desktop-functies.

Als u een van deze bewerkingen wilt uitvoeren, moet u werken op klantniveau.

Tabblad Softwarebeheer

Als software-inventarisscan is ingeschakeld voor workloads van klanten, kunnent u de resultaten van de softwarescans zien.

Workloads van specifieke klanten bekijken

Als partnerbeheerder kunt u de workloads bekijken van de klanttenants die u beheert.

De workloads van een specifieke klant bekijken

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik in de boomstructuur op **Machines met agents** om de lijst uit te vouwen.

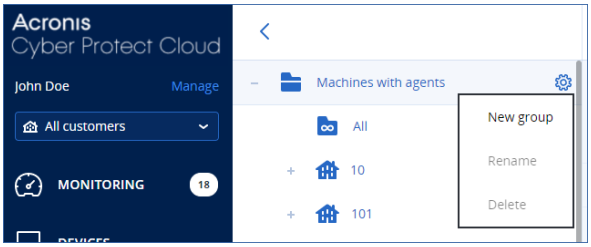
3. Klik op de naam van de klant van wie u de workloads wilt bekijken en beheren.

Een statische apparaatgroep maken op partnerniveau

U kunt statische apparaatgroepen maken op partnerniveau (**Alle apparaten**).

Een statische apparaatgroep maken op partnerniveau

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik op het tandwielpictogram naast **Machines met agents** en klik vervolgens op **Nieuwe groep**.



3. Geef de groepsnaam op.
4. [Optioneel] Voeg een beschrijving toe.
5. Klik op **OK**.

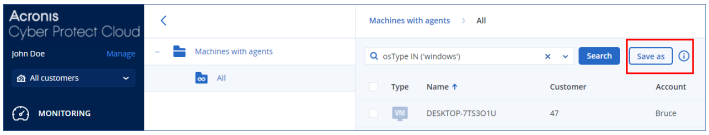
Een dynamische apparaatgroep maken op partnerniveau

U kunt dynamische apparaatgroepen maken op partnerniveau (**Alle apparaten**).

Een dynamische apparaatgroep maken op partnerniveau

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik in de boomstructuur op **Machines met agents** om de lijst uit te vouwen.
3. Klik op **Alle**.
4. Geef in het zoekveld de criteria op waarmee u een dynamische apparaatgroep wilt maken en klik vervolgens op **Zoeken**.

   Voor meer informatie over de beschikbare zoekcriteria: zie "Zoekkenmerken voor niet-cloud-to-cloud workloads" (p. 335) en "Zoekkenmerken voor cloud-to-cloud workloads" (p. 334).
5. Klik op **Opslaan als** en geef de groepsnaam op.



6. [Optioneel] Voeg een beschrijving toe.
7. Klik op **OK**.

Automatische detectie van machines op partnertenantniveau uitvoeren

U kunt automatische detectie van machines uitvoeren op partnertenantniveau (**Alle klanten**).

Vereisten

Er is minstens één machine met een geïnstalleerde beveiligingsagent in het lokale netwerk of Active Directory-domein van uw klant.

Belangrijk
Alleen agents die op Windows-machines zijn geïnstalleerd, kunnen detectieagents zijn. Als er geen detectieagents in uw omgeving zijn, kunt u de optie **Meerdere apparaten** in het deelvenster **Apparaten toevoegen** niet gebruiken.

Automatische detectie wordt niet ondersteund voor het toevoegen van domeincontrollers, vanwege de extra machtigingen die nodig zijn om de agentservice uit te voeren.

Externe installatie van agents wordt alleen ondersteund voor machines met Windows (Windows XP wordt niet ondersteund). Voor een externe installatie op een machine met Windows Server 2012 R2 moet Windows-update KB2999226 zijn geïnstalleerd.

Automatische detectie van machines op partnertenantniveau uitvoeren

1. Open de Cyber Protect-console en selecteer **Alle Klanten**.
2. Ga naar **Apparaten**> **Alle apparaten**.
3. Klik op **Toevoegen**.
4. Klik onder **Meerdere apparaten** op **Alleen Windows**. De detectiewizard wordt geopend.
5. Selecteer een klanttenant en selecteer vervolgens de detectieagent die de scan moet uitvoeren om machines te detecteren.
6. Selecteer de detectiemethode:
   - **Zoeken in Active Directory**. Controleer of de machine met de detectieagent het Active Directory-domeinlid is.
   - **Lokaal netwerk scannen**. Als de geselecteerde detectieagent geen machines kan vinden, selecteert u een andere detectieagent.
   - **Handmatig opgeven of importeren uit bestand**. Definieer handmatig de machines die u wilt toevoegen of importeer ze uit een tekstbestand.
7. [Als de detectiemethode met Active Directory is geselecteerd] Selecteer hoe u naar machines wilt zoeken:
   - **In de lijst met organisatie-eenheden**. Selecteer de groep machines die u wilt toevoegen.
   - **Met een query in LDAP-dialect**. Gebruik de query in LDAP-dialect om de machines te selecteren. **Zoekbasis**: hiermee bepaalt u waar moet worden gezocht; gebruik **Filter** om de criteria voor machineselectie op te geven.
8. Afhankelijk van de detectiemethode die u hebt geselecteerd, voert u een van de volgende acties

uit:

Detectiemethode	Actie
Zoeken in Active Directory	Open de lijst met gedetecteerde machines en selecteer de machines die u wilt toevoegen.
Lokaal netwerk scannen	Open de lijst met gedetecteerde machines en selecteer de machines die u wilt toevoegen.

Handmatig opgeven of importeren uit bestand	Geef de machine-IP-adressen of hostnamen op of importeer de lijst met machines uit een tekstbestand. Het bestand moet IP-adressen/hostnamen bevatten, één per regel. Hier is een voorbeeld van een bestand:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Wanneer u machineadressen handmatig hebt toegevoegd of hebt geïmporteerd uit een bestand, probeert de agent de toegevoegde machines te pingen en hun beschikbaarheid te definiëren.

9. Selecteer de acties die moeten worden uitgevoerd na de detectie:

Optie	Beschrijving
Agents installeren en machines registreren	U kunt selecteren welke onderdelen u wilt installeren op de machines door te klikken op **Onderdelen selecteren**. Voor meer details: zie "Onderdelen selecteren voor installatie" (p. 185).
Aanmelden bij de agentservice	Deze instelling is beschikbaar op het scherm **Onderdelen selecteren**. Deze instelling bepaalt voor welk account de services worden uitgevoerd. U kunt een van de volgende opties selecteren: • **Servicegebruikeraccounts gebruiken** (standaard voor de agentservice) Servicegebruikeraccounts zijn Windows-systeemaccounts die worden gebruikt om services uit te voeren. Het voordeel van deze instelling is dat de beleidsregels voor domeinbeveiliging geen invloed hebben op de gebruikersrechten van deze accounts. De agent wordt standaard uitgevoerd onder het **Lokale systeemaccount**. • **Een nieuw account maken** De accountnaam is Agent User voor de agent. • **Het volgende account gebruiken** Als u de agent installeert op een domeincontroller, wordt u gevraagd om bestaande accounts (of hetzelfde account) op te geven voor de agent. Uit veiligheidsoverwegingen worden er niet automatisch nieuwe accounts op een domeincontroller. Als u de optie **Een nieuw account maken** of **Het volgende account gebruiken**

Optie	Beschrijving
	kiest, controleer dan of het beveiligingsbeleid van het domein geen invloed heeft op de rechten van de gerelateerde accounts. Als de gebruikersrechten die tijdens de installatie zijn toegewezen, worden ingetrokken voor een account, werkt het onderdeel mogelijk onjuist of helemaal niet.
Machines registreren met geïnstalleerde agenten	Gebruik deze optie als de agent al op de machines is geïnstalleerd en u deze alleen hoeft te registreren in Cyber Protection. Als er geen agent op de machines wordt gevonden, worden ze toegevoegd als **Onbeheerde** machines.
Toevoegen als onbeheerde machines	Als u deze optie selecteert, wordt de agent niet op de machines geïnstalleerd. U kunt ze bekijken in de console en de agent later installeren of registreren.
Start de machine indien nodig opnieuw op	Deze optie wordt weergegeven wanneer **Agents installeren en machines registreren** is geselecteerd. Als u deze optie selecteert, wordt de machine zo vaak als nodig is opnieuw opgestart om de installatie te voltooien. De machine moet mogelijk opnieuw worden opgestart in een van de volgende gevallen: • De installatie van de vereiste voorbereidende items is voltooid en een herstart is vereist om de installatie voort te zetten. • De installatie is voltooid, maar een herstart is vereist, omdat sommige bestanden tijdens de installatie zijn vergrendeld. • De installatie is voltooid, maar een herstart is vereist voor andere eerder geïnstalleerde software.
Niet opnieuw opstarten als de gebruiker is aangemeld	Deze optie wordt weergegeven wanneer **De machine indien nodig opnieuw opstarten** is geselecteerd. Als u deze optie selecteert, wordt de machine niet automatisch opnieuw opgestart als de gebruiker is aangemeld bij het systeem. Als een gebruiker bijvoorbeeld aan het werk is terwijl de installatie een herstart vereist, wordt het systeem niet opnieuw opgestart. Als de vereiste voorbereidende items zijn geïnstalleerd, maar de machine niet opnieuw is opgestart omdat een gebruiker was aangemeld, moet de machine opnieuw opstarten en vervolgens de installatie opnieuw starten om deze te kunnen voltooien. Als de agent is geïnstalleerd, maar de machine vervolgens niet opnieuw is opgestart, moet u de machine opnieuw opstarten.
Gebruiker waarvoor u de machines wilt registreren	[Als er eenheden in uw organisatie zijn] Selecteer het gebruikersaccount van de eenheid of ondergeschikte eenheden waarvoor u de machines wilt registreren. [Bij het uitvoeren van automatische detectie op partnertenantniveau] In de lijst met klanttenants die u beheert, vouwt u de boomstructuur uit en selecteert u vervolgens het gebruikersaccount waarvoor u de machines wilt registreren.

Optie	Beschrijving
	[Bij het uitvoeren van automatische detectie als klantbeheerder] Als u **Agents installeren en machines registreren** of **Machines registreren met geïnstalleerde agenten** hebt geselecteerd, is er ook een optie om het beschermingsplan toe te passen op de machines. Als u meerdere beschermingsplannen hebt, kunt u selecteren welke u wilt gebruiken.

10. Geef de referenties op van de gebruiker met beheerdersrechten voor alle machines.

Belangrijk
De externe installatie van een agent zonder voorbereidingen werkt alleen als u de referenties van het ingebouwde beheerdersaccount opgeeft (het eerste account dat is gemaakt toen het besturingssysteem werd geïnstalleerd). Als u aangepaste beheerdersreferenties wilt definiëren, moet u dit voorbereiden met enkele aanvullende acties, zoals beschreven in "Vereisten" (p. 313).

11. Het systeem controleert de connectiviteit voor alle machines. Als de verbinding met sommige machines mislukt, kunt u de referenties voor deze machines wijzigen.

Nadat de detectie van machines is gestart, vindt u de bijbehorende taak in de activiteit **Monitoren**> **Activiteiten** > **Machines detecteren**.

Ondersteuning voor meerdere tenants

De Cyber Protection-service ondersteunt meerdere tenants, met beheer op de volgende niveaus:

- [Voor serviceproviders] Partnertenant (niveau **Alle klanten**)
  Dit niveau is alleen beschikbaar voor partnerbeheerders die klanttenants beheren.
- Klanttenantniveau
  Dit niveau wordt beheerd door bedrijfbeheerders.
  Partnerbeheerders kunnen ook op dit niveau werken voor de klanttenants die ze beheren. Op dit niveau hebben partnerbeheerders dezelfde rechten als de klantenbeheerders namens wie zij optreden.
- Eenheidniveau
  Dit niveau wordt beheerd door eenheidbeheerders en door bedrijfbeheerders van de bovenliggende klanttenant.
  Partnerbeheerders die de bovenliggende klanttenant beheren, hebben ook toegang tot het eenheidniveau. Op dit niveau hebben zij dezelfde rechten als de klantbeheerders namens wie zij optreden.

Beheerders kunnen objecten beheren in hun eigen tenant en de bijbehorende onderliggende tenants. Zij hebben geen zicht op of toegang tot eventuele objecten op een hoger beheerniveau.

Bedrijfbeheerders kunnen bijvoorbeeld beschermingsschema's beheren op klanttenantniveau en op eenheidniveau. Eenheidbeheerders kunnen alleen hun eigen beschermingsschema's op het eenheidniveau beheren. Zij kunnen geen beschermingsschema's beheren op het klanttenantniveau

en kunnen geen beschermingsschema's beheren die door de klantbeheerder op eenheidniveau zijn gemaakt.

Partnerbeheerders kunnen ook scripting-schema's maken en toepassen in de klanttenants die zij beheren. De bedrijfbeheerders in dergelijke tenants hebben alleen leestoegang tot de scripting-schema's die door een partnerbeheerder op hun workloads worden toegepast. Klantbeheerders kunnen echter hun eigen scripting- of beschermingsschema's maken en toepassen.

Workloads

Een workload is elk type beschermde resource, bijvoorbeeld een fysieke machine, een virtuele machine, een postvak of een database-exemplaar. In de Cyber Protect-console wordt de workload weergegeven als een object waarop u een schema kunt toepassen (beschermingsschema, back-upschema of scriptschema).

Voor sommige workloads moet u een beveiligingsagent installeren of een virtueel apparaat implementeren. U kunt agents installeren via de grafische gebruikersinterface of via de opdrachtregelinterface (installatie zonder toezicht). U kunt de installatie zonder toezicht gebruiken om de installatieprocedure te automatiseren. Zie "Cyber Protection-agents installeren en implementeren" (p. 60) voor meer informatie over het installeren van beveiligingsagents.

Een virtueel apparaat (VA) is een kant-en-klare virtuele machine die een beveiligingsagent bevat. Met een virtueel apparaat kunt u een back-up maken van andere virtuele machines in dezelfde omgeving zonder dat hierop een beveiligingsagent hoeft te worden geïnstalleerd (back-up zonder agent). De virtuele apparaten zijn beschikbaar in specifieke indelingen voor hypervisors, zoals .ovf, .ova of .qcow. Zie "Ondersteunde virtualisatieplatforms" (p. 32) voor meer informatie over welke virtualisatieplatforms back-ups zonder agent ondersteunen.

Belangrijk
Agents moeten minstens eenmaal per 30 dagen online zijn. Anders worden de betreffende schema's ingetrokken en zijn de workloads niet meer beschermd.

De onderstaande tabel geeft een overzicht van de typen workloads en de bijbehorende agents.

Type workload	Agent	Voorbeelden (lijst is niet uitputtend)
Fysieke machines	Op elke beschermde machine is een beveiligingsagent geïnstalleerd.	Werkstation Laptop Server
Virtuele machines	Afhankelijk van het virtualisatieplatform zijn mogelijk de volgende back-upmethoden beschikbaar: • Back-up met agent: op elke beschermde machine is een	Virtuele VMware-machine Virtuele Hyper-V-

Type workload	Agent	Voorbeelden (lijst is niet uitputtend)
	beveiligingsagent geïnstalleerd. • Back-up zonder agent: een beveiligingsagent wordt alleen geïnstalleerd op de hypervisorhost of op een speciale virtuele machine, of wordt geïmplementeerd als een virtueel apparaat. Deze agent maakt een back-up van alle virtuele machines in de omgeving.	machine Kernel-based Virtual Machines (KVM) beheerd door oVirt
Microsoft 365 Business-workloads Google Workspace-workloads	Van deze workloads wordt een back-up gemaakt door een cloudagent waarvoor geen installatie is vereist. Als u de cloudagent wilt gebruiken, moet u uw Microsoft 365- of Google Workspace-organisatie toevoegen aan de Cyber Protect-console. Daarnaast is er een lokale Agent voor Office 365 beschikbaar. Deze moet worden geïnstalleerd en kan alleen worden gebruikt voor back-ups van Exchange Online-postvakken. Voor meer informatie over de verschillen tussen de lokale en de cloudagent: zie "Microsoft 365-gegevens beschermen" (p. 632). .	Microsoft 365-postvak Microsoft 365 OneDrive Microsoft Teams SharePoint-site Google-postvak Google Drive
Applicaties	Voor de gegevens van specifieke toepassingen worden back-ups gemaakt door speciale agents, zoals Agent voor SQL, Agent voor Exchange, Agent voor MySQL/MariaDB of Agent voor Active Directory.	SQL Server-databases MySQL/MariaDB-databases Oracle-databases Active Directory
Mobiele apparaten	Er is een mobiele app geïnstalleerd op de beschermde apparaten.	Android- of iOS-apparaten
Websites	De websites worden ondersteund door een cloudagent waarvoor geen installatie is vereist.	Websites geopend via het SFTP- of SSH-protocol

Voor meer informatie over welke agent u nodig hebt en waar u deze moet installeren: zie "Welke agent heb ik nodig?" (p. 64)

Workloads toevoegen aan de Cyber Protect-console

Als u wilt beginnen met het beschermen van uw workloads, moet u deze eerst toevoegen aan de Cyber Protect-console.

Opmerking
Welke typen workloads u kunt toevoegen is afhankelijk van de servicequota's voor uw account. Als een specifiek type workload ontbreekt, wordt deze grijs weergegeven in het deelvenster **Apparaten toevoegen**.

Een partnerbeheerder kan de vereiste servicequota's inschakelen in de beheerportal. Zie "Informatie voor partnerbeheerders" (p. 323) voor meer informatie.

Een workload toevoegen:

1. Meld u aan bij de Cyber Protect-console.
2. Ga naar **Apparaten** > **Alle apparaten** en klik vervolgens op **Toevoegen**.
   Het deelvenster **Apparaten toevoegen** wordt geopend aan de rechterkant.
3. Selecteer het releasekanaal.
4. Klik op het type workload dat u wilt toevoegen en volg de instructies voor de specifieke workload die u hebt geselecteerd.

De volgende tabel geeft een overzicht van de typen workloads en de vereiste acties.

Workloads die u kunt toevoegen	Vereiste actie	Te volgen procedure
Meerdere Windows-machines	Voer automatische detectie uit in uw omgeving. Als u automatische detectie wilt uitvoeren, hebt u ten minste één machine met een geïnstalleerde beveiligingsagent nodig in uw lokale netwerk of Active Directory-domein. Deze agent wordt gebruikt als detectieagent.	"Automatische detectie en handmatige detectie uitvoeren" (p. 180)
Windows-werkstations Windows-servers	Installeer Agent voor Windows.	"Beveiligingsagents installeren in Windows" (p. 81) of "Beveiligingsagents installeren en verwijderen in Windows" (p. 88)
macOS-werkstations	Installeer Agent voor macOS.	"Beveiligingsagents installeren in macOS" (p. 86) of "Beveiligingsagents installeren en verwijderen in macOS" (p. 113)
Linux-servers	Installeer Agent voor Linux.	"Beveiligingsagents installeren in

Workloads die u kunt toevoegen	Vereiste actie	Te volgen procedure
		Linux" (p. 84) of "Beveiligingsagents installeren en verwijderen in Linux" (p. 106)
Mobiele apparaten (iOS, Android)	Installeer de mobiele app.	"Mobiele apparaten beschermen" (p. 624)
Cloud-to-cloud workloads		
Microsoft 365 Business	Voeg uw Microsoft 365-organisatie toe aan de Cyber Protect-console en gebruik de cloudagent om Exchange Online-postvakken, OneDrive-bestanden, Microsoft Teams en SharePoint-sites te beschermen. Als alternatief kunt u de lokale Agent voor Office 365 installeren. Deze biedt alleen een back-up van Exchange Online-postvakken. Zie "Microsoft 365-gegevens beschermen" (p. 632) voor meer informatie over de verschillen tussen de lokale agent en de cloudagent.	"Microsoft 365-gegevens beschermen" (p. 632)
Google Workspace	Voeg uw Google Workspace-organisatie toe aan de Cyber Protect-console en gebruik de cloudagent om Gmail-postvakken en Google Drive-bestanden te beschermen.	"Google Workspace-gegevens beveiligen" (p. 677)
Virtuele machines		
VMware ESXi	Implementeer Agent voor VMware (Virtual Appliance) in uw omgeving.	"Agent voor VMware (Virtual Appliance) implementeren" (p. 142)
	Installeer Agent voor VMware (Windows).	"Beveiligingsagents installeren in Windows" (p. 81) of "Beveiligingsagents installeren en verwijderen in Windows" (p. 88)
Virtuozzo Hybrid Infrastructure	Implementeer Agent voor Virtuozzo Hybrid Infrastructure	"Agent voor Virtuozzo Hybrid Infrastructure (Virtual Appliance)

Workloads die u kunt toevoegen	Vereiste actie	Te volgen procedure
	(Virtual Appliance) in uw omgeving.	implementeren" (p. 152)
Hyper-V	Installeer Agent voor Hyper-V.	"Beveiligingsagents installeren in Windows" (p. 81) of "Beveiligingsagents installeren en verwijderen in Windows" (p. 88)
Virtuozzo	Installeer Agent voor Virtuozzo.	"Beveiligingsagents installeren in Linux" (p. 84) of "Beveiligingsagents installeren en verwijderen in Linux" (p. 106)
KVM	Installeer Agent voor Windows.	"Beveiligingsagents installeren in Windows" (p. 81) of "Beveiligingsagents installeren en verwijderen in Windows" (p. 88)
	Installeer Agent voor Linux.	"Beveiligingsagents installeren in Linux" (p. 84) of "Beveiligingsagents installeren en verwijderen in Linux" (p. 106)
Red Hat Virtualization (oVirt)	Implementeer Agent voor oVirt (Virtual Appliance) in uw omgeving.	"Agent voor oVirt (Virtual Appliance) implementeren ..." (p. 160)
Citrix XenServer	Installeer Agent voor Windows.	"Beveiligingsagents installeren in Windows" (p. 81) of "Beveiligingsagents installeren en verwijderen in Windows" (p. 88)
	Installeer Agent voor Linux.	"Beveiligingsagents installeren in Linux" (p. 84) of "Beveiligingsagents installeren en verwijderen in Linux" (p. 106)

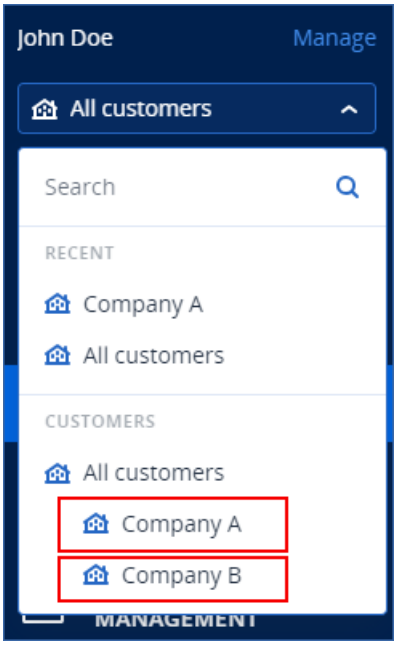
Workloads die u kunt toevoegen	Vereiste actie	Te volgen procedure
Nutanix AHV	Installeer Agent voor Windows.	"Beveiligingsagents installeren in Windows" (p. 81) of "Beveiligingsagents installeren en verwijderen in Windows" (p. 88)
	Installeer Agent voor Linux.	"Beveiligingsagents installeren in Linux" (p. 84) of "Beveiligingsagents installeren en verwijderen in Linux" (p. 106)
Oracle VM	Installeer Agent voor Windows.	"Beveiligingsagents installeren in Windows" (p. 81) of "Beveiligingsagents installeren en verwijderen in Windows" (p. 88)
	Installeer Agent voor Linux.	"Beveiligingsagents installeren in Linux" (p. 84) of "Beveiligingsagents installeren en verwijderen in Linux" (p. 106)
Scale Computing HC3	Implementeer Agent voor Scale Computing HC3 (Virtual Appliance) in uw omgeving.	"Agent voor Scale Computing HC3 (Virtual Appliance) implementeren ..." (p. 146)
Network-attached storage		
Synology	Implementeer Agent voor Synology (Virtual Appliance) in uw omgeving.	"Agent implementeren voor Synology" (p. 167)
Applicaties		
Microsoft SQL Server	Installeer Agent voor SQL.	"Beveiligingsagents installeren in Windows" (p. 81) of "Beveiligingsagents installeren en verwijderen in Windows" (p. 88)
Microsoft Exchange Server	Installeer Agent voor Exchange.	
Microsoft Active Directory	Installeer Agent voor Active Directory.	
Oracle Database	Installeer Agent voor Oracle.	"Oracle Database beschermen" (p. 703)

Workloads die u kunt toevoegen	Vereiste actie	Te volgen procedure
Website	Configureer de verbinding met de website.	"Websites en hostingservers beveiligen" (p. 711)

Zie "Welke agent heb ik nodig?" (p. 64) voor meer informatie over de beschikbare beveiligingsagents en waar u ze kunt installeren

Informatie voor partnerbeheerders

- Er ontbreekt mogelijk een type workload in het deelvenster **Apparaten toevoegen** als een vereiste servicequota niet is ingeschakeld in de beheerportal. Zie Opties in- of uitschakelen voor meer informatie over de servicequota's die vereist zijn voor verschillende workloads.
- Als partnerbeheerder kunt u geen workloads toevoegen op het niveau **Alle klanten**. Als u een workload wilt toevoegen, selecteert u een afzonderlijke klanttenant.



Workloads verwijderen uit de Cyber Protect-console

De workloads die u niet meer hoeft te beschermen, kunt u verwijderen uit de Cyber Protect-console. De procedure is afhankelijk van het type workload.

U kunt de agent ook verwijderen uit de beschermde workload. Wanneer u een agent verwijdert, wordt de beschermde workload automatisch verwijderd uit de Cyber Protect-console.

Belangrijk
Wanneer u een workload uit de Cyber Protect-console verwijdert, worden alle schema's ingetrokken die op die workload werden toegepast. Als u een workload verwijdert, worden er geen schema's of back-ups verwijderd en wordt ook de beveiligingsagent niet verwijderd.

De volgende tabel geeft een overzicht van de typen workloads en de vereiste acties.

Workloads die u kunt verwijderen	Vereiste acties	Te volgen procedure
Fysieke en virtuele machines		
Fysieke of virtuele machines waarop een beveiligingsagent is geïnstalleerd	1. Verwijder de workload uit de Cyber Protect-console. 2. [Optioneel] Verwijder de beveiligingsagent.	"Een workload verwijderen uit de Cyber Protect-console" (p. 325) (Workload met beveiligingsagent)
Virtuele machines waarvan een back-up wordt gemaakt op hypervisorniveau (back-up zonder agent)	1. Verwijder in de Cyber Protect-console het apparaat waarop de beveiligingsagent is geïnstalleerd. Alle virtuele machines waarvan een back-up wordt gemaakt door deze agent, worden automatisch verwijderd uit de console. 2. [Optioneel] Verwijder de beveiligingsagent.	"Een workload verwijderen uit de Cyber Protect-console" (p. 325) (Workload zonder beveiligingsagent)
Cloud-to-cloud workloads		
Microsoft 365 Business-workloads Google Workspace-workloads	Verwijder de Microsoft 365- of Google Workspace-organisatie uit de Cyber Protect-console. Alle resources in die organisatie worden automatisch verwijderd uit de console.	"Een workload verwijderen uit de Cyber Protect-console" (p. 325) (Cloud-to-cloud workload)
Mobiele apparaten		
Android-apparaten iOS-apparaten	1. Verwijder het mobiele apparaat uit de Cyber	"Een workload verwijderen uit de Cyber Protect-console" (p. 325)

Workloads die u kunt verwijderen	Vereiste acties	Te volgen procedure
	Protect-console. 2. [Optioneel] Verwijder de app op het mobiele apparaat.	(Mobiel apparaat)
Network-attached storage		
Synology	1. Verwijder de workload uit de Cyber Protect-console. 2. [Optioneel] Verwijder de beveiligingsagent.	"Een workload verwijderen uit de Cyber Protect-console" (p. 325) (Workload met een beveiligingsagent)
Applicaties		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Oracle Database	1. Verwijder in de Cyber Protect-console het apparaat waarop de beveiligingsagent is geïnstalleerd. De objecten waarvan een back-up wordt gemaakt door deze agent, worden automatisch verwijderd uit de console. 2. [Optioneel] Verwijder de beveiligingsagent.	"Een workload verwijderen uit de Cyber Protect-console" (p. 325) (Workload zonder beveiligingsagent)
Websites	Verwijder de website uit de Cyber Protect-console.	"Een workload verwijderen uit de Cyber Protect-console" (p. 325) (Website)

Een workload verwijderen uit de Cyber Protect-console

Workload met beveiligingsagent

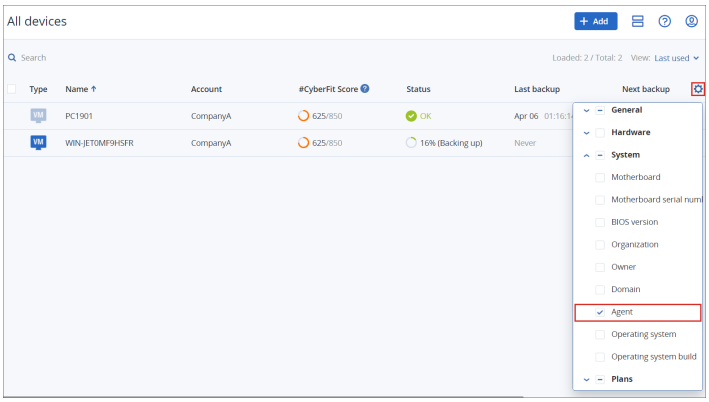
U kunt dit type workload rechtstreeks verwijderen.

1. Ga in de Cyber Protect-console, naar **Apparaten** > **Alle apparaten**.
2. Schakel het selectievakje in naast een of meer workloads die u wilt verwijderen.
3. Klik in het deelvenster **Acties** op **Verwijderen**.
4. Bevestig uw keuze door te klikken op **Verwijderen**.
5. [Optioneel] Verwijder de agent zoals beschreven in "Agenten verwijderen" (p. 86).

Workload zonder beveiligingsagent

Als u dit type workload wilt verwijderen, moet u de machine verwijderen waarop de beveiligingsagent is geïnstalleerd.

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op het tandwielpictogram in de rechterbovenhoek van de tabel en schakel het selectievakje **Agent** in.



   De kolom **Agent** wordt weergegeven.
3. Ga naar de kolom **Agent** en controleer de naam van de machine waarop de beveiligingsagent is geïnstalleerd.
4. Schakel in de Cyber Protect-console het selectievakje in naast de machine waarop de beveiligingsagent is geïnstalleerd.
5. Klik in het deelvenster **Acties** op **Verwijderen**.
6. Bevestig uw keuze door te klikken op **Verwijderen**.
7. [Optioneel] Verwijder de agent zoals beschreven in "Agenten verwijderen" (p. 86).

Cloud-to-cloud workload

Als u workloads wilt verwijderen waarvan een back-up is gemaakt door de cloudagent, verwijdert u uw Microsoft 365- of Google Workspace-organisatie uit de Cyber Protect-console.

1. Navigeer in de Cyber Protect-console naar **Apparaten** > **Microsoft 365** of **Apparaten** > **Google Workspace**.
2. Klik op de naam van uw Microsoft 365- of Google Workspace-organisatie.
3. Klik in het deelvenster **Acties** op **Groep verwijderen**.
4. Klik op **Verwijderen** om uw actie te bevestigen.

Mobiel apparaat

1. Ga in de Cyber Protect-console, naar **Apparaten** > **Alle apparaten**.
2. Schakel het selectievakje in naast de workload die u wilt verwijderen.
3. Klik in het deelvenster **Acties** op **Verwijderen**.
4. Bevestig uw keuze door te klikken op **Verwijderen**.
5. [Optioneel] Verwijder de app uit het mobiele apparaat.

Website

1. Ga in de Cyber Protect-console, naar **Apparaten** > **Alle apparaten**.
2. Schakel het selectievakje in naast de workload die u wilt verwijderen.
3. Klik in het deelvenster **Acties** op **Verwijderen**.
4. Bevestig uw keuze door te klikken op **Verwijderen**.

Apparaatgroepen

Als u apparaatgroepen gebruikt, kunt u meerdere vergelijkbare workloads beschermen met een groepsschema. Het schema wordt toegepast op de hele groep en kan niet worden ingetrokken voor alleen een lid van de groep.

Een workload kan lid zijn van meer dan één groep. Een workload die is opgenomen in een apparaatgroep, kan nog wel worden beschermd door individuele schema's.

U kunt alleen workloads van hetzelfde type toevoegen aan een apparaatgroep. Voor **Hyper-V** kunt u bijvoorbeeld alleen groepen van virtuele Hyper-V-machines maken. Voor **Machines met agents** kunt u alleen groepen machines met geïnstalleerde agents maken.

U kunt geen apparaatgroepen maken binnen een groep van het type **Alle**, zoals de hoofdgroep **Alle apparaten**, of ingebouwde groepen zoals **Machines met agents** > **Alle**, **Microsoft 365** > uw organisatie > **Gebruikers** > **Alle gebruikers**.

Ingebouwde groepen en aangepaste groepen

Ingebouwde groepen

Nadat u een workload in de Cyber Protect-console hebt geregistreerd, wordt de workload weergegeven in een van de ingebouwde hoofdgroepen op het tabblad **Apparaten**, zoals **Machines met agents**, **Microsoft 365** of **Hyper-V**.

Alle geregistreerde niet-cloud-to-cloud workloads worden ook vermeld in de hoofdgroep **Alle apparaten**. Een afzonderlijke ingebouwde hoofdgroep, met de naam van uw tenant, bevat alle niet-cloud-to-cloud workloads en alle eenheden in deze tenant.

U kunt de hoofdgroepen niet verwijderen of bewerken en u kunt hierop geen schema's toepassen.

Sommige hoofdgroepen bevatten een of meer niveaus ingebouwde subgroepen, bijvoorbeeld **Machines met agents** > **Alle**, **Microsoft 365** > uw organisatie > **Teams** > **Alle teams**, **Google Workspace** > uw organisatie > **Shared Drives** > **Alle Shared Drives**.

U kunt ingebouwde subgroepen niet bewerken of verwijderen.

Aangepaste groepen

Het is misschien niet handig om alle workloads in een ingebouwde groep te beschermen, omdat er mogelijk workloads zijn die andere beveiligingsinstellingen of een ander beschermingsschema vereisen.

In sommige hoofdgroepen, bijvoorbeeld in **Machines met agents**, **Microsoft 365**, of **Google Workspace**, kunt u aangepaste subgroepen maken. Deze subgroepen kunnen statisch of dynamisch zijn.

U kunt elke aangepaste groep bewerken of verwijderen en u kunt de naam ervan wijzigen.

Statische groepen en dynamisch groepen

U kunt de volgende typen aangepaste groepen maken:

- Statisch
- Dynamisch

Statische groepen

Statische groepen bevatten handmatig toegevoegde workloads.

De inhoud van een statische groep verandert alleen wanneer u expliciet een workload toevoegt of verwijdert.

Voorbeeld: U kunt een statische groep maken voor de boekhoudafdeling van uw bedrijf en handmatig de machines van de boekhouders toevoegen aan deze groep. Wanneer u een groepsschema toepast, worden de machines in die groep beschermd. Als een nieuwe boekhouder in dienst wordt genomen, moet u de machine van de boekhouder handmatig toevoegen aan de statische groep.

Dynamisch groepen

Dynamische groepen bevatten workloads die voldoen aan specifieke criteria. U definieert deze criteria vooraf door een zoekquery te maken met kenmerken (bijvoorbeeld `osType`), de bijbehorende waarden (bijvoorbeeld `Windows`) en zoekoperators (bijvoorbeeld `IN`).

U kunt dus een dynamische groep maken voor alle machines waarvan het besturingssysteem Windows is, of een dynamische groep met alle gebruikers in uw Microsoft 365-organisatie die en e-mailadres hebben dat begint met `jan`.

Alle workloads die de vereiste kenmerken en waarden hebben, worden automatisch toegevoegd aan de groep en elke workload die een vereist kenmerk of vereiste waarde verliest, wordt automatisch verwijderd uit de groep.

Voorbeeld 1: De hostnamen van de machines die horen bij de boekhoudafdeling, bevatten het woord boekhouding. U zoekt de machines waarvan de naam het woord boekhouding bevat en vervolgens slaat u de zoekresultaten op als dynamische groep. Vervolgens past u een beschermingsschema toe op de groep. Als een nieuwe boekhouder in dienst wordt genomen, krijgt de machine van die boekhouder een naam met het woord boekhouding. De nieuwe machine wordt automatisch toegevoegd aan de dynamische groep zodra u die machine registreert in de Cyber Protect-console.

Voorbeeld 2: De boekhoudafdeling creëert een afzonderlijke Active Directory-organisatie-eenheid (OU). U geeft de boekhouding-organisatie-eenheid op als vereist kenmerk en slaat de zoekresultaten op als dynamische groep. Vervolgens past u een beschermingsschema toe op de groep. Als een nieuwe boekhouder in dienst wordt genomen, wordt de machine van die boekhouder toegevoegd aan de dynamische groep zodra deze wordt toegevoegd aan de Active Directory-organisatie-eenheid en wordt geregistreerd in de Cyber Protect-console (ongeacht wat het eerst gebeurt).

Cloud-to-cloud groepen en niet-cloud-to-cloud groepen

Cloud-to-cloud groepen bevatten Microsoft 365- of Google Workspace-workloads waarvan een back-up wordt gemaakt door een cloudagent.

Niet-cloud-to-cloud groepen bevatten alle andere typen workloads.

Ondersteunde schema's voor apparaatgroepen

De volgende tabel bevat een overzicht van de schema's die u kunt toepassen op een apparaatgroep.

Groep	Beschikbare schema's	Locatie van schema
Cloud-to-cloud workloads (Microsoft 365- en Google Workspace-workloads)	Back-upschema	**Beheer** > **Back-up van cloudtoepassingen**
Niet-cloud-to-cloud workloads	Beschermingsschema	**Beheer** > **Beschermingsschema's**
	Schema voor extern beheer	**Beheer** > **Schema's voor extern beheer**
	Scripting-schema	**Beheer** > **Scripting-schema's**

Cloudresources, zoals Microsoft 365- of Google Workspace-gebruikers, OneDrive- en Google Drive-shares, Microsoft Teams of Azure AD-groepen, worden gesynchroniseerd met de Cyber Protect-console zodra u een Microsoft 365- of Google Workspace-organisatie toevoegt aan de console. Eventuele verdere wijzigingen in een organisatie worden één keer per dag gesynchroniseerd.

Als u een wijziging onmiddellijk wilt synchroniseren, navigeert u in de Cyber Protect-console respectievelijk naar **Apparaten** > **Microsoft 365** of **Apparaten** > **Google Workspace**. Vervolgens selecteert u de gewenste organisatie en klikt u op **Vernieuwen**.

Een statische groep maken

U kunt een lege statische groep maken en hieraan workloads toevoegen.

U kunt ook workloads selecteren en een nieuwe statische groep maken voor de geselecteerde workloads.

U kunt geen apparaatgroepen maken binnen een groep van het type **Alle**, zoals de hoofdgroep **Alle apparaten**, of ingebouwde groepen zoals **Machines met agents** > **Alle**, **Microsoft 365** > uw organisatie > **Gebruikers** > **Alle gebruikers**.

Een statische groep maken:

In het hoofdvenster

1. Klik op **Apparaten** en selecteer vervolgens de hoofdgroep die de workloads bevat waarvoor u een statische groep wilt maken.
2. [Optioneel] Als u een geneste groep wilt maken, navigeert u naar een bestaande statische groep.

   Opmerking
   Het maken van geneste statische groepen is niet beschikbaar voor cloud-to-cloud workloads.

3. Klik op **+ Nieuwe statische groep** onder de groepsstructuur of klik op **Nieuwe statische groep** in het deelvenster **Acties**.
4. Geef een naam op voor de nieuwe groep.
5. [Optioneel] Voeg een opmerking toe voor de groep.
6. Klik op **OK**.

In de groepsstructuur

1. Klik op **Apparaten** en selecteer vervolgens de hoofdgroep die de workloads bevat waarvoor u een statische groep wilt maken.
2. Klik op het tandwielpictogram naast de naam van de groep waarin u een nieuwe statische groep wilt maken.

   Opmerking
   Het maken van geneste statische groepen is niet beschikbaar voor cloud-to-cloud workloads.

3. Klik op **Nieuwe statische groep**.
4. Geef een naam op voor de nieuwe groep.
5. [Optioneel] Voeg een opmerking toe voor de groep.
6. Klik op **OK**.

Vanuit geselecteerde workloads

1. Klik op **Apparaten** en selecteer vervolgens de hoofdgroep die de workloads bevat waarvoor u een statische groep wilt maken.

   Opmerking
   U kunt geen apparaatgroepen maken binnen een groep van het type **Alle**, zoals de hoofdgroep **Alle apparaten**, of ingebouwde groepen zoals **Machines met agents** > **Alle**, **Microsoft 365** > uw organisatie > **Gebruikers** > **Alle gebruikers**.

2. Schakel de selectievakjes in naast de workloads waarvoor u een nieuwe groep wilt maken en klik vervolgens op **Toevoegen aan groep**.
3. Selecteer in de mapstructuur het bovenliggende niveau voor de nieuwe groep en klik vervolgens op **Nieuwe statische groep**.

   Opmerking
   Het maken van geneste statische groepen is niet beschikbaar voor cloud-to-cloud workloads.

4. Geef een naam op voor de nieuwe groep.
5. [Optioneel] Voeg een opmerking toe voor de groep.
6. Klik op **OK**.
   De nieuwe groep wordt weergegeven in de mapstructuur.
7. Klik op **Gereed**.

Workloads toevoegen aan een statische groep

U kunt eerst de doelgroep selecteren en vervolgens workloads toevoegen aan de doelgroep.

U kunt ook eerst de workloads selecteren en deze vervolgens toevoegen aan een groep.

Workloads toevoegen aan een statische groep:

Eerst de doelgroep selecteren

1. Klik op **Apparaten** en navigeer vervolgens naar uw doelgroep.
2. Selecteer de doelgroep en klik vervolgens op **Apparaten toevoegen**.
3. Selecteer in de mapstructuur de groep die de vereiste workloads bevat.
4. Schakel de selectievakjes in naast de workloads die u wilt toevoegen en klik vervolgens op **Toevoegen**.

Eerst de workloads selecteren

1. Selecteer **Apparaten** en selecteer vervolgens de hoofdgroep die de vereiste workloads bevat.
2. Schakel de selectievakjes in naast de workloads die u wilt toevoegen en klik vervolgens op **Toevoegen aan groep**.
3. Selecteer de doelgroep in de mapstructuur en klik vervolgens op **Gereed**.

Een dynamische groep maken

U maakt een dynamische groep door te zoeken naar workloads met specifieke kenmerken waarvan u de waarden definieert in een zoekopdracht. Vervolgens slaat u de zoekresultaten op als dynamische groep.

Welke kenmerken worden ondersteund voor het zoeken en maken van dynamische groepen, hangt af van de workload, namelijk of het al dan niet gaat om een cloud-naar-cloud workload. Voor meer informatie over ondersteunde kenmerken: zie "Zoekkenmerken voor niet-cloud-to-cloud workloads" (p. 335) en "Zoekkenmerken voor cloud-to-cloud workloads" (p. 334).

Dynamische groepen worden gemaakt in hun respectievelijke hoofdgroepen. Geneste dynamische groepen worden niet ondersteund.

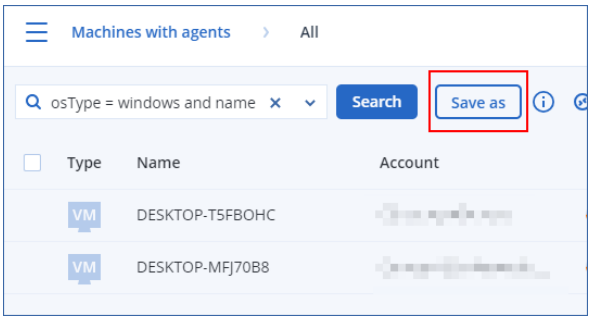
U kunt geen apparaatgroepen maken binnen een groep van het type **Alle**, zoals de hoofdgroep **Alle apparaten**, of ingebouwde groepen zoals **Machines met agents** > **Alle**, **Microsoft 365** > uw organisatie > **Gebruikers** > **Alle gebruikers**.

Een dynamische groep maken:

Niet-cloud-to-cloud workloads

1. Klik op **Apparaten** en selecteer vervolgens de groep die de workloads bevat waarvoor u een dynamische groep wilt maken.
2. Zoek naar workloads met behulp van de ondersteunde zoekkenmerken en operators.

   U kunt meerdere kenmerken en operators gebruiken in één enkele query. Voor meer informatie over de ondersteunde kenmerken: zie "Zoekkenmerken voor niet-cloud-to-cloud workloads" (p. 335).
3. Klik op **Opslaan als** naast het zoekveld.



Opmerking

De knop **Opslaan als** is niet beschikbaar wanneer u geen dynamische groep mag maken op een specifiek niveau, bijvoorbeeld in de hoofdgroep **Apparaten** > **Alle apparaten**.

Selecteer een ander niveau (bijvoorbeeld **Apparaten** > **Machines met agents** > **Alle**) en herhaal vervolgens de bovenstaande stappen. Met deze zoekopdracht kunt u een dynamische groep maken binnen **Machines met agents**, maar niet binnen **Machines met agents** > **Alle**.

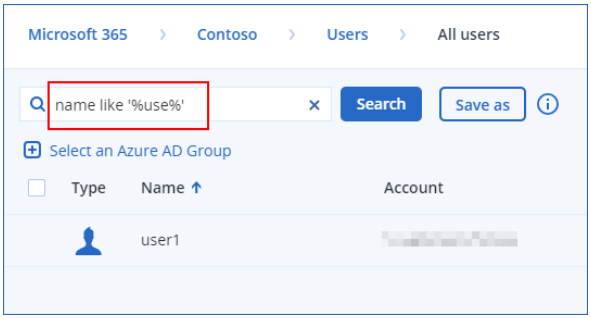
4. Geef een naam op voor de nieuwe groep.

5. [Optioneel] Voeg in het veld **Opmerking** een beschrijving toe voor de nieuwe groep.
6. Klik op **OK**.

Cloud-to-cloud workloads

1. Klik op **Apparaten** en selecteer vervolgens **Microsoft 365** of **Google Workspace**.
2. Selecteer de groep die de workloads bevat waarvoor u een nieuwe dynamische groep wilt maken. Bijvoorbeeld, **Gebruikers** > **Alle gebruikers**.
3. Zoek naar workloads met behulp van de ondersteunde zoekkenmerken en operators of door Microsoft 365-gebruikers te selecteren in een specifieke Active Directory-groep.

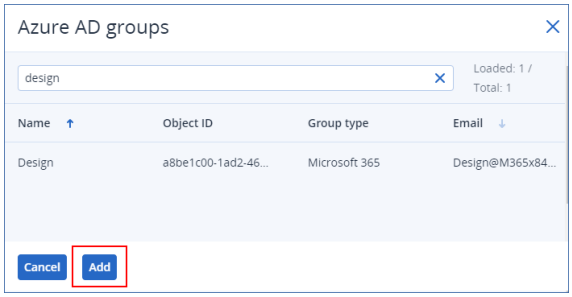
   U kunt meerdere kenmerken en operators gebruiken in één enkele query. Voor meer informatie over de ondersteunde kenmerken: zie "Zoekkenmerken voor cloud-to-cloud workloads" (p. 334).



4. [Alleen voor **Microsoft 365** > **Gebruikers**] Als u gebruikers wilt selecteren in een specifieke Active Directory-groep, gaat u als volgt te werk:
   a. Navigeer naar **Gebruikers** > **Alle gebruikers**.
   b. Klik op **Selecteer een Azure AD-groep**.

      Er wordt een lijst met de Active Directory-groepen in uw organisatie geopend.

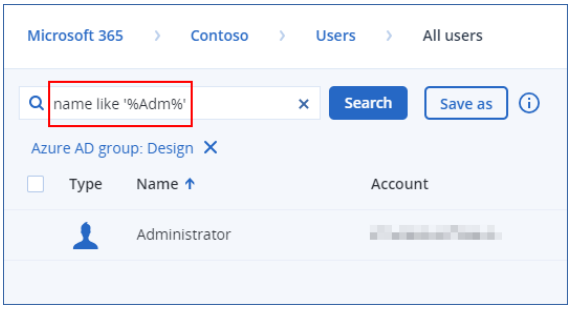
      In deze lijst kunt u zoeken naar een specifieke groep of de groepen sorteren op naam of e-mailadres.
   c. Selecteer de gewenste Active Directory-groep en klik vervolgens op **Toevoegen**.



   d. [Optioneel] Als u specifieke gebruikers wilt opnemen in of uitsluiten van de geselecteerde Active Directory-groep, maakt u een zoekopdracht met behulp van de ondersteunde zoekkenmerken en operators.

      U kunt meerdere kenmerken en operators gebruiken in één enkele query. Voor meer informatie over de ondersteunde kenmerken: zie "Zoekkenmerken voor cloud-to-cloud

workloads" (p. 334).



5. Klik op **Opslaan als** naast het zoekveld.

> **Opmerking**
> De knop **Opslaan als** is niet beschikbaar wanneer u geen dynamische groep mag maken op een specifiek niveau, bijvoorbeeld in **Microsoft 365** > uw organisatie > **Gebruikers**.
>
> Selecteer een ander niveau (bijvoorbeeld **Microsoft 365** > uw organisatie > **Gebruikers** > **Alles**) en herhaal vervolgens de bovenstaande stappen. Met deze zoekopdracht kunt u een dynamische groep maken binnen **Microsoft 365** > uw organisatie > **Gebruikers** >, maar niet binnen **Gebruikers** > **Alle**.

6. Geef een naam op voor de nieuwe groep.
7. [Optioneel] Voeg in het veld **Opmerking** een beschrijving toe voor de nieuwe groep.
8. Klik op **OK**.

Zoekkenmerken voor cloud-to-cloud workloads

De volgende tabel bevat een overzicht van de kenmerken die u kunt gebruiken in uw zoekopdrachten voor Microsoft 365- en Google Workspace-workloads.

Raadpleeg "Zoekkenmerken voor niet-cloud-to-cloud workloads" (p. 335) om te zien welke kenmerken u kunt gebruiken in zoekopdrachten voor andere typen workloads.

Kenmerk	Betekenis	Kan worden gebruikt in	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
`name`	Weergavenaam van een Microsoft 365- of Google Workspace-workload	Alle cloud-to-cloud resources	`name = 'My Name'` `name LIKE '*nam*'`	Ja
`email`	E-mailadres voor een Microsoft 365-gebruiker of	Microsoft 365 > Groepen Microsoft 365 >	`email = 'my_group_email@mycompany.com'` `email LIKE '*@company*'`	Ja

Kenmerk	Betekenis	Kan worden gebruikt in	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	-groep of een Google Workspace-gebruiker	Gebruikers Google Workspace > Gebruikers	`email NOT LIKE '*enterprise.com'`	
`siteName`	Naam van een site die is gekoppeld aan een Microsoft 365-groep	Microsoft 365 > Groepen	`siteName = 'my_site'` `siteName LIKE '*company.com*support*'`	Ja
`url`	Webadres voor een Microsoft 365-groep of SharePoint-site	Microsoft 365 > Groepen Microsoft 365 > Siteverzamelingen	`url = 'https://www.mycompany.com/'` `url LIKE '*www.mycompany.com*'`	Ja

Zoekkenmerken voor niet-cloud-to-cloud workloads

De volgende tabel bevat een overzicht van de kenmerken die u kunt gebruiken in uw zoekopdrachten voor niet-cloud-to-cloud workloads.

Raadpleeg "Zoekkenmerken voor cloud-to-cloud workloads" (p. 334) om te zien welke kenmerken u kunt gebruiken in zoekopdrachten voor cloud-to-cloud workloads.

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
Algemeen			
`name`	Naam van de workload, zoals: • Hostnaam voor fysieke machines • Naam voor virtuele machines • Databasenaam • E-mailadres voor postvakken	`name = 'en-00'`	Ja
`id`	Apparaat-id.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Ja

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	Als u de apparaat-ID wilt zien, gaat u naar **Apparaten**, selecteert u het apparaat en klikt u op **Details** > **Alle eigenschappen**'. De id wordt weergegeven in het veld `id`.		
`resourceType`	Type workload. Mogelijke waarden: • `'machine'` • `'exchange'` • `'mssql_server'` • `'mssql_instance'` • `'mssql_database'` • `'mssql_database_folder'` • `'msexchange_database'` • `'msexchange_storage_group'` • `'msexchange_mailbox.msexchange'` • `'msexchange_mailbox.office365'` • `'mssql_aag_group'` • `'mssql_aag_database'` • `'virtual_machine.vmww'` • `'virtual_machine.vmwesx'` • `'virtual_host.vmwesx'` • `'virtual_cluster.vmwesx'` • `'virtual_appliance.vmwesx'` • `'virtual_application.vmwesx'` • `'virtual_resource_pool.vmwesx'` • `'virtual_center.vmwesx'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Ja

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	• 'datastore.vmwesx' • 'datastore_cluster.vmwesx' • 'virtual_network.vmwesx' • 'virtual_data_center.vmwesx' • 'virtual_machine.vmww' • 'virtual_cluster.mshyperv' • 'virtual_machine.mshyperv' • 'virtual_host.mshyperv' • 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_machine.parallelsw' • 'virtual_host.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen' • 'bootable_media'		
chassis	Type chassis. Mogelijke waarden: • laptop • desktop • server • other	chassis = 'laptop' chassis IN ('laptop', 'desktop')	Ja

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	• unknown		
`ip`	IP-adres (uitsluitend voor fysieke machines).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Ja
`comment`	Opmerking voor een apparaat. Deze kan automatisch of handmatig worden opgegeven. Standaardwaarde: • Voor fysieke machines met Windows wordt de computerbeschrijving in Windows automatisch gekopieerd als opmerking. Deze waarde wordt elke 15 minuten gesynchroniseerd. • De waarde is leeg voor andere apparaten. **Opmerking** De automatische synchronisatie wordt uitgeschakeld als er handmatig tekst wordt toegevoegd in het opmerkingenveld. Wis deze tekst als u de synchronisatie weer wilt inschakelen. Als u de automatisch gesynchroniseerde opmerkingen voor uw workloads wilt vernieuwen, start u de Managed Machine Service opnieuw op in **Windows-services** of voert u de volgende	`comment = 'important machine'` `comment = ''` (alle machines zonder een opmerking)	Ja

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen

	opdrachten uit op de opdrachtprompt:
	`net stop mms`
	`net start mms`
	Als u een opmerking over een apparaat wilt bekijken, selecteert u het apparaat onder **Apparaten**, klikt u op **Details** en gaat u naar het gedeelte **Opmerking**.
	Als u een opmerking handmatig wilt toevoegen of wijzigen, klikt u op **Toevoegen** of **Bewerken**.
	Voor apparaten waarop een beveiligingsagent is geïnstalleerd, zijn er twee afzonderlijke velden voor opmerkingen:
	• Opmerking over agent
	◦ Voor fysieke machines met Windows wordt de computerbeschrijving in Windows automatisch gekopieerd als opmerking. Deze waarde wordt elke 15 minuten gesynchroniseerd.
	◦ De waarde is leeg voor andere apparaten.		

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	Opmerking De automatische synchronisatie wordt uitgeschakeld als er handmatig tekst wordt toegevoegd in het opmerkingenveld. Wis deze tekst als u de synchronisatie weer wilt inschakelen. • Opmerking over apparaat ◦ Als de opmerking over de agent automatisch wordt opgegeven, wordt deze gekopieerd als een opmerking over een apparaat. Handmatig toegevoegde opmerkingen over agenten worden niet gekopieerd als opmerkingen over apparaten. ◦ Opmerkingen over apparaten worden niet gekopieerd als opmerkingen over agenten. Voor een apparaat kan een van deze opmerkingen worden opgegeven, of ze kunnen allebei worden opgegeven of allebei blanco zijn. De opmerking over het apparaat heeft de prioriteit als beide opmerkingen zijn		

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	opgegeven. Als u een opmerking over een agent wilt bekijken, selecteert u onder **Instellingen** > **Agents** het apparaat met de agent, klikt u op **Details** en gaat u naar het gedeelte **Opmerking**. Als u een opmerking over een apparaat wilt bekijken, selecteert u het apparaat onder **Apparaten**, klikt u op **Details** en gaat u naar het gedeelte **Opmerking**. Als u een opmerking handmatig wilt toevoegen of wijzigen, klikt u op **Toevoegen** of **Bewerken**.		
`isOnline`	Beschikbaarheid van workload. Mogelijke waarden: • `true` • `false`	`isOnline = true`	Nee
`hasAsz`	Beschikbaarheid van Secure Zone. Mogelijke waarden: • `true` • `false`	`hasAsz = true`	Ja

`tzOffset`	Verschil (offset) van de tijdzone ten opzichte van Coordinated Universal Time (UTC), in minuten.	`tzOffset = 120`
		`tzOffset > 120`
		`tzOffset < 120`
			Ja

CPU, geheugen, schijven			
`cpuArch`	CPU-architectuur.	`cpuArch = 'x64'`	Ja

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	Mogelijke waarden: • `'x64'` • `'x86'`		
`cpuName`	CPU-naam.	`cpuName LIKE '%XEON%'`	Ja
`memorySize`	RAM-grootte in megabytes.	`memorySize < 1024`	Ja
`diskSize`	Grootte van de harde schijf in gigabytes of megabytes (alleen voor fysieke machines).	`diskSize < 300GB` `diskSize >= 3000000MB`	Nee
Besturingssysteem			
`osName`	Naam van besturingssysteem.	`osName LIKE '%Windows XP%'`	Ja
`osType`	Type besturingssysteem. Mogelijke waarden: • `'windows'` • `'linux'` • `'macosx'`	`osType = 'windows'` `osType IN ('linux', 'macosx')`	Ja
`osArch`	Architectuur van besturingssysteem. Mogelijke waarden: • `'x64'` • `'x86'`	`cpuArch = 'x86'`	Ja
`osProductType`	Producttype van het besturingssysteem. Mogelijke waarden: • `'dc'` Staat voor Domeincontroller.	`osProductType = 'server'`	Ja

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	Opmerking Wanneer de rol van de domeincontroller wordt toegewezen op een Windows-server, verandert `osProductType` van `server` in `dc`. Dergelijke machines worden niet opgenomen in de zoekresultaten voor `osProductType='server'`. • `'server'` • `'workstation'`		
`osSp`	Servicepakket van het besturingssysteem.	`osSp = 1`	Ja
`osVersionMajor`	Primaire versie van het besturingssysteem.	`osVersionMajor = 1`	Ja
`osVersionMinor`	Secundaire versie van het besturingssysteem.	`osVersionMinor > 1`	Ja
Agent			
`agentVersion`	Versie van de geïnstalleerde beveiligingsagent.	`agentVersion LIKE '12.0.*'`	Ja
`hostId`	Interne id van de beveiligingsagent. Als u de id van de beveiligingsagent wilt zien, gaat u naar **Apparaten**, selecteert u het apparaat en klikt u op **Details** > **Alle eigenschappen**'. Controleer de `id`-waarde van de eigenschap `agent`.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Ja
`virtualType`	Type virtuele machine. Mogelijke waarden:	`virtualType = 'vmwesx'`	Ja

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	• `'vmwesx'` Virtuele VMware-machines. • `'mshyperv'` Virtuele Hyper-V-machines. • `'pcs'` Virtuele Virtuozzo-machines. • `'hci'` Virtuele Virtuozzo Hybrid Infrastructure-machines. • `'scale'` Virtuele Scale Computing HC3-machines. • `'ovirt'` Virtuele oVirt-machines		
`insideVm`	Virtuele machine met een agent. Mogelijke waarden: • `true` • `false`	`insideVm = true`	Ja
Locatie			
`tenant`	De naam van de tenant waarvan het apparaat deel uitmaakt.	`tenant = 'Unit 1'`	Ja
`tenantId`	De id van de tenant waarvan het apparaat deel uitmaakt. Als u de tenant-ID wilt zien, gaat u naar **Apparaten**, selecteert u het apparaat en klikt u op **Details** > **Alle eigenschappen**'. De id wordt weergegeven in het	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Ja

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	veld `ownerId`.		
`ou`	Apparaten die deel uitmaken van de opgegeven Active Directory-organisatie-eenheid.	`ou IN ('RnD', 'Computers')`	Ja
Status			
`state`	Toestand van apparaat. Mogelijke waarden: • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`	`state = 'backup'`	Nee
status	Beveiligingsstatus. Mogelijke waarden: • `ok` • `warning` • `error` • `critical` • `protected` • `notProtected`	`status = 'ok'` `status IN ('error', 'warning')`	Nee
`protectedByPlan`	Apparaten die worden beschermd door een	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nee

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	beschermingsschema met een bepaalde id. Als u de schema-id wilt zien, selecteert u een schema in **Beheer** > **Beschermingsschema's**, klikt u op de balk in de kolom **Status** en klikt u vervolgens op de naam van de status. Er wordt een nieuwe zoekopdracht met de schema-id gemaakt.		
`okByPlan`	Apparaten die worden beschermd door een beschermingsschema met een bepaalde id en die de status **OK** hebben.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nee
`errorByPlan`	Apparaten die worden beschermd door een beschermingsschema met een bepaalde id en die de status **Fout** hebben.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nee
`warningByPlan`	Apparaten die worden beschermd door een beschermingsschema met een bepaalde id en die de status **Waarschuwing** hebben.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nee
`runningByPlan`	Apparaten die worden beschermd door een beschermingsschema met een bepaalde id en die de status **Wordt uitgevoerd** hebben.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nee
`interactionByPlan`	Apparaten die worden beschermd door een beschermingsschema met een bepaalde id en die de	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nee

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	status **Interactie vereist** hebben.		

`lastBackupTime`*	De datum en tijd van de laatste geslaagde back-up.
	De notatie is `'JJJJ-MM-DD UU:MM'`.
		`lastBackupTime > '2023-03-11'`
		`lastBackupTime <= '2023-03-11 00:15'`
		`lastBackupTime is null`
			Nee

`lastBackupTryTime`*	Het tijdstip van de laatste poging om een back-up te maken. De notatie is `'JJJJ-MM-DD UU:MM'`.	`lastBackupTryTime >= '2023-03-11'`	Nee
`nextBackupTime`*	Het tijdstip van de volgende back-up. De notatie is `'JJJJ-MM-DD UU:MM'`.	`nextBackupTime >= '2023-08-11'`	Nee

`lastVAScanTime`*	De datum en tijd van de laatst uitgevoerde evaluatie van beveiligingsproblemen.
	De notatie is `'JJJJ-MM-DD UU:MM'`.
		`lastVAScanTime > '2023-03-11'`
		`lastVAScanTime <= '2023-03-11 00:15'`
		`lastVAScanTime is null`
			Ja

`lastVAScanTryTime`*	Het tijdstip van de laatste poging om een evaluatie van beveiligingsproblemen uit te voeren. De notatie is `'JJJJ-MM-DD UU:MM'`.	`lastVAScanTimeTryTime >= '2022-03-11'`	Ja
`nextVAScanTime`*	Het tijdstip van de volgende evaluatie van beveiligingsproblemen. De notatie is `'JJJJ-MM-DD UU:MM'`.	`nextVAScanTime <= '2023-08-11'`	Ja
`network_status`	Status van de netwerkisolatie van Eindpuntdetectie en -	`network_status= 'connected'`	Ja

Kenmerk	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
	respons (EDR). Mogelijke waarden: • `connected` • `isolated`		

Opmerking
Als u uur en minuten overslaat, wordt de starttijd beschouwd als JJJJ-MM-DD 00:00 en wordt de eindtijd beschouwd als JJJJ-MM-DD 23:59:59. `lastBackupTime = 2023-01-20` betekent bijvoorbeeld dat de zoekresultaten alle back-ups bevatten van het interval tussen `lastBackupTime >= 2023-01-20 00:00` en `lastBackup time <= 2023-01-20 23:59:59`.

Zoekoperators

De volgende tabel bevat een overzicht van de beschikbare operators die u kunt gebruiken in uw zoekopdrachten.

U kunt meerdere operators gebruiken in één zoekopdracht.

Operator	Ondersteund voor	Betekenis	Voorbeelden
`AND`	Alle workloads	Operator voor logische samenvoeging	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Alle workloads	Operator voor logische scheiding	`state = 'backup' OR state = 'interactionRequired'`
`NOT`	Alle workloads	Operator voor logische negatie	`NOT(osProductType = 'workstation')`
`IN (<value1>,... <valueN>)`	Alle workloads	Deze operator wordt gebruikt om te controleren of een expressie overeenkomt met een waarde in een lijst met waarden.	`osType IN ('windows', 'linux')`
`NOT IN`	Alle workloads	Deze operator is het tegenovergestelde van de operator `IN`.	`NOT osType IN ('windows', 'linux')`
`LIKE 'wildcard`	Alle workloads	Deze operator wordt	`name LIKE 'en-00'`

Operator	Ondersteund voor	Betekenis	Voorbeelden

`pattern'`		gebruikt om te controleren of een expressie overeenkomt met het jokertekenpatroon.
		U kunt een van de volgende jokerteken-operators gebruiken:
		• * of % Het sterretje en het procentteken staan voor nul, één of meerdere tekens
		• _ Het onderstrepingsteken geeft een enkel teken aan
			`name LIKE '*en-00'`
			`name LIKE '*en-00*'`
			`name LIKE 'en-00_'`

`NOT LIKE 'wildcard pattern'`	Alle workloads	Deze operator is het tegenovergestelde van de operator `LIKE`.
		U kunt een van de volgende jokerteken-operators gebruiken:
		• * of % Het sterretje en het procentteken staan voor nul, één of meerdere tekens
		• _ Het onderstrepingsteken geeft een enkel teken aan
			`NOT name LIKE 'en-00'`
			`NOT name LIKE '*en-00'`
			`NOT name LIKE '*en-00*'`
			`NOT name LIKE 'en-00_'`

`RANGE (<starting_value>, <ending_value>)`	Alle workloads	Deze operator wordt gebruikt om te controleren of een expressie deel uitmaakt van een bereik van waarden (inbegrepen).
		Bij zoekopdrachten met alfanumerieke tekenreeksen wordt de ASCII-sorteervolgorde
			`ip RANGE ('10.250.176.1','10.250.176.50')`
			`name RANGE('a','d')`
			Met deze zoekopdracht kunt u alle namen filteren die beginnen met A, B en C, zoals `Alice`, `Bob` en `Claire`. Maar alleen de enkele letter D voldoet aan de eisen, dus namen met meer letters, zoals `Diana` of `Don` worden niet geretourneerd.

Operator	Ondersteund voor	Betekenis	Voorbeelden
		gebruikt, maar hoofdletters en kleine letters worden niet onderscheiden.	Voor hetzelfde resultaat kunt u ook de volgende zoekopdracht gebruiken: `name >= 'a' AND name <= 'd'`
= of ==	Alle workloads	Operator *Gelijk aan*	`osProductType = 'server'`
!= of <>	Alle workloads	Operator *Niet gelijk aan*	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
<	Niet-cloud-to-cloud workloads	Operator *Kleiner dan*	`memorySize < 1024`
>	Niet-cloud-to-cloud workloads	Operator *Groter dan*.	`diskSize > 300GB`
<=	Niet-cloud-to-cloud workloads	Operator *Kleiner dan of gelijk aan*	`lastBackupTime <= '2022-03-11 00:15'`
>=	Niet-cloud-to-cloud workloads	Operator *Groter dan of gelijk aan*	`nextBackupTime >= '2022-08-11'`

Een dynamische groep bewerken

U bewerkt een dynamische groep door de zoekopdracht te wijzigen die de groepsinhoud definieert.

In dynamische groepen die zijn gebaseerd op Active Directory, kunt u ook de Active Directory-groep wijzigen.

Een dynamische groep bewerken:

Door de zoekopdracht te wijzigen

1. Klik op **Apparaten**, navigeer naar de dynamische groep die u wilt bewerken en selecteer deze.
2. Klik op het tandwielpictogram naast de naam van de groep en klik vervolgens op **Bewerken**. U kunt ook op **Bewerken** klikken in het deelvenster **Acties**.
3. Wijzig de zoekopdracht door de zoekkenmerken, hun waarden of de zoekoperators aan te passen en klik vervolgens op **Zoeken**.
4. Klik op **Opslaan** naast het zoekveld.

Door de Active Directory-groep te wijzigen

Opmerking
Deze procedure is van toepassing op dynamische groepen die zijn gebaseerd op Active Directory. Dynamische groepen die zijn gebaseerd op Active Directory, zijn alleen beschikbaar in **Microsoft 365** > **Gebruikers**.

1. Klik op **Apparaten** en navigeer naar **Apparaten** > **Microsoft 365** > uw organisatie > **Gebruikers**.
2. Selecteer de dynamische groep die u wilt bewerken.
3. Klik op het tandwielpictogram naast de naam van de groep en klik vervolgens op **Bewerken**. U kunt ook op **Bewerken** klikken in het deelvenster **Acties**.
4. Wijzig de inhoud van de groep door een van de volgende handelingen uit te voeren:
   - Wijzig de reeds geselecteerde Active Directory-groep door op de naam ervan te klikken en vervolgens een nieuwe Active Directory-groep te selecteren in de lijst die wordt geopend.
   - Bewerk de zoekopdracht en klik vervolgens op **Zoeken**.
     De zoekopdracht is beperkt tot de geselecteerde Active Directory-groep.
5. Klik op **Opslaan** naast het zoekveld.

U kunt uw bewerkingen ook opslaan zonder de huidige groep te overschrijven. Als u de bewerkte configuratie wilt opslaan als nieuwe groep, klikt u op de pijlknop naast het zoekveld en vervolgens op **Opslaan als**.

Een groep verwijderen

Wanneer u een apparaatgroep verwijdert, worden alle schema's ingetrokken die op die groep zijn toegepast. De workloads in de groep zijn dan niet meer beschermd als er geen andere schema's op zijn toegepast.

Een apparaatgroep verwijderen:

1. Klik op **Apparaten** en navigeer naar de groep die u wilt verwijderen.
2. Klik op het tandwielpictogram naast de naam van de groep en klik vervolgens op **Verwijderen**.
3. Bevestig uw keuze door te klikken op **Verwijderen**.

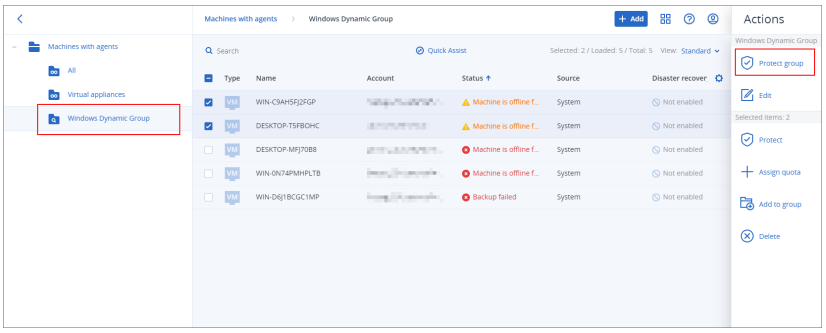
Een schema toepassen op een groep

U kunt een schema toepassen op een groep door eerst de groep te selecteren en vervolgens een schema toe te wijzen aan de groep.

U kunt ook een schema openen om het te bewerken en vervolgens een groep toevoegen aan het schema.

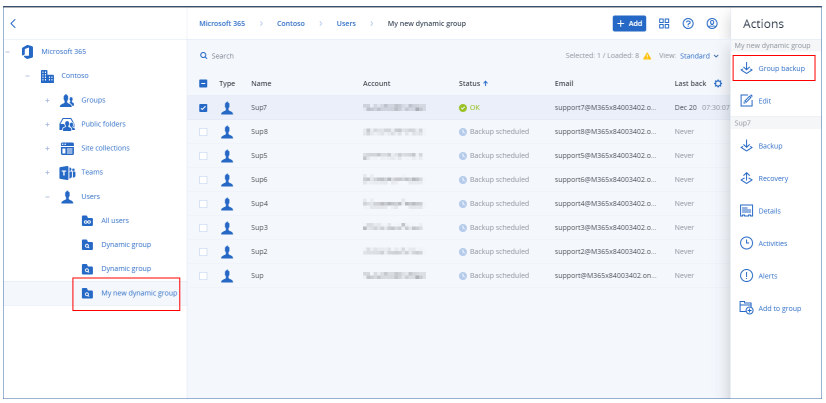
Een schema toepassen op een groep:

1. Klik op **Apparaten** en navigeer naar de groep waarop u een schema wilt toepassen.
2. [Voor niet-cloud-to-cloud workloads] Klik op **Groep beschermen**.



Er wordt een lijst weergegeven met schema's die kunnen worden toegepast.

3. [Voor cloud-to-cloud workloads] Klik op **Back-up van groep**.



Er wordt een lijst weergegeven met back-upschema's die kunnen worden toegepast.

4. [Een bestaand schema toepassen] Selecteer het schema en klik vervolgens op **Toepassen**.
5. [Een nieuw schema maken] Klik op **Schema maken**, selecteer het type schema en maak vervolgens het nieuwe schema.

   Zie "Ondersteunde schema's voor apparaatgroepen" (p. 329) voor meer informatie over de beschikbare typen schema's en hoe u deze kunt maken.

Opmerking
Back-upschema's die worden toegepast op cloud-to-cloud apparaatgroepen, worden volgens een vaste planning automatisch één keer per dag uitgevoerd. U kunt deze schema's niet op aanvraag uitvoeren door te klikken op **Nu uitvoeren**.

Een schema intrekken van een groep

U kunt een schema van een groep intrekken door eerst de groep te selecteren en vervolgens het schema van de groep in te trekken.

U kunt het schema ook openen om het te bewerken en vervolgens de groep eruit verwijderen.

Een schema intrekken van een groep:

1. Klik op **Apparaten** en navigeer naar de groep waarvoor u een abonnement wilt intrekken.
2. [Voor niet-cloud-to-cloud workloads] Klik op **Groep beschermen**.

   De beschermingsschema's die op de groep worden toegepast, worden weergegeven.

3. [Voor cloud-to-cloud workloads] Klik op **Back-up van groep**.
   U ziet dan de lijst met back-upschema's die kunnen worden toegepast op de groep.
4. Selecteer het schema dat u wilt intrekken.
5. [Voor niet-cloud-to-cloud workloads] Klik op het ellipspictogram (...) en klik vervolgens op **Intrekken**.
6. [Voor cloud-to-cloud workloads] Klik op het tandwielpictogram en klik vervolgens op **Intrekken**.

Werken met de module Apparaatbeheer

De apparaatbeheermodule[1], die deel uitmaakt van de beschermingsschema's van de Cyber Protection-service, maakt gebruik van een functionele subset van de agent voor preventie van gegevensverlies[2] op elke beschermde computer om ongeoorloofde toegang en verzending van gegevens via lokale computerkanalen te detecteren en te voorkomen. De module maakt gedetailleerde controle van diverse gegevenslekken mogelijk, waaronder gegevensuitwisseling via verwisselbare media, printers, virtuele en omgeleide apparaten en het Windows-klembord.

De module is beschikbaar voor de edities Cyber Protect Essentials, Cyber Protect Standard en Cyber Protect Advanced, die elk een licentie per workload hebben.

Opmerking
Voor de functies voor apparaatbeheer op Windows-machines moet Agent voor preventie van gegevensverlies zijn geïnstalleerd. Deze wordt automatisch geïnstalleerd voor beschermde workloads als de module **Apparaatbeheer** is ingeschakeld in de betreffende beschermingsschema's.

De apparaatbeheermodule maakt gebruik van de functies van de agent voor preventie van gegevensverlies[3] om contextuele controle af te dwingen over de toegang tot en overdracht van

[1]De apparaatbeheermodule, die deel uitmaakt van een beschermingsschema, maakt gebruik van een functionele subset van de agent voor preventie van gegevensverlies op elke beschermde computer om ongeoorloofde toegang en overdracht van gegevens via lokale computerkanalen te detecteren en te voorkomen. Dit geldt onder meer voor gebruikerstoegang tot randapparatuur en poorten, afdrukken van documenten, kopiëren/plakken van klembord, formatteren en uitwerpen van media en synchronisaties met lokaal aangesloten mobiele apparaten. De apparaatbeheermodule biedt gedetailleerde, contextuele controle over de typen apparaten en poorten waartoe gebruikers op de beschermde computer toegang hebben, en de acties die gebruikers op die apparaten kunnen uitvoeren.
[2]Een clientonderdeel van het systeem voor preventie van gegevensverlies dat de hostcomputer beschermt tegen ongeoorloofd gebruik, ongeoorloofde overdracht en ongeoorloofde opslag van vertrouwelijke, beschermde of gevoelige gegevens door een combinatie van context- en inhoudanalysetechnieken toe te passen en een centraal beheerd beleid voor preventie van gegevensverlies af te dwingen. Cyber Protection biedt een volledig functionele agent voor preventie van gegevensverlies. De functionaliteit van de agent op een beschermde computer is echter beperkt tot de reeks functies voor preventie van gegevensverlies waarvoor in Cyber Protection een licentie kan worden verkregen, en is afhankelijk van het beschermingsschema dat op die computer wordt toegepast.
[3]Een systeem van geïntegreerde technologieën en organisatorische maatregelen bedoeld om onopzettelijke of opzettelijke openbaarmaking van/toegang tot vertrouwelijke, beschermde of gevoelige gegevens door onbevoegde entiteiten buiten of binnen de organisatie, of de overdracht van dergelijke gegevens naar niet-vertrouwde omgevingen, te detecteren en voorkomen.

gegevens op de beschermde computer. Dit geldt onder meer voor gebruikerstoegang tot randapparatuur en poorten, afdrukken van documenten, kopiëren/plakken van klembord, formatteren en uitwerpen van media en synchronisaties met lokaal aangesloten mobiele apparaten. De agent voor preventie van gegevensverlies bevat een framework voor alle centrale beheer- en administratieonderdelen van de apparaatbeheermodule en moet daarom op elke computer worden geïnstalleerd die met deze module moet worden beschermd. De agent kan gebruikersacties toestaan, beperken of weigeren op basis van de instellingen voor apparaatbeheer in het beschermingsschema dat op de beschermde computer wordt toegepast.

Met de apparaatbeheermodule wordt de toegang tot diverse randapparaten geregeld, ongeacht of deze rechtstreeks op beschermde computers worden gebruikt of worden omgeleid in virtualisatieomgevingen die op beschermde computers worden gehost. De module herkent apparaten die zijn omgeleid in Microsoft Extern bureaublad-server, Citrix XenDesktop / XenApp / XenServer en VMware Horizon. Er kunnen ook gegevens worden gekopieerd tussen het klembord van het gastbesturingssysteem dat wordt uitgevoerd op VMware Workstation/Player, Oracle VM VirtualBox, of Windows Virtual PC, en het klembord van het hostbesturingssysteem dat wordt uitgevoerd op de beschermde computer.

De apparaatbeheermodule kan computers met de volgende besturingssystemen beschermen:

Apparaatbesturing

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

Opmerking
Agent voor preventie van gegevensverlies voor macOS ondersteunt alleen x64-processors. Apple silicon ARM-processors worden niet ondersteund.

Preventie van gegevensverlies

- Microsoft Windows 7 Service Pack 1 en later
- Microsoft Windows Server 2008 R2 en later

Opmerking
Agent voor preventie van gegevensverlies is een integraal onderdeel van Agent voor Mac en kan daarom worden geïnstalleerd op macOS-systemen die niet door de agent worden ondersteund. In dit geval zal de Cyber Protect-console aangeven dat Agent voor preventie van gegevensverlies is geïnstalleerd op de computer, maar de functie voor apparaatbeheer en preventie van gegevensverlies zal niet werken. De functie voor apparaatbeheer werkt alleen op macOS-systemen die worden ondersteund door Agent voor preventie van gegevensverlies.

Beperking voor het gebruik van de agent voor preventie van gegevensverlies met Hyper-V

Installeer Agent voor preventie van gegevensverlies niet op Hyper-V-hosts in Hyper-V-clusters vanwege eventuele crashes, vooral in Hyper-V-clusters met Cluster Shared Volumes (CSV).

Als u een van de volgende versies van Agent voor Hyper-V gebruikt, moet u Agent voor preventie van gegevensverlies handmatig verwijderen:

- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

Als u Agent voor preventie van gegevensverlies wilt verwijderen, voert u op de Hyper-V-host het installatieprogramma handmatig uit en schakelt u het selectievakje Agent voor preventie van gegevensverlies uit. U kunt ook de volgende opdracht uitvoeren:

```
<installer_name> --remove-components=agentForDlp -quiet
```

U kunt de module voor apparaatbeheer inschakelen en configureren in het gedeelte **Apparaatbeheer** van uw beschermingsschema in de Cyber Protect-console. Zie stappen om apparaatbeheer in of uit te schakelen voor instructies.

Het gedeelte **Apparaatbeheer** bevat een overzicht van de configuratie van de module:

- Toegangsinstellingen: Toont een overzicht van apparaattypen en poorten met beperkte toegang (geweigerd of alleen-lezen), indien van toepassing. Anders wordt hier aangegeven dat alle apparaattypen zijn toegestaan. Klik op dit overzicht om de toegangsinstellingen te bekijken of te wijzigen (zie stappen om de toegangsinstellingen te bekijken of te wijzigen).
- Acceptatielijst voor apparaattypen: Geeft aan hoeveel apparaatsubklassen zijn toegestaan doordat ze zijn uitgesloten van het apparaattoegangsbeheer, indien van toepassing. Anders wordt hier aangegeven dat de acceptatielijst leeg is. Klik op dit overzicht om de selectie van toegestane apparaatsubklassen te bekijken of te wijzigen (zie stappen om apparaatsubklassen uit te sluiten van toegangsbeheer).
- Acceptatielijst voor USB-apparaten: Geeft aan hoeveel USB-apparaten/modellen zijn toegestaan doordat ze zijn uitgesloten van het apparaattoegangsbeheer, indien van toepassing. Anders wordt hier aangegeven dat de acceptatielijst leeg is. Klik op dit overzicht om de lijst met toegestane USB-apparaten/modellen te bekijken of te wijzigen (zie stappen om afzonderlijke USB-apparaten uit te sluiten van toegangsbeheer).
- Uitsluitingen: Geeft aan hoeveel uitsluitingen voor toegangsbeheer zijn ingesteld voor Windows-klembord, schermopname, printers en mobiele apparaten.

Apparaatbeheer gebruiken

Dit gedeelte bevat stapsgewijze instructies voor basistaken bij het gebruik van de apparaatbeheermodule.

Apparaatbeheer inschakelen of uitschakelen

U kunt apparaatbeheer inschakelen wanneer u een beschermingsschema maakt. U kunt een bestaand beschermingsschema wijzigen om apparaatbeheer in of uit te schakelen.

Apparaatbeheer inschakelen of uitschakelen

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Voer een van de volgende handelingen uit om het deelvenster voor het beschermingsschema te openen:
   - Als u een nieuw beschermingsschema wilt maken, selecteert u een machine om te beschermen en klikt u vervolgens op **Beschermen** en op **Schema maken**.
   - Als u een bestaand beschermingsschema wilt wijzigen, selecteert u een beschermde machine, klikt u op **Beschermen**, klikt u op de ellips (...) naast de naam van het beschermingsschema en klikt u vervolgens op **Bewerken**.
3. Ga in het deelvenster voor het beschermingsschema naar het gebied **Apparaatbeheer** en schakel de optie **Apparaatbeheer** in of uit.
4. Voer een van de volgende handelingen uit om uw wijzigingen door te voeren:
   - Als u een beschermingsschema maakt, klikt u op **Maken**.
   - Als u een beschermingsschema bewerkt, klikt u op **Opslaan**.

Indien gewenst, kunt u het deelvenster voor het beschermingsschema ook openen vanaf het tabblad Beheer. Deze mogelijkheid is echter niet beschikbaar in alle edities van de Cyber Protection-service.

Het gebruik van de apparaatbeheermodule inschakelen op macOS

De instellingen voor apparaatbeheer van een beschermingsschema worden pas van kracht nadat het stuurprogramma voor apparaatbeheer op de beschermde workload is geladen. In dit gedeelte wordt beschreven hoe het stuurprogramma voor apparaatbeheer moet worden geladen om het gebruik van de apparaatbeheermodule op macOS mogelijk te maken. Dit is een eenmalige operatie waarvoor beheerdersrechten op de eindpuntmachine zijn vereist.

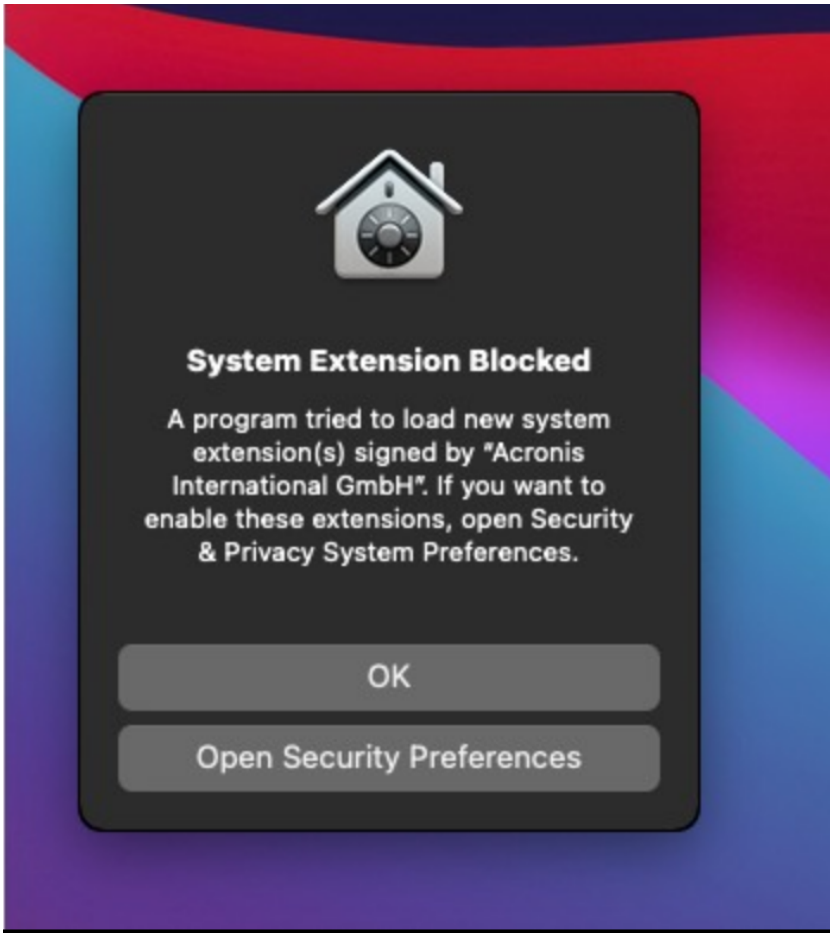
Ondersteunde macOS-versies:

- macOS 10.15 (Catalina) en later
- macOS 11.2.3 (Big Sur) en later
- macOS 12.2 (Monterey) en later
- macOS 13.2 (Ventura) en later

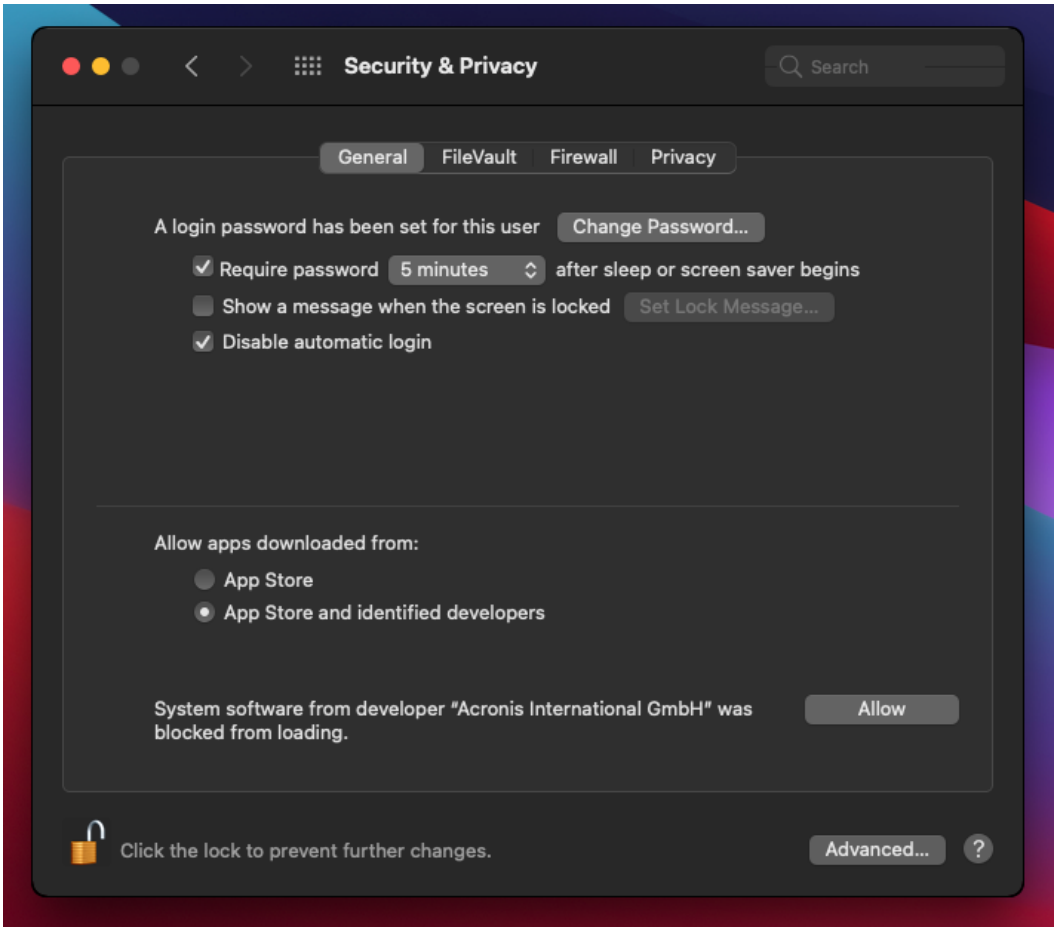
Het gebruik van de apparaatbeheermodule inschakelen op macOS

1. Installeer Agent voor Mac op de machine die u wilt beschermen.
2. Schakel de instellingen voor apparaatbeheer in het beschermingsschema in.
3. Pas het beschermingsschema toe.

4. De waarschuwing 'Systeemuitbreiding geblokkeerd' wordt weergegeven op de beschermde workload. Klik op **Beveiligingsvoorkeuren openen**.



5. In het deelvenster **Beveiliging en Privacy** dat wordt weergegeven, selecteert u **App Store en geïdentificeerde ontwikkelaars** en klikt u vervolgens op **Toestaan**.



6. In het dialoogvenster dat wordt weergegeven, klikt u op **Opnieuw starten** om de workload opnieuw te starten en de instellingen voor apparaatbeheer te activeren.

Opmerking
U hoeft deze stappen niet te herhalen als de instellingen voor apparaatbeheer zijn uitgeschakeld en vervolgens weer ingeschakeld.

Toegangsinstellingen bekijken of wijzigen

U kunt de toegangsinstellingen voor de apparaatbeheermodule beheren vanuit het deelvenster voor het beschermingsschema. Op die manier kunt u de toegang tot bepaalde soorten apparaten toestaan of weigeren, en meldingen en waarschuwingen in- of uitschakelen.

Toegangsinstellingen bekijken of wijzigen

1. Open het deelvenster voor het beschermingsschema en schakel apparaatbeheer in dat schema in (zie stappen om apparaatbeheer in of uit te schakelen).
2. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de link naast **Toegangsinstellingen**.

3. Op de pagina voor het beheer van toegangsinstellingen die wordt weergegeven, bekijkt of wijzigt u de toegangsinstellingen, al naargelang wat u wilt doen.

Opmerking
De toegangsinstellingen die zijn geconfigureerd in Apparaatbeheer, kunnen worden overschreven als zowel Apparaatbeheer als Advanced DLP wordt gebruikt om een workload te beschermen. Zie "Advanced Data Loss Prevention inschakelen in beschermingsschema's" (p. 927).

Meldingen en servicewaarschuwingen van het besturingssysteem inschakelen of uitschakelen

Bij het beheer van de toegangsinstellingen kunt u Meldingen en servicewaarschuwingen van het besturingssysteem inschakelen of uitschakelen. Deze meldingen en waarschuwingen informeren de gebruiker over pogingen om acties uit te voeren die niet zijn toegestaan.

Melding van besturingssysteem inschakelen of uitschakelen

1. Volg de stappen om de toegangsinstellingen te bekijken of te wijzigen.
2. Op de pagina voor het beheer van toegangsinstellingen ziet u het selectievakje **Melding van het besturingssysteem voor eindgebruikers als ze proberen een geblokkeerd apparaattype of geblokkeerde poort te gebruiken**. U kunt dit selectievakje inschakelen of uitschakelen.

Catalogisering inschakelen of uitschakelen

1. Volg de stappen om de toegangsinstellingen te bekijken of te wijzigen.
2. Op de pagina voor het beheer van de toegangsinstellingen schakelt u het selectievakje **Waarschuwing weergeven** in of uit voor het gewenste apparaattype/de gewenste apparaattypen.

Het selectievakje **Waarschuwing weergeven** is alleen beschikbaar voor apparaattypen met beperkte toegang (Alleen-lezen of Toegang geweigerd), behalve schermopname.

Apparaatsubklassen uitsluiten van toegangsbeheer

In het deelvenster voor het beschermingsschema kunt u de subklassen van apparaten kiezen die u wilt uitsluiten van het toegangsbeheer. Daardoor wordt toegang tot die apparaten toegestaan, ongeacht de toegangsinstellingen van het apparaatbeheer.

Subklassen van apparaten uitsluiten van toegangsbeheer

1. Open het deelvenster voor het beschermingsschema en schakel apparaatbeheer in dat schema in (zie stappen om apparaatbeheer in of uit te schakelen).
2. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de link naast **Acceptatielijst voor apparaattypen**.
3. Op de pagina voor het beheer van de acceptatielijst die wordt weergegeven, kunt u de selectie bekijken of wijzigen van de apparaatsubklassen die u wilt uitsluiten van het toegangsbeheer.

Afzonderlijke USB-apparaten uitsluiten van toegangsbeheer

In het deelvenster voor het beschermingsschema kunt u de afzonderlijke USB-apparaten of USB-apparaatmodellen opgeven die u wilt uitsluiten van het toegangsbeheer. Daardoor wordt toegang tot die apparaten toegestaan, ongeacht de toegangsinstellingen van het apparaatbeheer.

Een USB-apparaat uitsluiten van toegangsbeheer

1. Open het deelvenster voor het beschermingsschema en schakel apparaatbeheer in dat schema in (zie stappen om apparaatbeheer in of uit te schakelen).
2. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de link naast **Acceptatielijst voor USB-apparaten**.
3. Op de pagina voor het beheer van de acceptatielijst die wordt weergegeven, klikt u op **Toevoegen vanuit database**.
4. Op de pagina voor het selecteren van USB-apparaten die wordt weergegeven, selecteert u de gewenste apparaten die zijn geregistreerd in de database van USB-apparaten.
5. Klik op de knop **Toevoegen aan acceptatielijst**.

Een USB-apparaat niet meer uitsluiten van toegangsbeheer

1. Open het deelvenster voor het beschermingsschema en schakel apparaatbeheer in dat schema in (zie stappen om apparaatbeheer in of uit te schakelen).
2. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de link naast **Acceptatielijst voor USB-apparaten**.
3. Op de pagina voor het beheer van de acceptatielijst die wordt weergegeven, klikt u op het pictogram Verwijderen aan het einde van het lijstitem voor het gewenste USB-apparaat.

USB-apparaten toevoegen aan of verwijderen uit de database

Als u een bepaald USB-apparaat wilt uitsluiten van toegangsbeheer, moet u het toevoegen aan de database van USB-apparaten. Vervolgens kunt u apparaten toevoegen aan de acceptatielijst door ze te selecteren in die database.

De volgende procedures zijn van toepassing op beschermingsschema's waarvoor de functie voor apparaatbeheer is ingeschakeld.

USB-apparaten toevoegen aan de database

1. Open het beschermingsschema van een apparaat om dit te bewerken:
   Klik op de ellips (...) naast de naam van het beschermingsschema en selecteer **Bewerken**.

   Opmerking
   Apparaatbeheer moet zijn ingeschakeld in het schema, zodat u toegang krijgt tot de instellingen voor apparaatbeheer.

2. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de link naast **Acceptatielijst voor USB-apparaten**.

3. Op de pagina met de **acceptatielijst voor USB-apparaten** die wordt weergegeven, klikt u op **Toevoegen vanuit database**.
4. Op de pagina voor beheer van de database van USB-apparaten die wordt weergegeven, klikt u op **Toevoegen aan database**.
5. In het dialoogvenster **USB-apparaat toevoegen** dat wordt weergegeven, klikt u op de machine waarop het USB-apparaat is aangesloten.
   Alleen machines die online zijn, worden weergegeven in de lijst met computers.
   De lijst met USB-apparaten wordt alleen weergegeven voor machines waarop de agent voor de preventie van gegevensverlies is geïnstalleerd.
   De USB-apparaten worden weergegeven in een boomstructuur. Het eerste niveau van de boom komt overeen met een apparaatmodel. Het tweede niveau komt overeen met een specifiek apparaat van dat model.
   Een blauw pictogram naast de beschrijving van het apparaat geeft aan dat het apparaat momenteel is aangesloten op de computer. Als het apparaat niet op de computer is aangesloten, wordt het pictogram grijs weergegeven.
6. Schakel de selectievakjes in voor de USB-apparaten die u wilt toevoegen aan de database, en klik vervolgens op **Toevoegen aan database**.
   De geselecteerde USB-apparaten worden toegevoegd aan de database.
7. Sluit het beschermingsschema of sla het op.

USB-apparaten toevoegen aan de database vanuit het deelvenster met computergegevens

Opmerking
Deze procedure is alleen van toepassing op apparaten die online zijn en waarop de agent voor de preventie van gegevensverlies is geïnstalleerd. U kunt de lijst met USB-apparaten niet weergeven voor een computer die offline is of waarop de agent voor de preventie van gegevensverlies niet is geïnstalleerd.

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer een computer waarop het gewenste USB-apparaat ooit is aangesloten, en klik vervolgens in het menu rechts op **Inventaris**.
   Het deelvenster met computergegevens wordt geopend.
3. Klik in het deelvenster met computergegevens op het tabblad **USB-apparaten**.
   De lijst met USB-apparaten die bekend zijn op de geselecteerde computer, wordt geopend.
   De USB-apparaten worden weergegeven in een boomstructuur. Het eerste niveau van de boom komt overeen met een apparaatmodel. Het tweede niveau komt overeen met een specifiek apparaat van dat model.
   Een blauw pictogram naast de beschrijving van het apparaat geeft aan dat het apparaat momenteel is aangesloten op de computer. Als het apparaat niet op de computer is aangesloten, wordt het pictogram grijs weergegeven.
4. Schakel de selectievakjes in voor de USB-apparaten die u wilt toevoegen aan de database, en klik vervolgens op **Toevoegen aan database**.

USB-apparaten toevoegen aan de database vanuit servicewaarschuwingen

1. Ga in de Cyber Protect-console naar **Controle** > **Waarschuwingen**.
2. Zoek een waarschuwing van apparaatbeheer over het weigeren van toegang tot het USB-apparaat.
3. Klik in de eenvoudige weergave van de waarschuwing op **Dit USB-apparaat toestaan**.
   Hierdoor wordt het USB-apparaat uitgesloten van toegangsbeheer en wordt het voor later gebruik toegevoegd aan de database.

USB-apparaten toevoegen door een lijst met apparaten te importeren in de database

U kunt een JSON-bestand met een lijst met USB-apparaten importeren in de database. Zie "Een lijst met USB-apparaten importeren in de database" (p. 375).

USB-apparaten verwijderen uit de database

1. Open het beschermingsschema van een apparaat om dit te bewerken:
   Klik op de ellips (...) naast de naam van het beschermingsschema en selecteer **Bewerken**.

   Opmerking
   Apparaatbeheer moet zijn ingeschakeld in het schema, zodat u toegang krijgt tot de instellingen voor apparaatbeheer.

2. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de rij **Accceptatielijst voor USB-apparaten**.
3. Op de pagina voor het beheer van de acceptatielijst die wordt weergegeven, klikt u op **Toevoegen vanuit database**.
4. Klik op de pagina voor het selecteren van USB-apparaten uit de database op de ellips (...) aan het einde van het lijstitem voor het betreffende apparaat, klik vervolgens op **Verwijderen** en bevestig dat u wilt verwijderen.
   De USB-apparaten worden verwijderd uit de database.
5. Sluit het beschermingsschema of sla het op.

Waarschuwingen van apparaatbeheer bekijken

De apparaatbeheermodule kan worden geconfigureerd om waarschuwingen te genereren wanneer pogingen van een gebruiker om bepaalde apparaattypen te gebruiken worden geweigerd (zie Meldingen en servicewaarschuwingen van het besturingssysteem inschakelen of uitschakelen). Gebruik de volgende stappen om die waarschuwingen te bekijken.

Waarschuwingen van apparaatbeheer bekijken

1. Ga in de Cyber Protect-console naar **Controle** > **Waarschuwingen**.
2. Zoek waarschuwingen met de volgende status: 'Toegang tot randapparaat is geblokkeerd'.

Zie Waarschuwingen van apparaatbeheer voor meer informatie.

Toegangsinstellingen

Op de pagina **Toegangsinstellingen** kunt u toegang tot bepaalde typen apparaten toestaan of weigeren, en meldingen van het besturingssysteem en waarschuwingen van apparaatbeheer inschakelen of uitschakelen.

Opmerking
De toegangsinstellingen die zijn geconfigureerd in Apparaatbeheer, kunnen worden overschreven als zowel Apparaatbeheer als Advanced DLP wordt gebruikt om een workload te beschermen. Zie "Advanced Data Loss Prevention inschakelen in beschermingsschema's" (p. 927).

Met de toegangsinstellingen kunt u de toegang van gebruikers tot de volgende apparaattypen en poorten beperken:

- **Verwisselbaar** (toegangsbeheer per type apparaat): Apparaten met een willekeurige interface voor aansluiting op een computer (USB, FireWire, PCMCIA, IDE, SATA, SCSI, enz.) die door het besturingssysteem worden herkend als verwisselbare opslagapparaten (bijvoorbeeld USB-sticks, kaartlezers, magneto-optische stations, enz.). In het apparaatbeheer worden alle harde schijven die zijn aangesloten via USB, FireWire en PCMCIA, geclassificeerd als verwisselbare apparaten. Sommige harde schijven (meestal met SATA en SCSI) worden ook geclassificeerd als verwisselbare apparaten als ze de hot-plug-functie ondersteunen en geen actief besturingssysteem bevatten.

  U kunt volledige of alleen-lezen toegang toestaan of de toegang tot verwisselbare apparaten weigeren. Zo kunt u het kopiëren van gegevens van en naar elk verwisselbaar apparaat beheren op een beschermde computer. Toegangsrechten zijn niet van invloed op apparaten die zijn versleuteld met BitLocker of FileVault (alleen HFS+-bestandssysteem).

  Dit apparaattype wordt ondersteund op zowel Windows als macOS.
- **Versleuteld verwisselbaar** (toegangsbeheer per apparaattype): Verwisselbare apparaten die zijn versleuteld met BitLocker-stationsversleuteling (op Windows) of FileVault-stationsversleuteling (op macOS).

  Op macOS worden alleen versleutelde verwisselbare stations met het HFS+-bestandssysteem ondersteund (ook wel HFS Plus of Mac OS Extended of HFS Extended genoemd). Versleutelde verwisselbare stations die gebruikmaken van het APFS-bestandssysteem, worden behandeld als verwisselbare stations.

  U kunt volledige of alleen-lezen toegang toestaan of de toegang tot versleutelde verwisselbare apparaten weigeren. Zo kunt u het kopiëren van gegevens van en naar elk versleuteld verwisselbaar apparaat beheren op een beschermde computer. Toegangsrechten zijn alleen van invloed op apparaten die zijn versleuteld met BitLocker of FileVault (alleen HFS+-bestandssysteem).

  Dit apparaattype wordt ondersteund op zowel Windows als macOS.
- **Printers** (toegangsbeheer per type apparaat): Fysieke printers met een willekeurige interface voor aansluiting op een computer (USB, LPT, Bluetooth, enz.) en printers die toegankelijk zijn

vanaf een computer in het netwerk.

U kunt toegang tot printers toestaan of weigeren. Zo kunt u het afdrukken van documenten op printers beheren op een beschermde computer.

Opmerking

Wanneer u de toegangsinstelling voor printers wijzigt in **Weigeren**, moeten de toepassingen en processen die toegang hebben tot de printers, opnieuw worden opgestart om de nieuw geconfigureerde toegangsinstellingen af te dwingen. Start de beschermde workloads opnieuw op om te controleren of de toegangsinstellingen correct worden afgedwongen.

Dit apparaattype wordt alleen ondersteund op Windows.

- **Klembord** (toegangsbeheer per apparaattype): Windows-klembord.

  U kunt de toegang tot het klembord toestaan of weigeren. Zo kunt u het kopiëren/plakken via het Windows-klembord beheren op een beschermde computer.

  Opmerking

  Wanneer u de toegangsinstelling voor het klembord wijzigt in **Weigeren**, moeten de toepassingen en processen die toegang hebben tot het klembord, opnieuw worden opgestart om de nieuw geconfigureerde toegangsinstellingen af te dwingen. Start de beschermde workloads opnieuw op om te controleren of de toegangsinstellingen correct worden afgedwongen.

  Dit apparaattype wordt alleen ondersteund op Windows.

- **Schermopname** (toegangsbeheer per apparaattype): maakt schermopnamen van het volledige scherm, het actieve venster of een geselecteerd deel van het scherm mogelijk.

  U kunt de toegang tot de schermopname toestaan of weigeren. Zo kunt u schermopnamen beheren op een beschermde computer.

  Opmerking

  Wanneer u de toegangsinstelling voor schermopname wijzigt in **Weigeren**, moeten de toepassingen en processen die toegang hebben tot de schermopname, opnieuw worden opgestart om de nieuw geconfigureerde toegangsinstellingen af te dwingen. Start de beschermde workloads opnieuw op om te controleren of de toegangsinstellingen correct worden afgedwongen.

  Dit apparaattype wordt alleen ondersteund op Windows.

- **Mobiele apparaten** (toegangsbeheer per apparaattype): Apparaten (zoals Android-smartphones, enz.) die met een computer communiceren via het Media Transfer Protocol (MTP), ongeacht de interface voor aansluiting op een computer (USB, IP, Bluetooth).

  U kunt volledige of alleen-lezen toegang toestaan of de toegang tot mobiele apparaten weigeren. Zo kunt u het kopiëren van gegevens naar en van elk mobiel apparaat met MTP beheren op een beschermde computer.

Opmerking

Wanneer u de toegangsinstelling voor mobiele apparaten wijzigt in **Alleen-lezen** of **Weigeren**, moeten de toepassingen en processen die toegang hebben tot de mobiele apparaten, opnieuw worden opgestart om de nieuw geconfigureerde toegangsinstellingen af te dwingen. Start de beschermde workloads opnieuw op om te controleren of de toegangsinstellingen correct worden afgedwongen.

Dit apparaattype wordt alleen ondersteund op Windows.

- **Bluetooth** (toegangsbeheer per type apparaat): Externe en interne Bluetooth-apparaten met een willekeurige interface voor aansluiting op een computer (USB, PCMCIA, enz.). Met deze instelling wordt het gebruik van de apparaten van dit type geregeld, niet de gegevensuitwisseling via dergelijke apparaten.

  U kunt toegang tot Bluetooth toestaan of weigeren. Zo kunt u het gebruik van Bluetooth-apparaten beheren op een beschermde computer.

  Opmerking

  Op macOS zijn de toegangsrechten voor Bluetooth niet van invloed op Bluetooth HID-apparaten. De toegang tot deze apparaten wordt altijd toegestaan om te voorkomen dat draadloze HID-apparaten (muizen en toetsenborden) worden uitgeschakeld op iMac- en Mac Pro-hardware.

  Dit apparaattype wordt ondersteund op zowel Windows als macOS.
- **Optische stations** (toegangsbeheer per type apparaat): Externe en interne cd/dvd/bd-stations (inclusief schrijvers) met een willekeurige interface voor aansluiting op een computer (IDE, SATA, USB, FireWire, PCMCIA, enz.).

  U kunt volledige of alleen-lezen toegang toestaan of de toegang tot optische stations weigeren. Zo kunt u het kopiëren van gegevens naar en van elk optisch station beheren op een beschermde computer.

  Dit apparaattype wordt ondersteund op zowel Windows als macOS.
- **Diskettestations** (toegangsbeheer per type apparaat): Externe en interne diskettestations met een willekeurige interface voor aansluiting op een computer (IDE, USB, PCMCIA, enz.). Bepaalde modellen diskettestations worden door het besturingssysteem herkend als verwisselbare stations. In dat geval worden deze stations ook door het apparaatbeheer aangemerkt als verwisselbare apparaten.

  U kunt volledige of alleen-lezen toegang toestaan of de toegang tot diskettestations weigeren. Zo kunt u het kopiëren van gegevens naar en van elk diskettestation beheren op een beschermde computer.

  Dit apparaattype wordt alleen ondersteund op Windows.
- **USB** (toegangsbeheer per apparaatinterface): Alle apparaten die op een USB-poort zijn aangesloten, behalve hubs.

  U kunt volledige of alleen-lezen toegang toestaan of de toegang tot USB-poorten weigeren. Zo kunt u het kopiëren van gegevens beheren naar en van apparaten die zijn aangesloten op een USB-poort op een beschermde computer.

Dit apparaattype wordt ondersteund op zowel Windows als macOS.

- **FireWire** (toegangsbeheer per apparaatinterface): Alle apparaten die zijn aangesloten op een FireWire-poort (IEEE 1394), behalve hubs.

  U kunt volledige of alleen-lezen toegang toestaan of de toegang tot FireWire-poorten weigeren. Zo kunt u het kopiëren van gegevens beheren naar en van apparaten die zijn aangesloten op een FireWire-poort op een beschermde computer.

  Dit apparaattype wordt ondersteund op zowel Windows als macOS.
- **Omgeleide apparaten** (toegangsbeheer per apparaatinterface): Toegewezen schijven (harde schijven, verwisselbare en optische stations), USB-apparaten en het klembord omgeleid naar sessies van virtuele toepassingen/bureaubladen.

  Apparaatbeheer herkent apparaten die worden omgeleid via protocollen voor externe communicatie (Microsoft RDP, Citrix ICA, VMware PCoIP en HTML5/WebSockets) in de virtualisatieomgevingen Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer en VMware Horizon die worden gehost op beschermde Windows-computers. Met apparaatbeheer kunnen ook gegevens worden gekopieerd tussen het Windows-klembord van het gastbesturingssysteem op VMware Workstation, VMware Player, Oracle VM VirtualBox of Windows Virtual PC en het klembord van het hostbesturingssysteem op een beschermde Windows-computer.

  Dit apparaattype wordt alleen ondersteund op Windows.

  U kunt de toegang tot omgeleide apparaten als volgt configureren:

  - **Toegewezen stations**: U kunt volledige of alleen-lezen toegang toestaan of de toegang weigeren. Zo kunt u het kopiëren van gegevens beheren naar en van elke harde schijf, verwisselbare schijf of optische schijf die wordt omgeleid naar de sessie op een beschermde computer.
  - **Klembord van inkomende gegevens**: U kunt de toegang toestaan of weigeren. Zo kunt u het kopiëren van gegevens via het klembord naar de sessie op een beschermde computer beheren.

    Opmerking
    Wanneer u de toegangsinstelling voor het klembord van inkomende gegevens wijzigt in **Weigeren**, moeten de toepassingen en processen die toegang hebben tot het klembord, opnieuw worden opgestart om de nieuw geconfigureerde toegangsinstellingen af te dwingen. Start de beschermde workloads opnieuw op om te controleren of de toegangsinstellingen correct worden afgedwongen.

  - **Klembord van uitgaande gegevens**: U kunt de toegang toestaan of weigeren. Zo kunt u het kopiëren van gegevens via het klembord vanuit de sessie op een beschermde computer beheren.

Opmerking
Wanneer u de toegangsinstelling voor het klembord van uitgaande gegevens wijzigt in **Weigeren**, moeten de toepassingen en processen die toegang hebben tot het klembord, opnieuw worden opgestart om de nieuw geconfigureerde toegangsinstellingen af te dwingen. Start de beschermde workloads opnieuw op om te controleren of de toegangsinstellingen correct worden afgedwongen.

- **USB-poorten**: U kunt de toegang toestaan of weigeren. Zo kunt u het kopiëren van gegevens beheren naar en van apparaten die zijn aangesloten op een USB-poort die wordt omgeleid naar de sessie op een beschermde computer.

Instellingen voor apparaatbeheer hebben op alle gebruikers dezelfde invloed. Als u bijvoorbeeld de toegang tot verwisselbare apparaten weigert, voorkomt u dat een gebruiker gegevens kopieert naar en van dergelijke apparaten op een beschermde computer. U kunt selectief toegang te verlenen tot afzonderlijke USB-apparaten door ze uit te sluiten van toegangsbeheer (zie Acceptatielijst voor apparaattypen en Acceptatielijst voor USB-apparaten).

Wanneer de toegang tot een apparaat zowel per type als per interface wordt beheerd, heeft het weigeren van toegang op interfaceniveau voorrang. Als bijvoorbeeld de toegang tot USB-poorten wordt geweigerd (apparaatinterface), dan wordt ook de toegang geweigerd tot mobiele apparaten die zijn aangesloten op een USB-poort, ongeacht of de toegang tot mobiele apparaten is toegestaan of geweigerd (apparaattype). Als u toegang wilt verlenen tot een dergelijk apparaat, moet u zowel de interface als het type toestaan.

Opmerking
Als het beschermingsschema dat op macOS wordt gebruikt, instellingen bevat voor apparaattypen die alleen op Windows worden ondersteund, dan worden de instellingen voor deze apparaattypen op macOS genegeerd.

Belangrijk
Wanneer een verwisselbaar apparaat, een versleuteld verwisselbaar apparaat, een printer of een Bluetooth-apparaat is aangesloten op een USB-poort, heeft het toestaan van toegang tot dat apparaat voorrang boven de toegangsweigering die is ingesteld voor de USB-interface. Als u een dergelijk apparaattype toestaat, wordt de toegang tot het apparaat toegestaan, ongeacht of de toegang tot de USB-poort wordt geweigerd.

Meldingen en servicewaarschuwingen van het besturingssysteem

U kunt apparaatbeheer configureren om een melding van het besturingssysteem weer te geven voor eindgebruikers als ze proberen een geblokkeerd apparaattype te gebruiken op beschermde computers. Wanneer het selectievakje **Melding van het besturingssysteem weergeven voor eindgebruikers als ze proberen een geblokkeerd apparaattype of geblokkeerde poort te gebruiken** is ingeschakeld in de toegangsinstellingen, geeft de agent een pop-upbericht weer in het

meldingsgebied van de beschermde computer als zich een van de volgende gebeurtenissen voordoet:

- Een geweigerde poging om een apparaat op een USB- of FireWire-poort te gebruiken. Deze melding wordt weergegeven wanneer de gebruiker een USB- of FireWire-apparaat aansluit dat is geweigerd op interfaceniveau (bijvoorbeeld wanneer de toegang tot de USB-poort wordt geweigerd) of vanwege het type (bijvoorbeeld wanneer het gebruik van verwisselbare apparaten wordt geweigerd). Deze melding geeft aan dat de gebruiker geen toegangsrechten heeft voor het opgegeven apparaat/station.
- Een geweigerde poging om een gegevensobject (zoals een bestand) te kopiëren vanaf een bepaald apparaat. Deze melding wordt weergegeven wanneer leestoegang wordt geweigerd voor de volgende apparaten: diskettestations, optische stations, verwisselbare apparaten, versleutelde verwisselbare apparaten, mobiele apparaten, omgeleide toegewezen stations, en inkomende gegevens van het omgeleide klembord. De melding geeft aan dat de gebruiker het opgegeven gegevensobject niet mag ophalen van het opgegeven apparaat.

  De melding 'lezen geweigerd' wordt ook weergegeven bij het weigeren van lees-/schrijftoegang tot Bluetooth of een FireWire-poort, USB-poort of omgeleide USB-poort.
- Een geweigerde poging om een gegevensobject (zoals een bestand) te kopiëren naar een bepaald apparaat. Deze melding wordt weergegeven wanneer schrijftoegang wordt geweigerd voor de volgende apparaten: diskettestations, optische stations, verwisselbare apparaten, versleutelde verwisselbare apparaten, mobiele apparaten, lokaal klembord, schermopname, printers, omgeleide toegewezen stations, en uitgaande gegevens van het omgeleide klembord. Deze melding geeft aan dat de gebruiker geen rechten heeft om het opgegeven gegevensobject te verzenden naar het opgegeven apparaat.

Pogingen van gebruikers om toegang te krijgen tot geblokkeerde apparaattypen op beschermde computers kunnen waarschuwingen genereren die worden geregistreerd in de Cyber Protect-console. U kunt waarschuwingen voor elk apparaattype (behalve schermopname) of elke poort afzonderlijk inschakelen door het selectievakje **Waarschuwing weergeven** in te schakelen in de toegangsinstellingen. Als bijvoorbeeld de toegang tot verwisselbare apparaten is beperkt tot alleen-lezen en het selectievakje **Waarschuwing weergeven** is ingeschakeld voor dat apparaattype, wordt er een waarschuwing geregistreerd telkens wanneer een gebruiker op een beschermde computer probeert gegevens te kopiëren naar een verwisselbaar apparaat. Zie Waarschuwingen van apparaatbeheer voor meer informatie.

Zie ook Stappen om meldingen en servicewaarschuwingen van het besturingssysteem in of uit te schakelen.

Acceptatielijst voor apparaattypen

Op de pagina **Acceptatielijst voor apparaattypen** kunt u apparaatsubklassen kiezen die u wilt uitsluiten van het apparaattoegangsbeheer. Daardoor wordt toegang tot die apparaten toegestaan, ongeacht de toegangsinstellingen in de apparaatbeheermodule.

De apparaatbeheermodule biedt de mogelijkheid om toegang te verlenen tot apparaten van bepaalde subklassen binnen een geweigerd apparaattype. Met deze optie kunt u alle apparaten van een bepaald type weigeren, behalve sommige subklassen van apparaten van dit type. Dit kan bijvoorbeeld nuttig zijn wanneer u de toegang tot alle USB-poorten wilt blokkeren, maar tegelijkertijd het gebruik van een USB-toetsenbord en -muis wilt toestaan.

Bij het configureren van de apparaatbeheermodule kunt u opgeven welke apparaatsubklassen u wilt uitsluiten van het apparaattoegangsbeheer. Wanneer een apparaat tot een uitgesloten subklasse behoort, wordt de toegang tot dat apparaat toegestaan, ongeacht of het apparaattype of de poort al dan niet wordt geweigerd. U kunt de volgende apparaatsubklassen selectief uitsluiten van het apparaattoegangsbeheer:

- **USB HID (muis, toetsenbord, enz.)**: Wanneer u dit selecteert, wordt toegang verleend tot Human Interface-apparaten (muis, toetsenbord, enz.) die zijn aangesloten op een USB-poort, zelfs als USB-poorten worden geweigerd. Standaard is dit item geselecteerd, zodat het toetsenbord en de muis niet worden uitgeschakeld door de toegang tot de USB-poort te weigeren.
  Ondersteund op zowel Windows als macOS.
- **USB- en FireWire-netwerkkaarten**: Wanneer u dit selecteert, wordt toegang verleend tot netwerkkaarten die zijn aangesloten op een USB- of FireWire (IEEE 1394)-poort, zelfs als USB-poorten en/of FireWire-poorten worden geweigerd.
  Ondersteund op zowel Windows als macOS.
- **USB-scanners en apparaten voor stilstaand beeld**: Wanneer u dit selecteert, wordt toegang verleend tot scanners en apparaten voor stilstaand beeld die zijn aangesloten op een USB-poort, zelfs als USB-poorten worden geweigerd.
  Alleen ondersteund op Windows.
- **USB-audioapparaten**: Wanneer u dit selecteert, wordt toegang verleend tot audioapparaten, zoals headsets en microfoons, die zijn aangesloten op een USB-poort, zelfs als USB-poorten worden geweigerd.
  Alleen ondersteund op Windows.
- **USB-camera's**: Wanneer u dit selecteert, wordt toegang verleend tot webcamera's die zijn aangesloten op een USB-poort, zelfs als USB-poorten worden geweigerd.
  Alleen ondersteund op Windows.
- **Bluetooth HID (muis, toetsenbord, enz.)**: Wanneer u dit selecteert, wordt toegang verleend tot Human Interface-apparaten (muis, toetsenbord, enz.) die zijn aangesloten via Bluetooth, zelfs als Bluetooth wordt geweigerd.
  Alleen ondersteund op Windows.
- **Klembord kopiëren/plakken binnen toepassing**: Wanneer u dit selecteert, kunnen gegevens via het klembord binnen dezelfde toepassing worden gekopieerd/geplakt, zelfs als het klembord wordt geweigerd.
  Alleen ondersteund op Windows.

Opmerking
Instellingen voor niet-ondersteunde apparaatsubklassen worden genegeerd als deze instellingen zijn geconfigureerd in het toegepaste beschermingsschema.

Houd rekening met het volgende wanneer u appraattypen toevoegt aan de acceptatielijst:

- U kunt alleen een hele subklasse van apparaten toestaan op de acceptatielijst voor apparaattypen. Het is niet mogelijk om een specifiek apparaatmodel toe te staan en alle andere apparaten van dezelfde subklasse te weigeren. Als u bijvoorbeeld USB-camera's uitsluit van het toegangsbeheer, staat u het gebruik van elke USB-camera toe, ongeacht het model en de leverancier. Zie Acceptatielijst voor USB-apparaten voor het toestaan van individuele apparaten/modellen.
- Apparaattypen kunnen alleen worden geselecteerd in een gesloten lijst van apparaatsubklassen. Als u een apparaat van een andere subklasse wilt toestaan, kunt u hiervoor niet de acceptatielijst voor apparaattypen gebruiken. Een subklasse zoals USB-smartcardlezers kan bijvoorbeeld niet worden toegevoegd aan de acceptatielijst. Als u een USB-smartcardlezer wilt toestaan wanneer USB-poorten worden geweigerd, volgt u de instructies in de Acceptatielijst voor USB-apparaten.
- De acceptatielijst voor apparaattypen werkt alleen voor apparaten die standaard-Windows-stuurprogramma's gebruiken. Mogelijk wordt de subklasse van sommige USB-apparaten met eigen stuurprogramma's niet herkend door het apparaatbeheer. De acceptatielijst voor apparaattypen kan daarom niet worden gebruikt om de toegang tot dergelijke USB-apparaten toe te staan. In dit geval kunt u toegang toestaan per apparaat/model (zie Acceptatielijst voor USB-apparaten).

Acceptatielijst voor USB-apparaten

De acceptatielijst is bedoeld om het gebruik van bepaalde USB-apparaten toe te staan, ongeacht andere instellingen voor apparaatbeheer. U kunt afzonderlijke apparaten of apparaatmodellen toevoegen aan de acceptatielijst om het toegangsbeheer voor die apparaten uit te schakelen. Als u bijvoorbeeld een mobiel apparaat met een unieke id toevoegt aan de acceptatielijst, staat u het gebruik van dat specifieke apparaat toe, ook al wordt het gebruik van andere USB-apparaten geweigerd.

Op de pagina **Acceptatielijst voor USB-apparaten** kunt u afzonderlijke USB-apparaten of USB-apparaatmodellen opgeven die u wilt uitsluiten van het apparaattoegangsbeheer. Daardoor wordt toegang tot die apparaten toegestaan, ongeacht de toegangsinstellingen in de apparaatbeheermodule.

Er zijn twee manieren om apparaten te identificeren in de acceptatielijst:

- Model van apparaat: Alle apparaten van een bepaald model. Elk apparaatmodel wordt geïdentificeerd door een leverancier-id (VID) en een product-id (PID), zoals USB\VID_0FCE&PID_E19E.

  Met deze combinatie van VID en PID wordt niet een specifiek apparaat geïdentificeerd, maar een volledig apparaatmodel. Als u een apparaatmodel toevoegt aan de acceptatielijst, staat u toegang

toe tot elk apparaat van dat model. Zo kunt u bijvoorbeeld het gebruik van USB-printers van een bepaald model toestaan.

- Uniek apparaat: Identificeert een bepaald apparaat. Elk uniek apparaat wordt geïdentificeerd door een leverancier-id (VID), een product-id (PID) en een serienummer, zoals USB\VID_0FCE&PID_E19E\D55E7FCA.

  Er wordt niet aan alle USB-apparaten een serienummer toegewezen. U kunt een apparaat alleen als uniek apparaat toevoegen aan de acceptatielijst als het apparaat tijdens de productie een serienummer heeft gekregen. Bijvoorbeeld een USB-stick met een uniek serienummer.

Als u een apparaat aan de acceptatielijst wilt toevoegen, moet u het eerst toevoegen aan de database van USB-apparaten. Vervolgens kunt u apparaten toevoegen aan de acceptatielijst door ze te selecteren in die database.

De acceptatielijst wordt beheerd op een afzonderlijke configuratiepagina met de naam **Acceptatielijst voor USB-apparaten**. Elk item in de lijst vertegenwoordigt een apparaat of apparaatmodel en heeft de volgende velden:

- **Beschrijving**: Bij het aansluiten van het USB-apparaat wordt automatisch een bepaalde beschrijving toegewezen. U kunt de beschrijving van het apparaat wijzigen in de database van USB-apparaten (zie de pagina voor beheer van de database van USB-apparaten).
- **Apparaattype**: Geeft 'Uniek' weer als het lijstitem een uniek apparaat is, of 'Model' als het gaat om een apparaatmodel.
- **Alleen-lezen**: Wanneer u dit selecteert, kunt u alleen gegevens van het apparaat ontvangen. Als het apparaat geen alleen-lezen-toegang ondersteunt, dan wordt de toegang tot het apparaat geblokkeerd. Schakel dit selectievakje uit om volledige toegang tot het apparaat toe te staan.
- **Opnieuw initialiseren**: Wanneer u deze optie selecteert, simuleert het apparaat dat de verbinding wordt verbroken/opnieuw tot stand wordt gebracht wanneer een nieuwe gebruiker zich aanmeldt. Sommige USB-apparaten moeten opnieuw worden geïnitialiseerd voor een goede werking, dus we raden aan dit selectievakje voor dergelijke apparaten (muis, toetsenbord) in te schakelen. We raden ook aan om dit selectievakje uit te schakelen voor gegevensopslagapparaten (USB-sticks, optische stations, externe harde schijven, enzovoort). Mogelijk kunnen sommige USB-apparaten met eigen stuurprogramma's niet opnieuw worden geïnitialiseerd door het apparaatbeheer. Als er geen toegang is tot een dergelijk apparaat, moet u het USB-apparaat uit de USB-poort halen en weer terugplaatsen.

Opmerking
Het veld **Opnieuw initialiseren** is standaard verborgen. Als u deze wilt weergeven in de tabel, klikt u op het tandwielpictogram rechtsboven in de tabel en schakelt u het selectievakje **Opnieuw initialiseren** in.

Opmerking
De velden **Alleen-lezen** en **Opnieuw initialiseren** worden niet ondersteund op macOS. Als deze velden in het toegepaste beschermingsschema zijn geconfigureerd, worden ze genegeerd.

U kunt als volgt apparaten/modellen toevoegen aan of verwijderen uit de acceptatielijst:

- Klik op **Toevoegen uit database** boven de lijst en selecteer vervolgens de gewenste apparaten die zijn geregistreerd in de database van USB-apparaten. Het geselecteerde apparaat wordt toegevoegd aan de lijst, waar u de instellingen kunt configureren en de wijzigingen kunt bevestigen.
- Klik op **Dit USB-apparaat toestaan** in een waarschuwing die meldt dat de toegang tot het USB-apparaat wordt geweigerd (zie Waarschuwingen van apparaatbeheer). Hierdoor wordt het apparaat toegevoegd aan de acceptatielijst en aan de database van USB-apparaten.
- Klik op het pictogram Verwijderen aan het einde van een lijstitem. Hierdoor wordt het betreffende apparaat/model verwijderd uit de acceptatielijst.

Database van USB-apparaten

In de apparaatbeheermodule wordt een database van USB-apparaten onderhouden waaruit u apparaten kunt toevoegen aan de uitsluitingslijst (zie Accceptatielijst voor USB-apparaten). Een USB-apparaat kan op een van de volgende manieren worden geregistreerd bij de database:

- Een apparaat toevoegen op de pagina die wordt weergegeven wanneer u een apparaat toevoegt aan de uitsluitingslijst (zie de pagina voor beheer van de database van USB-apparaten).
- Een apparaat toevoegen via de Cyber Protect-console > deelvenster Inventaris van een computer > tabblad USB-apparaten (zie Lijst met USB-apparaten op een computer).
- Sta toe dat de toegang tot het USB-apparaat wordt geweigerd na een waarschuwing (zie Waarschuwingen van apparaatbeheer).

Zie ook stappen om USB-apparaten toe te voegen of te verwijderen uit de database.

Pagina voor beheer van de database van USB-apparaten

Bij het configureren van de acceptatielijst voor USB-apparaten kunt u een apparaat uit de database toevoegen. Als u deze optie kiest, wordt een beheerpagina met een lijst met apparaten weergegeven. Op deze pagina kunt een lijst bekijken met alle apparaten die zijn geregistreerd in de database, u kunt apparaten selecteren die u aan de acceptatielijst wilt toevoegen, en u kunt de volgende bewerkingen uitvoeren:

Een apparaat registreren in de database

1. Klik op **Toevoegen aan database** bovenaan de pagina.
2. Klik in het dialoogvenster **USB-apparaat toevoegen** dat wordt weergegeven, op de machine waarop het USB-apparaat is aangesloten.
   Alleen machines die online zijn, worden weergegeven in de lijst met computers.
   De lijst met USB-apparaten wordt alleen weergegeven voor machines waarop de agent voor de preventie van gegevensverlies is geïnstalleerd.
   De USB-apparaten worden weergegeven in een boomstructuur. Het eerste niveau van de boom komt overeen met een apparaatmodel. Het tweede niveau komt overeen met een specifiek apparaat van dat model.

Een blauw pictogram naast de beschrijving van het apparaat geeft aan dat het apparaat momenteel is aangesloten op de computer. Als het apparaat niet op de computer is aangesloten, wordt het pictogram grijs weergegeven.

3. Schakel het selectievakje in voor het USB-apparaat dat u wilt registreren en klik op **Toevoegen aan database**.

De beschrijving van een apparaat wijzigen

1. Klik op de pagina **Database van USB-apparaten** op de ellips (...) aan het einde van het lijstitem voor het betreffende apparaat en klik vervolgens op **Bewerken**.
2. Wijzig de beschrijving in het dialoogvenster dat wordt geopend.

Een apparaat verwijderen uit de database

1. Klik op de ellips (...) aan het einde van het lijstitem voor het betreffende apparaat.
2. Klik op **Verwijderen** en bevestig dat u wilt verwijderen.

De lijst op de pagina bevat de volgende informatie voor elk apparaat:

- **Beschrijving**: Een leesbare identificatie voor het apparaat. U kunt de beschrijving eventueel wijzigen.
- **Apparaattype**: Geeft 'Uniek' weer als het lijstitem een uniek apparaat is, of 'Model' als het gaat om een apparaatmodel. Een uniek apparaat moet een serienummer hebben in combinatie met een leverancier-id (VID) en product-id (PID). Een apparaatmodel wordt geïdentificeerd door een combinatie van VID en PID.
- **Leverancier-id**, **Product-id**, **Serienummer**: Deze waarden vormen samen de apparaat-id met de indeling USB\VID_<leverancier-id>&PID_<product-id>\<serienummer>.
- **Account**: Geeft de tenant aan waartoe dit apparaat behoort. Dit is de tenant die het gebruikersaccount bevat waarmee het toestel is geregistreerd bij de database.

Opmerking
Deze kolom is standaard verborgen. Als u deze wilt weergeven in de tabel, klikt u op het tandwielpictogram rechtsboven in de tabel en vervolgens selecteert u **Account**.

In de kolom aan de linkerkant kunt u de apparaten selecteren die u aan de acceptatielijst wilt toevoegen: Schakel het selectievakje in voor elk apparaat dat u wilt toevoegen en klik vervolgens op de knop **Toevoegen aan acceptatielijst**. Als u alle selectievakjes wilt selecteren of wissen, klikt u op het selectievakje in de kolomkop.

U kunt de lijst met apparaten doorzoeken of filteren:

- Klik op **Zoeken** bovenaan de pagina en voer een zoekreeks in. De lijst geeft de apparaten weer waarvan de beschrijving overeenkomt met de door u ingevoerde zoekreeks.
- Klik op **Filter** en configureer een filter. Pas dit filter toe in het dialoogvenster dat wordt weergegeven. De lijst is beperkt tot apparaten met het type, de leverancier-id, de product-id en het account die u hebt geselecteerd bij het configureren van het filter. Als u het filter wilt annuleren en alle apparaten wilt weergeven, klikt u op **Terugzetten naar standaardwaarden**.

De lijst met USB-apparaten in de database exporteren

U kunt de lijst met de aan de database toegevoegde USB-apparaten exporteren.

1. Open het beschermingsschema van een apparaat om dit te bewerken.
2. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de rij **Acceptatielijst voor USB-apparaten**.
3. Klik op de pagina met de acceptatielijst voor USB-apparaten op **Toevoegen vanuit database**.
4. Klik op de pagina voor beheer van de database van USB-apparaten die wordt weergegeven, op **Exporteren**.
   Het standaarddialoogvenster Bladeren wordt geopend.
5. Selecteer de locatie waar u het bestand wilt opslaan, voer zo nodig een nieuwe bestandsnaam in en klik op **Opslaan**.

De lijst met USB-apparaten wordt geëxporteerd naar een JSON-bestand.

U kunt het resulterende JSON-bestand bewerken om er apparaten aan toe te voegen of eruit te verwijderen, en om groepsgewijze wijzigingen aan te brengen in de apparaatbeschrijvingen.

Een lijst met USB-apparaten importeren in de database

In plaats van USB-apparaten toe te voegen vanuit de Cyber Protect-console, kunt u een lijst met USB-apparaten importeren. De lijst is een bestand in JSON-indeling.

Opmerking
U kunt JSON-bestanden importeren in een database die niet de apparaten bevat die in het bestand worden beschreven. Als u een gewijzigd bestand wilt importeren in de database van waaruit het werd geëxporteerd, moet u de database eerst leegmaken omdat u geen dubbele vermeldingen kunt importeren. Als u de lijst met USB-apparaten exporteert, wijzigt, en probeert te importeren naar dezelfde database zonder deze op te schonen, zal de import mislukken.

1. Open het beschermingsschema van een apparaat om dit te bewerken.
2. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de rij **Acceptatielijst voor USB-apparaten**.
3. Klik op de pagina met de acceptatielijst voor USB-apparaten op **Toevoegen vanuit database**.
4. Klik op de pagina voor beheer van de database van USB-apparaten die wordt weergegeven, op **Importeren**.
   Het dialoogvenster USB-apparaten importeren uit bestand wordt geopend.
5. Gebruik slepen en neerzetten (of blader) voor het bestand dat u wilt importeren.

De Cyber Protect-console controleert of de lijst dubbele vermeldingen bevat die al in de database bestaan en slaat deze over. De USB-apparaten die niet in de database worden gevonden, worden aan de database toegevoegd.

Lijst met USB-apparaten op een computer

Het deelvenster Inventaris van een computer in de Cyber Protect-console bevat het tabblad **USB-apparaten**. Als de computer online is en de agent voor preventie van gegevensverlies hierop is geïnstalleerd, wordt op het tabblad **USB-apparaten** een lijst weergegeven met alle USB-apparaten die ooit op die computer zijn aangesloten.

De USB-apparaten worden weergegeven in een boomstructuur. Het eerste niveau van de boom komt overeen met een apparaatmodel. Het tweede niveau komt overeen met een specifiek apparaat van dat model.

De lijst geeft de volgende informatie voor elk apparaat:

- **Beschrijving**: Bij het aansluiten van het USB-apparaat wordt automatisch een beschrijving toegewezen. Deze beschrijving kan dienen als een leesbare identificatie voor het apparaat.

  Een blauw pictogram naast de beschrijving van het apparaat geeft aan dat het apparaat momenteel is aangesloten op de computer. Als het apparaat niet op de computer is aangesloten, wordt het pictogram grijs weergegeven.
- **Apparaat-id**: De identificatie die door het besturingssysteem is toegewezen aan het apparaat. Deze id heeft de volgende indeling: USB\VID_<leverancier-id>&PID_<product-id>\<serienummer> waarbij <serienummer> optioneel is. Voorbeelden: USB\VID_0FCE&PID_ADDE\D55E7FCA (apparaat met een serienummer); USB\VID_0FCE&PID_ADDE (apparaat zonder serienummer).

Als u apparaten wilt toevoegen aan de database van USB-apparaten, schakelt u de selectievakjes in voor de gewenste apparaten en klikt u vervolgens op de knop **Toevoegen aan database**.

Processen uitsluiten van toegangsbeheer

De toegang tot het Windows-klembord, schermopname, printers en mobiele apparaten wordt beheerd via hooks die in processen worden geïnjecteerd. Als er geen hooks worden gebruikt in de processen, wordt de toegang tot deze apparaten niet beheerd.

Opmerking
Het uitsluiten van processen voor toegangscontrole wordt niet ondersteund op macOS. Als een lijst met uitgesloten processen is geconfigureerd in het toegepaste beschermingsschema, wordt deze genegeerd.

Op de pagina **Uitsluitingen** kunt u een lijst met processen opgeven waarin geen hooks worden gebruikt. Dit betekent dat het toegangsbeheer voor klemborden (lokaal en omgeleid), schermopname, printers en mobiele apparaten niet op dergelijke processen wordt toegepast.

U hebt bijvoorbeeld een beschermingsschema toegepast dat de toegang tot printers weigert en vervolgens hebt u de Microsoft Word-toepassing gestart. Een poging om vanuit deze toepassing af te drukken wordt dan geblokkeerd. Maar als u het Microsoft Word-proces toevoegt aan de lijst met uitsluitingen, dan worden er geen hooks gebruikt voor de toepassing. Het afdrukken vanuit

Microsoft Word wordt dan niet geblokkeerd, maar het afdrukken vanuit andere toepassingen wordt wel geblokkeerd.

Processen toevoegen aan uitsluitingen

1. Open het beschermingsschema van een apparaat om dit te bewerken:
   Klik op de ellips (...) naast de naam van het beschermingsschema en selecteer **Bewerken**.

   Opmerking
   Apparaatbeheer moet zijn ingeschakeld in het schema, zodat u toegang krijgt tot de instellingen voor apparaatbeheer.

2. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de rij **Uitsluitingen**.
3. Klik op de pagina **Uitsluitingen**, in de rij **Processen en mappen** op **+Toevoegen**.
4. Voeg de processen toe die u wilt uitsluiten van het toegangsbeheer.
   Bijvoorbeeld: `C:\map\submap\process.exe`.
   U kunt jokertekens gebruiken:
   - * vervangt een willekeurig aantal tekens.
   - ? vervangt één teken.

   Bijvoorbeeld:

   ```
   C:\map\*
   *\map\submap?\*
   *\process.exe
   ```
5. Klik op het vinkje en klik vervolgens op **Gereed**.
6. Klik in het beschermingsschema op **Opslaan**.
7. Herstart de processen die u hebt uitgesloten, om te controleren of de hooks correct zijn verwijderd.

De uitgesloten processen hebben dan toegang tot het klembord, schermopname, printers en mobiele apparaten, ongeacht de toegangsinstellingen voor die apparaten.

Een proces verwijderen uit de uitsluitingen

Open het beschermingsschema van een apparaat om dit te bewerken:

Klik op de ellips (...) naast de naam van het beschermingsschema en selecteer **Bewerken**.

Opmerking
Apparaatbeheer moet zijn ingeschakeld in het schema, zodat u toegang krijgt tot de instellingen voor apparaatbeheer.

1. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de rij **Uitsluitingen**.

2. Klik op de pagina **Uitsluitingen** op het pictogram van de prullenbak naast het proces dat u wilt verwijderen uit de uitsluitingen.
3. Klik op **Gereed**.
4. Klik in het beschermingsschema op **Opslaan**.
5. Herstart het proces om te controleren of de hooks correct zijn geïnjecteerd.

De toegangsinstellingen van het beschermingsschema worden dan toegepast op de processen die u hebt verwijderd uit de uitsluitingen.

Een proces in uitsluitingen bewerken

1. Open het beschermingsschema van een apparaat om dit te bewerken:
   Klik op de ellips (...) naast de naam van het beschermingsschema en selecteer **Bewerken**.

   Opmerking
   Apparaatbeheer moet zijn ingeschakeld in het schema, zodat u toegang krijgt tot de instellingen voor apparaatbeheer.

2. Klik op het pijltje naast de schakelaar **Apparaatbeheer** om de instellingen uit te breiden en klik vervolgens op de rij **Uitsluitingen**.
3. Klik op de pagina **Uitsluitingen** op het pictogram **Bewerken** naast het proces dat u wilt bewerken.
4. Pas de wijzigingen toe en klik op het vinkje om te bevestigen.
5. Klik op **Gereed**.
6. Klik in het beschermingsschema op **Opslaan**.
7. Herstart de betreffende processen om te controleren of uw wijzigingen correct zijn toegepast.

Waarschuwingen van apparaatbeheer

Met apparaatbeheer wordt een gebeurtenissenlogboek bijgehouden van de pogingen door gebruikers om toegang te krijgen tot beheerde apparaattypen, poorten en interfaces. Bepaalde gebeurtenissen kunnen waarschuwingen genereren die worden geregistreerd in de Cyber Protect-console. De apparaatbeheermodule kan bijvoorbeeld worden geconfigureerd om het gebruik van verwisselbare apparaten te voorkomen, waarbij een waarschuwing wordt geregistreerd wanneer een gebruiker probeert gegevens te kopiëren naar of van een dergelijk apparaat.

Bij de configuratie van de apparaatbeheermodule kunt u waarschuwingen inschakelen voor de meeste items die zijn vermeld onder Apparaattype (behalve schermopname) of onder Poorten. Als waarschuwingen zijn ingeschakeld, wordt er een waarschuwingen gegenereerd bij elke poging van een gebruiker om een bewerking uit te voeren die niet is toegestaan. Als bijvoorbeeld de toegang tot verwisselbare apparaten is beperkt tot alleen-lezen en de optie **Waarschuwing weergeven** is geselecteerd voor dat apparaattype, wordt er een waarschuwing gegenereerd telkens wanneer een gebruiker op een beschermde computer probeert gegevens te kopiëren naar een verwisselbaar apparaat.

Als u waarschuwingen wilt weergeven in de Cyber Protect-console, gaat u naar **Controle** > **Waarschuwingen**. Bij elke waarschuwing van apparaatbeheer wordt in de console de volgende informatie weergegeven over de betreffende gebeurtenis:

- **Type**: Waarschuwing.
- **Status**: De volgende mededeling wordt weergegeven: 'Toegang tot het randapparaat is geblokkeerd'.
- **Bericht**: Het volgende bericht wordt weergegeven: 'Toegang tot '<apparaattype of poort>' op '<computernaam>' is geblokkeerd'. Bijvoorbeeld: 'Toegang tot 'verwisselbaar' op 'accountant-pc' is geblokkeerd'.
- **Datum en tijd**: De datum en tijd van de gebeurtenis.
- **Apparaat**: De naam van de computer waarop de gebeurtenis heeft plaatsgevonden.
- **Schemanaam**: De naam van het beschermingsschema waardoor de gebeurtenis is gegenereerd.
- **Bron**: Het apparaattype of de poort waarop de gebeurtenis betrekking heeft. Bijvoorbeeld: In het geval van een geweigerde gebruikerspoging om toegang te krijgen tot een verwisselbaar apparaat, wordt in dit veld 'Verwisselbaar apparaat' weergegeven.
- **Actie**: De bewerking die de gebeurtenis heeft veroorzaakt. Bijvoorbeeld: In het geval van een geweigerde gebruikerspoging om gegevens naar een apparaat te kopiëren, wordt in dit veld 'Schrijven' weergegeven. Zie Waarden voor het veld Actie voor meer informatie.
- **Naam**: De naam van het doelobject van de gebeurtenis, zoals het bestand dat de gebruiker probeerde te kopiëren of het apparaat dat de gebruiker probeerde te gebruiken. Wordt niet weergegeven als het doelobject niet kan worden geïdentificeerd.
- **Informatie**: Aanvullende informatie over het doelapparaat van de gebeurtenis, zoals de apparaat-id voor USB-apparaten. Wordt niet weergegeven als er geen aanvullende informatie over het doelapparaat beschikbaar is.
- **Gebruiker**: De naam van de gebruiker die de gebeurtenis heeft veroorzaakt.
- **Proces**: Het volledig gekwalificeerde pad naar het uitvoerbare bestand van de toepassing die de gebeurtenis heeft veroorzaakt. In sommige gevallen kan de procesnaam worden weergegeven in plaats van het pad. Wordt niet weergegeven als er geen procesinformatie beschikbaar is.

Als een waarschuwing van toepassing is op een USB-apparaat (waaronder verwisselbare apparaten en versleutelde verwisselbare apparaten), kan de beheerder het apparaat direct vanuit de waarschuwing toevoegen aan de acceptatielijst. De apparaatbeheermodule kan de toegang tot dat specifieke apparaat dan niet meer beperken. Als u klikt op **Dit USB-apparaat toestaan** wordt het apparaat toegevoegd aan de acceptatielijst voor toegestane USB-apparaten in de configuratie van de apparaatbeheermodule en ook aan de database van USB-apparaten voor later gebruik.

Zie ook stappen om waarschuwingen van apparaatbeheer te bekijken.

Waarden voor het veld Actie

Het veld met de waarschuwing **Actie** kan de volgende waarden bevatten:

- **Lezen**: Haal gegevens op van het apparaat of de poort.
- **Schrijven**: Verzend gegevens naar het apparaat of de poort.
- **Formatteren**: Directe toegang (formatteren, schijfcontrole, enz.) tot het apparaat. In het geval van een poort is dit van toepassing op het apparaat dat op die poort is aangesloten.
- **Uitwerpen**: Verwijder het apparaat uit het systeem of werp de media uit uit het apparaat. In het geval van een poort is dit van toepassing op het apparaat dat op die poort is aangesloten.
- **Afdrukken**: Verzend een document naar de printer.
- **Audio kopiëren**: Kopieer/plak audiogegevens via het lokale klembord.
- **Bestand kopiëren**: Kopieer/plak een bestand via het lokale klembord.
- **Image kopiëren**: Kopieer/plak een afbeelding via het lokale klembord.
- **Tekst kopiëren**: Kopieer/plak tekst via het lokale klembord.
- **Niet-geïdentificeerde inhoud kopiëren**: Kopieer/plak andere gegevens via het lokale klembord.
- **RTF-gegevens (image) kopiëren**: Gebruik Rich Text Format om een afbeelding te kopiëren/plakken via het lokale klembord.
- **RTF-gegevens (bestand) kopiëren**: Gebruik Rich Text Format om een bestand te kopiëren/plakken via het lokale klembord.
- **RTF-gegevens (tekst, image) kopiëren**: Gebruik Rich Text Format om tekst met een afbeelding te kopiëren/plakken via het lokale klembord.
- **RTF-gegevens (tekst, bestand) kopiëren**: Gebruik Rich Text Format om een tekst met een bestand te kopiëren/plakken via het lokale klembord.
- **RTF-gegevens (image, bestand) kopiëren**: Gebruik Rich Text Format om een afbeelding met een bestand te kopiëren/plakken via het lokale klembord.
- **RTF-gegevens (tekst, image, bestand) kopiëren**: Gebruik Rich Text Format om een tekst met een afbeelding en een bestand te kopiëren/plakken via het lokale klembord.
- **Verwijderen**: Gegevens van het apparaat verwijderen (bijvoorbeeld een verwisselbaar apparaat, een mobiel apparaat, enzovoort).
- **Apparaattoegang**: Toegang tot een apparaat of poort (bijvoorbeeld een Bluetooth-apparaat, een USB-poort, enzovoort).
- **Inkomende audio**: - Kopieer/plak audiogegevens van de clientcomputer naar de gehoste sessie via het omgeleide klembord.
- **Inkomend bestand**: Kopieer/plak een bestand van de clientcomputer naar de gehoste sessie via het omgeleide klembord.
- **Inkomende afbeelding**: Kopieer/plak een afbeelding van de clientcomputer naar de gehoste sessie via het omgeleide klembord.
- **Inkomende tekst**: Kopieer/plak tekst van de clientcomputer naar de gehoste sessie via het omgeleide klembord.
- **Inkomende niet-geïdentificeerde inhoud**: Kopieer/plak andere gegevens van de clientcomputer naar de gehoste sessie via het omgeleide klembord.

- **Inkomende RTF-gegevens (image)**: Gebruik Rich Text Format om een afbeelding van de clientcomputer naar de gehoste sessie te kopiëren/plakken via het omgeleide klembord.
- **Inkomende RTF-gegevens (bestand)**: Gebruik Rich Text Format om een bestand van de clientcomputer naar de gehoste sessie te kopiëren/plakken via het omgeleide klembord.
- **Inkomende RTF-gegevens (tekst, image)**: Gebruik Rich Text Format om tekst met een afbeelding van de clientcomputer naar de gehoste sessie te kopiëren/plakken via het omgeleide klembord.
- **Inkomende RTF-gegevens (tekst, bestand)**: Gebruik Rich Text Format om tekst met een bestand van de clientcomputer naar de gehoste sessie te kopiëren/plakken via het omgeleide klembord.
- **Inkomende RTF-gegevens (image, bestand)** - Gebruik Rich Text Format om een afbeelding met een bestand van de clientcomputer naar de gehoste sessie te kopiëren/plakken via het omgeleide klembord.
- **Inkomende RTF-gegevens (tekst, image, bestand)**: Gebruik Rich Text Format om tekst met een afbeelding en een bestand van de clientcomputer naar de gehoste sessie te kopiëren/plakken via het omgeleide klembord.
- **Invoegen**: Sluit een USB-apparaat of een FireWire-apparaat aan.
- **Uitgaande audio**: Kopieer/plak audiogegevens van de gehoste sessie naar de clientcomputer via het omgeleide klembord.
- **Uitgaand bestand**: Kopieer/plak een bestand van de gehoste sessie naar de clientcomputer via het omgeleide klembord.
- **Uitgaande afbeelding**: Kopieer/plak een afbeelding van de gehoste sessie naar de clientcomputer via het omgeleide klembord.
- **Uitgaande tekst**: Kopieer/plak tekst van de gehoste sessie naar de clientcomputer via het omgeleide klembord.
- **Uitgaande niet-geïdentificeerde inhoud**: Kopieer/plak andere gegevens van de gehoste sessie naar de clientcomputer via het omgeleide klembord.
- **Uitgaande RTF-gegevens (image)**: Gebruik Rich Text Format om een afbeelding van de gehoste sessie naar de clientcomputer te kopiëren/plakken via het omgeleide klembord.
- **Uitgaande RTF-gegevens (bestand)**: Gebruik Rich Text Format om een bestand van de gehoste sessie naar de clientcomputer te kopiëren/plakken via het omgeleide klembord.
- **Uitgaande RTF-gegevens (tekst, image)**: Gebruik Rich Text Format om tekst met een afbeelding van de gehoste sessie naar de clientcomputer te kopiëren/plakken via het omgeleide klembord.
- **Uitgaande RTF-gegevens (tekst, bestand)**: Gebruik Rich Text Format om tekst met een bestand van de gehoste sessie naar de clientcomputer te kopiëren/plakken via het omgeleide klembord.
- **Uitgaande RTF-gegevens (image, bestand)**: Gebruik Rich Text Format om een afbeelding met een bestand van de gehoste sessie naar de clientcomputer te kopiëren/plakken via het omgeleide klembord.
- **Uitgaande RTF-gegevens (tekst, image, bestand)**: Gebruik Rich Text Format om tekst met een afbeelding en een bestand van de gehoste sessie naar de clientcomputer te kopiëren/plakken via het omgeleide klembord.

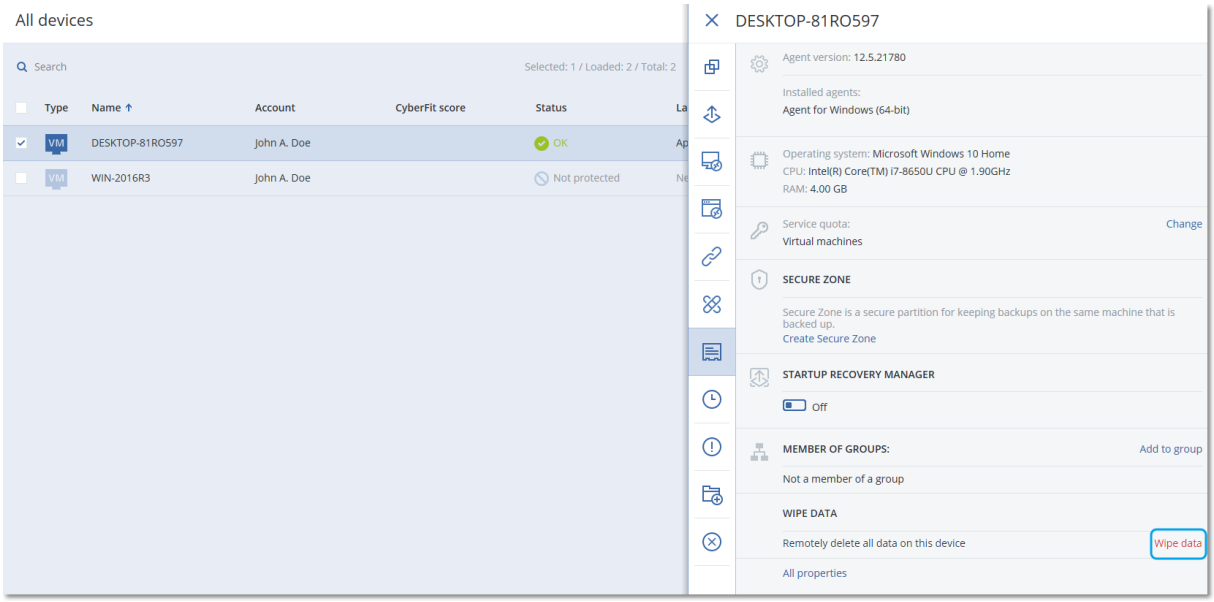
- **Naam wijzigen**: Wijzig de naam van bestanden op een apparaat (bijvoorbeeld op verwisselbare apparaten, mobiele apparaten, enzovoort).

Gegevens wissen in een beheerde workload

Opmerking
Wissen op afstand is beschikbaar met het Advanced Security-pakket.

Beheerders van de Cyber Protection-service en machine-eigenaren kunnen extern wissen gebruiken om de gegevens op een beheerde machine te verwijderen, bijvoorbeeld als deze verloren gaat of wordt gestolen. Zo wordt ongeoorloofde toegang tot gevoelige informatie voorkomen.

Extern wissen is alleen beschikbaar voor machines met Windows versie 10 en later. De machine moet zijn ingeschakeld en verbinding hebben met internet om de opdracht voor wissen te kunnen ontvangen.



Gegevens van een machine wissen

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de machine waarvan u de gegevens wilt wissen.

   Opmerking
   U kunt gegevens van één machine tegelijk wissen.

3. Klik op **Details** en klik vervolgens op **Gegevens wissen**.
   Als de geselecteerde machine offline is, is de optie **Gegevens wissen** niet toegankelijk.
4. Bevestig uw keuze.
5. Voer de referenties in van de lokale beheerder van deze machine en klik vervolgens op **Gegevens wissen**.

Opmerking
Ga naar **Controle** > **Activiteiten** om de details over het wissen te bekijken en te controleren wie de bewerking heeft gestart.

Workloads bekijken die worden beheerd door RMM-integraties

Opmerking
Deze functie is alleen beschikbaar als de Advanced Automation-service is ingeschakeld.

Wanneer u een RMM-platform integreert als onderdeel van de Advanced Automation-service, kunt u informatie van door het RMM-platform beheerde apparaten bekijken en controleren. Deze informatie is beschikbaar in de Cyber Protect-console via **Apparaten**.

Workloads bekijken die worden beheerd door RMM-integraties:

1. Ga naar **Apparaten > Alle apparaten**.
2. (Optioneel) Sorteer de kolom **RMM integratie** om de gewenste integraties te vinden.
3. Selecteer de gewenste workload.
4. Ga naar het deelvenster **Acties** en selecteer **Details**.
5. In het weergegeven deelvenster wordt een van de volgende drie opties getoond, afhankelijk van hoe u de workload hebt geconfigureerd:
   - Als er Acronis-services zijn gedefinieerd voor de workload, maar zonder RMM-integratie: Als de workload is geconfigureerd om alleen met Acronis-services te werken, wordt er geen informatie van de RMM-integratie weergegeven.
   - Als er zowel Acronis-services als een RMM-integratie zijn geconfigureerd voor de workload: De gegevens van de Acronis-services en de RMM-integratie worden weergegeven op twee tabbladen, **Overzicht** en **RMM-integratie**. Klik op **RMM-integratie** om de gegevens van de integratie te bekijken, waaronder de naam en het type van de workload (opgehaald uit het RMM-platform), de beschrijving en locatie. Daarnaast worden ook alle geïnstalleerde en ingeschakelde add-ons voor RMM-agents weergegeven.
   - Als de workload is geconfigureerd met alleen een RMM-integratie: De gegevens van de RMM-integratie worden weergegeven, waaronder de naam en het type workload (opgehaald uit het RMM-platform), de beschrijving en locatie. Daarnaast worden ook alle geïnstalleerde en ingeschakelde add-ons voor RMM-agents weergegeven.

   Let op: wanneer de workload is geconfigureerd met RMM-integratie (in combinatie met Acronis-services of alleen met een RMM-integratie), kunt u het volgende doen:
   - Een externe verbinding tot stand brengen (beschikbaar voor integraties met Datto RMM, N-able N-central en N-able RMM)
   - Geïnstalleerde add-ons op het RMM-apparaat van derden bekijken (alleen beschikbaar voor N-able RMM)

- Directe toegang krijgen tot de gegevens van het RMM-apparaat van derden (beschikbaar voor Datto RMM, N-able N-central, NinjaOne)

CyberApp-workloads

CyberApp-workloads worden gemaakt door ISV's (Independent software vendors, onafhankelijke softwareleveranciers) en worden weergegeven in de Cyber Protect-console nadat u een CyberApp-integratie hebt ingeschakeld. Er moet aan de volgende voorwaarden worden voldaan:

- Het uitbreidingspunt **Workloads en acties** moet zijn ingeschakeld in de CyberApp.
- Er moet ten minste één **Type workload** zijn gedefinieerd in de CyberApp.
- De CyberApp-workloads moeten worden toegevoegd aan en bijgewerkt op het Acronis-platform via de connectorservice die door de ISV wordt gehost.

Voor meer informatie over de leverancierspportal en het maken van CyberApps raadpleegt u de Gebruikershandleiding voor de leverancierspportal.

Geaggregeerde workloads

Op een fysieke workload kunnen tegelijkertijd een Cyber Protect-agent en een of meerdere CyberApp-agents zijn geïnstalleerd. In dit geval wordt dezelfde workload meer dan één keer weergegeven op het scherm **Alle apparaten**. Er wordt een afzonderlijke record weergegeven voor de Acronis-workload en voor elke CyberApp-workload. Als het automatisch samenvoegen van workloads is ingeschakeld en geconfigureerd vanuit de leverancierspportal of de Cyber Protect-console, worden de hostadressen en de MAC-adressen van de Acronis-workloads en de CyberApp-workloads automatisch vergeleken en worden alle weergaven samengevoegd tot één geaggregeerde workload. U kunt workloads ook handmatig samenvoegen en weer splitsen via de Cyber Protect-console.

Werken met CyberApp-workloads

Naast de standaardacties die zijn ingebouwd in de Cyber Protect-console, kunt u de volgende acties uitvoeren die beschikbaar zijn zodra de CyberApp-workloads worden weergegeven in de console: workloads handmatig samenvoegen tot een geaggregeerde workload en aangepaste acties uitvoeren die zijn geconfigureerd in de CyberApp.

Samenvoegen

Vereisten

- Er zijn workloads uit verschillende bronnen beschikbaar voor de tenant.

U kunt een Acronis-workload handmatig samenvoegen met een of meerdere CyberApp-workloads en hiervan één geaggregeerde workload maken.

Workloads handmatig samenvoegen tot een geaggregeerde workload:

1. Ga naar het scherm **Alle apparaten** en selecteer de workloads die u wilt samenvoegen.

   Opmerking
   De samenvoegactie wordt weergegeven als u workloads uit verschillende bronnen selecteert, zoals een Acronis-workload en een CyberApp-workload.

2. Klik op **Workloads samenvoegen**.

Aangepaste acties uitvoeren

Vereisten

- Er is een CyberApp-integratie met gedefinieerde **Workloadacties** ingeschakeld voor de tenant.

Aangepaste acties zijn acties die zijn geconfigureerd in de CyberApp en die beschikbaar zijn voor de betreffende CyberApp-workload zodra u de CyberApp-integratie voor de tenant inschakelt.

Aangepaste acties uitvoeren:

1. Klik in het scherm **Alle apparaten** op de workload.
2. Klik op **Acties van geïntegreerde apps**.
3. Klik op de actie.

Werken met geaggregeerde workloads

Naast de standaardacties die zijn ingebouwd in de Cyber Protect-console, kunt u de volgende bewerkingen uitvoeren met geaggregeerde workloads: details bekijken, bronworkloads splitsen en aangepaste acties uitvoeren die zijn geconfigureerd in de CyberApps.

Details weergeven

Vereisten

- Er is ten minste één geaggregeerde workload beschikbaar voor de tenant.

De details van een geaggregeerde workload bekijken:

1. Klik in het scherm **Alle apparaten** op de geaggregeerde workload.
2. Klik op **Details**.

   De details van de geaggregeerde workload zijn verdeeld over verschillende tabbladen. Op elk tabblad worden de details voor de betreffende workload weergegeven.

Samenvoeging opheffen

Vereisten

- Er is ten minste één geaggregeerde workload beschikbaar voor de tenant.

Wanneer u een geaggregeerde workload splitst, wordt deze niet meer weergegeven in de lijst met apparaten. In plaats daarvan ziet u een afzonderlijke vermelding voor elke bronworkload die is samengevoegd in de geaggregeerde workload.

Een geaggregeerde workload splitsen

1. Klik in het scherm **Alle apparaten** op de geaggregeerde workload die u wilt splitsen.
2. Klik op **Samenvoeging van bronworkloads opheffen**.
3. Klik in het bevestigingsvenster op **Samenvoeging opheffen**.

Aangepaste acties uitvoeren

Vereisten

- Er is ten minste één CyberApp-integratie met gedefinieerde **Workloadacties** ingeschakeld voor de tenant.

Aangepaste acties zijn acties die zijn geconfigureerd in de CyberApps en die beschikbaar zijn voor de betreffende CyberApp-workload zodra u de CyberApp-integratie voor de tenant inschakelt.

Aangepaste acties uitvoeren:

1. Klik in het scherm **Alle apparaten** op de workload.
2. Klik op **Acties van geïntegreerde apps**.
3. Afhankelijk van de beschikbare aangepaste acties voert u een van de volgende handelingen uit.
   - Als de geaggregeerde workload één CyberApp-workload bevat, klikt u op de actie.
   - Als de samengevoegde workload meer dan één CyberApp-workload bevat, klikt u op de naam van de CyberApp en vervolgens op de actie.

Workloads koppelen aan specifieke gebruikers

Opmerking
Deze functie is alleen beschikbaar als de Advanced Automation-service is ingeschakeld.

Wanneer u een workload koppelt aan een specifieke gebruiker, kunt u de workload automatisch koppelen aan nieuwe servicedesk-tickets die worden gemaakt door of toegewezen aan de gebruiker.

Een workload koppelen aan een gebruiker:

1. Ga naar **Apparaten > Alle apparaten** en selecteer vervolgens de betreffende workload.
2. Ga naar het deelvenster **Acties** en selecteer **Koppelen aan gebruiker**.
3. Selecteer de betreffende gebruiker.
   U kunt indien nodig ook de geselecteerde gebruiker wijzigen voor bestaande gekoppelde workloads.

4. Klik op **Gereed**. De geselecteerde gebruiker wordt nu weergegeven in de kolom **Gekoppelde gebruiker**.

Een workload ontkoppelen van een gebruiker

1. Ga naar **Apparaten > Alle apparaten** en selecteer vervolgens de betreffende workload.
2. Ga naar het deelvenster **Acties** en selecteer **Koppelen aan gebruiker**.
3. Klik op **Gebruiker ontkoppelen**.
4. Klik op **Gereed**.

Zoek de laatst aangemelde gebruiker

Als u apparaten wilt beheren, moeten de beheerders bepalen welke gebruiker is en was ingelogd op een apparaat. Deze informatie wordt weergegeven in het Dashboard of in de details van de workloads.

U kunt de weergave van de laatste aanmeldingsgegevens in abonnementen voor Schema's voor extern beheer in- of uitschakelen.

In het Dashboard:

1. Klik op **Apparaten**. Het venster **Alle apparaten** wordt weergegeven.
2. In de kolom **Laatste aanmelding** wordt voor elk apparaat de naam weergegeven van de gebruiker die zich de laatste keer heeft aangemeld.
3. In de kolom **Tijd van laatste aanmelding** wordt voor elk apparaat de tijd weergegeven waarop de gebruiker zich de laatste keer heeft aangemeld.

In Apparaatgegevens:

1. Klik op **Apparaten**. Het venster **Alle apparaten** wordt weergegeven.
2. Klik op het apparaat waarvan u de gegevens wilt verifiëren.
3. Klik op het pictogram **Details**. De naam van de gebruiker en de datum en tijd van de laatste aanmeldingen voor het geselecteerde apparaat worden weergegeven in het gedeelte **Laatst aangemelde gebruikers**.

Opmerking
In het gedeelte **Laatst aangemelde gebruikers** worden maximaal 5 verschillende gebruikers weergegeven die zich op het apparaat hebben aangemeld.

De kolommen Laatste aanmelding en Tijd van laatste aanmelding weergeven of verbergen in het dashboard

1. Klik op **Apparaten**. Het venster **Alle apparaten** wordt weergegeven.
2. Klik op het tandwielpictogram in de rechterbovenhoek en voer een van de volgende acties uit in het gedeelte **Algemeen**:

- Schakel de kolommen **Laatste aanmelding** en **Tijd van laatste aanmelding** in als u ze wilt weergeven op het dashboard.
- Schakel de kolommen **Laatste aanmelding** en **Tijd van laatste aanmelding** uit als u ze wilt verbergen op het dashboard.

#CyberFit-score voor machines

#CyberFit-score biedt u een mechanisme voor de evaluatie van de beveiliging en scores. Hiermee wordt de beveiligingsstatus van uw machine geëvalueerd. Beveiligingslacunes in de IT-omgeving en open aanvalsvectoren naar eindpunten worden opgespoord en er worden verbeteracties aanbevolen in de vorm van een rapport. Deze functie is beschikbaar in alle Cyber Protect-edities.

De functionaliteit voor de #CyberFit-score wordt ondersteund voor:

- Windows 7 (eerste versie) en latere versies
- Windows Server 2008 R2 en latere versies

Zo werkt het

De beveiligingsagent die is geïnstalleerd op een machine, voert een evaluatie van de beveiliging uit en berekent de #CyberFit-score voor de machine. De #CyberFit-score van een machine wordt regelmatig automatisch opnieuw berekend.

Mechanisme voor #CyberFit-scores

De #CyberFit-score voor een machine wordt berekend aan de hand van de volgende metrieken:

- Antimalwarebeveiliging 0-275
- Back-upbescherming 0-175
- Firewall 0-175
- Virtueel particulier netwerk (VPN) 0-75
- Volledige schijfversleuteling 0-125
- Netwerkbeveiliging 0-25

De maximale #CyberFit-score voor een machine is 850.

Metriek	Wat wordt geëvalueerd?	Aanbevelingen voor gebruikers	Scores
Antimalware	De agent controleert of er antimalwaresoftware is geïnstalleerd op een machine.	Bevindingen: • U hebt antimalwarebeveiliging ingeschakeld (+275 punten)	275: er is antimalwaresoftware geïnstalleerd op een machine

		• U hebt geen antimalwarebeveiliging, er is mogelijk een risico voor uw systeem (0 punten) Aanbevelingen van #CyberFit-score: Op uw machine moet een antimalwareoplossing zijn geïnstalleerd en ingeschakeld om u te beschermen tegen veiligheidsrisico's. Raadpleeg websites zoals AV-Test of AV-Comparatives voor een lijst met aanbevolen antimalwareoplossingen.	0: er is geen antimalwaresoftware geïnstalleerd op een machine
Back-up	De agent controleert of er een back-upoplossing is geïnstalleerd op een machine.	Bevindingen: • U hebt een back-upoplossing die uw gegevens beschermt (+175 punten) • Er is geen back-upoplossing gevonden, er is mogelijk een risico voor uw gegevens (0 punten) Aanbevelingen van #CyberFit-score: We raden aan om regelmatig een back-up van uw gegevens te maken om gegevensverlies of ransomwareaanvallen te voorkomen. Hieronder vindt u enkele back-upoplossingen die u kunt overwegen: • Acronis Cyber Protect / Cyber Backup / True Image • Windows Server Backup (Windows Server 2008 R2 en later)	175: er is een back-upoplossing geïnstalleerd op een machine 0: er is geen back-upoplossing geïnstalleerd op een machine
Firewall	De agent controleert of er een firewall beschikbaar is en of deze is ingeschakeld in	Bevindingen: • U hebt een firewall ingeschakeld voor	100: openbare firewall van Windows is ingeschakeld

	uw omgeving. De agent doet het volgende: 1. Controleert Windows Firewall- en netwerkbeveiliging, of er een openbare firewall is ingeschakeld. 2. Controleert Windows Firewall- en netwerkbeveiliging, of er een particuliere firewall is ingeschakeld. 3. Controleert op een firewalloplossing/agent van derden als openbare en particuliere firewalls van Windows zijn uitgeschakeld.	openbare en particuliere netwerken, of er is een firewalloplossing van derden gevonden (+175 punten) • U hebt alleen een firewall ingeschakeld voor openbare netwerken (+100 punten) • U hebt alleen een firewall ingeschakeld voor particuliere netwerken (+75 punten) • U hebt geen firewall ingeschakeld, uw netwerkverbinding is niet veilig (0 punten) Aanbevelingen van #CyberFit-score: We raden u aan om een firewall in te schakelen voor uw openbare en privénetwerken om de beveiliging tegen schadelijke aanvallen op uw systeem te verbeteren. Hieronder vindt u gedetailleerde handleidingen voor het instellen van uw Windows-firewall, afhankelijk van uw beveiligingsbehoeften en netwerkarchitectuur: Handleidingen voor eindgebruikers/werknemers: Windows Defender Firewall instellen op uw pc Windows Firewall instellen op uw pc Handleidingen voor systeembeheerders en -engineers: Windows Defender Firewall implementeren met Advanced Security	75: particuliere firewall van Windows is ingeschakeld 175: openbare en particuliere firewall van Windows zijn ingeschakeld OF een firewalloplossing van derden is ingeschakeld 0: er is geen Windows-firewall en geen firewalloplossing van derden ingeschakeld

		Geavanceerde regels maken in Windows Firewall	
Virtueel particulier netwerk (VPN)	De agent controleert of een VPN-oplossing is geïnstalleerd op een machine en of het VPN is ingeschakeld en actief is.	Bevindingen: • U hebt een VPN-oplossing en u kunt veilig gegevens ontvangen en verzenden via openbare en gedeelde netwerken (+75 punten) • Er is geen VPN-oplossing gevonden, uw verbinding met openbare en gedeelde netwerken is niet veilig (0 punten) Aanbevelingen van #CyberFit-score: We raden aan om VPN te gebruiken voor toegang tot uw bedrijfsnetwerk en vertrouwelijke gegevens. Het is essentieel om een VPN te gebruiken om uw communicatie veilig en privé te houden, vooral als u gratis internettoegang gebruikt vanuit een café, bibliotheek, luchthaven of elders. Hieronder vindt u enkele VPN-oplossingen die u kunt overwegen: • Acronis Business VPN • OpenVPN • Cisco AnyConnect • NordVPN • TunnelBear • ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81 • VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN	75: VPN is ingeschakeld en actief 0: VPN is niet ingeschakeld

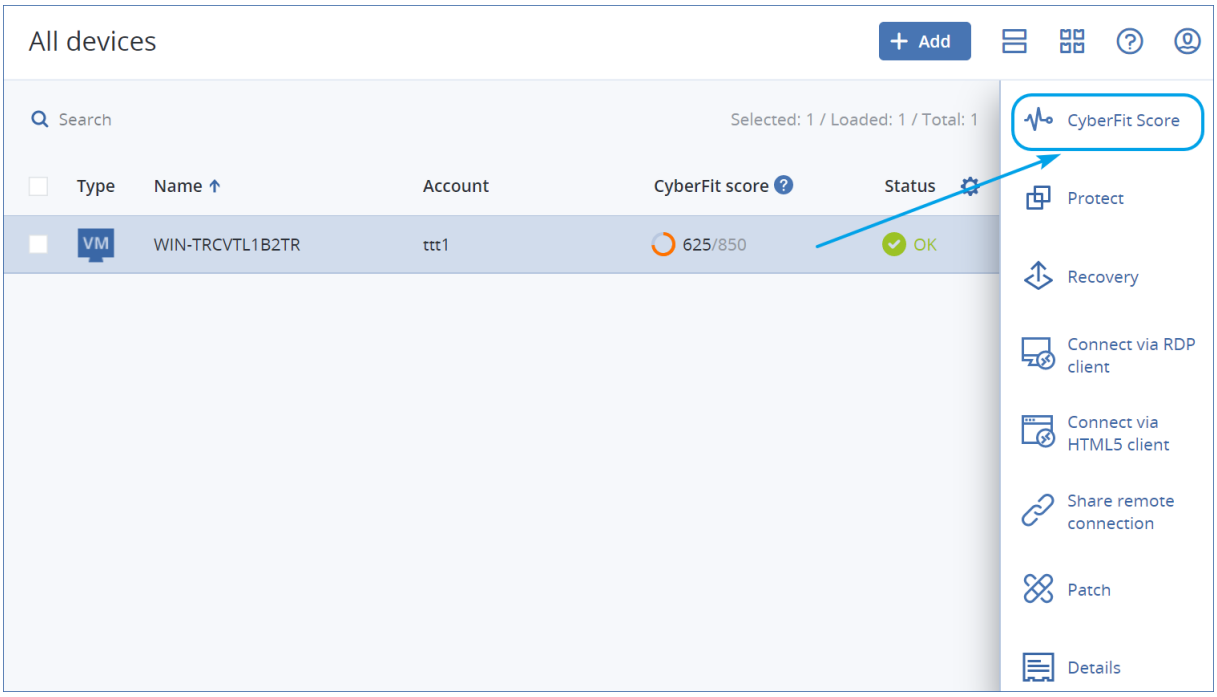
		• SonicWall GVPN • LANCOM VPN	
Schijfversleuteling	De agent controleert of schijfversleuteling is ingeschakeld op een machine. De agent controleert of Windows BitLocker is ingeschakeld.	Bevindingen: • U hebt volledige schijfversleuteling ingeschakeld, uw machine is beschermd tegen ongewenste wijzigingen (+125 punten) • Slechts enkele harde schijven zijn versleuteld, er is mogelijk een risico van ongewenste wijzigingen op uw machine (+75 punten) • Er is geen schijfversleuteling gevonden, er is een risico van ongewenste wijzigingen op uw machine (0 punten) Aanbevelingen van #CyberFit-score: We raden aan om Windows BitLocker in te schakelen als u de bescherming van uw gegevens en bestanden wilt verbeteren. Handleiding: Apparaatversleuteling inschakelen in Windows	125: alle schijven zijn versleuteld 75: ten minste één schijf is versleuteld, maar er zijn ook schijven die niet zijn versleuteld 0: er zijn geen schijven versleuteld
Netwerkbeveiliging (uitgaand NTLM-verkeer naar externe servers)	De agent controleert of uitgaand NTLM-verkeer naar externe servers is beperkt op een machine.	Bevindingen: • Uitgaand NTLM-verkeer naar externe servers wordt geweigerd, uw referenties worden beschermd (+25 punten) • Uitgaand NTLM-verkeer naar externe servers wordt niet geweigerd, uw referenties kunnen mogelijk bekend worden gemaakt (0 punten)	25: uitgaand NTLM-verkeer is ingesteld op DenyAll (alles weigeren) 0: uitgaand NTLM-verkeer is ingesteld op een andere waarde

		Aanbevelingen van #CyberFit-score: Voor een betere beveiliging raden we aan om al het uitgaande NTLM-verkeer naar externe servers te weigeren. Informatie over het wijzigen van de NTLM-instellingen en het toevoegen van uitzonderingen vindt u via de volgende koppeling. Handleiding: Uitgaand NTLM-verkeer naar externe servers beperken	

Met de som van de punten die aan elke metriek zijn toegekend, kan de totale #CyberFit-score van een machine worden bepaald en kan het beschermingsniveau van het eindpunt worden vastgesteld:

- 0 – 579: Zwak
- 580 – 669: Redelijk
- 670 – 739: Goed
- 740 – 799: Zeer goed
- 800 – 850: Uitstekend

U kunt de #CyberFit-score voor uw machines zien in de Cyber Protect-console via **Apparaten** > **Alle apparaten**. In de lijst met apparaten ziet u de kolom **#CyberFit-score**. U kunt ook een scan van de #CyberFit-score uitvoeren voor een machine om de beveiligingsstatus van die machine te controleren.

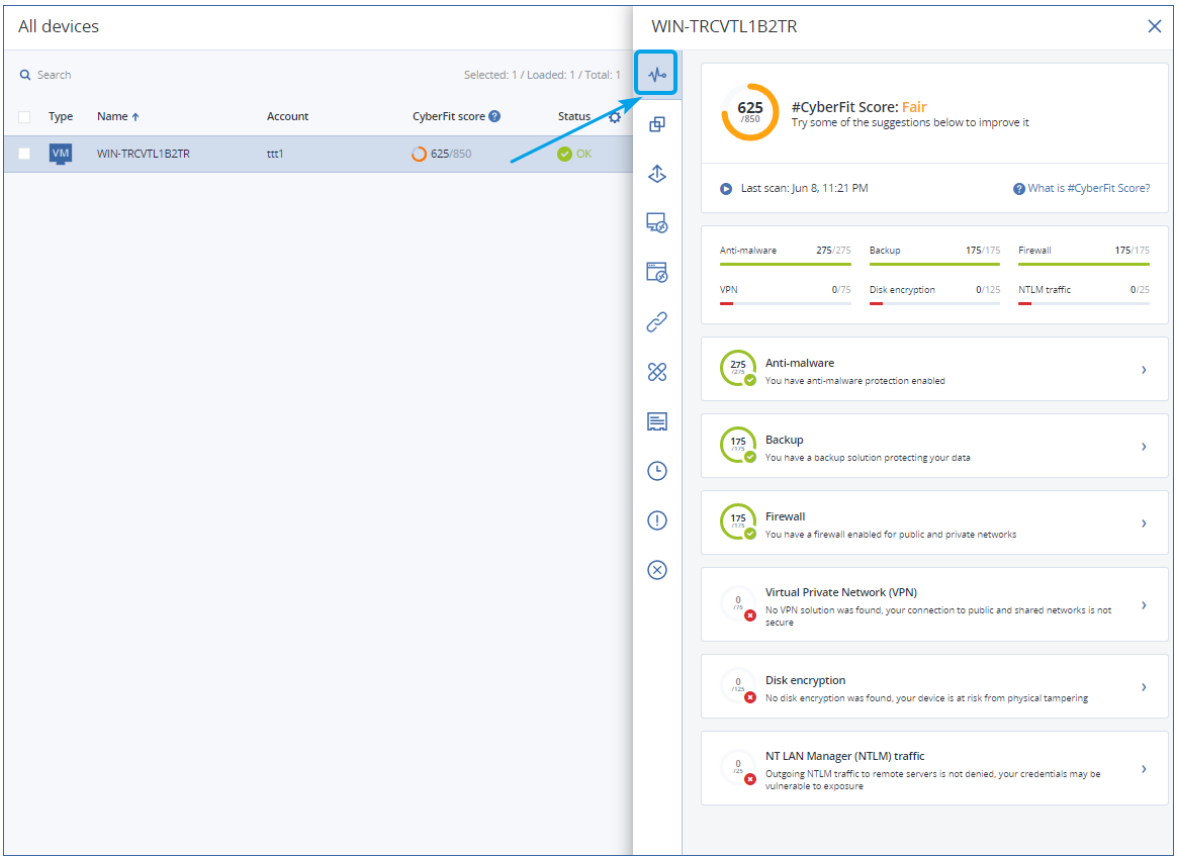


Informatie over de #CyberFit-score vindt u ook op de betreffende pagina's van de widget en het rapport.

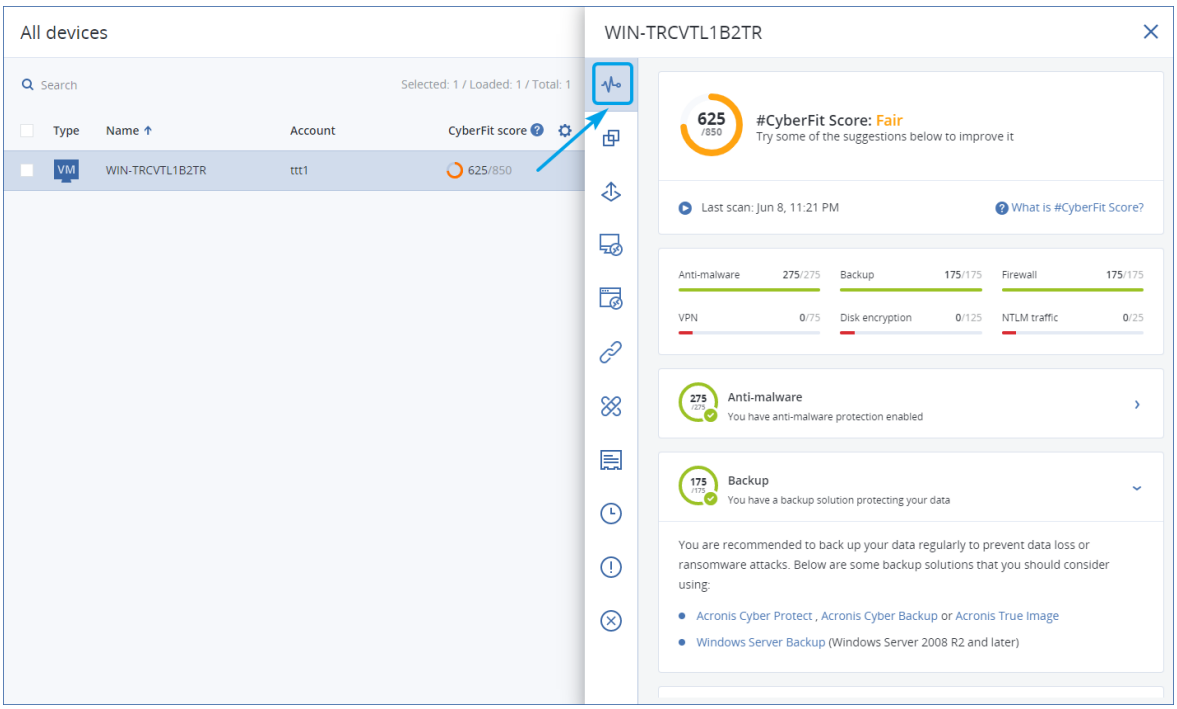
Scan van een #CyberFit-score uitvoeren

Scan van een #CyberFit-score uitvoeren

1. Ga in de Cyber Protect-console naar **Apparaten**.
2. Selecteer de machine en klik op **#CyberFit-score**.
3. Als de machine nog niet eerder is gescand, klikt u op **Een eerste scan uitvoeren**.
4. Nadat de scan is voltooid, ziet u de totale #CyberFit-score voor de machine samen met de scores voor elk van de zes geëvalueerde metrieken: antimalware, back-up, firewall, Virtual Private Network (VPN), schijfversleuteling en NTLM-verkeer (NT LAN Manager).



5. Als u wilt controleren hoe u de score kunt verhogen van elke metriek waarvoor de beveiligingsconfiguraties kunnen worden verbeterd, vouwt u het bijbehorende gedeelte uit en leest u de aanbevelingen.



6. Nadat u de aanbevelingen hebt toegepast, kunt u de #CyberFit-score van de machine altijd opnieuw berekenen door op de pijlknop rechts onder de totale #CyberFit-score te klikken.

Cyber Scripting

Met Cyber Scripting kunt u routinematige bewerkingen op Windows- en macOS-machines in uw omgeving automatiseren, bijvoorbeeld software installeren, configuraties wijzigen, services starten of stoppen en nieuwe accounts maken. Zo bent u minder tijd kwijt aan dergelijke bewerkingen en vermindert u het risico van fouten in vergelijking met handmatige bewerkingen.

Cyber Scripting is beschikbaar voor beheerders en gebruikers op klantniveau, maar ook voor partnerbeheerders (serviceproviders). Zie "Ondersteuning voor meerdere tenants" (p. 316) voor meer informatie over de verschillende beheerniveaus.

De scripts die u kunt gebruiken, moeten vooraf worden goedgekeurd. Alleen de beheerders met de rol **Cyberbeheerder** kunnen nieuwe scripts goedkeuren en testen. Zie "De scriptstatus wijzigen" (p. 407) voor meer informatie over het wijzigen van de scriptstatus.

Afhankelijk van uw gebruikersrol kunt u verschillende bewerkingen uitvoeren met scripts en scripting-plannen. Zie "Gebruikersrollen en Cyber Scripting-rechten" (p. 397) voor meer informatie over de rollen.

Vereisten

- Voor Cyber Scripting-functionaliteit is het Advanced Management-pakket vereist.
- Als u alle functies van Cyber Scripting wilt gebruiken, zoals scripts bewerken, scripts uitvoeren, scripting-schema's maken, enzovoort, moet u tweeledige verificatie inschakelen voor uw account.

Beperkingen

- De volgende scripttalen worden ondersteund:
  - PowerShell
  - Bash
- Cyber Scripting-bewerkingen kunnen alleen worden uitgevoerd op doelmachines waarop een beveiligingsagent is geïnstalleerd.

Ondersteunde platforms

Cyber Scripting is beschikbaar voor Windows- en macOS-workloads.

De volgende tabel bevat een overzicht van de ondersteunde versies.

Besturingssysteem	Versie
Windows	Windows 7 SP1 en later – alle edities
	Windows 8/8.1 – alle edities (x86, x64), met uitzondering van de Windows RT-edities.
	Windows 10 – Home, Pro, Education, Enterprise en IoT Enterprise Edition
	Windows 11
	Windows Server 2008 R2 SP1 en later – Standard, Enterprise, Datacenter, Foundation en Web Edition
	Windows Server 2012/2012 R2 – alle edities
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Storage Server (2008 R2, 2012, 2012 R2, 2016)
macOS	macOS Mojave 10.14
	macOS Catalina 10.15
	macOS Big Sur 11
	macOS Monterey 12

Gebruikersrollen en Cyber Scripting-rechten

Welke acties voor scripts en scripting-schema's beschikbaar zijn, hangt af van de status van het script en uw gebruikersrol.

Beheerders kunnen objecten beheren in hun eigen tenant en de bijbehorende onderliggende tenants. Zij hebben geen zicht op of toegang tot eventuele objecten op een hoger beheerniveau.

Beheerders op lager niveau hebben alleen leestoegang tot de scripting-schema's die door een beheerder op hoger niveau zijn toegepast op hun workloads.

De volgende rollen hebben rechten voor Cyber Scripting:

- **Bedrijfbeheerder**
  Deze rol heeft volledige beheerdersrechten voor alle services. Voor Cyber Scripting worden dezelfde rechten toegekend als aan de rol Cyberbeheerder.
- **Cyberbeheerder**
  Deze rol heeft volledige rechten, inclusief de goedkeuring van scripts die in de tenant kunnen worden gebruikt, en de mogelijkheid om scripts met de status **Testen** uit te voeren.
- **Beheerder**

Deze rol heeft gedeeltelijke rechten, met de mogelijkheid om goedgekeurde scripts uit te voeren en om scripting-schema's met goedgekeurde scripts te maken en uit te voeren.

- **Alleen-lezen beheerder**

  Deze rol heeft beperkte rechten, met de mogelijkheid om de in de tenant gebruikte scripts en beschermingsschema's te bekijken.
- **Gebruiker**

  Deze rol heeft gedeeltelijke rechten, met de mogelijkheid om goedgekeurde scripts uit te voeren en om scripting-schema's met goedgekeurde scripts te maken en uit te voeren, maar alleen op de eigen machine van de gebruiker.

De volgende tabel bevat een overzicht van alle beschikbare acties, afhankelijk van de scriptstatus en de gebruikersrol.

Rol	Object	Scriptstatus		
		Concept	**Testen**	**Goedgekeurd**
Cyberbeheerder **Bedrijfbeheerder**	Scripting-schema	Bewerken (een conceptscript uit een schema verwijderen) Verwijderen Intrekken Uitschakelen Stoppen	Maken Bewerken Toepassen Inschakelen Uitvoeren Verwijderen Intrekken Uitschakelen Stoppen	Maken Bewerken Toepassen Inschakelen Uitvoeren Verwijderen Intrekken Uitschakelen Stoppen
	Script	Maken Bewerken Status wijzigen Klonen Verwijderen Uitvoering annuleren	Maken Bewerken Status wijzigen Uitvoeren Klonen Verwijderen Uitvoering annuleren	Maken Bewerken Status wijzigen Uitvoeren Klonen Verwijderen Uitvoering annuleren
Beheerder **Gebruiker** (voor de eigen workloads)	Scripting-schema	Weergeven Intrekken Uitschakelen	Weergeven Uitvoering annuleren	Maken Bewerken Toepassen

		Stoppen		Inschakelen Uitvoeren Verwijderen Intrekken Uitschakelen Stoppen
	Script	Maken Bewerken Klonen Verwijderen Uitvoering annuleren	Weergeven Klonen Uitvoering annuleren	Uitvoeren Klonen Uitvoering annuleren
Alleen-lezen beheerder	Scripting-schema	Weergeven	Weergeven	Weergeven
	Script	Weergeven	Weergeven	Weergeven

Scripts

Een script is een reeks instructies die tijdens runtime worden geïnterpreteerd en op een doelmachine worden uitgevoerd. Het is een handige oplossing voor het automatiseren van repetitieve of complexe taken.

Met Cyber Scripting kunt u een vooraf gedefinieerd script uitvoeren of een aangepast script maken. Alle scripts die voor u beschikbaar zijn, kunt u bekijken in **Beheer** > **Opslagplaats voor scripts**. De vooraf gedefinieerde scripts vindt u in het gedeelte **Bibliotheek**. De scripts die u hebt gemaakt of gekloond naar uw tenant, vindt u in het gedeelte **Mijn scripts**.

U kunt een script gebruiken door het op te nemen in een scripting-plan of door middel van een bewerking **Script snel uitvoeren**.

Opmerking
U kunt alleen scripts gebruiken die in uw tenant zijn gemaakt of die naar uw tenant zijn gekloond. Als een script is verwijderd uit de opslagplaats voor scripts of als de status is gewijzigd in **Concept**, dan wordt het script niet uitgevoerd. U kunt de details van een scriptbewerking controleren of de bewerking annuleren via **Monitoren** > **Activiteiten**.

De volgende tabel geeft meer informatie over de mogelijke acties met een script, afhankelijk van de status.

Status	Mogelijke acties
Concept	De nieuwe scripts die u maakt en de scripts die u naar uw opslagplaats kloont, hebben de status **Concept**. Het is niet toegestaan om deze scripts uit te voeren of op te nemen in scripting-plannen.
Testen	Beheerders met de rol **Cyberbeheerder** kunnen deze scripts uitvoeren en opnemen in scripting-plannen.
Goedgekeurd	U kunt deze scripts uitvoeren en ze opnemen in scripting-plannen.

Alleen beheerders met de rol **Cyberbeheerder** kunnen de status van een script wijzigen of een goedgekeurd script verwijderen. Zie "De scriptstatus wijzigen" (p. 407) voor meer informatie.

Een script maken

U kunt een script maken door de code handmatig te schrijven.

Een script maken

1. In de Cyber Protect-console: ga naar **Beheer** > **Opslagplaats voor scripts**.
2. Klik in **Mijn scripts** op **Script maken met behulp van AI**.
3. Schrijf de hoofdtekst van het script in het hoofdvenster.

   Belangrijk
   Wanneer u een script maakt, moet u een controle van de afsluitcode opnemen voor elke bewerking. Anders wordt een mislukte bewerking mogelijk genegeerd en wordt de status van de scripting-activiteit in **Controle** > **Activiteiten** mogelijk onjuist weergegeven als **Voltooid**.

4. Geef de scriptinstellingen op.

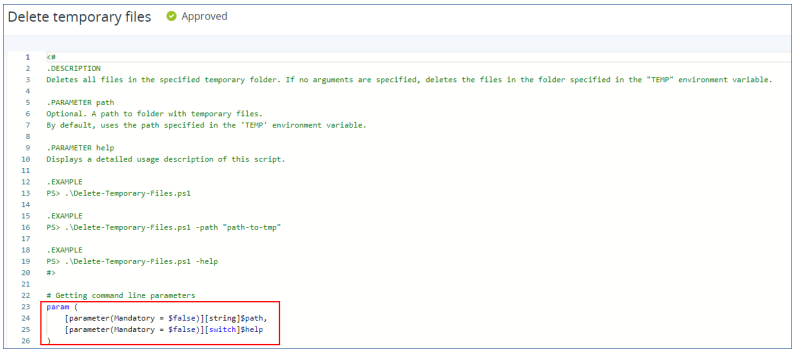
Instelling	Beschrijving
Naam van script	Scriptnaam. Het veld wordt automatisch ingevuld, maar u kunt de waarde wijzigen.
Beschrijving	Beschrijving van het script. Deze instelling is optioneel. [Voor scripts gegenereerd door AI] Het veld wordt automatisch ingevuld tijdens het genereren van het script. U kunt de door AI verstrekte beschrijving bewerken.
Taal	Taal van het script. De beschikbare waarden zijn: • **PowerShell**. Dit is de standaardwaarde. • **Bash** [Voor scripts gegenereerd door AI] Deze instelling wordt geconfigureerd voordat het script wordt gegenereerd.
Besturingssysteem	Besturingssysteem dat is geïnstalleerd op de doelworkload waarop het script zal worden uitgevoerd. De beschikbare waarden zijn:

Instelling	Beschrijving
	• **Windows**. Dit is de standaardwaarde. • **macOS** [Voor scripts gegenereerd door AI] Deze instelling wordt geconfigureerd voordat het script wordt gegenereerd.
Status	Status van het script. • **Concept**. Dit is de standaardwaarde. De nieuwe scripts die u maakt en de scripts die u naar uw opslagplaats kloont, hebben de status **Concept**. Het is niet toegestaan om scripts met de status **Concept** uit te voeren of ze op te nemen in scripting-plannen. • **Testen**. Alleen beheerders met de rol van **Cyberbeheerder** kunnen de status van een script wijzigen in **Testen**, scripts met de status **Testen** uitvoeren en scripting-plannen met dergelijke scripts uitvoeren. • **Goedgekeurd**. U kunt scripts met de status **Goedgekeurd** uitvoeren en opnemen in scripting-plannen. Alleen beheerders met de rol **Cyberbeheerder** kunnen de status van een script wijzigen of een goedgekeurd script verwijderen. Zie "De scriptstatus wijzigen" (p. 407) voor meer informatie.
Tags	De tags zijn niet hoofdlettergevoelig en kunnen maximaal 32 tekens lang zijn. U kunt geen ronde haken en punthaken, komma's en spaties gebruiken. Deze instelling is optioneel. [Voor scripts gegenereerd door AI] De tag **AI-gegenereerd** wordt automatisch toegevoegd bij het genereren van scripts. U kunt deze tag handmatig verwijderen of meer tags toevoegen.

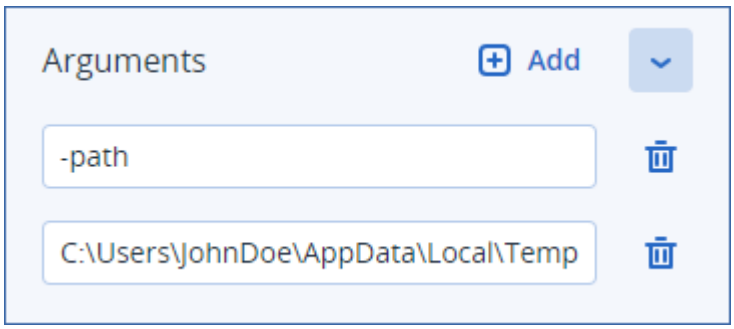
5. [Alleen voor scripts waarvoor referenties zijn vereist] Geef de referenties op.

   U kunt een enkele referentie gebruiken (bijvoorbeeld een token) of een paar referenties (bijvoorbeeld een gebruikersnaam en een wachtwoord).
6. [Alleen voor scripts waarvoor argumenten zijn vereist] Geef de argumenten en bijbehorende waarden op, als volgt:
   a. Klik op **Toevoegen**.
   b. In het veld **Argumenten toevoegen** geeft u het argument op.
   c. Klik op **Toevoegen**.
   d. In het tweede veld dat wordt weergegeven, geeft u de argumentwaarde op.

Opmerking
U kunt alleen argumenten opgeven die u al in de hoofdtekst van het script hebt gedefinieerd.



Bijvoorbeeld:



e. Herhaal bovenstaande stappen als u meer dan één argument wilt toevoegen.

7. Klik op **Opslaan**.

Het script wordt opgeslagen in uw opslagplaats, met de status **Concept**.

U kunt het script niet gebruiken totdat een beheerder met de rol **Cyberbeheerder** de status ervan wijzigt in **Goedgekeurd**. Zie "De scriptstatus wijzigen" (p. 407) Voor meer informatie.

Als u een script wilt gebruiken in een andere tenant die u beheert, moet u het script klonen naar die tenant. Zie "Een script klonen" (p. 405) voor meer informatie.

Een script maken met behulp van AI

Opmerking
Voor deze functionaliteit is het Advanced Management-pakket vereist.

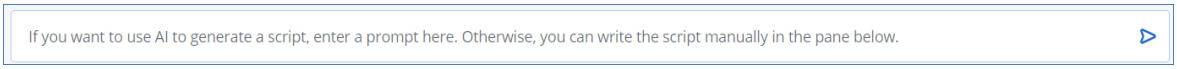
U kunt AI gebruiken om prompts om te zetten in krachtige scripts, waardoor u tijd en moeite bespaart. U kunt de functionaliteit op de volgende manieren gebruiken:

- Voer een prompt in om AI te vragen een compleet nieuw script te genereren.
- Voer een prompt in om AI te vragen een door u in de scripttekst ingevoerde code te beoordelen en te voltooien. U kunt deze mogelijkheid gebruiken in het geval van complexere codes.

De functionaliteit maakt gebruik van het GPT-4 model van OpenAI. U kunt gratis maximaal 100 scripts per kalendermaand maken voor uw organisatie.

Een script maken met behulp van AI:

1. In de Cyber Protect-console: ga naar **Beheer** > **Opslagplaats voor scripts**.
2. Klik in **Mijn scripts** op **Een script maken met behulp van AI**.
3. Voer in de prompt een beschrijving in van wat het script moet doen. Maak de beschrijving zo duidelijk en gedetailleerd mogelijk.

   Bijvoorbeeld:

   ```
   I need a script that deletes Temporary files for all users (including user profiles +
   Windows Temps) and disable Windows Update Service to allow the script to run
   ```

4. Klik in de prompt op de pijlknop.
5. Ga naar het bevestigingsvenster, selecteer Taal en Besturingssysteem en klik vervolgens op **Genereren**.

   Het script dat door AI wordt gegenereerd, wordt weergegeven in het hoofdvenster. De naam en beschrijving van het script worden automatisch door AI gegenereerd zodat ze overeenkomen met het script. De tag **AI-gegenereerd** wordt automatisch toegewezen aan het script.
6. Bekijk het script dat door AI is gegenereerd en bewerk het handmatig, indien nodig.
7. Bewerk de scriptinstellingen, indien nodig.

Instelling	Beschrijving
Naam van script	Scriptnaam. Het veld wordt automatisch ingevuld, maar u kunt de waarde wijzigen.
Beschrijving	Beschrijving van het script. Deze instelling is optioneel. [Voor scripts gegenereerd door AI] Het veld wordt automatisch ingevuld tijdens het genereren van het script. U kunt de door AI verstrekte beschrijving bewerken.
Taal	Taal van het script. De beschikbare waarden zijn: • **PowerShell**. Dit is de standaardwaarde. • **Bash** [Voor scripts gegenereerd door AI] Deze instelling wordt geconfigureerd voordat het script wordt gegenereerd.
Besturingssysteem	Besturingssysteem dat is geïnstalleerd op de doelworkload waarop het script zal worden uitgevoerd. De beschikbare waarden zijn: • **Windows**. Dit is de standaardwaarde. • **macOS** [Voor scripts gegenereerd door AI] Deze instelling wordt geconfigureerd

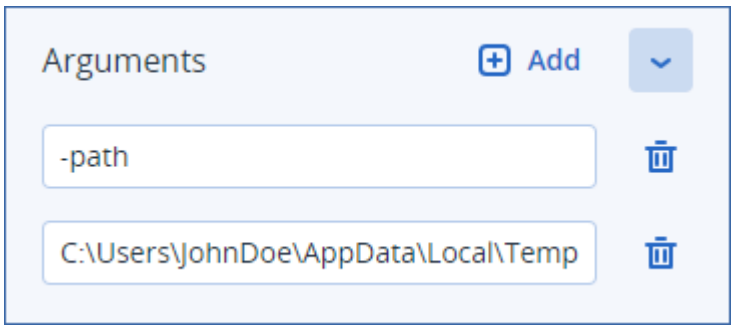
Instelling	Beschrijving
	voordat het script wordt gegenereerd.
Status	Status van het script. • **Concept**. Dit is de standaardwaarde. De nieuwe scripts die u maakt en de scripts die u naar uw opslagplaats kloont, hebben de status **Concept**. Het is niet toegestaan om scripts met de status **Concept** uit te voeren of ze op te nemen in scripting-plannen. • **Testen**. Alleen beheerders met de rol van **Cyberbeheerder** kunnen de status van een script wijzigen in **Testen**, scripts met de status **Testen** uitvoeren en scripting-plannen met dergelijke scripts uitvoeren. • **Goedgekeurd**. U kunt scripts met de status **Goedgekeurd** uitvoeren en opnemen in scripting-plannen. Alleen beheerders met de rol **Cyberbeheerder** kunnen de status van een script wijzigen of een goedgekeurd script verwijderen. Zie "De scriptstatus wijzigen" (p. 407) voor meer informatie.
Tags	De tags zijn niet hoofdlettergevoelig en kunnen maximaal 32 tekens lang zijn. U kunt geen ronde haken en punthaken, komma's en spaties gebruiken. Deze instelling is optioneel. [Voor scripts gegenereerd door AI] De tag **AI-gegenereerd** wordt automatisch toegevoegd bij het genereren van scripts. U kunt deze tag handmatig verwijderen of meer tags toevoegen.

8. [Optioneel] [Alleen voor scripts waarvoor referenties zijn vereist] Geef de referenties op.
   U kunt een enkele referentie gebruiken (bijvoorbeeld een token) of een paar referenties (bijvoorbeeld een gebruikersnaam en een wachtwoord).
9. [Alleen voor scripts waarvoor argumenten zijn vereist] Geef de argumenten en bijbehorende waarden op, als volgt:
   a. Klik op **Toevoegen**.
   b. In het veld **Argumenten toevoegen** geeft u het argument op.
   c. Klik op **Toevoegen**.
   d. In het tweede veld dat wordt weergegeven, geeft u de argumentwaarde op.

Opmerking

U kunt alleen argumenten opgeven die u al in de hoofdtekst van het script hebt gedefinieerd.

Bijvoorbeeld:



e. Herhaal bovenstaande stappen als u meer dan één argument wilt toevoegen.

10. Klik op **Opslaan**.

    Het script wordt opgeslagen in uw opslagplaats, met de status **Concept**.

    U kunt het script niet gebruiken totdat een beheerder met de rol **Cyberbeheerder** de status ervan wijzigt in **Goedgekeurd**. Zie "De scriptstatus wijzigen" (p. 407) Voor meer informatie.

    Als u een script wilt gebruiken in een andere tenant die u beheert, moet u het script klonen naar die tenant. Zie "Een script klonen" (p. 405) voor meer informatie.

Een script klonen

Het klonen van een script is vereist in de volgende gevallen:

- Voordat u een script uit **Bibliotheek** gebruikt. In dit geval moet u eerst het script klonen naar het gedeelte **Mijn scripts**.
- Wanneer u scripts die u hebt gemaakt in een bovenliggende tenant, wilt klonen naar onderliggende tenants of eenheden.

Een script klonen

1. In **Opslagplaats voor scripts**: zoek het script dat u wilt klonen.
2. Voer een van de volgende handelingen uit:
   - [Als u een script uit **Mijn scripts** wilt klonen] Klik op de ellips (...) naast de naam van het script en klik vervolgens op **Klonen**.

- [Als u een script kloont uit **Bibliotheek**] Klik op **Klonen** naast de naam van het script dat u hebt geselecteerd.

3. Ga naar het pop-upvenster **Script klonen** en selecteer een van de volgende scriptstatussen in de vervolgkeuzelijst **Status**:
   - **Concept** (standaard): met deze status kunt u het script niet meteen uitvoeren.
   - **Testen** (standaard): met deze status kunt u het script uitvoeren.
   - **Goedgekeurd**: met deze status kunt u het script uitvoeren.
4. [Als u meer dan één tenant of eenheid beheert] Selecteer waar u het script wilt klonen.
   In het dialoogvenster **Script klonen** ziet u alleen de tenants die u kunt beheren en waarop het Advanced Management-pakket is toegepast.

Als resultaat wordt het script gekloond naar het gedeelte **Mijn scripts** van de tenant of eenheid die u hebt geselecteerd. Als u slechts één tenant zonder eenheden beheert, wordt het script automatisch gekopieerd naar het gedeelte **Mijn scripts**.

Belangrijk
Referenties die door een script worden gebruikt, worden niet gekopieerd wanneer u een script kloont naar een andere tenant dan de oorspronkelijke tenant.

Een script bewerken of verwijderen

Opmerking
Afhankelijk van uw gebruikersrol kunt u verschillende bewerkingen uitvoeren met scripts en scripting-plannen. Zie "Gebruikersrollen en Cyber Scripting-rechten" (p. 397) voor meer informatie over de rollen.

Een script bewerken

1. In **Opslagplaats voor scripts**: ga naar **Mijn scripts** en zoek het script dat u wilt bewerken.
2. Klik op de ellips (...) naast de naam van het script en klik vervolgens op **Bewerken**.
3. Bewerk het script en klik op **Opslaan**.
4. [Als u een script bewerkt dat wordt gebruikt door een scripting-schema] Bevestig uw keuze door te klikken op **Script opslaan**.

   Opmerking
   De meest recente versie van het script zal worden gebruikt bij de volgende keer dat het scripting-schema wordt uitgevoerd.

Scriptversies

Een nieuwe versie van het script wordt gemaakt als u een van de volgende scriptkenmerken wijzigt:

- hoofdtekst van script
- naam van script
- beschrijving
- taal van script
- referenties
- argumenten

Als u andere kenmerken wijzigt, worden uw bewerkingen toegevoegd aan de huidige scriptversie. Zie "Scriptversies vergelijken" (p. 408) voor meer informatie over versies en hoe u deze kunt vergelijken.

Opmerking
De scriptstatus wordt alleen bijgewerkt wanneer u de waarde in het veld **Status** wijzigt. Alleen beheerders met de rol Cyberbeheerder kunnen de status van een script wijzigen.

Een script verwijderen

1. In **Opslagplaats voor scripts**: ga naar **Mijn scripts** en zoek het script dat u wilt verwijderen.
2. Klik op de ellips (...) naast de naam van het script en klik vervolgens op **Verwijderen**.
3. Klik op **Verwijderen**.
4. [Als u een script wilt verwijderen dat wordt gebruikt door een scripting-schema] Bevestig uw keuze door te klikken op **Script opslaan**.

   Opmerking
   Scripting-schema's waarin het verwijderde script wordt gebruikt, kunnen dan niet meer worden uitgevoerd.

De scriptstatus wijzigen

Een nieuw script dat is gemaakt en de status **Concept** heeft, kan niet worden gebruikt totdat de status is gewijzigd in **Goedgekeurd**. Afhankelijk van het gebruiksscenario kan een script gedurende een bepaalde periode de status **Testen** hebben voordat het wordt goedgekeurd.

Opmerking
Afhankelijk van uw gebruikersrol kunt u verschillende bewerkingen uitvoeren met scripts en scripting-plannen. Zie "Gebruikersrollen en Cyber Scripting-rechten" (p. 397) voor meer informatie over de rollen.

Vereisten

- Uw gebruiker is een beheerder aan wie de rol van **Cyberbeheerder** is toegewezen.
- Een script met de overeenkomstige status is beschikbaar.

De scriptstatus wijzigen

1. Open **Opslagplaats voor scripts** en ga naar **Mijn scripts**.
2. Klik op de ellips (...) naast de naam van het script en klik vervolgens op **Bewerken**.
3. Open de vervolgkeuzelijst **Status** en selecteer de status.
4. Klik op **Opslaan**.
5. [Als u de status van een goedgekeurd script wijzigt] Bevestig de wijziging door te klikken op **Script opslaan**.

Opmerking
Als de scriptstatus is gedowngraded naar **Concept**, worden de betreffende scripting-schema's niet uitgevoerd.
Alleen beheerders met de rol **Cyberbeheerder** kunnen scripts met de status **Testen** en scripting-plannen met dergelijke scripts uitvoeren.

Scriptversies vergelijken

U kunt twee versies van een script vergelijken en terugkeren naar een eerdere versie. U kunt ook controleren wie een bepaalde versie heeft gemaakt, en wanneer deze is gemaakt.

Scriptversies vergelijken

1. In **Opslagplaats voor scripts**: ga naar **Mijn scripts** en zoek het script waarvan u de versies wilt vergelijken.
2. Klik op de ellips (...) naast de naam van het script en klik vervolgens op **Versiegeschiedenis**.
3. Selecteer de twee versies die u wilt vergelijken en klik vervolgens op **Versies vergelijken**.
   Alle wijzigingen in de hoofdtekst van het script en de argumenten of de referenties worden gemarkeerd.

Terugkeren naar een eerdere versie:

1. Klik in het venster **Scriptversies vergelijken** op **Terugzetten naar deze versie**.
2. Ga naar het pop-upvenster **Teruggaan naar een vorige versie** en selecteer de scriptstatus in de vervolgkeuzelijst **Status**.

De geselecteerde versie wordt hersteld en opgeslagen als de meest recente versie in de versiegeschiedenis.

Als u een script wilt herstellen, kunt u ook een versie selecteren in het venster **Versiegeschiedenis** en vervolgens op de knop **Herstellen** klikken.

Belangrijk
U kunt alleen scripts uitvoeren met de status **Testen** of **Goedgekeurd**. Zie "De scriptstatus wijzigen" (p. 407) voor meer informatie.

De uitvoer van een scriptbewerking downloaden

U kunt de uitvoer van een scriptbewerking downloaden als zipbestand. Het bevat twee tekstbestanden: `stdout` en `stderr`. In `stdout` ziet u de resultaten van een uitgevoerde scriptbewerking. Het bestand `stderr` bevat informatie over de fouten die zich hebben voorgedaan tijdens de scriptbewerking.

Het gewenste uitvoerbestand downloaden

1. In de Cyber Protect-console: ga naar **Controle** > **Activiteiten**.
2. Klik op de Cyber Scripting-activiteit waarvan u de uitvoer wilt downloaden.
3. Klik in het scherm **Activiteitgegevens** op **Uitvoer downloaden**.

Opslagplaats voor scripts

U kunt de opslagplaats voor scripts vinden op het tabblad **Beheer**. In de opslagplaats kunt u de scripts zoeken op naam en beschrijving. U kunt ook filters gebruiken of de scripts sorteren op naam of status.

Als u een script wilt beheren, klikt u op de ellips (...) naast de naam van het script en selecteert u vervolgens de gewenste actie. U kunt ook op het script klikken en de knoppen gebruiken op het scherm dat wordt weergegeven.

De opslagplaats voor scripts bevat de volgende gedeelten:

- **Mijn scripts**
  Hier vindt u de scripts die u direct in uw omgeving kunt gebruiken. Dit zijn de scripts die u zelf hebt gemaakt en de scripts die u hier hebt gekloond.
  U kunt de scripts in dit gedeelte filteren op de volgende criteria:
  - Tags
  - Status
  - Taal
  - Besturingssysteem
  - Eigenaar van script
- **Bibliotheek**
  De bibliotheek bevat vooraf gedefinieerde scripts die u in uw omgeving kunt gebruiken nadat u ze hebt gekloond naar het gedeelte **Mijn scripts**. U kunt deze scripts alleen inspecteren en klonen.
  U kunt de scripts in dit gedeelte filteren op de volgende criteria:
  - Tags
  - Taal

- Besturingssysteem

Zie Door de leverancier goedgekeurde scripts (70595) voor meer informatie.

Scripting-schema's

U kunt een scripting-schema gebruiken om een script voor meerdere workloads uit te voeren, de uitvoering van een script te plannen en aanvullende instellingen te configureren.

De scripting-schema's die u hebt gemaakt en de schema's die worden toegepast op uw workloads, kunt u vinden in **Beheer** > **Scripting-schema's**. Hier kunt u de plaats van uitvoering van het schema, de eigenaar of de status controleren.

De statussen van scripting-schema's worden weergegeven op een klikbare balk met de volgende kleurcodes:

- Actief (blauw)
- Controleren op compatibiliteit (donkergrijs)
- Uitgeschakeld (lichtgrijs)
- OK (groen)
- Kritieke waarschuwing (rood)
- Fout (oranje)
- Waarschuwing (geel)

Als u op de balk klikt, kunt u zien welke status een schema heeft en voor hoeveel workloads. Elke status kan ook worden aangeklikt.

Op het tabblad **Scripting-schema's** kunt u de schema's beheren door de volgende acties uit te voeren:

- Uitvoeren
- Stoppen
- Bewerken
- Naam wijzigen
- Uitschakelen
- Inschakelen
- Klonen
- Exporteren. De configuratie van het plan wordt geëxporteerd in een JSON-indeling naar de lokale machine.
- Verwijderen

In hoeverre een scripting-schema zichtbaar is en welke acties mogelijk zijn, hangt af van de eigenaar van het schema en uw gebruikersrol. Bedrijfbeheerders kunnen bijvoorbeeld alleen scripting-

schema's van partners zien die op hun workloads worden toegepast, en kunnen geen acties voor deze schema's uitvoeren.

Zie "Gebruikersrollen en Cyber Scripting-rechten" (p. 397) voor meer informatie over wie scripting-schema's kan maken en beheren.

Een scripting-schema beheren

1. In de Cyber Protect-console: ga naar **Beheer** > **Scripting-schema's**.
2. Zoek het schema dat u wilt beheren en klik vervolgens op de ellips (...) naast het betreffende schema.
3. Selecteer de gewenste actie en volg de instructies op het scherm.

Een scripting-schema maken

U kunt een scripting-schema op de volgende manieren maken:

- Op het tabblad **Apparaten**
  Selecteer workloads en maak hier een scripting-schema voor.
- Op het tabblad **Beheer** > **Scripting-schema's**
  Maak een scripting-schema en selecteer vervolgens de workloads waarop het schema moet worden toegepast.

Een scripting-schema maken op het tabblad Apparaten

1. In de Cyber Protect-console: ga naar **Apparaten** > **Machine met agents**.
2. Selecteer de workloads of de apparaatgroepen waarop u een scripting-schema wilt toepassen en klik vervolgens respectievelijk op **Beschermen** of **Groep beschermen**.
3. [Indien er reeds toegepaste schema's zijn] Klik op **Schema toevoegen**.
4. Klik op **Schema maken** > **Scripting-schema**.
   Er wordt een sjabloon voor het scripting-schema geopend.
5. [Optioneel] Klik op het potloodpictogram om de naam van het scripting-schema te wijzigen.
6. Klik op **Script kiezen**, selecteer het script dat u wilt gebruiken en klik op **Gereed**.

   Opmerking
   U kunt alleen uw goedgekeurde scripts gebruiken uit **Opslagplaats voor scripts** > **Mijn scripts**. Alleen een beheerder met de rol **Cyberbeheerder** kan scripts met de status **Testen** gebruiken. Zie "Gebruikersrollen en Cyber Scripting-rechten" (p. 397) voor meer informatie over de rollen.

7. Configureer het schema en de startvoorwaarden voor het scripting-schema.
8. Kies onder welk account het script wordt uitgevoerd voor de doelworkload. De volgende opties zijn beschikbaar:
   - Systeemaccount (in macOS is dit het rootaccount)
   - Momenteel aangemeld account

9. Geef op hoe lang het script kan worden uitgevoerd voor de doelworkload.
   Als het script niet geheel binnen de ingestelde tijd kan worden uitgevoerd, mislukt de Cyber Scripting-bewerking.
   De minimumwaarde die u kunt opgeven, is één minuut en de maximumwaarde is 1440 minuten.
10. [Alleen voor PowerShell-scripts] Configureer het uitvoeringsbeleid voor PowerShell.
    Zie de Microsoft-documentatie voor meer informatie over dit beleid.
11. Klik op **Maken**.

Een scripting-schema maken op het tabblad Scripting-schema's

1. In de Cyber Protect-console: ga naar **Beheer** > **Scripting-schema's**.
2. Klik op **Schema maken**.
   Er wordt een sjabloon voor het scripting-schema geopend.
3. [Optioneel] Klik op **Workloads toevoegen** om de workloads of apparaatgroepen te selecteren waarop u het nieuwe schema wilt toepassen.
   a. Klik op **Machines met agents** om de lijst uit te vouwen en selecteer vervolgens de gewenste workloads of apparaatgroepen.
   b. Klik op **Toevoegen**.

   Zie "Tabblad Apparaten" (p. 311) voor meer informatie over het maken van apparaatgroepen op partnerniveau.

   Opmerking
   U kunt ook workloads of apparaatgroepen selecteren nadat u het schema hebt gemaakt.

4. [Optioneel] Klik op het potloodpictogram om de naam van het scripting-schema te wijzigen.
5. Klik op **Script kiezen**, selecteer het script dat u wilt gebruiken en klik op **Gereed**.

   Opmerking
   U kunt alleen uw goedgekeurde scripts gebruiken uit **Opslagplaats voor scripts** > **Mijn scripts**.
   Alleen een beheerder met de rol **Cyberbeheerder** kan scripts met de status **Testen** gebruiken.
   Zie "Gebruikersrollen en Cyber Scripting-rechten" (p. 397) voor meer informatie over de rollen.

6. Configureer het schema en de startvoorwaarden voor het scripting-schema.
7. Kies onder welk account het script wordt uitgevoerd voor de doelworkload. De volgende opties zijn beschikbaar:
   - Systeemaccount (in macOS is dit het rootaccount)
   - Momenteel aangemeld account
8. Geef op hoe lang het script kan worden uitgevoerd voor de doelworkload.
   Als het script niet geheel binnen de ingestelde tijd kan worden uitgevoerd, mislukt de Cyber Scripting-bewerking.
   De minimumwaarde die u kunt opgeven, is één minuut en de maximumwaarde is 1440 minuten.
9. [Alleen voor PowerShell-scripts] Configureer het uitvoeringsbeleid voor PowerShell.

Zie de Microsoft-documentatie voor meer informatie over dit beleid.

10. Klik op **Maken**.

Schema en startvoorwaarden

Planning

Bij de configuratie van een scripting-schema kunt u kiezen of het eenmalig of herhaaldelijk wordt uitgevoerd, en of het volgens schema of door een bepaalde gebeurtenis wordt gestart.

De volgende opties zijn beschikbaar:

- Eenmalig uitvoeren

  Bij deze optie moet u de datum en tijd configureren wanneer het schema wordt uitgevoerd.
- Planning op tijd

  Met deze optie kunt u scripting-schema's configureren die elk uur, elke dag of eens per maand worden uitgevoerd.

  Als u een schema slechts tijdelijk wilt gebruiken, schakelt u het selectievakje **Uitvoeren binnen een datumbereik** in en configureert u de periode gedurende welke het geplande schema wordt uitgevoerd.
- Wanneer de gebruiker zich aanmeldt bij het systeem

  U kunt kiezen of het scripting-schema kan worden gestart door een specifieke gebruiker of elke gebruiker die zich aanmeldt.
- Wanneer de gebruiker zich afmeldt bij het systeem

  U kunt kiezen of het scripting-schema kan worden gestart door een specifieke gebruiker of elke gebruiker die zich afmeldt.
- Wanneer het systeem wordt opgestart
- Wanneer het systeem wordt uitgeschakeld

  Opmerking
  Deze planningsoptie werkt alleen met scripts die worden uitgevoerd voor het systeemaccount.
- Wanneer het systeem online gaat

Startvoorwaarden

Startvoorwaarden geven meer flexibiliteit aan uw geplande schema's. Als u meerdere voorwaarden configureert, moet er tegelijkertijd aan al deze voorwaarden worden voldaan om een schema te kunnen starten.

Startvoorwaarden zijn niet effectief als u het schema handmatig uitvoert met de optie **Nu uitvoeren**.

Voorwaarde	Beschrijving
Alleen uitvoeren als de workload online is	Het script wordt uitgevoerd wanneer de doelworkload is verbonden met internet.
Gebruiker is niet-actief	Aan deze voorwaarde wordt voldaan wanneer er op de machine een schermbeveiliging wordt uitgevoerd of wanneer de machine is vergrendeld.
Gebruiker afgemeld	Met deze voorwaarde kunt u een gepland scripting-schema uitstellen totdat de gebruiker van de doelworkload zich afmeldt.
Binnen tijdsinterval	Met deze voorwaarde kan een scripting-schema alleen worden gestart binnen het opgegeven tijdsinterval. U kunt deze voorwaarde bijvoorbeeld gebruiken om de voorwaarde **Gebruiker afgemeld** te beperken.
Batterijstroom besparen	Met deze voorwaarde kunt u waarborgen dat het scripting-schema niet wordt onderbroken vanwege een bijna lege batterij. De volgende opties zijn beschikbaar: • Niet starten bij gebruik van batterijstroom Het schema wordt alleen gestart als de machine is aangesloten op een stroombron. • Starten bij gebruik van batterijstroom als het batterijniveau hoger is dan Het schema wordt gestart als het apparaat is aangesloten op een stroombron of als het batterijniveau hoger is dan de opgegeven waarde.
Niet starten bij verbinding met een datalimiet	Deze voorwaarde voorkomt dat het schema wordt gestart als de doelworkload toegang heeft tot internet via een verbinding met een datalimiet.
Niet starten indien verbonden met de volgende wifinetwerken	Deze voorwaarde voorkomt dat het schema wordt gestart als de doelworkload is verbonden met een van de opgegeven draadloze netwerken. Als u deze voorwaarde wilt gebruiken, moet u de SSID van het verboden netwerk opgeven. De beperking is van toepassing op alle netwerken die de opgegeven naam als substring bevatten in hun naam (niet hoofdlettergevoelig). Als u bijvoorbeeld `telefoon` opgeeft als de netwerknaam, wordt het schema niet gestart wanneer het apparaat is verbonden met een van de volgende netwerken: `Jans telefoon`, `telefoon_wifi` of `mijn_TELEFOON_wifi`.
IP-adres van apparaat controleren	Deze voorwaarde voorkomt dat het schema wordt gestart als een van de IP-adressen van de doelworkload binnen of buiten het bereik van de opgegeven IP-adressen is. De volgende opties zijn beschikbaar: • Starten indien buiten IP-bereik • Starten indien binnen IP-bereik Alleen IPv4-adressen worden ondersteund.

Voorwaarde	Beschrijving
De taak uitvoeren zelfs als niet aan de startvoorwaarden wordt voldaan	Met deze optie kunt u het tijdsinterval instellen waarna het schema zal worden uitgevoerd, ongeacht eventuele andere voorwaarden. De taak wordt gestart zodra aan de andere voorwaarden wordt voldaan of wanneer de opgegeven periode eindigt, afhankelijk van wat als eerste plaatsvindt. Deze optie is niet beschikbaar als u hebt geconfigureerd dat het scripting-schema slechts eenmaal wordt uitgevoerd.

De doelworkloads voor een schema beheren

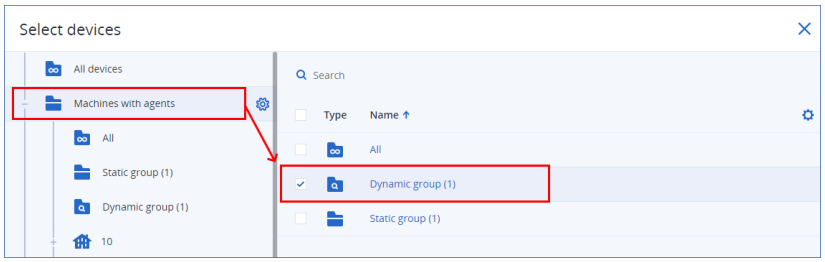
U kunt de workloads of de apparaatgroepen selecteren waarop u een scripting-schema wilt toepassen. U kunt dit doen terwijl u het schema maakt of later.

Partnerbeheerders kunnen hetzelfde schema toepassen op workloads van verschillende klanten en kunnen apparaatgroepen maken die workloads van verschillende klanten bevatten. Raadpleeg "Tabblad Apparaten" (p. 311) om te zien hoe u een statische of een dynamische apparaatgroep op partnerniveau maakt.

Initiële workloads toevoegen aan een schema

1. In de Cyber Protect-console: ga naar **Beheer** > **Scripting-schema's**.
2. Klik op de naam van het schema waarvoor u doelworkloads wilt opgeven.
3. Klik op **Workloads toevoegen**.
4. Selecteer de gewenste workloads of apparaatgroepen en klik vervolgens op **Toevoegen**.

Opmerking
Als u een apparaatgroep wilt selecteren, klikt u op het bovenliggende niveau en vervolgens schakelt u in het hoofdvenster het selectievakje naast de naam in.



5. Klik op **Opslaan** om het bewerkte schema op te slaan.

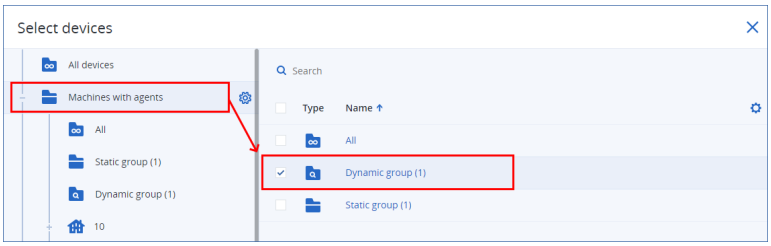
Bestaande workloads voor een schema beheren

1. In de Cyber Protect-console: ga naar **Beheer** > **Scripting-schema's**.
2. Klik op de naam van het schema waarvan u de doelworkloads wilt wijzigen.
3. Klik op **Workloads beheren**.

Op het scherm **Apparaten** wordt een lijst weergegeven van de workloads waarop het scripting-schema momenteel wordt toegepast. Als u meer dan één tenant beheert, worden de workloads gesorteerd per tenant.

- Als u nieuwe workloads of apparaatgroepen wilt toevoegen, klikt u op **Toevoegen**.
  a. Selecteer de gewenste workloads of apparaatgroepen. U kunt workloads toevoegen van alle tenants die u beheert.

  Opmerking
  Als u een apparaatgroep wilt selecteren, klikt u op het bovenliggende niveau en vervolgens schakelt u in het hoofdvenster het selectievakje naast de naam in.

  b. Klik op **Toevoegen**.
- Als u workloads of apparaatgroepen wilt verwijderen, selecteert u ze en klikt u vervolgens op **Verwijderen**.

4. Klik op **Gereed**.
5. Klik op **Opslaan** om het bewerkte schema op te slaan.

Schema's op verschillende beheerniveaus

De volgende tabel bevat een overzicht van de schema's die beheerders van verschillende niveaus kunnen zien en beheren.

Beheerder	Beheerniveau	Schema's	Rechten
Partnerbeheerder	Partnerniveau	Eigen schema's	Volledige toegang
		Klantschema's (inclusief schema's in eenheden)	Volledige toegang
		Eenheidschema's	Volledige toegang
	Klantniveau (voor klanten die worden beheerd door de serviceprovider)	Partnerschema's die worden toegepast op de workloads van deze klant	Alleen-lezen
		Klantschema's (inclusief schema's in eenheden)	Volledige toegang
		Eenheidschema's	Volledige

Beheerder	Beheerniveau	Schema's	Rechten
			toegang
	Eenheidniveau (voor klanten die worden beheerd door de serviceprovider)	Partnerschema's die worden toegepast op workloads van deze eenheid	Alleen-lezen
		Klantschema's die worden toegepast op workloads van deze eenheid	Alleen-lezen
		Eenheidschema's	Volledige toegang
Bedrijfbeheerder	Klantniveau	Partnerschema's die worden toegepast op de workloads van deze klant of eenheid	Alleen-lezen
		Klantschema's (inclusief schema's in eenheden)	Volledige toegang
		Eenheidschema's	Volledige toegang
	Eenheidniveau	Partnerschema's die worden toegepast op workloads van deze eenheid	Alleen-lezen
		Klantschema's die worden toegepast op workloads van deze eenheid	Alleen-lezen
		Eenheidschema's	Volledige toegang
Eenheidbeheerder	Eenheidniveau	Partnerschema's die worden toegepast op workloads van deze eenheid	Alleen-lezen
		Klantschema's die worden toegepast op workloads van deze eenheid	Alleen-lezen
		Eenheidschema's	Volledige toegang

Belangrijk

De eigenaar van een schema's is de tenant waarvoor het schema is gemaakt. Dus als een partnerbeheerder een schema heeft gemaakt op het klanttenantniveau, is de klanttenant de eigenaar van dat schema.

Compatibiliteitsproblemen met scripting-schema's

In sommige gevallen kunnen compatibiliteitsproblemen optreden wanneer u een scripting-schema toepast op een workload. De volgende compatibiliteitsproblemen kunnen voorkomen:

- Incompatibel besturingssysteem: dit probleem doet zich voor wanneer het besturingssysteem van de workload niet wordt ondersteund.
- Niet-ondersteunde agent: dit probleem doet zich voor wanneer de versie van de beveiligingsagent voor de workload verouderd is en geen ondersteuning biedt voor de Cyber Scripting-functionaliteit.
- Onvoldoende quota: dit probleem doet zich voor wanneer de tenant onvoldoende servicequota heeft om aan de geselecteerde workloads toe te wijzen.

Als het scripting-schema wordt toegepast op maximaal 150 afzonderlijk geselecteerde workloads, wordt u gevraagd de bestaande conflicten op te lossen voordat u het schema opslaat. U kunt een conflict oplossen door de hoofdoorzaak ervan weg te nemen of door de betreffende workloads te verwijderen uit het schema. Zie "Compatibiliteitsproblemen met scripting-schema's oplossen" (p. 418) voor meer informatie. Als u het schema opslaat zonder de conflicten op te lossen, wordt het automatisch uitgeschakeld voor de incompatibele workloads en worden er waarschuwingen weergegeven.

Als het scripting-schema wordt toegepast op meer dan 150 workloads of op apparaatgroepen, wordt het opgeslagen en vervolgens gecontroleerd op compatibiliteit. Het schema wordt automatisch uitgeschakeld voor de incompatibele workloads en er worden waarschuwingen weergegeven.

Compatibiliteitsproblemen met scripting-schema's oplossen

Bij het maken van een nieuw scripting-schema kunt u verschillende acties uitvoeren om compatibiliteitsproblemen op te lossen, al naargelang de oorzaak van de problemen.

Opmerking
Wanneer u een compatibiliteitsprobleem oplost door workloads te verwijderen uit een schema, dan is het niet mogelijk de workloads te verwijderen die deel uitmaken van een apparaatgroep.

Compatibiliteitsproblemen oplossen:

1. Klik op **Problemen bekijken**.
2. [Compatibiliteitsproblemen met incompatibele besturingssystemen oplossen]
   a. Ga naar het tabblad **Niet-compatibel besturingssysteem** en selecteer de workloads die u wilt verwijderen.
   b. Klik op **Workloads verwijderen uit schema**.
   c. Klik op **Verwijderen** en vervolgens op **Sluiten**.

3. [Compatibiliteitsproblemen met niet-ondersteunde agents oplossen door workloads te verwijderen uit het schema]
   a. Ga naar het tabblad **Niet-ondersteunde agents** en selecteer de workloads die u wilt verwijderen.
   b. Klik op **Workloads verwijderen uit schema**.
   c. Klik op **Verwijderen** en vervolgens op **Sluiten**.
4. [Compatibiliteitsproblemen met niet-ondersteunde agents oplossen door de agentversie bij te werken] Klik op **Ga naar lijst met agents**.

   Opmerking
   Deze optie is alleen beschikbaar voor klantbeheerders.

5. [Compatibiliteitsproblemen met onvoldoende quota oplossen door workloads te verwijderen uit het schema]
   a. Ga naar het tabblad **Onvoldoende quota** en selecteer de workloads die u wilt verwijderen.
   b. Klik op **Workloads verwijderen uit schema**.
   c. Klik op **Verwijderen** en vervolgens op **Sluiten**.
6. [Compatibiliteitsproblemen met onvoldoende quota oplossen door de quota van de tenant te verhogen]

   Opmerking
   Deze optie is alleen beschikbaar voor partnerbeheerders.

   a. Klik op het tabblad **Onvoldoende quota** op **Ga naar de beheerportal**.
   b. Verhoog de servicequota voor de klant.

Script snel uitvoeren

U kunt een script onmiddellijk uitvoeren zonder het op te nemen in een scripting-plan. U kunt deze bewerking niet gebruiken voor meer dan 150 workloads, voor offline workloads of voor apparaatgroepen.

Aan de doelworkload moet een servicequota zijn toegewezen die de functie Script snel uitvoeren ondersteunt, en het Advanced Management-pakket moet zijn ingeschakeld voor de betreffende tenant. Een passende servicequota wordt automatisch toegewezen als deze beschikbaar is in de tenant.

Opmerking
U kunt alleen uw goedgekeurde scripts gebruiken uit **Opslagplaats voor scripts** > **Mijn scripts**. Alleen een beheerder met de rol **Cyberbeheerder** kan scripts met de status **Testen** gebruiken. Zie "Gebruikersrollen en Cyber Scripting-rechten" (p. 397) voor meer informatie over de rollen.

U kunt een snelle uitvoering op de volgende manieren starten:

- Vanaf het tabblad **Apparaten**
  Selecteer een of meer workloads en selecteer vervolgens het script dat u hiervoor wilt uitvoeren.
- Vanaf het tabblad **Beheer** > **Opslagplaats voor scripts**
  Selecteer een script en selecteer vervolgens een of meer doelworkloads.

Een script uitvoeren vanaf het tabblad Apparaten

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de workload waarvoor u het script wilt uitvoeren en klik vervolgens op **Beschermen**.
3. Klik op **Script snel uitvoeren**.
4. Klik op **Script kiezen**, selecteer het script dat u wilt gebruiken en klik op **Gereed**.
5. Kies onder welk account het script wordt uitgevoerd voor de doelworkload. De volgende opties zijn beschikbaar:
   - Systeemaccount (in macOS is dit het rootaccount)
   - Momenteel aangemeld account
6. Geef op hoe lang het script kan worden uitgevoerd voor de doelworkload.
   Als het script niet geheel binnen de ingestelde tijd kan worden uitgevoerd, mislukt de Cyber Script-bewerking.
   U kunt waarden gebruiken tussen 1 en 1440 minuten.
7. [Alleen voor PowerShell-scripts] Configureer het uitvoeringsbeleid voor PowerShell.
   Zie de Microsoft documentatie voor meer informatie over dit beleid.
8. Klik op **Nu uitvoeren**.

Een script uitvoeren vanaf het tabblad Opslagplaats voor scripts

1. In de Cyber Protect-console: ga naar **Beheer** > **Opslagplaats voor scripts**.
2. Selecteer het script dat u wilt uitvoeren en klik vervolgens op **Script snel uitvoeren**.
3. Klik op **Workloads toevoegen** om de doelworkloads te selecteren en klik vervolgens op **Toevoegen**.
4. Klik op **Script kiezen**, selecteer het script dat u wilt gebruiken en klik op **Gereed**.
5. Kies onder welk account het script wordt uitgevoerd voor de doelworkload. De volgende opties zijn beschikbaar:
   - Systeemaccount (in macOS is dit het rootaccount)
   - Momenteel aangemeld account
6. Geef op hoe lang het script kan worden uitgevoerd voor de doelworkload.
   Als het script niet geheel binnen de ingestelde tijd kan worden uitgevoerd, mislukt de Cyber Script-bewerking.
   U kunt waarden gebruiken tussen 1 en 1440 minuten.
7. [Alleen voor PowerShell-scripts] Configureer het uitvoeringsbeleid voor PowerShell.

Zie de Microsoft documentatie voor meer informatie over dit beleid.

8. Klik op **Nu uitvoeren**.

Back-up en herstel van workloads en bestanden beheren

Met de back-upmodule kunt u back-up- en herstelbewerkingen uitvoeren voor fysieke en virtuele machines, bestanden en databases in een lokale opslag of cloudopslag.

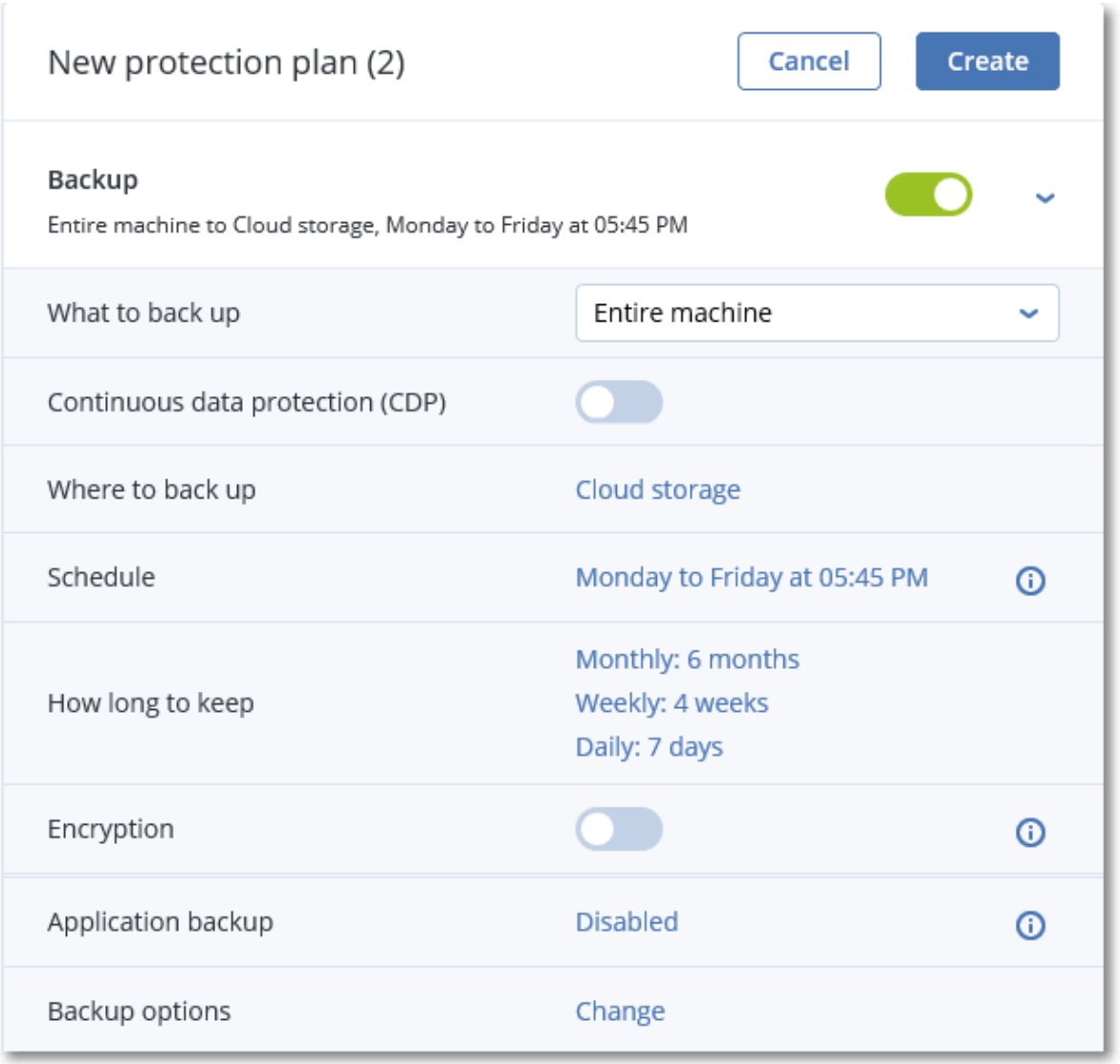
Back-up

Een beschermingsschema in de back-upmodule is een set regels die bepaalt hoe de desbetreffende gegevens op een bepaalde machine worden beschermd.

Een beschermingsschema kan worden toegepast op meerdere machines wanneer u het schema aanmaakt of later.

Het eerste beschermingsschema maken terwijl de back-upmodule is ingeschakeld

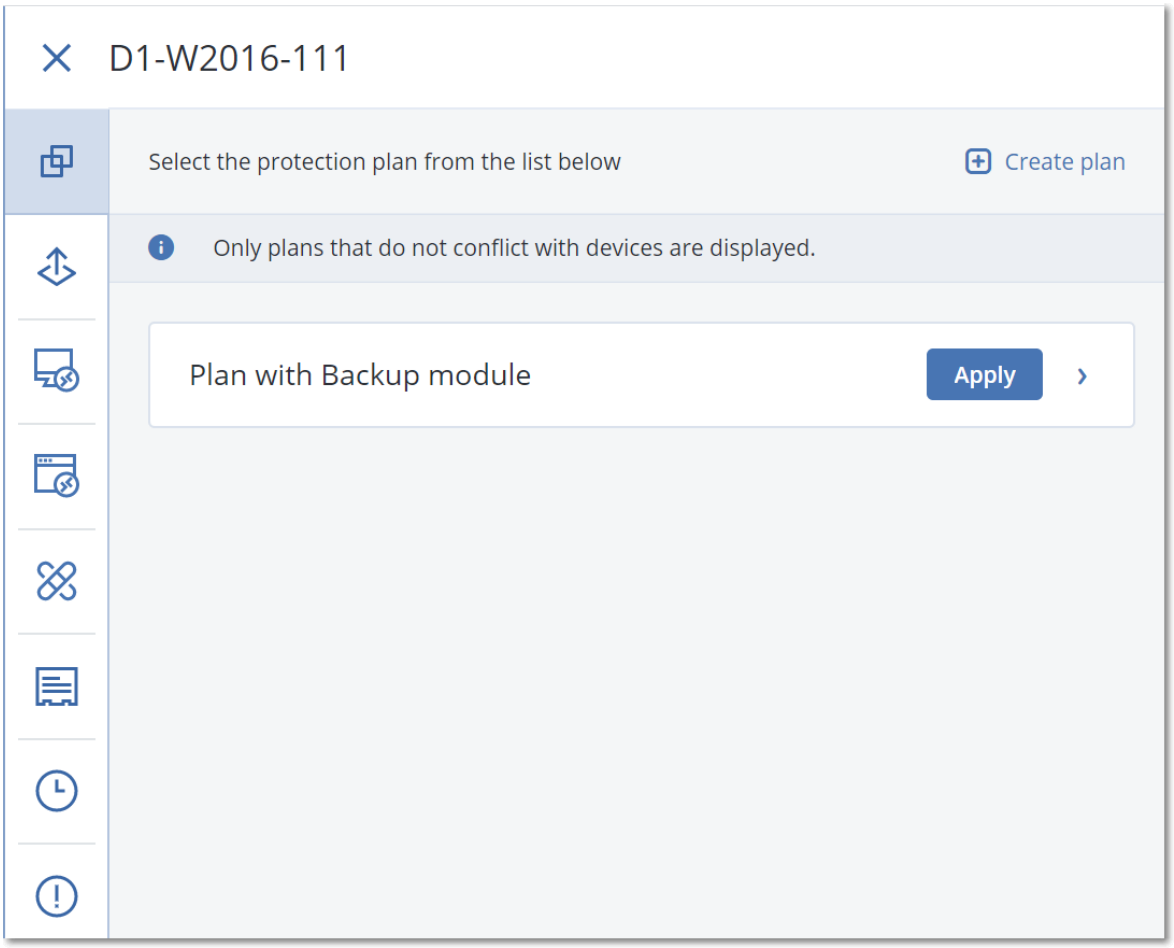
1. Selecteer de machines waarvan u een back-up wilt maken.
2. Klik op **Beschermen**.
   De beschermingsschema's die op de machine worden toegepast, worden weergegeven. Als er nog geen schema's aan de machine zijn toegewezen, dan ziet u het standaardbeschermingsschema dat kan worden toegepast. U kunt de instellingen naar wens aanpassen en dit schema toepassen of een nieuw schema maken.
3. Als u een nieuw schema wilt maken, klikt u op **Schema maken**. Schakel de **back-up**module in en maak de instellingen ongedaan.



4. [Optioneel] Klik op de standaardnaam om de naam van het beschermingsschema te wijzigen.
5. [Optioneel] Als u de parameters van de back-upmodule wilt wijzigen, klikt u op de betreffende instelling in het deelvenster voor het beschermingsschema.
6. [Optioneel] Als u de back-upopties wilt wijzigen, klikt u op **Wijzigen** naast **Back-upopties**.
7. Klik op **Maken**.

Een bestaand beschermingsschema toepassen

1. Selecteer de machines waarvan u een back-up wilt maken.
2. Klik op **Beschermen**. Als er al een algemeen beschermingsschema wordt toegepast op de geselecteerde machines, klikt u op **Schema toevoegen**.
   De eerder gemaakte beschermingsschema's worden weergegeven.



3. Selecteer een beschermingsschema om toe te passen.
4. Klik op **Toepassen**.

Referentiemateriaal voor beschermingsschema

De volgende tabel bevat een overzicht van de beschikbare parameters voor beschermingsschema's. Gebruik de tabel om een beschermingsschema te maken dat is afgestemd op uw behoeften.

BACK-UP MAKEN VAN	ITEMS WAARVAN EEN BACK-UP MOET WORDEN GEMAAKT Selectiemethoden	LOCATIE VAN BACK-UP	PLANNING Back-upschema's	BEWAARTIJD
Schijven/volumes (fysieke machines[1])	Rechtstreekse selectie Beleidsregels Bestandsfilters	Cloud Lokale map Netwerkmap NFS*	Altijd incrementeel (één bestand) Altijd volledig	Op leeftijd van de back-up (één regel/per back-upset) Op aantal

[1]Een machine waarvan een back-up wordt gemaakt door een agent die in het besturingssysteem is geïnstalleerd.

		Secure Zone**	Wekelijks volledig, Dagelijks incrementeel Maandelijks volledig, Wekelijks differentieel, Dagelijks incrementeel (GFS) Altijd incrementeel (één bestand) Altijd volledig Aangepast (F-D-I)	back-ups Op totale grootte van de back-ups*** Permanent bewaren
Schijven/volumes (virtuele machines[1])	Beleidsregels Bestandsfilters	Cloud Lokale map Netwerkmap NFS*		
Bestanden (alleen fysieke machines[2])	Rechtstreekse selectie Beleidsregels Bestandsfilters	Cloud Lokale map Netwerkmap NFS* Secure Zone**	Wekelijks volledig, Dagelijks incrementeel Maandelijks volledig, Wekelijks differentieel, Dagelijks incrementeel (GFS) Aangepast (F-D-I)	
ESXi-configuratie	Rechtstreekse selectie	Lokale map Netwerkmap NFS*		
Websites (bestanden en MySQL-databases)	Rechtstreekse selectie	Cloud	—	

[1]Een virtuele machine waarvan een back-up op hypervisorniveau wordt gemaakt door een externe agent zoals Agent voor VMware of Agent voor Hyper-V. Back-ups voor een virtuele machine met agent worden op dezelfde manier gemaakt als voor een fysieke machine.
[2]Een machine waarvan een back-up wordt gemaakt door een agent die in het besturingssysteem is geïnstalleerd.

<table>
<tr><td colspan="2">Systeemstatus</td><td rowspan="3">Rechtstreekse selectie</td><td rowspan="3">Cloud
Lokale map
Netwerkmap</td><td rowspan="3">Altijd volledig
Wekelijks volledig, Dagelijks incrementeel
Aangepast (F-I)
Altijd incrementeel (één bestand) - alleen voor SQL-databases</td><td rowspan="9"></td></tr>
<tr><td colspan="2">SQL-databases</td></tr>
<tr><td colspan="2">Exchange-databases</td></tr>
<tr><td rowspan="7">Microsoft 365</td><td>Postvakken
(lokale agent voor Microsoft 365)</td><td>Rechtstreekse selectie</td><td>Cloud
Lokale map
Netwerkmap</td><td>Altijd incrementeel (één bestand)</td></tr>
<tr><td rowspan="3">Postvakken
(cloudagent voor Microsoft 365)
Openbare mappen
Teams</td><td rowspan="3">Rechtstreekse selectie</td><td rowspan="4">Cloud</td><td>Altijd incrementeel (één bestand) - alleen voor SQL-databases</td></tr>
<tr><td rowspan="3">Maximaal 6 back-ups per dag</td></tr>
<tr><td rowspan="2">OneDrive-bestanden
SharePoint Online-gegevens</td><td rowspan="2">Rechtstreekse selectie
Beleidsregels</td></tr>
<tr><td rowspan="3">Google Workspace</td><td>Gmail-postvakken</td><td>Rechtstreekse selectie</td><td rowspan="3">Cloud</td><td rowspan="3">Maximaal 6 back-ups per dag</td></tr>
<tr><td>Google Drive-bestanden</td><td rowspan="2">Rechtstreekse selectie
Beleidsregels</td></tr>
<tr><td>Gedeelde Drive-bestanden</td></tr>
</table>

* Back-up naar NFS-shares is niet beschikbaar in Windows.

** Secure Zone kan niet worden gemaakt op een Mac.

*** De bewaarregel **Op totale grootte van de back-ups** is niet beschikbaar voor het back-upschema **Altijd incrementeel (één bestand)** of wanneer u een back-up maakt naar de cloudopslag.

Gegevens voor de back-up selecteren

Volledige machine selecteren

Een back-up van een volledige machine is een back-up van alle bijbehorende niet-verwisselbare schijven. Zie "Schijven of volumes selecteren" (p. 427) voor meer informatie over back-ups van schijven.

Beperkingen

- Back-ups op schijfniveau worden niet ondersteund voor versleutelde APFS-volumes die zijn vergrendeld. Tijdens een back-up van een volledige machine worden dergelijke volumes overgeslagen.
- De hoofdmap van OneDrive is standaard uitgesloten van back-upbewerkingen. Als u een back-up maakt van specifieke OneDrive-bestanden en -mappen, wordt er wel een back-up gemaakt van deze bestanden en mappen. Bestanden die niet beschikbaar zijn op het apparaat, krijgen ongeldige inhoud in de back-upset.

Schijven of volumes selecteren

Een back-up op schijfniveau bevat een kopie van een schijf of volume in pakketvorm. Vanaf een back-up op schijfniveau kunt u schijven, volumes, mappen en bestanden herstellen.

Voor elke afzonderlijke workload in het beschermingsschema kunt u de schijven of volumes selecteren waarvan u een back-up wilt maken (rechtstreekse selectie) of u kunt beleidsregels configureren voor meerdere workloads. U kunt ook bestandsfilters configureren om alleen specifieke bestanden uit te sluiten van of op te nemen in een back-up. Zie "Bestandsfilters (uitsluiten/opnemen)" (p. 488) voor meer informatie.

Schijven of volumes selecteren:

Rechtstreekse selectie

Rechtstreekse selectie is alleen beschikbaar voor fysieke machines.

1. Selecteer bij **Back-up maken van** de optie **Schijven/volumes**.
2. Klik op **Items waarvan een back-up moet worden gemaakt**.
3. Selecteer bij **Items voor back-up selecteren** de optie **Rechtstreeks**.
4. Schakel voor elk van de workloads in het beschermingsschema de selectievakjes in naast de schijven of volumes waarvan u een back-up wilt maken.
5. Klik op **Gereed**.

Via beleidsregels

1. Selecteer bij **Back-up maken van** de optie **Schijven/volumes**.
2. Klik op **Items waarvan een back-up moet worden gemaakt**.
3. Selecteer bij **Items voor back-up selecteren** de optie **Beleidsregels gebruiken**.
4. Selecteer een van de vooraf gedefinieerde regels of geef uw eigen regels of een combinatie van beide op.

   Zie "Beleidsregels voor schijven en volumes" (p. 430) voor meer informatie over de beschikbare beleidsregels.

   De beleidsregels worden toegepast op alle workloads die in het beschermingsschema zijn opgenomen.

   Als geen van de opgegeven regels kan worden toegepast op een workload, mislukt de back-up van die workload.
5. Klik op **Gereed**.

Beperkingen

- Back-ups op schijfniveau worden niet ondersteund voor versleutelde APFS-volumes die zijn vergrendeld. Tijdens een back-up van een volledige machine worden dergelijke volumes overgeslagen.
- De hoofdmap van OneDrive is standaard uitgesloten van back-upbewerkingen. Als u een back-up maakt van specifieke OneDrive-bestanden en -mappen, wordt er wel een back-up gemaakt van deze bestanden en mappen. Bestanden die niet beschikbaar zijn op het apparaat, krijgen ongeldige inhoud in de back-upset.
- U kunt een back-up maken van schijven die zijn verbonden met een fysieke machine via het iSCSI-protocol. Er zijn echter beperkingen als u Agent voor VMware of Agent voor Hyper-V gebruikt voor het maken van back-ups van de schijven die zijn verbonden via iSCSI. Zie "Beperkingen" (p. 33) voor meer informatie.

Wat wordt er in een schijf- of volumeback-up opgeslagen?

In een schijf- of volumeback-up wordt het **bestandssysteem** van een schijf of volume als geheel opgeslagen en in de back-up bevindt zich alle informatie die nodig is voor het opstarten van het besturingssysteem. Het is mogelijk om schijven of volumes als geheel te herstellen vanuit back-ups, maar dit is ook mogelijk met afzonderlijke mappen of bestanden.

Als de back-upoptie **sector-voor-sector (RAW-modus)** is ingeschakeld, worden alle schijfsectoren opgeslagen in een schijfback-up. De back-upoptie sector-voor-sector kan worden gebruikt voor het maken van schijfback-ups met niet-herkende of niet-ondersteunde bestandssystemen en andere fabriekseigen gegevensindelingen.

Windows

In een volumeback-up worden alle bestanden en mappen van het geselecteerde volume opgeslagen, onafhankelijk van hun kenmerken (inclusief verborgen bestanden en

systeembestanden), het opstartrecord, de bestandstoewijzingstabel (FAT) als dit aanwezig is, de root en track nul van de harde schijf met het master boot record (MBR).

In een schijfback-up worden alle volumes van de geselecteerde schijf opgeslagen (inclusief verborgen volumes, zoals de onderhoudspartities van de leverancier) en track nul met het master boot record.

De volgende items zijn *niet* opgenomen in een schijf- of volumeback-up (en ook niet in een back-up op bestandsniveau):

- Het wisselbestand (pagefile.sys) en het bestand met de RAM-inhoud als de machine in de sluimerstand gaat (hiberfil.sys). Na het herstellen worden de bestanden opnieuw aangemaakt op de juiste plaats met de grootte nul.
- Als de back-up wordt uitgevoerd onder het besturingssysteem (in tegenstelling tot opstartmedia of het maken van back-ups van virtuele machines op hypervisorniveau):
  - Windows-schaduwopslag. Het pad erheen wordt bepaald in de registerwaarde **VSS Default Provider** in de registersleutel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. Dit betekent dat er in besturingssystemen vanaf Windows Vista geen back-ups van Windows-herstelpunten worden gemaakt.
  - Als de back-upoptie **Volume Shadow Copy Service (VSS)** is ingeschakeld, bestanden en mappen die zijn opgegeven in de registersleutel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** .

Linux

In een volumeback-up worden alle bestanden en directory's van het geselecteerde volume opgeslagen, onafhankelijk van hun kenmerken, een opstartrecord en het bovenliggende blok van het bestandssysteem.

In een schijfback-up worden alle schijfvolumes opgeslagen, plus track nul met het master boot record.

Mac

In een schijf- of volumeback-up worden alle bestanden en directory's van de geselecteerde schijf of het geselecteerde volume opgeslagen, plus een beschrijving van de volume-indeling.

De volgende items zijn uitgesloten:

- Metagegevens van het systeem, zoals het bestandssysteemjournaal en de Spotlight-index
- De prullenbak
- Starttijd machineback-ups

Van schijven en volumes op een Mac worden fysiek back-ups op bestandsniveau gemaakt. Bare Metal Recovery uit schijf- en volumeback-ups is mogelijk, maar de back-upmodus sector-voor-sector is niet beschikbaar.

Beleidsregels voor schijven en volumes

Wanneer u schijven of volumes selecteert waarvan u een back-up wilt maken, kunt u de volgende beleidsregels gebruiken, afhankelijk van het besturingssysteem van de beschermde workload.

Windows

- `[All Volumes]`: hiermee worden alle volumes op de machine geselecteerd.
- Stationsletter (bijvoorbeeld `C:\`): hiermee wordt het volume met de opgegeven stationsletter geselecteerd.
- `[Fixed Volumes (physical machines)]`: hiermee worden alle volumes van een fysieke machine geselecteerd. Er worden geen verwisselbare media geselecteerd. Vaste volumes zijn bijvoorbeeld volumes op SCSI-, ATAPI-, ATA-, SSA-, SAS- en SATA-apparaten en op RAID-matrices.
- `[BOOT+SYSTEM]`: hiermee worden het systeem en de opstartvolumes geselecteerd. Dit is de minimale combinatie van waaruit je een besturingssysteem kunt herstellen.
- `[Disk 1]`: hiermee wordt de eerste schijf van de machine, inclusief alle volumes op de desbetreffende schijf, geselecteerd. Als u een andere schijf wilt selecteren, geeft u het bijbehorende nummer op.

Linux

- `[All Volumes]`: hiermee worden alle gekoppelde volumes op de machine geselecteerd.
- `/dev/hda1`: hiermee wordt het eerste volume op de eerste IDE-schijf geselecteerd.
- `/dev/sda1`: hiermee wordt het eerste volume op de eerste SCSI-schijf geselecteerd.
- `/dev/md1`: hiermee wordt de eerste softwarematige RAID-schijf geselecteerd.
- Als u andere basisvolumes wilt selecteren, geeft u `/dev/xdyN` op, waarbij:
  - de 'x' voor het schijftype staat
  - de 'y' voor het schijfnummer staat (a voor de eerste schijf, b voor de tweede schijf enzovoort)
  - 'N' is het volumenummer.
- Als u een logisch volume wilt selecteren, geeft u het pad op zoals weergegeven na het uitvoeren van de opdracht `ls /dev/mapper` onder het rootaccount.

  Bijvoorbeeld:

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  Deze uitvoer geeft twee logische volumes weer (`lv1` en `lv2`) die behoren tot de volumegroep `vg_1`. Als u een back-up wilt maken van deze volumes, geeft u het volgende op:

  `/dev/mapper/vg_1-lv1`
  `/dev/mapper/vg-l-lv2`

macOS

- `[All Volumes]`: hiermee worden alle gekoppelde volumes op de machine geselecteerd.
- `[Disk 1]`: hiermee wordt de eerste schijf van de machine, inclusief alle volumes op de desbetreffende schijf, geselecteerd. Als u een andere schijf wilt selecteren, geeft u het betreffende nummer op.

Bestanden of mappen selecteren

Gebruik een back-up op bestandsniveau als u alleen specifieke gegevens wilt beschermen, bijvoorbeeld de bestanden in uw huidige project. Back-ups op bestandsniveau zijn kleiner dan back-ups op schijfniveau en daarmee bespaart u opslagruimte.

Belangrijk
U kunt geen besturingssysteem herstellen vanaf een back-up op bestandsniveau.

Voor elke afzonderlijke workload in het beschermingsschema kunt u de bestanden en mappen selecteren waarvan u een back-up wilt maken (rechtstreekse selectie) of u kunt beleidsregels configureren voor meerdere workloads. U kunt ook specifieke bestanden uitsluiten van of opnemen in een back-up door filters te configureren. Zie "Bestandsfilters (uitsluiten/opnemen)" (p. 488) voor meer informatie.

Bestanden of mappen selecteren:

Rechtstreekse selectie

1. Selecteer bij **Back-up maken van** de optie **Bestanden/mappen**.
2. Klik in **Items om een back-up van te maken** op **Opgeven**.
3. Selecteer bij **Items voor back-up selecteren** de optie **Rechtstreeks**.
4. Geef voor elke workload in het beschermingsschema op van welke bestanden of mappen u een back-up wilt maken.
   a. Klik op **Bestanden en mappen selecteren**.
   b. Klik op **Lokale map** of **Netwerkmap**.
      Netwerkmappen moeten toegankelijk zijn vanaf de geselecteerde machine.
      Wanneer u **Netwerkmap** selecteert als bron, kunt u een back-up maken van gegevens van Network-attached storages (NAS), zoals NetApp-apparaten. NAS-apparaten van alle leveranciers worden ondersteund.
   c. Navigeer in de mappenstructuur naar de gewenste bestanden of mappen.
      U kunt ook het pad ernaartoe opgeven en vervolgens op de pijlknop klikken.
   d. [Voor gedeelde mappen] Geef desgevraagd de toegangsreferenties voor de gedeelde map op.
      Een back-up maken van mappen met anonieme toegang wordt niet ondersteund.
   e. Selecteer de gewenste bestanden en mappen.
   f. Klik op **Gereed**.

Via beleidsregels

1. Selecteer bij **Back-up maken van** de optie **Bestanden/mappen**.
2. Klik in **Items om een back-up van te maken** op **Opgeven**.
3. Selecteer bij **Items voor back-up selecteren** de optie **Beleidsregels gebruiken**.
4. Selecteer een van de vooraf gedefinieerde regels of geef uw eigen regels of een combinatie van beide op.

   Zie "Beleidsregels voor bestanden en mappen" (p. 432) voor meer informatie over de beschikbare beleidsregels.

   De beleidsregels worden toegepast op alle workloads die in het beschermingsschema zijn opgenomen.

   Als geen van de opgegeven regels kan worden toegepast op een workload, mislukt de back-up van die workload.
5. Klik op **Gereed**.

Beperkingen

- U kunt bestanden en mappen selecteren wanneer u een back-up maakt van fysieke machines of virtuele machines waarop een agent is geïnstalleerd (back-up met agent). Back-up op bestandsniveau is niet beschikbaar voor virtuele machines waarvan u een back-up maakt in de modus zonder agent. Zie "Back-ups met en zonder agent" (p. 63) voor meer informatie over de verschillen tussen deze typen back-ups.
- De hoofdmap van OneDrive is standaard uitgesloten van back-upbewerkingen. Als u een back-up maakt van specifieke OneDrive-bestanden en -mappen, wordt er wel een back-up gemaakt van deze bestanden en mappen. Bestanden die niet beschikbaar zijn op het apparaat, krijgen ongeldige inhoud in de back-upset.
- U kunt een back-up maken van mappen en bestanden op schijven die zijn verbonden met een fysieke machine via het iSCSI-protocol. Er zijn enkele beperkingen van toepassing als u Agent voor VMware of Agent voor Hyper-V gebruikt voor het maken van back-ups van de gegevens op schijven die zijn verbonden via iSCSI.

Beleidsregels voor bestanden en mappen

Wanneer u bestanden of mappen selecteert waarvan u een back-up wilt maken, kunt u de volgende beleidsregels gebruiken, afhankelijk van het besturingssysteem van de beschermde workload.

Windows

- Volledig pad naar een bestand of map. Bijvoorbeeld: `D:\Work\Text.doc` of `C:\Windows`.
- Vooraf gedefinieerde regels:
  - `[All Files]`: hiermee worden alle bestanden op alle volumes van de machine geselecteerd.
  - `[All Profiles Folder]`: hiermee wordt de map geselecteerd waarin alle gebruikersprofielen zijn opgeslagen. Bijvoorbeeld: `C:\Users` of `C:\Documents and Settings`.
- Omgevingsvariabelen:

- `%ALLUSERSPROFILE%`: hiermee wordt de map met de algemene gegevens van alle gebruikersprofielen geselecteerd. Bijvoorbeeld: `C:\ProgramData` of `C:\Documents and Settings\All Users`.
- `%PROGRAMFILES%`: hiermee wordt de map `Program Files` geselecteerd. Bijvoorbeeld: `C:\Program Files`.
- `%WINDIR%` hiermee wordt de map `Windows` geselecteerd. Bijvoorbeeld: `C:\Windows`.

U kunt andere omgevingsvariabelen of een combinatie van omgevingsvariabelen en tekst gebruiken. Als u bijvoorbeeld de map Java in de map Program Files wilt selecteren, geeft u het volgende op: `%PROGRAMFILES%\Java`.

Linux

- Volledig pad naar een bestand of directory.
  Als u bijvoorbeeld een back-up wilt maken van het bestand `file.txt` op het volume `/dev/hda3` dat is gekoppeld op `/home/usr/docs`, geeft u `/dev/hda3/file.txt` of `/home/usr/docs/file.txt` op.
- Vooraf gedefinieerde regels:
  - `[All Profiles Folder]`: hiermee wordt `/home` geselecteerd. Standaard worden alle gebruikersprofielen in deze map opgeslagen.
  - `/home`: hiermee wordt de home directory van de algemene gebruikers geselecteerd.
  - `/root`: hiermee wordt de home directory van de rootgebruiker geselecteerd.
  - `/usr`: hiermee wordt de directory voor alle gebruikersgerelateerde programma's geselecteerd.
  - `/etc`: hiermee wordt de directory voor systeemconfiguratiebestanden geselecteerd.

macOS

- Volledig pad naar een bestand of directory.
  Bijvoorbeeld:
  - Als u een back-up wilt maken van `file.txt` op het bureaublad van een gebruiker, geeft u `/Users/<gebruikersnaam>/Desktop/file.txt` op.
  - Als u een back-up wilt maken van het `Desktop`, de map `Documents` en de map `Downloads` van een gebruiker, geeft u respectievelijk `/Users/<gebruikersnaam>/Desktop`, `/Users/<gebruikersnaam>/Documents` en `/Users/<gebruikersnaam>/Downloads` op.
  - Als u een back-up wilt maken van de basismappen van alle gebruikers die een account op deze machine hebben, geeft u `/Users` op.
  - Als u een back-up wilt maken van de directory waar de toepassingen zijn geïnstalleerd, geeft u `/Applications` op.
- Vooraf gedefinieerde regels
  - `[All Profiles Folder]`: hiermee wordt `/Users` geselecteerd. Standaard worden alle gebruikersprofielen in deze map opgeslagen.

Systeemstatus selecteren

Opmerking
Back-up van systeemstatus is beschikbaar voor machines met Windows 7 of later waarop Agent voor Windows is geïnstalleerd. Back-up van de systeemstatus is niet beschikbaar voor virtuele machines waarvan een back-up is gemaakt op hypervisorniveau (back-up zonder agent).

Als u een back-up van de systeemstatus wilt maken, selecteert u bij **Back-up maken van** de optie **Systeemstatus**.

Een back-up van de systeemstatus omvat de volgende bestanden:

- Configuratie van de taakplanner
- VSS Metadata Store
- Configuratiegegevens voor het prestatiemeteritem
- MSSearch-service
- Background Intelligent Transfer Service (BITS)
- Het register
- Windows Management Instrumentation (WMI)
- Component Services Class-registratiedatabase

ESXi-configuratie selecteren

Met een back-up van een ESXi-hostconfiguratie kunt u een ESXi-host herstellen naar bare metal. Het herstel wordt uitgevoerd met opstartmedia.

De virtuele machines die op de host worden uitgevoerd, worden niet inbegrepen in de back-up. Back-up en herstel hiervan kunnen afzonderlijk worden uitgevoerd.

Een back-up van een ESXi-hostconfiguratie omvat het volgende:

- De bootloader en boot bank-partities van de host.
- De status van de host (configuratie van virtuele netwerken en opslag, SSL-sleutels, servernetwerkinstellingen en gegevens van lokale gebruikers).
- Extensies en patches die zijn geïnstalleerd of gepreconfigureerd op de host.
- Logbestanden.

Vereisten

- SSH moet zijn ingeschakeld in het **Beveiligingsprofiel** van de ESXi-hostconfiguratie.
- U moet het wachtwoord voor het rootaccount op de ESXi-host kennen.

Beperkingen

- Back-ups van ESXi-configuratie worden niet ondersteund voor hosts met VMware ESXi 7.0 en later.
- Er kan geen back-up in de cloudopslag worden gemaakt van een ESXi-configuratie.

Een ESXi-configuratie selecteren

1. Klik op **Apparaten** > **Alle apparaten** en selecteer vervolgens de ESXi-hosts waarvan u een back-up wilt maken.
2. Klik op **Beschermen**.
3. Ga naar **Back-up maken van** en selecteer **ESXi-configuratie**.
4. Geef in **ESXi-rootwachtwoord** een wachtwoord op voor het rootaccount op elk van de geselecteerde hosts of pas hetzelfde wachtwoord toe voor alle hosts.

Continue gegevensbescherming (CDP)

Continue gegevensbescherming (CDP) maakt deel uit van het Advanced Backup-pakket. Met Continue gegevensbescherming (CDP) wordt er een back-up van kritieke gegevens gemaakt onmiddellijk nadat deze gegevens zijn gewijzigd. Hierdoor gaan er geen wijzigingen verloren als uw systeem uitvalt tussen twee geplande back-ups. U kunt Continue gegevensbescherming configureren voor de volgende gegevens:

- Bestanden of mappen op specifieke locaties
- Bestanden die door specifieke toepassingen zijn gewijzigd

Momenteel wordt Continue gegevensbescherming alleen ondersteund voor het NTFS-bestandssysteem en de volgende besturingssystemen:

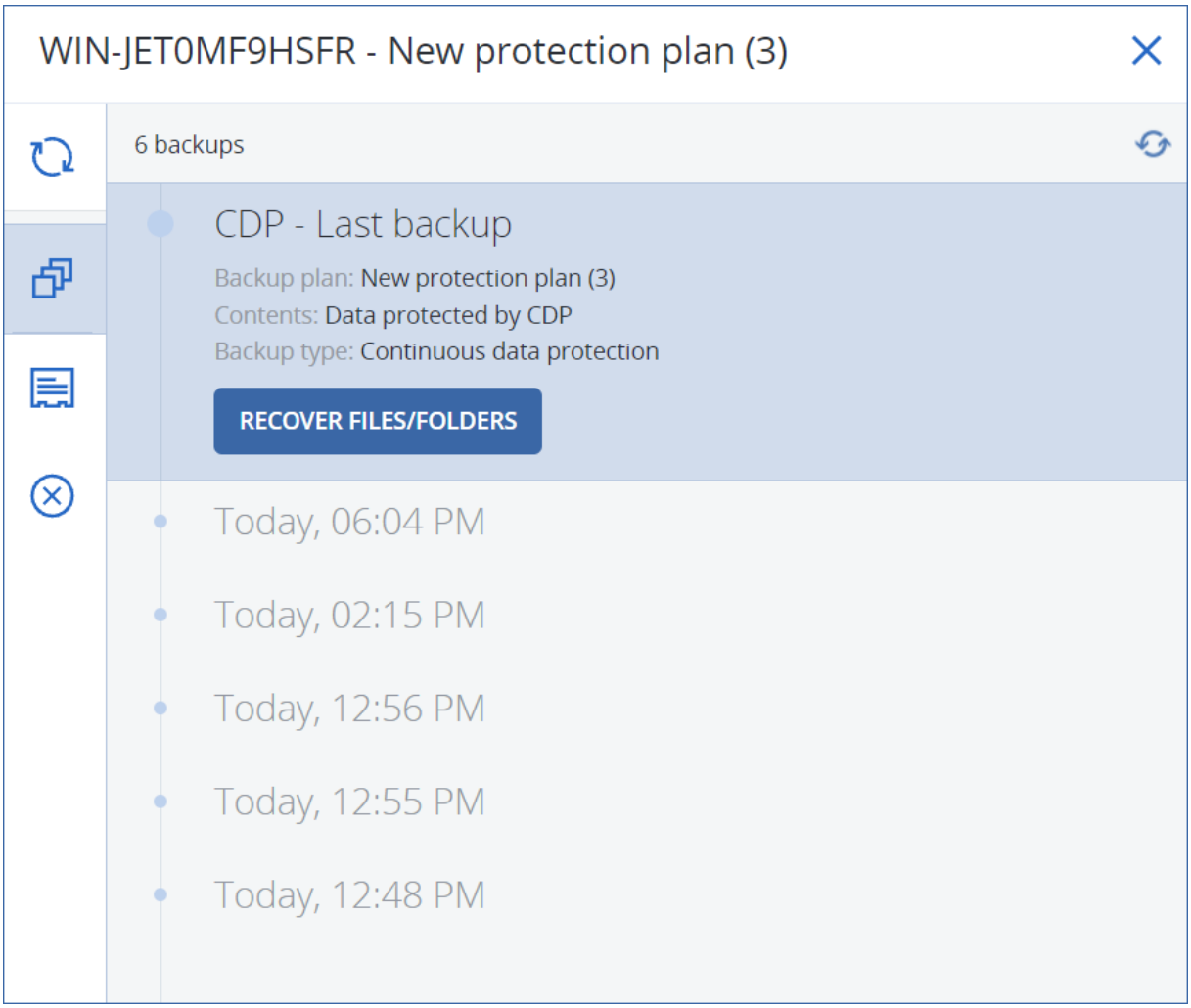
- Desktop: Windows 7 en later
- Server: Windows Server 2008 R2 en later

Alleen lokale mappen worden ondersteund. Netwerkmappen kunnen niet worden geselecteerd voor Continue gegevensbescherming.

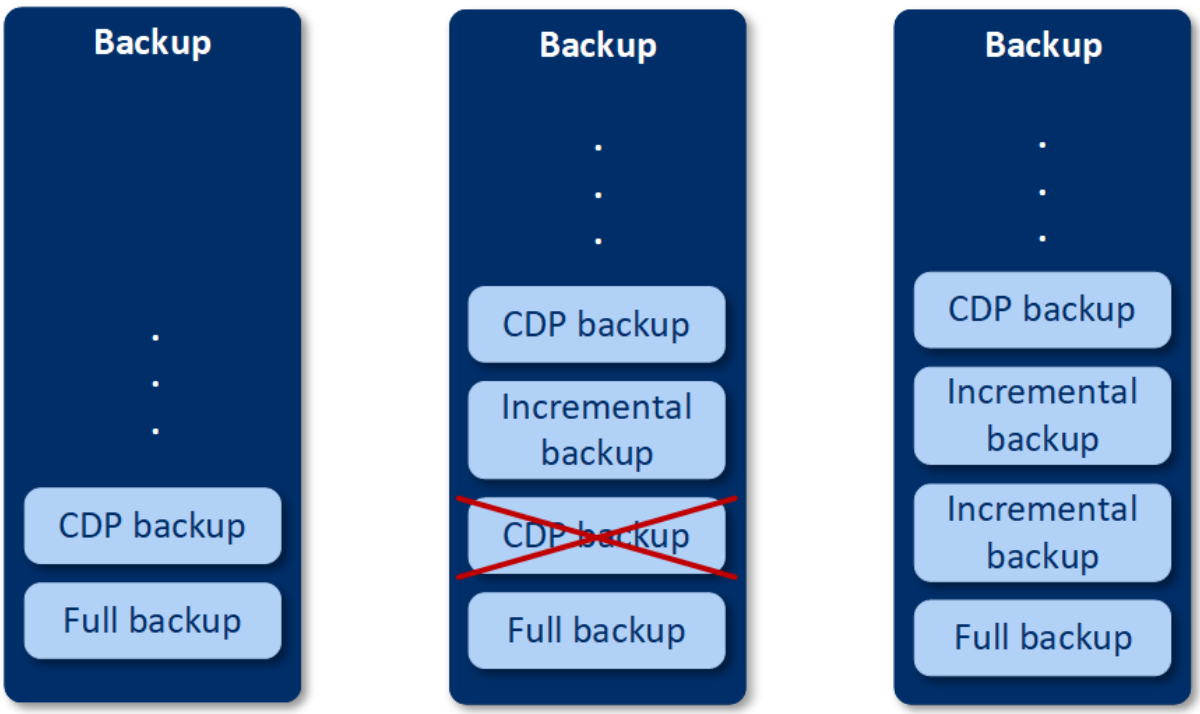
Continue gegevensbescherming is niet compatibel met de optie **Back-up van toepassingen**.

Zo werkt het

Wijzigingen in de bestanden en mappen die worden bijgehouden door Continue gegevensbescherming, worden onmiddellijk opgeslagen in een speciale CDP-back-up. Er is slechts één CDP-back-up in een back-upset, en deze is altijd de meest recente.



Wanneer een geplande regelmatige back-up begint, wordt Continue gegevensbescherming in de wachtstand geplaatst omdat de nieuwste gegevens in de geplande back-up moeten worden opgenomen. Wanneer de geplande back-up is voltooid, wordt Continue gegevensbescherming hervat, wordt de oude CDP-back-up verwijderd en wordt een nieuwe CDP-back-up gemaakt. De CDP-back-up blijft dus altijd de nieuwste back-up in de back-upset en bevat altijd de meest recente status van de bijgehouden bestanden of mappen.



Als uw machine tijdens een regelmatige back-up crasht, wordt Continue gegevensbescherming automatisch hervat nadat de machine opnieuw is opgestart en wordt een CDP-back-up gemaakt na de laatst voltooide geplande back-up.

Voor Continue gegevensbescherming moet ten minste één regelmatige back-up worden gemaakt voorafgaand aan de CDP-back-up. Wanneer u voor het eerst een beschermingsschema met Continue gegevensbescherming uitvoert, wordt daarom een volledige back-up gemaakt, en wordt hieraan onmiddellijk een CDP-back-up toegevoegd. Als u de optie **Continue gegevensbescherming** inschakelt voor een bestaand beschermingsschema, wordt de CDP-back-up aan de bestaande back-upset toegevoegd.

Opmerking
Continue gegevensbescherming wordt standaard ingeschakeld voor beschermingsschema's die u maakt vanuit het tabblad **Apparaten**, als de Advanced Backup-functionaliteit voor u is ingeschakeld en u geen andere Advanced Backup-functies gebruikt voor de geselecteerde machines. Als u al een schema hebt met Continue gegevensbeveiliging voor een geselecteerde machine, wordt Continue gegevensbeveiliging niet standaard ingeschakeld voor die machine in nieuw gemaakte schema's. Continue gegevensbescherming wordt niet standaard ingeschakeld voor schema's die zijn gemaakt voor apparaatgroepen.

Ondersteunde gegevensbronnen

U kunt Continue gegevensbescherming configureren met de volgende gegevensbronnen:

- Volledige machine
- Schijven/volumes

- Bestanden/mappen

Wanneer u de gegevensbron hebt geselecteerd in het gedeelte **Welke back-ups moeten worden uitgevoerd?** van het beschermingsschema, gaat u naar het gedeelte **Items die voortdurend moeten worden beschermd** en selecteert u de bestanden, mappen of toepassingen voor Continue gegevensbescherming. Zie "CDP-back-up configureren" (p. 438) voor meer informatie over het configureren van Continue gegevensbescherming.

Ondersteunde bestemmingen

U kunt Continue gegevensbescherming configureren met de volgende bestemmingen:

- Lokale map
- Netwerkmap
- Cloudopslag
- Acronis Cyber Infrastructure
- Locatie gedefinieerd door een script

Opmerking
U kunt met een script alleen de hierboven vermelde locaties definiëren.

CDP-back-up configureren

U kunt Continue gegevensbescherming (CDP) configureren in de module **Back-up** van een beschermingsschema. Zie "Een beschermingsschema maken" (p. 217) voor meer informatie over het maken van een beschermingsschema.

Instellingen voor Continue gegevensbescherming configureren

1. Ga naar de **Back-up**-module van een beschermingsschema en zet de schakelaar **Continue gegevensbescherming (CDP)** aan.
   Deze schakelaar is alleen beschikbaar voor de volgende gegevensbronnen:
   - Volledige machine
   - Schijven/volumes
   - Bestanden/mappen
2. In **Items die voortdurend moeten worden beschermd** configureert u Continue gegevensbescherming voor **Applicaties** of **Bestanden/mappen** of beide.
   - Klik op **Applicaties** om CDP-back-up te configureren voor bestanden die worden gewijzigd door specifieke toepassingen.
     U kunt de toepassingen uit de vooraf gedefinieerde categorieën selecteren of andere toepassingen toevoegen door het pad naar het uitvoerbare bestand van de toepassing op te geven, bijvoorbeeld:

- `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
- `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

- Klik op **Bestanden/mappen** om CDP-back-up te configureren voor bestanden op specifieke locaties.

  U kunt deze locaties definiëren door selectieregels te gebruiken of door de bestanden en mappen rechtstreeks te selecteren.
  - [Voor alle machines] Gebruik het tekstvak om een selectieregel te maken.

    U kunt de volledige paden naar bestanden of paden met jokertekens (* en ?) gebruiken. Het sterretje (*) komt overeen met nul of meer tekens. Het vraagteken komt overeen met één enkel teken.

    Belangrijk
    Als u een CDP-back-up voor een map wilt maken, moet u de inhoud ervan opgeven met het sterretje als jokerteken:

    Correct pad:`D:\Data\*`

    Onjuist pad: `D:\Data\`
  - [Voor online machines] Bestanden en mappen rechtstreeks selecteren:
    - Ga naar **Machine waarmee u wilt bladeren** en selecteer de machine met de bestanden of mappen.
    - Klik op **Bestanden en mappen selecteren** om naar de geselecteerde machine te bladeren.

      Bij een rechtstreekse selectie wordt een selectieregel gemaakt. Als u het beschermingsschema toepast op meerdere machines en een selectieregel niet geldig is voor een machine, dan wordt deze regel overgeslagen op deze machine.

3. Klik in het deelvenster voor het beschermingsschema op **Maken**.

Tussen de geplande back-ups worden er dan continu back-ups gemaakt van de door u opgegeven gegevens.

Een bestemming selecteren

Klik op **Waar back-up maken** en selecteer een van de volgende opties:

- **Cloudopslag**

  De back-ups worden opgeslagen in het clouddatacentrum.
- **Lokale mappen**

  Als er één machine is geselecteerd, bladert u naar een map op de geselecteerde machine of geeft u het pad naar de map op.

  Als er meerdere machines zijn geselecteerd, geeft u het pad naar de map op. De back-ups worden opgeslagen in deze map op elk van de geselecteerde fysieke machines of op de machine waarop de agent voor virtuele machines is geïnstalleerd. Als de map niet bestaat, wordt deze gemaakt.

- **Netwerkmap**

  Deze map wordt gedeeld via SMB/CIFS/DFS.

  Blader naar de betreffende gedeelde map of geef het pad op in de volgende indeling:

  - Voor SMB/CIFS-shares: `\\<hostnaam>\<pad>\` of `smb://<hostnaam>/<pad>/`
  - Voor DFS-shares: `\\<volledige DNS-domeinnaam>\<DFS-root>\<pad>`

    Bijvoorbeeld: `\\voorbeeld.bedrijf.com\gedeelde\bestanden`

  Klik vervolgens op de pijlknop. Geef desgevraagd de gebruikersnaam en het wachtwoord voor de gedeelde map op. U kunt deze referenties op elk moment wijzigen door op het sleutelpictogram naast de mapnaam te klikken.

  Een back-up maken naar een map met anonieme toegang wordt niet ondersteund.
- **Openbare cloud**

  Deze optie is beschikbaar als onderdeel van het Advanced Backup-pakket.

  Hiermee kunt u een directe back-up configureren naar een openbare cloudopslag, zonder dat u extra onderdelen (zoals Microsoft Azure of andere virtuele machines als gateways) hoeft te implementeren. Selecteer en maak indien nodig verbinding met de betreffende openbare cloud.

  Zie "Back-ups van workloads maken in openbare clouds" (p. 572) voor meer informatie.
- **NFS-map** (beschikbaar voor machines met Linux of macOS)

  Controleer of het nfs-utils-pakket is geïnstalleerd op de Linux-server waarop de Agent voor Linux is geïnstalleerd.

  Blader naar de vereiste NFS-map of geef het pad op in de volgende indeling:

  `nfs://<hostnaam>/<geëxporteerde map>:/<submap>`

  Klik vervolgens op de pijlknop.

  Opmerking
  U kunt geen back-up maken van een NFS-map die is beveiligd met een wachtwoord.

- **Secure Zone** (beschikbaar indien aanwezig op elk van de geselecteerde machines)

  Secure Zone is een beveiligde partitie op een schijf van de machine waarvan een back-up wordt gemaakt. Deze partitie moet u handmatig maken voordat u een back-up configureert. Voor informatie over hoe u een Secure Zone maakt, en wat de voordelen en beperkingen zijn, raadpleegt u "Over Secure Zone" (p. 441).

Geavanceerde opslagoptie

Opmerking
Deze functionaliteit is alleen beschikbaar in de Advanced Edition van de Cyber Protection-service.

Gedefinieerd door een script (beschikbaar voor machines met Windows)

U kunt de back-ups van elke machine opslaan in een map die is gedefinieerd door een script. De software ondersteunt scripts in JScript, VBScript of Python 3.5. Wanneer u het beschermingsschema implementeert, voert de software het script uit op elke machine. De scriptuitvoer voor elke machine

moet een pad naar een lokale of netwerkmap zijn. Als een map niet bestaat, wordt deze gemaakt (beperking: er kunnen geen mappen op netwerkshares worden gemaakt met scripts geschreven in Python). Op het tabblad **Back-upopslag** wordt elke map weergegeven als afzonderlijke back-uplocatie.

In **Type script** selecteert u het scripttype (**JScript**, **VBScript** of **Python**) en vervolgens importeert, of kopieert en plakt u het script. Voor netwerkmappen geeft u de toegangsreferenties met de lees/schrijfmachtigingen op.

Voorbeelden:

- Het volgende JScript-script geeft de back-uplocatie voor een machine weer in de indeling `\\bkpsrv\<machinenaam>`:

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  Hierdoor worden de back-ups van elke machine opgeslagen in een map van dezelfde naam op de server **bkpsrv**.
- Het volgende JScript-script geeft de back-uplocatie weer in een map op de machine waarop het script wordt uitgevoerd:

  ```
  WScript.Echo("C:\\Backup");
  ```

  Hierdoor worden de back-ups van deze machine opgeslagen in de map `C:\Backup` op dezelfde machine.

Opmerking
Het locatiepad in deze scripts is hoofdlettergevoelig. Daarom worden `C:\Backup` en `C:\backup` weergegeven als verschillende locaties in de Cyber Protect-console. Gebruik ook hoofdletters voor de stationsletter.

Over Secure Zone

Secure Zone is een beveiligde partitie op een schijf van de machine waarvan een back-up wordt gemaakt. Hier kunnen back-ups worden opgeslagen van schijven of bestanden van deze machine.

Als de schijf een fysiek defect heeft, kunnen de back-ups in Secure Zone verloren gaan. Daarom moet u Secure Zone niet als enige locatie gebruiken om back-ups op te slaan. In bedrijfsomgevingen kunt u Secure Zone beschouwen als een tussenliggende locatie voor back-ups wanneer een gebruikelijke locatie tijdelijk niet beschikbaar is of wanneer deze is verbonden via een langzaam of drukbezet kanaal.

Waarom Secure Zone gebruiken?

Secure Zone:

- Herstel van een schijf naar dezelfde schijf waarop de back-up van de schijf wordt opgeslagen.
- Kosteneffectieve en handige methode voor de beveiliging van gegevens tegen softwarestoringen, virusaanvallen, menselijke fouten.
- Geen afzonderlijke media of netwerkverbinding nodig voor het maken van een back-up of het herstellen van gegevens. Dit is vooral handig voor roaming-gebruikers.
- Kan dienen als primaire bestemming bij replicatie van back-ups.

Beperkingen

- Secure Zone kan niet worden ingericht op een Mac.
- Secure Zone is een partitie op een standaardschijf. Deze kan niet worden ingericht op een dynamische schijf en kan niet worden gemaakt als logisch volume (beheerd met LVM).
- Secure Zone wordt geformatteerd met het FAT32-bestandssysteem. De bestandsgrootte van FAT32 is beperkt tot 4 GB, dus grotere back-ups worden opgesplitst wanneer ze worden opgeslagen in Secure Zone. Dit heeft geen invloed op de herstelprocedure en de snelheid.

Schijftransformatie door het maken van Secure Zone

- Secure Zone wordt altijd gemaakt aan het einde van de harde schijf.
- Als er geen of onvoldoende niet-toegewezen ruimte is aan het einde van de schijf, maar er wel niet-toegewezen ruimte tussen volumes is, worden de volumes verplaatst om meer niet-toegewezen ruimte toe te voegen aan het einde van de schijf.
- Wanneer alle niet-toegewezen ruimte is verzameld, maar deze toch nog onvoldoende is, neemt de software vrije schijfruimte van de door u geselecteerde volumes, waarbij de grootte van de volumes proportioneel wordt verkleind.
- Er moet wel voldoende vrije schijfruimte op een volume zijn voor een goede werking van het besturingssysteem en applicaties, bijvoorbeeld voor het maken van tijdelijke bestanden. De software verkleint geen volumes als de beschikbare vrije schijfruimte 25 procent of minder van de totale volumegrootte bedraagt (of zou bedragen na de bewerking). Alleen wanneer er slechts 25 procent of minder vrije schijfruimte beschikbaar is op alle volumes van de schijf, zal de software de volumes proportioneel verkleinen.

Zoals uit het hier vermelde blijkt, wordt het niet aanbevolen de maximaal mogelijke grootte van Secure Zone op te geven. Het resultaat kan zijn dat er op geen enkel volume meer vrije schijfruimte beschikbaar is, waardoor het besturingssysteem of applicaties onstabiel kunnen worden of zelfs mogelijk niet meer starten.

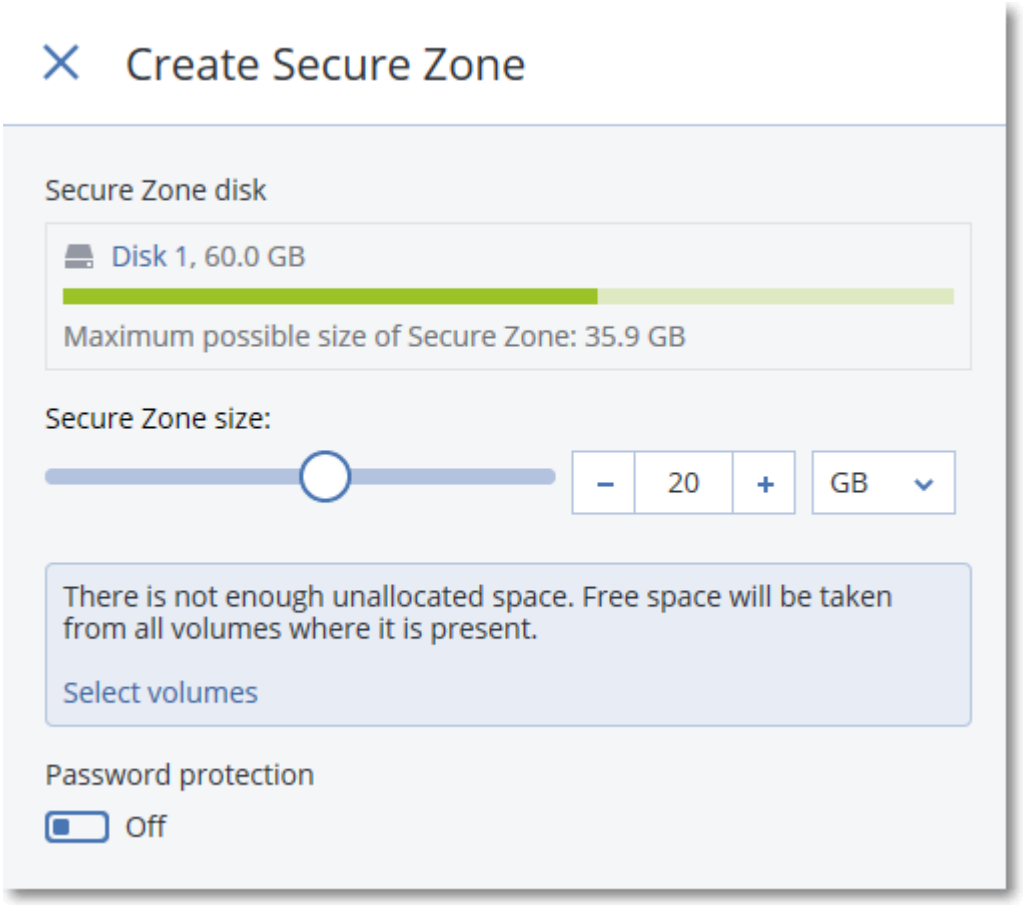
Belangrijk
Als u het volume waarvan het systeem wordt opgestart, verplaatst of de grootte ervan verandert, moet het systeem opnieuw worden opgestart.

Secure Zone maken

1. Selecteer de machine waarop u Secure Zone wilt maken.
2. Klik op **Details** > **Secure Zone maken** .
3. Klik onder **Secure Zone-schijf** op **Selecteren** en selecteer een harde schijf (als er meerdere zijn) waarop u de zone wilt maken.

   De software berekent de maximaal mogelijke grootte van Secure Zone.
4. Geef de grootte van Secure Zone op of sleep de schuifregelaar om een grootte tussen de minimale en maximale grootte te selecteren.

   De minimale grootte is ongeveer 50 MB, afhankelijk van de geometrie van de harde schijf. De maximale grootte is gelijk aan de niet-toegewezen ruimte op de schijf plus de totale vrije schijfruimte op alle volumes van de schijf.
5. Wanneer alle niet-toegewezen ruimte onvoldoende is voor de door u opgegeven grootte, neemt de software vrije schijfruimte van de bestaande volumes. Standaard worden alle volumes geselecteerd. Als u bepaalde volumes wilt uitsluiten, klikt u op **Volumes selecteren**. Anders kunt u deze stap overslaan.



6. [Optioneel] Schakel de optie **Wachtwoordbescherming** in en geef een wachtwoord op.

Het wachtwoord is vereist om toegang te krijgen tot de back-ups in Secure Zone. Als u een back-up maakt van Secure Zone, hebt u geen wachtwoord nodig, tenzij de back-up wordt uitgevoerd op opstartmedia.

7. Klik op **Maken**.
   De software geeft de verwachte partitielay-out weer. Klik op **OK**.
8. Wacht totdat Secure Zone is gemaakt door de software.

U kunt dan Secure Zone kiezen in **Waar back-up maken** wanneer u een beschermingsschema maakt.

Secure Zone verwijderen

1. Selecteer een machine met Secure Zone.
2. Klik op **Details**.
3. Klik op het tandwielpictogram naast **Secure Zone** en klik vervolgens op **Verwijderen**.
4. [Optioneel] Geef de volumes op waar de vrijgekomen ruimte van de zone wordt toegevoegd.
   Standaard worden alle volumes geselecteerd.
   De ruimte wordt evenredig verdeeld over de geselecteerde volumes. Als u geen volumes selecteert, wordt de vrijgekomen ruimte niet toegewezen.
   Als u de grootte verandert van het volume waarvan het systeem wordt opgestart, moet het systeem opnieuw worden opgestart.
5. Klik op **Verwijderen**.

Secure Zone wordt dan verwijderd, inclusief alle back-ups die daar zijn opgeslagen.

Back-upschema

U kunt een back-up zo configureren dat deze automatisch wordt uitgevoerd op een bepaald tijdstip, met specifieke intervallen of bij een specifieke gebeurtenis.

Geplande back-ups voor niet-cloud-to-cloud resources worden uitgevoerd volgens de tijdzone-instellingen van de workload waarvoor de beveiligingsagent is geïnstalleerd. Als u bijvoorbeeld hetzelfde beschermingsschema toepast op workloads met verschillende tijdzone-instellingen, worden de back-ups gestart volgens de lokale tijdzone van elke workload.

Het plannen van een back-up omvat de volgende acties:

- Een back-upschema selecteren
- De tijd configureren waarop of de gebeurtenis selecteren waardoor de back-up wordt geactiveerd
- Optionele instellingen en startvoorwaarden configureren

Back-upschema's

Een back-upschema maakt deel uit van het beschermingsschema en bepaalt welk type back-up (volledig, differentieel of incrementeel) wordt gemaakt en wanneer dit wordt gemaakt. U kunt een van de vooraf gedefinieerde back-upschema's selecteren of een aangepast schema maken.

De beschikbare back-upschema's en -typen zijn afhankelijk van de locatie en bron van de back-up. Differentiële back-up is bijvoorbeeld niet beschikbaar wanneer u een back-up van SQL-gegevens, Exchange-gegevens of de systeemstatus maakt. Het schema **Altijd incrementeel (één bestand)** wordt niet ondersteund voor tapeapparaten.

Back-upschema	Beschrijving	Configureerbare elementen
Altijd incrementeel (één bestand)	De eerste back-up is een volledige back-up en kan de nodige tijd in beslag nemen. Daaropvolgende back-ups zijn incrementele back-ups en zijn aanzienlijk sneller. Voor de back-ups wordt de indeling voor enkelvoudig back-upbestand[1]* gebruikt. Er worden standaard dagelijks back-ups gemaakt, van maandag tot en met vrijdag. We raden u aan dit schema te gebruiken wanneer u uw back-ups opslaat in de cloudopslag, omdat incrementele back-ups snel zijn en er minder netwerkverkeer nodig is.	• Type schema: maandelijks, wekelijks, dagelijks, per uur • Back-uptrigger: tijdstip of gebeurtenis • Starttijd • Startvoorwaarden • Aanvullende opties
Altijd volledig	Alle back-ups in de back-upset zijn volledige back-ups. Er worden standaard dagelijks back-ups gemaakt, van maandag tot en met vrijdag.	• Type schema: maandelijks, wekelijks, dagelijks, per uur • Back-uptrigger: tijdstip of gebeurtenis • Starttijd • Startvoorwaarden • Aanvullende opties
Wekelijks volledig, dagelijks incrementeel	Er wordt eens per week een volledige back-up gemaakt. Andere back-ups zijn incrementeel.	• Back-uptrigger: tijdstip of gebeurtenis

[1]Een nieuwe back-upindeling waarin de initiële volledige back-up en de daaropvolgende incrementele back-ups worden opgeslagen in één TIBX-bestand. Deze indeling maakt gebruik van de snelheid van de incrementele back-upmethode, terwijl tegelijkertijd het grootste nadeel, namelijk het feit dat verouderde back-ups moeilijk verwijderbaar zijn, wordt vermeden. De software markeert de blokken die worden gebruikt door verouderde back-ups, als 'vrij' en schrijft nieuwe back-ups naar deze blokken. Dit resulteert in een zeer snel opschoonproces met een minimum aan resourceverbruik. Enkelvoudig back-upbestand is niet beschikbaar wanneer u een back-up maakt naar locaties die geen ondersteuning bieden voor lees - en schrijfbewerkingen via random-access.

Back-upschema	Beschrijving	Configureerbare elementen
	De eerste back-up is een volledige back-up en de andere back-ups gedurende de week zijn incrementeel. Vervolgens wordt de cyclus herhaald. Als u wilt selecteren op welke dag de wekelijkse volledige back-up wordt gemaakt, klikt u in het beschermingsschema op het tandwielpictogram en vervolgens gaat u naar **Back-upopties** > **Wekelijkse back-up**. Er worden standaard dagelijks back-ups gemaakt, van maandag tot en met vrijdag.	• Starttijd • Startvoorwaarden • Aanvullende opties
Maandelijks volledig, Wekelijks differentieel, Dagelijks incrementeel (GFS)	Standaard worden er dagelijks back-ups gemaakt, van maandag tot en met vrijdag. Elke zaterdag worden er differentiële back-ups gemaakt. Volledige back-ups worden op de eerste dag van elke maand gemaakt. **Opmerking** Dit is een vooraf gedefinieerd aangepast schema. In het beschermingsschema wordt dit weergegeven als **Aangepast**.	• Het bestaande schema wijzigen per back-uptype: ◦ Type schema: maandelijks, wekelijks, dagelijks, per uur ◦ Back-uptrigger: tijdstip of gebeurtenis ◦ Starttijd ◦ Startvoorwaarden ◦ Aanvullende opties • Nieuwe schema's toevoegen per back-uptype
Aangepast	U moet de back-uptypen selecteren (volledig, differentieel en incrementeel) en voor elk type een afzonderlijk schema configureren*.	• Het bestaande schema wijzigen per back-uptype: ◦ Type schema: maandelijks, wekelijks, dagelijks, per uur ◦ Back-uptrigger: tijdstip of gebeurtenis ◦ Starttijd ◦ Startvoorwaarden ◦ Aanvullende opties • Nieuwe schema's

Back-upschema	Beschrijving	Configureerbare elementen
		toevoegen per back-uptype

* Nadat u een beschermingsschema hebt gemaakt, kunt u niet schakelen tussen **Altijd incrementeel (één bestand)** en de andere back-upschema's, en omgekeerd. Het schema **Altijd incrementeel (één bestand)** is een indeling met één bestand, terwijl alle andere schema's een indeling met meerdere bestanden hebben. Als u tussen indelingen wilt schakelen, maakt u een nieuw beschermingsschema.

Back-uptypen

De volgende back-uptypen zijn beschikbaar:

- Volledig: Een volledige back-up bevat alle brongegevens. Deze back-up is zelfvoorzienend. Als u gegevens wilt herstellen, hebt u geen toegang tot andere back-ups nodig.

  Opmerking
  De eerste back-up die wordt gemaakt door een beschermingsschema, is een volledige back-up.

- Incrementeel: Met een incrementele back-up worden gegevens opgeslagen die zijn gewijzigd ten opzichte van de laatste back-up, ongeacht of deze volledig, differentieel of incrementeel is. Als u gegevens wilt herstellen, hebt u de hele back-upketen nodig waarvan de incrementele back-up afhankelijk is, vanaf de eerste volledige back-up.
- Differentieel: Met een differentiële back-up worden gegevens opgeslagen die zijn gewijzigd sinds de laatste volledige back-up. Als u gegevens wilt herstellen, hebt u zowel de differentiële back-up nodig als de bijbehorende volledige back-up waarvan de differentiële back-up afhankelijk is.

Een back-up uitvoeren volgens schema

Als u een back-up automatisch wilt uitvoeren op een bepaald tijdstip of bij een specifieke gebeurtenis, kunt u een schema inschakelen voor het beschermingsschema.

Een schema inschakelen:

1. Vouw in het beschermingsschema de module **Back-up maken van** uit.
2. Klik op **Planning**.
3. Schakel de schakelaar Schema in.
4. Selecteer het back-upschema.
5. Configureer het schema zoals vereist en klik vervolgens op **Gereed**.
   Zie "Planning op tijd" (p. 448) en "Planning op gebeurtenissen" (p. 450) voor meer informatie over de beschikbare schemaopties.

6. [Optioneel] Configureer startvoorwaarden of aanvullende schemaopties.
7. Sla het beschermingsschema op.

Elke keer dat aan de schemavoorwaarden wordt voldaan, wordt dan een back-upbewerking gestart.

Een schema uitschakelen:

1. Vouw in het beschermingsschema de module **Back-up maken van** uit.
2. Klik op **Planning**.
3. Schakel de schakelaar Schema uit.
4. Sla het beschermingsschema op.

De back-up wordt dan alleen uitgevoerd als u deze handmatig start.

Opmerking
Als het schema is uitgeschakeld, worden de bewaarregels niet automatisch toegepast. Als u deze wilt toepassen, moet u de back-up handmatig uitvoeren.

Planning op tijd

De volgende tabel bevat een overzicht van de planningsopties die zijn gebaseerd op tijd. Of deze opties beschikbaar zijn, hangt af van het back-upschema. Zie "Back-upschema's" (p. 445) voor meer informatie.

Optie	Beschrijving	Voorbeelden
Maandelijks	Selecteer de maanden, dagen van de maand of dagen van de week en selecteer vervolgens de starttijd van de back-up.	Voer een back-up uit op 1 januari en 3 februari om 00.00 uur. Voer een back-up uit op de eerste dag van elke maand, om 10.00 uur. Voer een back-up uit op 1 maart, 5 maart, 1 april en 5 april om 09.00 uur. Voer een back-up uit op de tweede en derde vrijdag van elke maand om 11.00 uur. Voer een back-up uit op de laatste woensdag van de maand, om 22.30 uur.
Wekelijks	Selecteer de dagen van de week en selecteer vervolgens de starttijd van de back-up.	Voer een back-up uit van maandag t/m vrijdag om 10.00 uur. Voer een back-up uit op maandag om 23.00 uur. Voer een back-up uit op dinsdag en zaterdag om 08.00 uur.

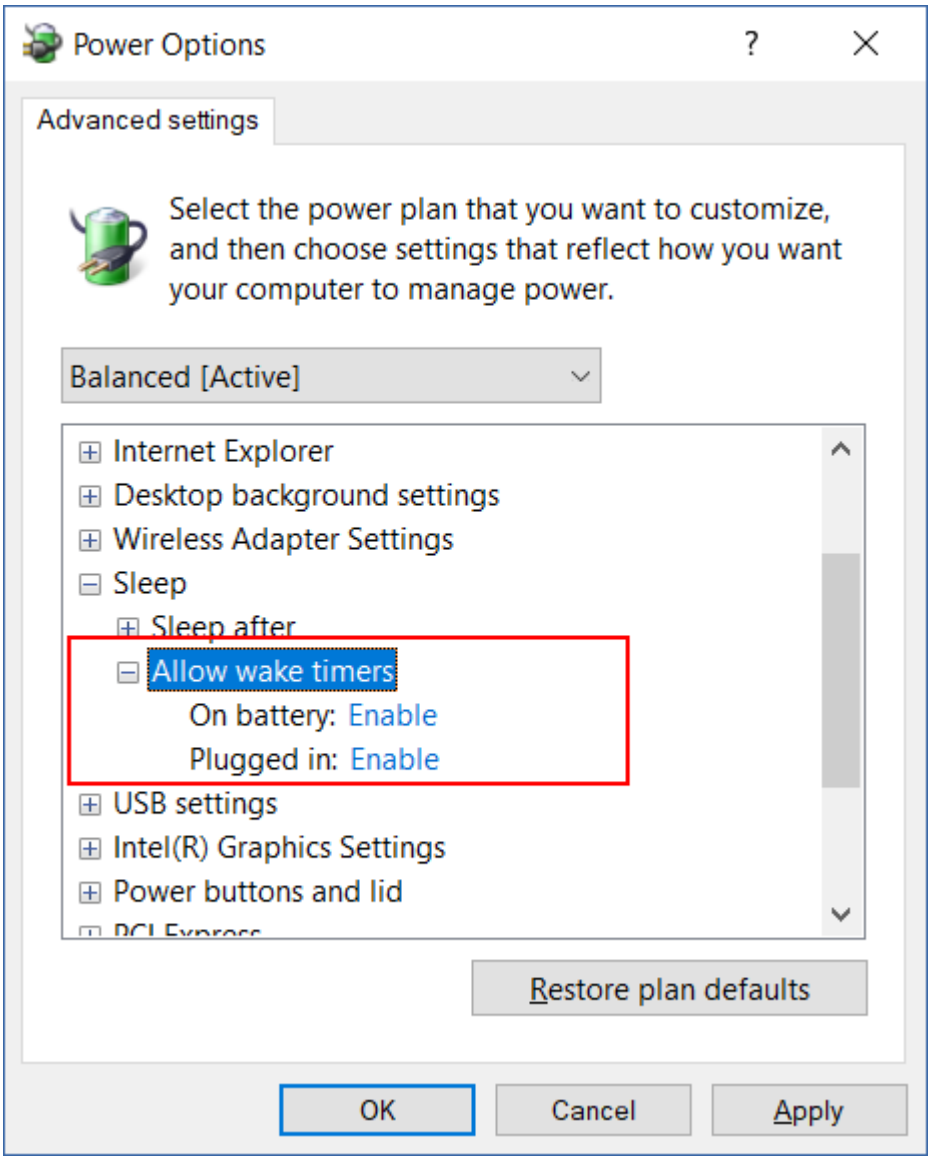
Optie	Beschrijving	Voorbeelden
Dagelijks	Selecteer de dagen (elke dag of alleen weekdagen) en selecteer vervolgens de starttijd van de back-up.	Voer elke dag een back-up uit om 11.45 uur. Voer een back-up uit van maandag t/m vrijdag om 21.30 uur.
Elk uur	Selecteer de dagen van de week en selecteer vervolgens een tijdinterval tussen twee opeenvolgende back-ups en het tijdbereik waarbinnen de back-ups worden uitgevoerd. Wanneer u het interval configureert in minuten, kunt u een voorgesteld interval tussen 10 en 60 minuten selecteren, of een aangepast interval opgeven, bijvoorbeeld 45 of 75 minuten.	Voer een back-up uit van maandag t/m vrijdag gedurende elk uur tussen 08.00 en 18.00 uur. Voer een back-up uit op zaterdag en zondag om de 3 uur tussen 01.00 en 18.00 uur.

Aanvullende opties

Wanneer u een back-up op tijd plant, zijn de volgende aanvullende planningsopties beschikbaar.

U kunt deze openen via het deelvenster **Planning** > **Meer weergeven**.

- **Als de machine is uitgeschakeld, gemiste taken uitvoeren wanneer de machine wordt opgestart**
  Standaardinstelling: Uitgeschakeld.
- **De slaapstand of stand-bymodus verhinderen tijdens het maken van een back-up**
  Deze optie is alleen van toepassing op machines met Windows.
  Standaardinstelling: Ingeschakeld.
- **De slaapstand of stand-bymodus beëindigen om een geplande back-up te starten**
  Deze optie is alleen van toepassing op machines met Windows waarop **Activeringstimers toestaan** is ingeschakeld in de energiebeheerschema's.



Deze optie maakt geen gebruik van de Wake-on-LAN-functionaliteit en is niet van toepassing op uitgeschakelde machines.

Standaardinstelling: Uitgeschakeld.

Planning op gebeurtenissen

Als u een back-up wilt configureren die wordt uitgevoerd na een specifieke gebeurtenis, selecteert u een van de volgende opties.

Optie	Beschrijving	Voorbeelden
Op tijd sinds de laatste back-up	Er wordt een back-up gestart na een bepaalde periode na de laatst uitgevoerde back-up.	Voer een back-up uit één dag na de laatste succesvolle back-up. Voer een back-up uit vier uur na de laatste succesvolle back-up.

Optie	Beschrijving	Voorbeelden
	Opmerking Deze optie is afhankelijk van hoe de vorige back-up is voltooid. Als een back-up mislukt, wordt de volgende back-up niet automatisch gestart. In dat geval moet u de back-up handmatig uitvoeren en controleren of deze met succes is voltooid, voordat u het schema opnieuw kunt instellen.	
Wanneer een gebruiker zich aanmeldt bij het systeem	Er wordt een back-up gestart wanneer een gebruiker zich aanmeldt op de machine. U kunt deze optie configureren voor elke aanmelding of voor een aanmelding van een specifieke gebruiker. **Opmerking** Er wordt geen back-up gestart als u zich aanmeldt met een tijdelijk gebruikersprofiel.	Voer een back-up uit wanneer gebruiker Jan Jansen inlogt.
Wanneer een gebruiker zich afmeldt bij het systeem	Er wordt een back-up getart wanneer een gebruiker zich afmeldt op de machine. U kunt deze optie configureren voor elke afmelding of voor de afmelding van een specifieke gebruiker. **Opmerking** Er wordt geen back-up gestart als u zich afmeldt met een tijdelijk gebruikersprofiel. Er wordt geen back-up gestart wanneer u de machine afsluit.	Voer een back-up uit wanneer elke gebruiker zich afmeldt.
Wanneer het systeem wordt opgestart	Er wordt een back-up uitgevoerd wanneer de beschermde machine wordt opgestart.	Voer een back-up uit wanneer een gebruiker de machine opstart.
Wanneer het systeem wordt afgesloten	Er wordt een back-up gemaakt wanneer de beschermde machine wordt afgesloten.	Voer een back-up uit wanneer een gebruiker de machine afsluit.

Optie	Beschrijving	Voorbeelden
Bij een gebeurtenis in het Windows-gebeurtenislogboek	Een back-up wordt uitgevoerd in het geval van een bepaalde Windows-gebeurtenis die door u is opgegeven.	Voer een back-up uit wanneer de gebeurtenis 7 van het type fout en met schijf als bron wordt geregistreerd in het systeemlogboek van Windows.

Of deze opties beschikbaar zijn, hangt af van de back-upbron en het besturingssysteem van de beschermde workloads. De onderstaande tabel bevat een overzicht van de beschikbare opties voor Windows, Linux en macOS.

Gebeurtenis	Back-upbron (Back up maken van)					
	Volledige machine, schijven/volumes of bestanden/mappen (fysieke machines)	**Volledige machines of Schijven/volumes (virtuele machines)**	**ESXi-configuratie**	**Microsoft 365-postvakken**	**Databases en postvakken en uitwisselen**	**SQL-databases**
Op tijd sinds de laatste back-up	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Wanneer een gebruiker zich aanmeldt bij het systeem	Windows	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Wanneer een gebruiker zich afmeldt bij het systeem	Windows	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Wanneer het systeem wordt opgestart	Windows, Linux, macOS	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Wanneer het systeem wordt afgesloten	Windows	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Bij een gebeurtenis in het Windows-gebeurtenislogboek	Windows	N.v.t.	N.v.t.	Windows	Windows	Windows

Bij een gebeurtenis in het Windows-gebeurtenislogboek

U kunt een back-up automatisch laten uitvoeren wanneer een specifieke gebeurtenis wordt geregistreerd in een Windows-gebeurtenislogboek, zoals het toepassingslogboek, het beveiligingslogboek of het systeemlogboek.

Opmerking
U kunt door de gebeurtenissen bladeren en de bijbehorende eigenschappen bekijken in **Computerbeheer** > **Windows Logboeken** in Windows. Als u het beveiligingslogboek wilt openen, hebt u beheerdersrechten nodig.

Gebeurtenisparameters

De volgende tabel bevat een overzicht van de parameters die u moet opgeven bij het configureren van de optie **Bij een gebeurtenis in het Windows-gebeurtenislogboek**.

Parameter	Beschrijving
Logboeknaam	De naam van het logboek. Selecteer de naam van een standaard logboek (Toepassing, Beveiliging, of Systeem) in de lijst, of geef een andere logboeknaam op. Bijvoorbeeld Microsoft Office-sessies.
Gebeurtenisbron	De gebeurtenisbron geeft aan door welk programma of systeemonderdeel de gebeurtenis is gegenereerd. Bijvoorbeeld schijf. De geplande back-up wordt geactiveerd door elke gebeurtenisbron die de opgegeven tekenreeks bevat. Deze optie is niet hoofdlettergevoelig. Als u bijvoorbeeld de tekenreeks `service` opgeeft, wordt een back-up geactiveerd door zowel de gebeurtenisbron Servicebesturingsbeheer als de gebeurtenisbron Tijdservice.
Gebeurtenistype	Het type van de gebeurtenis: Fout, Waarschuwing, Informatie, Audit voltooid of Audit mislukt.
Gebeurtenis-id	De gebeurtenis-id identificeert een bepaald soort gebeurtenis binnen een gebeurtenisbron. Bijvoorbeeld: een gebeurtenis Fout met gebeurtenisbron schijf en gebeurtenis-id 7 doet zich voor als er een beschadigd blok op een schijf wordt gedetecteerd in Windows, en een gebeurtenis Fout met gebeurtenisbron schijf en gebeurtenis-id 15 doet zich voor wanneer een schijf nog niet gereed is voor toegang.

Voorbeeld: Noodback-up in geval van beschadigde blokken op de harde schijf

Als een harde schijf een of meer beschadigde blokken bevat, kan er mogelijk binnenkort een fout optreden op die schijf. U doet er dus goed aan om een back-up te maken wanneer er een beschadigd blok wordt gedetecteerd.

Wanneer er in Windows een beschadigd blok op een harde schijf wordt gedetecteerd, wordt er in het systeemlogboek een fout geregistreerd met schijf als gebeurtenisbron en het gebeurtenisnummer 7. Ga naar het beschermingsschema en configureer het volgende schema:

- Schema: Bij een gebeurtenis in het Windows-gebeurtenislogboek
- Logboeknaam: Systeem
- Gebeurtenisbron: schijf
- Gebeurtenistype: Fout
- Gebeurtenis-id: 7

Belangrijk
Als u wilt dat de back-up ondanks de beschadigde blokken toch wordt voltooid, gaat u naar **Back-upopties**, **Foutafhandeling** en vervolgens schakelt u het selectievakje **Beschadigde sectoren negeren** in.

Startvoorwaarden

Als u een back-up alleen wilt uitvoeren als aan bepaalde voorwaarden is voldaan, moet u een of meer startvoorwaarden configureren. Als u meerdere voorwaarden configureert, moet er tegelijkertijd aan al deze voorwaarden worden voldaan om een back-up te kunnen starten. U kunt een periode opgeven waarna de back-ups worden uitgevoerd, ongeacht of aan de voorwaarden is voldaan. Zie "Startvoorwaarden voor taak" (p. 520) voor meer informatie over deze back-upoptie.

De startvoorwaarden zijn niet van toepassing wanneer u een back-up handmatig start.

De onderstaande tabel toont de startvoorwaarden die beschikbaar zijn voor verschillende gegevens onder Windows, Linux en macOS.

Startvoorwaarde	Back-upbron (Back up maken van)					
	Volledige machine, schijven/volumes of bestanden/mappen (fysieke machines)	**Volledige machines of Schijven/volumes (virtuele machines)**	**ESXi-configuratie**	**Microsoft 365-postvakken**	**Databases en postvakken en uitwisselen**	**SQL-databases**
Gebruiker is niet-actief	Windows	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
De host voor de back-uplocatie is beschikbaar	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Gebruikers zijn afgemeld	Windows	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.

Startvoorwaarde	Back-upbron (Back up maken van)					
	Volledige machine, schijven/volumes of bestanden/mappen (fysieke machines)	**Volledige machines of Schijven/volumes (virtuele machines)**	**ESXi-configuratie**	**Microsoft 365-postvakken**	**Databases en postvakken uitwisselen**	**SQL-databases**
Past in het tijdinterval	Windows, Linux, macOS	Windows, Linux	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Batterijstroom besparen	Windows	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Niet starten bij verbinding met een datalimiet	Windows	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
Niet starten indien verbonden met de volgende wifinetwerken	Windows	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.
IP-adres van apparaat controleren	Windows	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.

Gebruiker is niet-actief

'Gebruiker is niet-actief' betekent dat er op de machine een schermbeveiliging wordt uitgevoerd of dat de machine is vergrendeld.

Voorbeeld

Voer elke dag een back-up uit om 21.00 uur, bij voorkeur wanneer de gebruiker niet actief is. Voer de back-up uit, ook als de gebruiker om 23.00 nog actief is.

- Schema: **Dagelijks**, **Iedere dag uitvoeren**. Starten om: **21.00 uur**.
- Voorwaarde: **Gebruiker is niet-actief**.
- Startvoorwaarden voor back-up: **Wachten tot aan de voorwaarden is voldaan**, **De taak hoe dan ook starten na 2** uur.

Het resultaat:

- Als de gebruiker niet meer actief is om 21.00 uur, wordt de back-up gestart om 21.00 uur.
- Als de activiteit van de gebruiker stopt tussen 21.00 en 23.00 uur, wordt de back-up onmiddellijk op dat moment gestart.
- Als de gebruiker nog actief is om 23.00 uur, wordt de back-up gestart om 23.00 uur.

De host voor de back-uplocatie is beschikbaar

'De host voor de back-uplocatie is beschikbaar' betekent dat de machine met de back-uplocatie beschikbaar is via het netwerk.

Deze voorwaarde is van toepassing voor netwerkmappen, de cloudopslag en locaties die worden beheerd door een opslagknooppunt.

Deze voorwaarde heeft geen betrekking op de beschikbaarheid van de locatie zelf, alleen op de beschikbaarheid van de host. Als de host bijvoorbeeld beschikbaar is, maar de netwerkmap op deze host niet is gedeeld of de referenties voor de map niet meer geldig zijn, wordt deze voorwaarde nog steeds beschouwd als voldaan.

Voorbeeld

Elke werkdag om 21.00 uur worden er back-ups uitgevoerd in een netwerkmap. Als de machine waarop de map wordt gehost, op dat moment niet beschikbaar is (bijvoorbeeld vanwege onderhoud), kunt u de back-up overslaan en wachten op de geplande start op de volgende werkdag.

- Schema: **Dagelijks**, **uitvoeren van maandag tot en met vrijdag**. Starten om: **21.00 uur**.
- Voorwaarde: **De host voor de back-uplocatie is beschikbaar**.
- Startvoorwaarden voor back-up: **De geplande back-up overslaan**.

Het resultaat:

- Als de host om 21.00 uur beschikbaar is, wordt de back-up onmiddellijk gestart.
- Als de host om 21.00 uur niet beschikbaar is, wordt de back-up de volgende werkdag gestart (indien de host op die dag beschikbaar is om 21.00 uur).
- Als de host nooit beschikbaar is op werkdagen om 21.00 uur, wordt de back-up nooit gestart.

Gebruikers zijn afgemeld

Gebruik deze startvoorwaarde om een back-up uit te stellen totdat alle gebruikers zijn afgemeld bij een Windows-machine.

Voorbeeld

Voer de back-up uit elke vrijdag om 20.00 uur, bij voorkeur wanneer alle gebruikers zijn afgemeld. Voer de back-up toch uit als er om 23.00 uur nog een gebruiker is aangemeld.

- Schema: **Wekelijks** op vrijdag. Starten om: **20.00 uur**.
- Voorwaarde: **Gebruikers zijn afgemeld**.
- Startvoorwaarden voor back-up: **Wachten tot aan de voorwaarden is voldaan**, **De back-up hoe dan ook uitvoeren na 3** uur.

Het resultaat:

- Als alle gebruikers zijn afgemeld om 20.00 uur, wordt de back-up gestart om 20.00 uur.
- Als de laatste gebruiker zich afmeldt tussen 20.00 en 23.00 uur, wordt de back-up onmiddellijk gestart.
- Als er om 23.00 uur nog steeds aangemelde gebruikers zijn, wordt de back-up gestart om 23.00 uur.

Past in het tijdinterval

Gebruik deze startvoorwaarde om de start van een back-up te beperken tot een opgegeven interval.

Voorbeeld

Een bedrijf gebruikt verschillende locaties op dezelfde aan het netwerk gekoppelde opslag om een back-up te maken van de gegevens en servers van gebruikers.

De werkdag begint om 08.00 uur en eindigt om 17.00 uur. Zodra de gebruikers zich afmelden, maar niet vroeger dan 16.30 uur, moet er een back-up van hun gegevens worden gemaakt.

Elke dag om 23.00 uur wordt er een back-up gemaakt van de servers van het bedrijf. Het verdient daarom de voorkeur om vóór 23.00 uur een back-up te maken van de gebruikersgegevens, zodat er netwerkbandbreedte vrij wordt gemaakt voor de serverback-ups.

Het maken van een back-up van gebruikersgegevens duurt niet meer dan één uur, dus de uiterste starttijd voor de back-up is 22.00 uur. Als een gebruiker nog steeds is aangemeld binnen het opgegeven tijdinterval of zich op een ander tijdstip afmeldt, moet de back-up van de gegevens van de gebruiker worden overgeslagen.

- Gebeurtenis: **Wanneer een gebruiker zich afmeldt bij het systeem**. Geef het gebruikersaccount op: **Elke gebruiker**.
- Voorwaarde: **Past in het tijdinterval** van **16.30 uur** tot **22.00 uur**.
- Startvoorwaarden voor back-up: **De geplande back-up overslaan**.

Het resultaat:

- Als de gebruiker zich afmeldt tussen 16.30 en 22.00 uur, wordt de back-up onmiddellijk gestart.
- Als de gebruiker zich afmeldt op een ander tijdstip, wordt de back-up overgeslagen.

Batterijstroom besparen

Gebruik deze startvoorwaarde om te verhinderen dat er back-ups worden gemaakt als een machine (bijvoorbeeld een laptop of tablet) niet is aangesloten op een stroombron. Afhankelijk van de

waarde van de optie Startvoorwaarden voor back-up, wordt de overgeslagen back-up al dan niet gestart wanneer de machine is aangesloten op een stroombron.

De volgende opties zijn beschikbaar:

- **Niet starten bij gebruik van batterijstroom**
  Een back-up wordt alleen gestart als de machine is aangesloten op een stroombron.
- **Starten bij gebruik van batterijstroom als het batterijniveau hoger is dan**
  Een back-up wordt gestart als de machine is aangesloten op een stroombron of als het batterijniveau hoger is dan de opgegeven waarde.

Voorbeeld

U maakt elke werkdag om 21.00 uur een back-up van uw gegevens. Als de machine niet is aangesloten op een stroombron, wilt u de back-up mogelijk overslaan om batterijstroom te sparen en wacht u totdat de machine is aangesloten op een stroombron.

- Schema: **Dagelijks**, **uitvoeren van maandag tot en met vrijdag**. Starten om: **21.00 uur**.
- Voorwaarde: **Batterijstroom besparen**, **Niet starten bij gebruik van batterijstroom**.
- Startvoorwaarden voor back-up: **Wachten tot aan de voorwaarden is voldaan**.

Het resultaat:

- Als de machine is aangesloten op een stroombron om 21.00 uur, wordt de back-up onmiddellijk gestart.
- Als de machine om 21.00 uur op batterijvoeding werkt, wordt de back-up gestart wanneer u de machine aansluit op een stroombron.

Niet starten bij verbinding met een datalimiet

Gebruik deze startvoorwaarde om het maken van back-ups (waaronder een back-up naar een lokale schijf) te voorkomen als de machine is verbonden met internet via een verbinding met datalimiet in Windows. Zie https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq voor meer informatie over verbindingen met een datalimiet in Windows.

De aanvullende startvoorwaarde **Niet starten indien verbonden met de volgende wifinetwerken** wordt automatisch ingeschakeld wanneer u de voorwaarde **Niet starten bij verbinding met een datalimiet** inschakelt. Dit is een aanvullende maatregel om back-ups via mobiele hotspots te voorkomen. De volgende netwerknamen worden standaard opgegeven: android, telefoon, mobiel en modem.

Als u deze namen wilt verwijderen uit de lijst, klikt u op de X. Als u een nieuwe naam wilt toevoegen, typt u deze in het lege veld.

Voorbeeld

U maakt elke werkdag om 21.00 uur een back-up van uw gegevens. Als de machine met internet is verbonden via een verbinding met datalimiet, wilt u de back-up mogelijk overslaan om minder

netwerkverkeer te hebben en wacht u tot de geplande start op de volgende werkdag.

- Schema: **Dagelijks**, **uitvoeren van maandag tot en met vrijdag**. Starten om: **21.00 uur**.
- Voorwaarde: **Niet starten bij verbinding met een datalimiet**.
- Startvoorwaarden voor back-up: **De geplande back-up overslaan**.

Het resultaat:

- Als de machine om 21.00 uur niet met internet is verbonden via een verbinding met datalimiet, wordt de back-up onmiddellijk gestart.
- Als de machine om 21.00 uur wel met internet is verbonden via een verbinding met datalimiet, wordt de back-up op de volgende werkdag gestart.
- Als de machine om 21.00 uur op werkdagen altijd met internet is verbonden via een verbinding met datalimiet, wordt de back-up nooit gestart.

Niet starten indien verbonden met de volgende wifinetwerken

Gebruik deze startvoorwaarde om het maken van back-ups (waaronder een back-up naar een lokale schijf) te voorkomen als de machine is verbonden met een van de opgegeven draadloze netwerken (bijvoorbeeld als u back-ups via een hotspot op mobiele telefoons wilt beperken).

U kunt de namen van wifinetwerken (of SSID, Service Set Identifiers) opgeven. De beperking is van toepassing op alle netwerken die de opgegeven naam als subtekenreeks bevatten in hun naam (niet hoofdlettergevoelig). Als u bijvoorbeeld `phone` opgeeft als de netwerknaam, wordt de back-up niet gestart wanneer de machine is verbonden met een van de volgende netwerken: `John's iPhone`, `phone_wifi` of `my_PHONE_wifi`.

De startvoorwaarde **Niet starten indien verbonden met de volgende wifinetwerken** wordt automatisch ingeschakeld wanneer u de voorwaarde **Niet starten bij verbinding met een datalimiet** inschakelt. De volgende netwerknamen worden standaard opgegeven: android, `telefoon`, `mobiel` en modem.

Als u deze namen wilt verwijderen uit de lijst, klikt u op de X. Als u een nieuwe naam wilt toevoegen, typt u deze in het lege veld.

Voorbeeld

U maakt elke werkdag om 21.00 uur een back-up van uw gegevens. Als de machine met internet is verbonden via een mobiele hotspot, wilt u de back-up mogelijk overslaan en wachten tot de geplande start op de volgende werkdag.

- Schema: **Dagelijks**, **uitvoeren van maandag tot en met vrijdag**. Starten om: **21.00 uur**.
- Voorwaarde: **Niet starten indien verbonden met de volgende wifinetwerken**, **Netwerknaam**: `<SSID van het hotspotnetwerk>`.
- Startvoorwaarden voor back-up: **De geplande back-up overslaan**.

Het resultaat:

- Als de machine niet is verbonden met het opgegeven netwerk om 21.00 uur, wordt de back-up onmiddellijk gestart.
- Als de machine wel is verbonden met het opgegeven netwerk om 21.00 uur, wordt de back-up de volgende werkdag gestart.
- Als de machine altijd is verbonden met het opgegeven netwerk om 21.00 uur op werkdagen, wordt de back-up nooit gestart.

IP-adres van apparaat controleren

Gebruik deze startvoorwaarde om het maken van back-ups (waaronder een back-up naar een lokale schijf) te voorkomen als een of meer IP-adressen van een machine ofwel binnen ofwel buiten het opgegeven IP-adresbereik zijn. Zo kunt u bijvoorbeeld hoge kosten voor gegevensoverdracht vermijden wanneer u een back-up maakt van machines van gebruikers die zich in het buitenland bevinden, of kunt u back-ups via een VPN-verbinding (Virtual Private Network) voorkomen.

De volgende opties zijn beschikbaar:

- **Starten indien buiten IP-bereik**
- **Starten indien binnen IP-bereik**

U kunt voor elk van beide opties meerdere bereiken opgeven. Alleen IPv4-adressen worden ondersteund.

Voorbeeld

U maakt elke werkdag om 21.00 uur een back-up van uw gegevens. Als de machine is verbonden met het bedrijfsnetwerk via een VPN-tunnel, wilt u de back-up mogelijk overslaan.

- Schema: **Dagelijks**, **uitvoeren van maandag tot en met vrijdag**. Starten om **21.00 uur**.
- Voorwaarde: **IP-adres van apparaat controleren**, **Starten indien buiten IP-bereik**, **Van**: `<begin van het IP-adresbereik van VPN>`, **Tot**: `<einde van het IP-adresbereik van VPN>`.
- Startvoorwaarden voor back-up: **Wachten tot aan de voorwaarden is voldaan**.

Het resultaat:

- Als het IP-adres van de machine niet in het opgegeven bereik is om 21.00 uur, wordt de back-up onmiddellijk gestart.
- Als het IP-adres van de machine binnen het opgegeven bereik is om 21.00 uur, wordt de back-up gestart wanneer de machine een IP-adres verkrijgt dat niet een VPN-adres is.
- Als het IP-adres van de machine altijd in het opgegeven bereik is om 21.00 uur op werkdagen, wordt de back-up nooit gestart.

Aanvullende planningsopties

U kunt de back-ups zo configureren dat ze alleen worden uitgevoerd als aan bepaalde voorwaarden wordt voldaan, dat ze alleen gedurende een bepaalde periode worden uitgevoerd of dat ze met een vertraging worden uitgevoerd in vergelijking met de planning.

Startvoorwaarden configureren:

1. Vouw in het beschermingsschema de module **Back-up maken van** uit.
2. Klik op **Planning**.
3. Klik in het deelvenster **Planning** op **Meer weergeven**.
4. Schakel de selectievakjes in naast de startvoorwaarden die u wilt toevoegen en klik vervolgens op **Gereed**.
   Zie "Startvoorwaarden" (p. 454) voor meer informatie over de beschikbare startvoorwaarden en hoe u deze kunt configureren.
5. Sla het beschermingsschema op.

Een tijdbereik configureren:

1. Vouw in het beschermingsschema de module **Back-up maken van** uit.
2. Klik op **Planning**.
3. Schakel het selectievakje **Het schema uitvoeren binnen een datumbereik** in.
4. Geef de gewenste periode op en klik vervolgens op **Gereed**.
5. Sla het beschermingsschema op.

De back-ups worden dan alleen gedurende de opgegeven periode uitgevoerd.

Een vertraging configureren:

Er is een back-upoptie waarmee u een kleine willekeurige vertraging kunt configureren. Dit is handig om een te grote belasting van het netwerk te voorkomen wanneer u een back-up maakt van meerdere workloads op een netwerklocatie. U kunt deze optie uitschakelen of de instelling ervan wijzigen.

1. Vouw in het beschermingsschema de module **Back-up maken van** uit.
2. Klik op **Back-upopties** en selecteer vervolgens **Plannen**.
   De waarde van de vertraging voor elke workload wordt willekeurig geselecteerd tussen nul en de door u opgegeven maximumwaarde. De maximumwaarde is standaard ingesteld op 30 minuten.
   Voor meer informatie over deze back-upoptie: zie "Plannen" (p. 518)
   De waarde van de vertraging voor elke workload wordt berekend op het moment dat het beschermingsschema wordt toegepast op die workload. Deze waarde verandert niet totdat u de maximumwaarde voor de vertraging wijzigt.
3. Geef de gewenste periode op en klik vervolgens op **Gereed**.
4. Sla het beschermingsschema op.

Een back-up handmatig starten

U kunt geplande en ongeplande back-ups handmatig uitvoeren.

Een back-up handmatig starten:

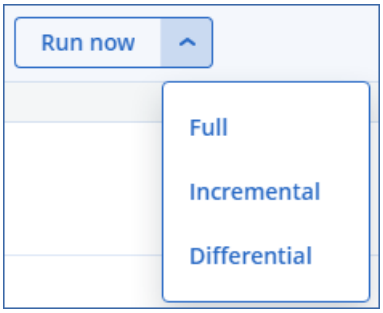
1. Ga in de Cyber Protect-console naar **Apparaten**.
2. Selecteer de workload waarvoor u een back-up wilt uitvoeren en klik vervolgens op **Beschermen**.
3. Selecteer het beschermingsschema waarvoor u de back-up wilt maken.

   Als er geen beschermingsschema wordt toegepast voor de workload, pas dan een bestaand schema toe of maak een nieuw schema.

   Zie "Een beschermingsschema maken" (p. 217) voor meer informatie over het maken van een beschermingsschema.
4. [Het standaardtype back-up maken] Klik in het beschermingsschema op het pictogram **Nu uitvoeren**.

   Of u kunt in het beschermingsschema de module **Back-up** uitvouwen en vervolgens op de knop **Nu uitvoeren** klikken.
5. [Een specifiek type back-up maken] Vouw in het beschermingsschema de module **Back-up** uit, klik op de pijl naast de knop **Nu uitvoeren** en selecteer vervolgens het back-uptype.

   Opmerking
   Het selecteren van een type is niet beschikbaar voor back-upschema's waarin slechts één back-upmethode wordt gebruikt, bijvoorbeeld **Altijd incrementeel (één bestand)** of **Altijd volledig**.

De back-upbewerking wordt dan gemaakt. U kunt de voortgang en de resultaten bekijken op het tabblad **Apparaten** in de kolom **Status**.

Bewaarregels

Als u oudere back-ups automatisch wilt verwijderen, moet u de regels voor het bewaren van back-ups in het beschermingsschema configureren.

U kunt de bewaarregels baseren op een van de volgende back-upeigenschappen:

- Nummer
- Leeftijd
- Grootte

De beschikbare bewaarregels en de bijbehorende opties zijn afhankelijk van het back-upschema. De regels zijn ook relevant voor agents, workloads en cloud-to-cloud back-ups. Zie "Bewaarregels volgens het back-upschema" (p. 463) voor meer informatie.

Afhankelijk van de configuratie van het beschermingsplan worden er bewaarregels toegepast op een archief voor of na een back-up.

U kunt het automatisch opschonen van oudere back-ups uitschakelen door tijdens het configureren van de bewaarregels de optie **Back-ups bewaren zonder tijdsbeperkingen** te selecteren. Dit kan resulteren in een verhoogd opslaggebruik en u moet de overbodige oude back-ups handmatig verwijderen.

Belangrijke tips

- Bewaarregels maken deel uit van het beschermingsschema. Als u een schema intrekt of verwijdert, worden de bewaarregels in dat schema niet meer toegepast. Zie "Back-ups verwijderen" (p. 565) voor meer informatie over het verwijderen van de back-ups die u niet meer nodig hebt.
- Als volgens het back-upschema en de back-upindeling elke back-up wordt opgeslagen als een afzonderlijk bestand, kunt u geen back-up verwijderen waarvan andere incrementele of differentiële back-ups afhankelijk zijn. Deze back-up wordt verwijderd volgens de bewaarregels die van toepassing zijn op de afhankelijke back-ups. Deze configuratie kan ertoe leiden dat meer opslagruimte wordt gebruikt omdat sommige back-ups pas later worden verwijderd. Daarnaast worden mogelijk de opgegeven waarden voor back-upleeftijd, het aantal back-ups of de grootte van de back-ups overschreden. Zie "Back-up consolideren" (p. 477) voor meer informatie over hoe u dit gedrag kunt wijzigen.
- De nieuwste back-up die met een beschermingsschema wordt gemaakt, wordt standaard nooit verwijderd. Als u echter een bewaarregel configureert om de back-ups op te schonen voordat u een nieuwe back-upbewerking wordt gestart, en u het aantal te behouden back-ups op nul instelt, wordt de nieuwste back-up ook verwijderd.

Waarschuwing!
Als u deze bewaarregel toepast op een back-upset met één back-up en de back-up mislukt, kunt u uw gegevens niet herstellen, omdat de bestaande back-up wordt verwijderd voordat er een nieuwe wordt gemaakt.

Bewaarregels volgens het back-upschema

Welke bewaarregels en instellingen beschikbaar zijn, hangt af van het back-upschema dat u gebruikt in het beschermingsschema. Zie "Back-upschema's" (p. 445) voor meer informatie over de back-upschema's.

De volgende tabel bevat een overzicht van de bewaarregels en bijbehorende instellingen.

Back-upschema	Planning	Beschikbare bewaarregels en instellingen
Altijd incrementeel (één bestand)	Maandelijks Wekelijks Dagelijks Elk uur Door gebeurtenissen geactiveerde back-ups	Op aantal back-ups Op leeftijd van de back-up (afzonderlijke instellingen voor maandelijkse, wekelijkse, dagelijkse en uurlijkse back-ups) Back-ups voor onbepaalde tijd bewaren
Altijd volledig	Maandelijks Wekelijks Dagelijks Elk uur Door gebeurtenissen geactiveerde back-ups	Op aantal back-ups Op leeftijd van de back-up (afzonderlijke instellingen voor maandelijkse, wekelijkse, dagelijkse en uurlijkse back-ups) Op totale grootte van de back-ups Back-ups voor onbepaalde tijd bewaren
Wekelijks volledig, dagelijks incrementeel	Dagelijks Door gebeurtenissen geactiveerde back-ups	Op aantal back-ups Op leeftijd van de back-up (afzonderlijke instellingen voor wekelijkse en dagelijkse back-ups) Op totale grootte van de back-ups Back-ups voor onbepaalde tijd bewaren
Maandelijks volledig, Wekelijks differentieel, Dagelijks incrementeel	Maandelijks Wekelijks Dagelijks Elk uur Door gebeurtenissen geactiveerde back-ups	Op aantal back-ups Op leeftijd van de back-up (afzonderlijke instellingen voor volledige, differentiële en incrementele back-ups) Op totale grootte van de back-ups Back-ups voor onbepaalde tijd bewaren
Aangepast	Maandelijks Wekelijks Dagelijks Elk uur Door gebeurtenissen geactiveerde back-ups	Op aantal back-ups Op leeftijd van de back-up (afzonderlijke instellingen voor volledige, differentiële en incrementele back-ups) Op totale grootte van de back-ups Back-ups voor onbepaalde tijd bewaren

Waarom zijn er maandelijkse back-ups met een uurschema?

Afhankelijk van het back-upschema kunt u de optie **Op leeftijd van de back-up** configureren voor een van de volgende back-ups:

- Maandelijkse, wekelijkse, dagelijkse en uurlijkse back-ups.

  Deze instellingen zijn beschikbaar voor alle niet-aangepaste back-upschema's en zijn gebaseerd op de tijd. Al deze back-ups (maandelijks, wekelijks, dagelijks en uurlijks) zijn beschikbaar, zelfs als u uw back-ups zo configureert dat ze elk uur worden uitgevoerd. Zie het onderstaande voorbeeld.

Back-up	Beschrijving
Maandelijks	Een maandelijkse back-up is de eerste back-up van de maand.
Wekelijks	Een wekelijkse back-up is de eerste back-up die wordt gemaakt op de dag van de week die u opgeeft in de optie Wekelijkse back-up. Deze dag wordt beschouwd als het begin van de week voor de bewaarregels. Als een wekelijkse back-up de eerste back-up van de maand is, wordt deze back-up beschouwd als een maandelijkse back-up. In dit geval wordt een wekelijkse back-up gemaakt op de geselecteerde dag van de volgende week.
Dagelijks	Een dagelijkse back-up is de eerste back-up van de dag, tenzij deze back-up overeenkomt met de definitie van een maandelijkse of wekelijkse back-up. In dit geval wordt de dagelijkse back-up de volgende dag gemaakt.
Elk uur	Een uurlijkse back-up is de eerste back-up van het uur, tenzij deze back-up overeenkomt met de definitie van een maandelijkse, wekelijkse of dagelijkse back-up. In dit geval wordt de uurlijkse back-up het volgende uur gemaakt.

- Volledige, differentiële en incrementele back-ups.

  Deze instellingen zijn beschikbaar voor het **aangepaste** back-upschema en hangen af van de back-upmethode. **Maandelijks volledig, Wekelijks differentieel, Dagelijks incrementeel** is een vooraf geconfigureerd aangepast schema.

Voorbeeld

U gebruikt het back-upschema **Altijd incrementeel (één bestand)** met de standaardinstelling voor uurlijkse back-ups:

- Gepland op tijd.
- Back-up uurlijks uitvoeren: Maandag tot en met vrijdag, elk uur, van 08.00 tot 18.00 uur.
- De optie **Wekelijkse back-up** is ingesteld op maandag.

In het gedeelte **Bewaartijd** van het beschermingsschema kunt u bewaarregels toepassen voor maandelijkse, wekelijkse, dagelijkse en uurlijkse back-ups.

De volgende tabel bevat een overzicht van de back-uptypen die gedurende een periode van 8 dagen zijn gemaakt.

Datum	Dag van week	Beschrijving
1 juli	Maandag	De eerste back-up van de maand is de maandelijkse back-up, dus de eerste back-up van vandaag is een maandelijkse back-up. De andere back-ups gedurende de dag zijn uurlijkse back-ups. Deze week wordt de eerste back-up beschouwd als de maandelijkse back-up. Daarom is er geen wekelijkse back-up. De eerste back-up van volgende week is dan de wekelijkse back-up.
2 juli	Dinsdag	De eerste back-up is dagelijks, de andere back-ups gedurende de dag zijn uurlijkse back-ups.
3 juli	Woensdag	De eerste back-up is dagelijks, de andere back-ups gedurende de dag zijn uurlijkse back-ups.
4 juli	Donderdag	De eerste back-up is dagelijks, de andere back-ups gedurende de dag zijn uurlijkse back-ups.
5 juli	Vrijdag	De eerste back-up is dagelijks, de andere back-ups gedurende de dag zijn uurlijkse back-ups.
6 juli	Zaterdag	De eerste back-up is dagelijks, de andere back-ups gedurende de dag zijn uurlijkse back-ups.
7 juli	Zondag	De eerste back-up is dagelijks, de andere back-ups gedurende de dag zijn uurlijkse back-ups.
8 juli	Maandag	De eerste back-up is wekelijks, de andere back-ups gedurende de dag zijn uurlijkse back-ups.

Bewaarregels configureren

De bewaarregels maken deel uit van het beschermingsschema en de beschikbaarheid en opties zijn afhankelijk van het back-upschema. Zie "Bewaarregels volgens het back-upschema" (p. 463) voor meer informatie.

De bewaarregels configureren:

1. Vouw in het beschermingsschema de module **Back-up maken van** uit.
2. Klik op **Hoeveel wilt u behouden**.

3. Selecteer een van de volgende opties:
   - **Op aantal back-ups**
   - **Op leeftijd van de back-up**

     Er zijn afzonderlijke instellingen voor maandelijkse, wekelijkse, dagelijkse en uurlijkse back-ups beschikbaar. De maximumwaarde voor alle typen is 9999.

     U kunt ook één instelling gebruiken voor alle back-ups.
   - **Op totale grootte van de back-ups**

     Deze instelling is niet beschikbaar voor het back-upschema **Altijd incrementeel (één bestand)**.
   - **Back-ups voor onbepaalde tijd bewaren**
4. [Als u **Back-ups voor onbepaalde tijd bewaren** niet hebt geselecteerd] Configureer de waarden voor de geselecteerde optie.
5. [Als u **Back-ups voor onbepaalde tijd bewaren** niet hebt geselecteerd] Selecteer wanneer de bewaarregels worden toegepast:
   - Na een back-up
   - Vóór een back-up

     Deze optie is niet beschikbaar wanneer een back-up wordt gemaakt van Microsoft SQL Server-clusters of Microsoft Exchange Server-clusters.
6. Klik op **Gereed**.
7. Sla het beschermingsschema op.

Replicatie

Met replicatie wordt elke nieuwe back-up automatisch gekopieerd naar een replicatielocatie. De back-ups in de replicatielocatie zijn niet afhankelijk van de back-ups in de bronlocatie en vice versa.

Alleen de laatste back-up in de bronlocatie wordt gerepliceerd. Maar als eerdere back-ups niet zijn gerepliceerd (bijvoorbeeld vanwege een probleem met de netwerkverbinding), dan omvat de replicatiebewerking alle back-ups die zijn gemaakt na de laatste goed uitgevoerde replicatie.

Als een replicatiebewerking wordt onderbroken, worden de verwerkte gegevens gebruikt bij de volgende replicatiebewerking.

Opmerking
In dit onderwerp wordt replicatie beschreven als onderdeel van een beveiligingsplan. Je kunt ook een afzonderlijk back-upreplicatieplan maken. Zie "Back-upreplicatie" (p. 225) voor meer informatie.

Voorbeelden van gebruik

- Betrouwbaar herstel

  Sla uw back-ups zowel op locatie (voor onmiddellijk herstel) als extern op (hiermee beveiligt u de back-ups tegen fouten in de opslag of natuurrampen op de primaire locatie).
- Bescherm gegevens tegen een natuurramp via cloudopslag

Repliceer de back-ups naar de cloudopslag door alleen gegevenswijzigingen over te brengen.

- Bewaar alleen de meest recente herstelpunten

  Gebruik bewaarregels om oudere back-ups te verwijderen uit een snelle opslag, zodat u geen onnodige opslagkosten hebt.

Ondersteunde locaties

Locatie	Als bronlocatie	Als replicatielocatie
Lokale map	+	+
Netwerkmap	+	+
Cloudopslag	-	+
Secure Zone	+	–
Openbare cloud	+	+

Replicatie inschakelen:

1. Vanuit een beschermingsschema vouwt u de module **Back-up** uit en vervolgens klikt u op **Locatie toevoegen**.

   Opmerking
   De optie **Locatie toevoegen** is niet beschikbaar wanneer u de cloudopslag selecteert in **Locatie van back-up**.

2. Open de lijst met beschikbare locaties en selecteer de replicatielocatie.

   De locatie wordt in het beschermingsplan weergegeven als **2e locatie**, **3e locatie**, **4e locatie** of **5e locatie**, afhankelijk van het aantal locaties dat u hebt toegevoegd voor replicatie.
3. [Optioneel] Klik op het tandwielpictogram om de opties voor de replicatielocatie te configureren.
   - **Prestatie- en back-upvenster**: stel het back-upvenster voor de geselecteerde locatie in, zoals beschreven in "Prestatie- en back-upvenster" (p. 507). Met deze instellingen worden de replicatieprestaties gedefinieerd.
   - **Locatie verwijderen**: verwijder de momenteel geselecteerde replicatielocatie.
   - [Alleen voor cloudopslag] **Physical Data Shipping**: sla de initiële back-up op een verwisselbaar opslagapparaat op en verzend de back-up voor upload naar de cloudopslag in plaats van deze te repliceren via internet.

     Deze optie is geschikt voor locaties met een trage netwerkverbinding of wanneer u bandbreedte wilt besparen bij de overdracht van grote bestanden via het netwerk. Voor het inschakelen van de optie zijn geen geavanceerde Cyber Protect-servicequota's nodig, maar u hebt wel een Physical Data Shipping-servicequota nodig om een verzendorder te maken en te volgen. Zie "Physical Data Shipping" (p. 511).

Opmerking
Deze optie wordt ondersteund met de versie van de beveiligingsagent vanaf release C21.06.

4. [Optioneel] Ga naar de rij **Te bewaren aantal** onder de replicatielocatie en configureer de bewaarregels voor die locatie, zoals beschreven in "Bewaarregels" (p. 462).
5. [Optioneel] Herhaal stappen 1 – 4 als u meer replicatielocaties wilt toevoegen.
   U kunt maximaal vier replicatielocaties configureren (**2e locatie**, **3e locatie**, **4e locatie** en **5e locatie**). Als u **cloudopslag** selecteert, is het niet mogelijk om meer replicatielocaties toe te voegen.

Belangrijk
Als u back-up en replicatie in hetzelfde beschermingsschema inschakelt, moet u ervoor zorgen dat de replicatie is voltooid vóór de volgende geplande back-up. Als de replicatie nog wordt uitgevoerd, wordt de geplande back-up niet gestart. Een geplande back-up die eenmaal per 24 uur wordt uitgevoerd, start bijvoorbeeld niet als de replicatie 26 uur duurt.

U kunt deze afhankelijkheid vermijden door een afzonderlijk plan te gebruiken voor back-upreplicatie. Zie "Back-upreplicatie" (p. 225) voor meer informatie over dit specifieke plan.

Versleuteling

Het cryptografische Advanced Encryption Standard (AES)- algoritme werkt in de Galois/Counter (GCM)-modus, waarbij een willekeurig gegenereerde 256-bitssleutel wordt gebruikt. De versleutelingssleutel wordt vervolgens versleuteld met het AES-256-algoritme via een SHA-2 (256 bits)-hash van het wachtwoord als sleutel. Het wachtwoord zelf wordt nergens op de schijf of in de back-ups opgeslagen, en de wachtwoordhash wordt gebruikt voor verificatie.

Met deze tweelaagse beveiliging zijn de back-upgegevens beschermd tegen ongeautoriseerde toegang, maar het is niet mogelijk een verloren wachtwoord te herstellen.

Opmerking
Het AES-256 algoritme met een sterk wachtwoord biedt kwantumbestendige versleuteling en is veilig tegen cryptanalytische aanvallen die gebruikmaken van kwantumcomputing.

We raden u aan om alle back-ups te versleutelen die worden opgeslagen in de cloudopslag, vooral als uw bedrijf is gebonden aan regelgeving hierover.

U kunt versleuteling op de volgende manieren configureren:

- In het beschermingsplan
- Als machine-eigenschap, via Cyber Protect Monitor of de opdrachtregelinterface

Versleuteling configureren in het beschermingsplan

In een beschermingsplan is versleuteling standaard ingeschakeld. Het AES-256-algoritme wordt gebruikt.

Met een sterk wachtwoord biedt het AES-256-algoritme kwantumresistente versleuteling.

Voor accounts in de compliancemodus kunt u geen versleuteling configureren in het beschermingsplan. Zie "Versleuteling configureren als machine-eigenschap" (p. 470) voor meer informatie over het configureren van versleuteling op het beschermde apparaat.

Versleuteling configureren:

1. Breid de **Backup**-module uit in een beschermingsschema.
2. Ga naar **Versleuteling** en klik op **Wachtwoord opgeven**.
3. Geef het versleutelingswachtwoord op en bevestig dit.
4. Klik op **OK**.

Waarschuwing!
Er is geen manier om versleutelde back-ups te herstellen als u het wachtwoord verliest of vergeet.

U kunt de versleutelingsinstellingen niet wijzigen nadat u het beschermingsplan hebt toegepast. Als u verschillende versleutelingsinstellingen wilt gebruiken, maakt u een nieuw plan.

Versleuteling configureren als machine-eigenschap

U kunt back-upversleuteling configureren als een machine-eigenschap. In dit geval wordt back-upversleuteling niet geconfigureerd in het beschermingsplan, maar in de beschermde workload. Bij versleuteling als machine-eigenschap wordt het AES-algoritme met een 256-bits sleutel (AES-256) gebruikt.

Opmerking
Het AES-256 algoritme met een sterk wachtwoord biedt kwantumbestendige versleuteling en is veilig tegen cryptanalytische aanvallen die gebruikmaken van kwantumcomputing.

Als u versleuteling configureert als machine-eigenschap, worden de beschermingsplannen hierdoor als volgt beïnvloed:

- **Beschermingsschema's die al worden toegepast op de machine.** Als de versleutelingsinstellingen in een beschermingsschema anders zijn, mislukken de back-ups.
- **Beveiligingsplannen die later op de machine worden toegepast.** De versleutelingsinstellingen die op de machine zijn opgeslagen, overschrijven de versleutelingsinstellingen in het beschermingsplan. Elke back-up wordt versleuteld, zelfs als versleuteling is uitgeschakeld in de instellingen van de Back-upmodule.

Voor accounts in de compliancemodus is alleen versleuteling als machine-eigenschap beschikbaar.

Als u meer dan één Agent voor VMware hebt verbonden met dezelfde vCenter Server, en u configureert versleuteling als machine-eigenschap, moet u hetzelfde versleutelingswachtwoord gebruiken op alle machines met Agent voor VMware (dit is vanwege de belastingverdeling tussen de agents).

U kunt versleuteling als machine-eigenschap op de volgende manieren configureren:

- Op de opdrachtregel
- In Cyber Protect Monitor (beschikbaar voor Windows en macOS)

Versleuteling configureren:

Op de opdrachtregel

1. Meld u aan als beheerder (in Windows) of rootgebruiker (in Linux).
2. Voer op de opdrachtregel de volgende opdracht uit:
   - Voor Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
     <encryption_password>
     ```

     Standaard is het installatiepad: `%ProgramFiles%\BackupClient`.
   - Voor Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   - Voor een virtueel apparaat:

     ```
      /./sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   Waarschuwing!
   Er is geen manier om versleutelde back-ups te herstellen als u het wachtwoord verliest of vergeet.

In Cyber Protect Monitor

1. Meld u aan als beheerder.
2. Klik op het Cyber Protect Monitor-pictogram in het systeemvak (in Windows) of op de menubalk (in macOS).
3. Klik op het tandwielpictogram en klik vervolgens op **Instellingen** > **Versleuteling**.
4. Selecteer **Een wachtwoord instellen voor deze machine**. Geef het versleutelingswachtwoord op en bevestig het.
5. Klik op **Opslaan**.

Waarschuwing!
Er is geen manier om versleutelde back-ups te herstellen als u het wachtwoord verliest of vergeet.

De versleutelingsinstellingen resetten:

1. Meld u aan als beheerder (in Windows) of rootgebruiker (in Linux).
2. Voer op de opdrachtregel de volgende opdracht uit:
   - Voor Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
     ```

     Standaard is het installatiepad: `%ProgramFiles%\BackupClient`.
   - Voor Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --reset
     ```

   - Voor een virtueel apparaat:

     ```
     /./sbin/acropsh -m manage_creds --reset
     ```

Belangrijk
Als u de versleuteling opnieuw instelt als machine-eigenschap of het versleutelingswachtwoord wijzigt nadat een beschermingsplan een back-up heeft gemaakt, zal de volgende back-upbewerking mislukken. U moet een nieuw beschermingsplan maken als u back-ups van de workload wilt kunnen blijven maken.

Notarisatie

Opmerking
Deze functie is alleen beschikbaar met het Advanced Backup-pakket.

Met notarisatie kunt u bewijzen dat een bestand authentiek en ongewijzigd is sinds er een back-up van is gemaakt. Het wordt aanbevolen om notarisatie in te schakelen wanneer u back-ups maakt van bestanden met juridische documenten of andere bestanden waarvoor bewezen authenticiteit is vereist.

Notarisatie is alleen beschikbaar voor het maken van back-ups op bestandsniveau. Bestanden met digitale handtekening worden overgeslagen, omdat deze niet hoeven te worden genotariseerd.

Notarisatie is *niet* beschikbaar:

- Als de back-upindeling is ingesteld op **Versie 11**
- Als Secure Zone de back-upbestemming is

Notarisatie gebruiken

Als u notarisatie wilt inschakelen voor alle bestanden die zijn geselecteerd voor het maken van een back-up (behalve de bestanden met een digitale handtekening), dan schakelt u de optie **Notarisatie** in wanneer u een beschermingsschema maakt.

Wanneer u herstel configureert, worden de genotariseerde bestanden gemarkeerd met een speciaal pictogram en kunt u de authenticiteit van het bestand verifiëren.

Zo werkt het

Tijdens een back-up berekent de agent de hashcodes van de bestanden waarvan een back-up is gemaakt. Daarnaast wordt een hash-boom gemaakt (op basis van de mapstructuur), wordt de boom opgeslagen in de back-up en wordt de root van de hash-boom verzonden naar de Notary-service. De Notary-service slaat de root van de hash-boom op in de Ethereum-blockchaindatabase om te waarborgen dat deze waarde niet wordt gewijzigd.

Wanneer u de authenticiteit van een bestand verifieert, berekent de agent de hash van het bestand en vergelijkt deze met de hash die is opgeslagen in de hash-boom binnen de back-up. Als deze hashes niet overeenkomen, wordt het bestand beschouwd als niet-authentiek. In andere gevallen wordt de authenticiteit van een bestand gegarandeerd door de hash-boom.

De agent verzendt de root van de hash-boom naar de Notary-service om te verifiëren of de hash-boom niet zelf is aangetast. De Notary-service vergelijkt deze met de root die is opgeslagen in de blockchaindatabase. Als de hashes overeenkomen, is het geselecteerde bestand gegarandeerd authentiek. Zo niet, dan ziet u een bericht dat het bestand niet authentiek is.

Standaardback-upopties

De standaardwaarden van de back-upopties worden gebruikt op het niveau van bedrijven, eenheden of gebruikers. Wanneer een eenheid of een gebruikersaccount wordt gemaakt binnen een bedrijf of binnen een eenheid, worden de standaardwaarden overgenomen die zijn ingesteld voor dat bedrijf of die eenheid.

Bedrijfbeheerders, eenheidbeheerders en alle gebruikers zonder beheerdersrechten kunnen een vooraf gedefinieerde standaardwaarde voor een optie wijzigen. Na de wijziging wordt de nieuwe waarde standaard gebruikt in alle beschermingsschema's die worden gemaakt op het betreffende niveau.

Wanneer u een beschermingsschema maakt, kunt u een standaardwaarde overschrijven met een aangepaste waarde die specifiek is voor alleen dit schema.

De waarde voor een standaardoptie wijzigen

1. Voer een van de volgende handelingen uit:
   - Als u de standaardwaarde voor het bedrijf wilt wijzigen, meldt u zich als bedrijfbeheerder aan bij de Cyber Protect-console.
   - Als u de standaardwaarde voor een eenheid wilt wijzigen, meldt u zich als beheerder van de eenheid aan bij de Cyber Protect-console.
   - Als u de standaardwaarde voor uzelf wilt wijzigen, meldt u zich bij de Cyber Protect-console aan met een account zonder beheerdersrechten.
2. Klik op **Instellingen** > **Systeeminstellingen**.

3. Vouw het gedeelte **Standaardback-upopties** uit.
4. Selecteer de optie en breng vervolgens de noodzakelijke wijzigingen aan.
5. Klik op **Opslaan**.

Back-upopties

Als u de back-upopties van een beschermingsschema wilt wijzigen, gaat u in de module **Back-up** naar het veld **Back-upopties** en klikt u op **Wijzigen**.

Beschikbaarheid van de back-upopties

Welke back-upopties beschikbaar zijn, hangt af van:

- De omgeving waarin de agent wordt uitgevoerd (Windows, Linux, macOS).
- Het type gegevens waarvan een back-up wordt gemaakt (schijven, bestanden, virtuele machines, applicatiegegevens).
- De back-upbestemming (cloudopslag, lokale map of netwerkmap).

De volgende tabel bevat een overzicht van de beschikbare back-upopties.

	Back-up op schijfniveau			**Back-up op bestandsniveau**			**Virtuele machines**			**SQL en Exchange**
	Windows	**Linux**	**macOS**	**Windows**	**Linux**	**macOS**	**ESXi**	**Hyper-V**	**Virtuozzo**	**Windows**
Waarschuwingen	+	+	+	+	+	+	+	+	+	+
Back-up consolideren	+	+	+	+	+	+	+	+	+	-
Naam van back-upbestand	+	+	+	+	+	+	+	+	+	+
Back-upindeling	+	+	+	+	+	+	+	+	+	+
Back-up valideren	+	+	+	+	+	+	+	+	+	+
Changed Block Tracking (CBT, Gewijzigde blokken bijhouden)	+	-	-	-	-	-	+	+	-	-
Clusterback-upmodus	-	-	-	-	-	-	-	-	-	+
Compressieniveau	+	+	+	+	+	+	+	+	+	+

Foutafhandeling										
Opnieuw proberen als er een fout optreedt	+	+	+	+	+	+	+	+	+	+
Geen berichten en dialoogvensters weergeven tijdens de verwerking (silent mode)	+	+	+	+	+	+	+	+	+	+
Beschadigde sectoren negeren	+	-	+	+	-	+	+	+	+	-
Opnieuw proberen als er een fout optreedt tijdens het maken van een momentopname van een VM	-	-	-	-	-	-	+	+	+	-
Snelle incrementele/differentiële back-up	+	+	+	-	-	-	-	-	-	-
Momentopname voor back-up op bestandsniveau	-	-	-	+	+	+	-	-	-	-
Bestandsfilters	+	+	+	+	+	+	+	+	+	-
Forensische gegevens	+	-	-	-	-	-	-	-	-	-
Ingekort logboek	-	-	-	-	-	-	+	+	-	Alleen SQL
LVM-momentopname maken	-	+	-	-	-	-	-	-	-	-
Koppelpunten	-	-	-	+	-	-	-	-	-	-
Momentopname van meerdere volumes	+	+	-	+	+	-	-	-	-	-
Herstel met één klik	+	+	-	-	-	-	-	-	-	-
Prestatie- en back-	+	+	+	+	+	+	+	+	+	+

upvenster										
Physical Data Shipping	+	+	+	+	+	+	+	+	+	-
Aangepaste opdrachten	+	+	+	+	+	+	+	+	+	+
Aangepaste opdrachten voor gegevensvastlegging	+	+	+	+	+	+	-	-	-	+
Plannen										
Starttijden binnen een tijdvenster distribueren	+	+	+	+	+	+	+	+	+	+
Het aantal gelijktijdig uitgevoerde back-ups beperken	-	-	-	-	-	-	+	+	+	-
Back-up sector-voor-sector	+	+	-	-	-	-	+	+	+	-
Splitsen	+	+	+	+	+	+	+	+	+	+
Taakfout afhandelen	+	+	+	+	+	+	+	+	+	+
Startvoorwaarden voor taak	+	+	-	+	+	-	+	+	+	+
Volume Shadow Copy Service (VSS)	+	-	-	+	-	-	-	+	-	+
Volume Shadow Copy Service (VSS) voor virtuele machines	-	-	-	-	-	-	+	+	-	-
Wekelijkse back-up	+	+	+	+	+	+	+	+	+	+
Windows-gebeurtenislogboek	+	-	-	+	-	-	+	+	-	+

Waarschuwingen

Er zijn geen back-ups gemaakt gedurende een bepaald aantal dagen

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Met deze optie bepaalt u of een waarschuwing moet worden gegenereerd als er sinds een ingestelde tijdsduur geen back-ups meer zijn gemaakt volgens het beschermingsschema. De software telt niet alleen de mislukte back-ups, maar ook back-ups die niet volgens schema zijn uitgevoerd (gemiste back-ups).

De waarschuwingen worden gegenereerd per machine en worden weergegeven op het tabblad **Waarschuwingen**.

U kunt opgeven na hoeveel dagen zonder back-up de waarschuwing wordt gegenereerd.

Back-up consolideren

Deze optie bepaalt of back-ups worden geconsolideerd tijdens het opruimen of dat volledige back-upreeksen worden verwijderd.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Consolidatie is het proces waarbij twee of meer achtereenvolgende back-ups worden gecombineerd in één enkele back-up.

Als deze optie is ingeschakeld, wordt een back-up die moet worden verwijderd bij het opschonen, geconsolideerd met de volgende afhankelijke back-up (incrementeel of differentieel).

Anders wordt de back-up bewaard totdat alle afhankelijke back-ups worden verwijderd. Op die manier wordt de potentieel tijdrovende consolidatie vermeden, maar is er wel extra ruimte vereist voor de opslag van back-ups waarvan het verwijderen is uitgesteld. De leeftijd van de back-ups en het aantal back-ups kunnen de opgegeven waarden in de bewaarregels overschrijden.

Belangrijk
Denk eraan dat consolidatie slechts een methode voor verwijderen is, maar geen alternatief. De resulterende back-up bevat geen gegevens die aanwezig waren in de verwijderde back-up, maar die afwezig waren in de bewaarde incrementele of differentiële back-up.

Deze optie is *niet* effectief onder één van de volgende omstandigheden:

- De back-upbestemming is de cloudopslag.
- Het back-upschema is ingesteld op **Altijd incrementeel (één bestand)**.
- Het back-upformaat is ingesteld op **Versie 12**.

Back-ups die worden opgeslagen in de cloudopslag en back-ups met één bestand (zowel in de indeling van versie 11 als 12) worden altijd geconsolideerd, omdat hun interne structuur zorgt voor snelle en eenvoudige consolidatie.

Als u de indeling van versie 12 gebruikt en er meerdere back-upketens aanwezig zijn (elke reeks wordt opgeslagen in een afzonderlijk TIBX-bestand), dan werkt consolidatie alleen binnen de laatste keten. Elke andere reeks wordt als geheel verwijderd, behalve de eerste, die tot de minimumgrootte wordt ingekrompen om de metagegevens te behouden (~ 12 kB). Deze metagegevens zijn vereist om de gegevensconsistentie te waarborgen tijdens gelijktijdige lees- en schrijfbewerkingen. De back-ups in deze reeksen worden niet meer weergegeven in de GUI zodra de bewaarregel wordt toegepast. Ze blijven echter fysiek bestaan totdat de volledige keten wordt verwijderd.

In alle andere gevallen worden back-ups waarvan de verwijdering is uitgesteld, gemarkeerd met het prullenbakpictogram ( ) in de GUI. Als u een dergelijke back-up verwijdert door op de X te klikken, wordt de consolidatie uitgevoerd.

Naam van back-upbestand

Met deze optie definieert u de namen van de back-upbestanden die worden gemaakt door het beschermingsschema of het back-upschema voor cloudtoepassingen.

De namen van de back-upbestanden die worden gemaakt door beveiligingsschema's, kunt u bekijken in een toepassing voor bestandsbeheer wanneer u door de back-uplocatie bladert.

Wat is een back-up bestand?

Bij elk beschermingsschema worden een of meer bestanden gemaakt in de back-uplocatie, afhankelijk van het back-upschema en de gebruikte back-upindeling. In de onderstaande tabel vindt u welke bestanden kunnen worden gemaakt per machine of postvak.

	Altijd incrementeel (één bestand)	**Andere back-upschema's**
Back-upindeling **Versie 11**	Eén TIB-bestand en één XML-metagegevensbestand	Meerdere TIB-bestanden en één XML-metagegevensbestand
Back-upindeling **Versie 12**	Eén TIBX-bestand per back-upreeks (een volledige of differentiële back-up en alle incrementele back-ups die ervan afhankelijk zijn). Als de grootte van een bestand dat is opgeslagen in een lokale of netwerkmap (SMB), groter is dan 200 GB, wordt het bestand standaard opgesplitst in bestanden van 200 GB.	

Alle bestanden hebben dezelfde naam, met of zonder tijdstempel of volgnummer. U kunt deze naam (oftewel 'naam van back-upbestand') opgeven wanneer u een beschermingsschema of een back-upschema voor cloudtoepassingen maakt of bewerkt.

Opmerking
Een tijdstempel wordt alleen aan de naam van het back-upbestand toegevoegd in de back-upindeling Versie 11.

Als u de naam van een back-upbestand in een beschermingsschema of een back-upschema voor cloudtoepassingen wijzigt, is de volgende back-up een volledige back-up.

Als u de naam van een bestaand back-upbestand van dezelfde machine opgeeft, wordt er een volledige, incrementele of differentiële back-up gemaakt volgens de planning van het schema.

Opmerking
Als u back-upbestanden (.tibx) verplaatst uit hun oorspronkelijke opslag, moet u de naam ervan niet wijzigen. Bestanden met een gewijzigde naam worden behandeld als beschadigde bestanden en u kunt hiervan geen gegevens herstellen.

Het is mogelijk namen van back-upbestanden in te stellen voor locaties die niet toegankelijk zijn voor bestandsbeheer (zoals de cloudopslag). In dit geval kunt u de aangepaste namen zien op het tabblad **Back-upopslag**.

Waar kan ik de namen van back-upbestanden zien?

Voor beschermingsschema's: open het tabblad **Back-upopslag**, selecteer de locatie en selecteer vervolgens het back-uparchief.

- De standaardnaam voor back-upbestanden wordt weergegeven in het deelvenster **Details**.
- Als u een andere naam dan de standaardnaam voor back-upbestanden selecteert, wordt deze op het tabblad **Back-upopslag** weergegeven in de kolom **Naam**.

Voor back-upschema's van cloudtoepassingen: open het tabblad **Back-upopslag**, selecteer de locatie, selecteer het back-uparchief en klik vervolgens op het tandwielpictogram.

Beperkingen voor namen van back-upbestanden

- De naam van een back-upbestand kan niet eindigen op een cijfer.
  Om te voorkomen dat de standaardnaam voor back-upbestanden eindigt op een cijfer, wordt de letter 'A' toegevoegd aan het eind. Als u een aangepaste naam maakt, dient u ervoor te zorgen dat deze niet op een cijfer eindigt. De naam mag niet eindigen op een variabele, aangezien een variabele mogelijk eindigt op een cijfer.
- De naam van een back-upbestand mag de volgende symbolen niet bevatten: **()&?*$<>":\|/#**, regeleinden (**\n**) of tabs (**\t**).

Opmerking
Kies gebruiksvriendelijke namen voor de back-upbestanden. Zo kunt u eenvoudig onderscheid maken tussen back-ups wanneer u met bestandsbeheer door de back-uplocatie bladert.

Standaardnaam voor back-upbestanden

De standaardnaam voor back-upbestanden voor back-ups van volledige fysieke en virtuele machines, schijven/volumes, bestanden/mappen, Microsoft SQL Server-databases, Microsoft Exchange Server-databases en ESXi-configuratie is `[Machine Name]-[Plan ID]-[Unique ID]A`.

De standaardnaam voor back-ups van Exchange-postvakken en Microsoft 365-postvakken die door een lokale Agent voor Microsoft 365 zijn gemaakt, is `[Mailbox ID]_mailbox_[Plan ID]A`.

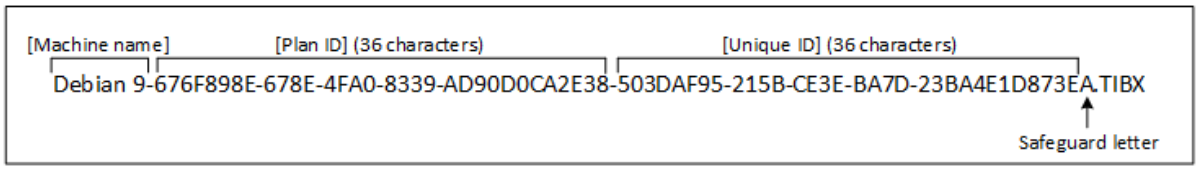
De standaardnaam voor Microsoft Azure-back-ups wordt voorafgegaan door `[Mailbox ID]_`. Dit voorvoegsel kan niet worden verwijderd.

De standaardnaam voor back-ups van cloudtoepassingen die door cloudagenten worden gemaakt, is `[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`.

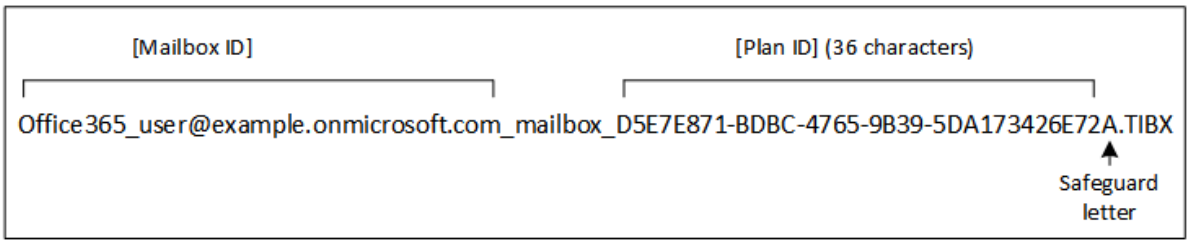
De standaardnaam bestaat uit de volgende variabelen:

- `[Machine Name]` Deze variabele wordt vervangen door de naam van de machine (dezelfde naam die wordt weergegeven in de Cyber Protect-console).
- `[Plan ID]`, `[Plan Id]` Deze variabelen worden vervangen door de unieke id van het beschermingsschema. Deze waarde verandert niet als de naam van het schema wordt gewijzigd.
- `[Unique ID]` Deze variabele wordt vervangen door de unieke id van de geselecteerde machine. Deze waarde verandert niet als de naam van de machine wordt gewijzigd.
- `[Mailbox ID]` Deze variabele wordt vervangen door de principal-naam van de gebruiker van het postvak (UPN).
- `[Resource Name]` Deze variabele wordt vervangen door de naam van de cloudgegevensbron, zoals de principal-naam van de gebruiker (UPN), de URL van de SharePoint-site of de naam van de gedeelde Drive.
- `[Resource Type]` Deze variabele wordt vervangen door het type van de cloudgegevensbron, zoals `mailbox`, `O365Mailbox`, `O365PublicFolder`, `OneDrive`, `SharePoint`, `GDrive`.
- `[Resource ID]` Deze variabele wordt vervangen door de unieke id van de cloudgegevensbron. Deze waarde verandert niet als de naam van de cloudgegevensbron wordt gewijzigd.
- `'A'` is een letter die wordt toegevoegd aan het eind om te voorkomen dat de naam op een cijfer eindigt.

In het onderstaande diagram wordt de standaardnaam voor back-upbestanden weergegeven.



In het onderstaande diagram wordt de standaardnaam voor back-upbestanden weergegeven voor back-ups van Microsoft 365-postvakken die door een lokale agent worden uitgevoerd.



Namen zonder variabelen

Als u de naam van het back-upbestand wijzigt in `MyBackup`, zullen de back-upbestanden eruitzien als in de volgende voorbeelden. Bij beide voorbeelden wordt uitgegaan van incrementele back-ups die

vanaf 13 september 2016 dagelijks zijn gepland om 14:40 uur.

Voor de indeling Versie 12 met het back-upschema **Altijd incrementeel (één bestand)**:

```
MyBackup.tibx
```

Voor de indeling Versie 12 met andere back-upschema's:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Variabelen gebruiken

Naast de variabelen die standaard worden gebruikt, kunt u gebruikmaken van de volgende variabelen:

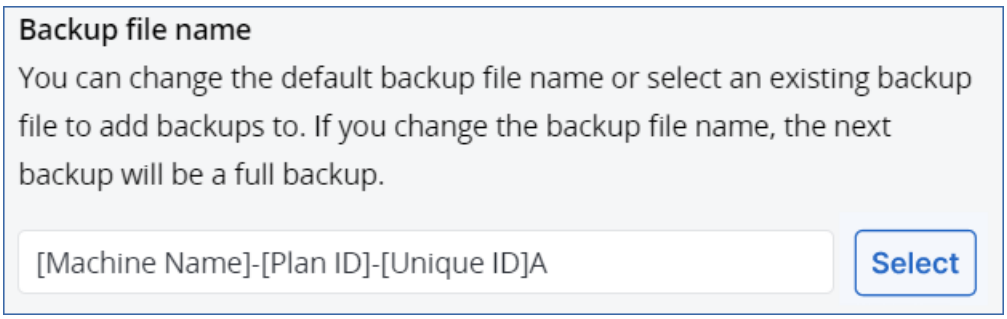
- De variabele `[Plan name]`, die wordt vervangen door de naam van het beschermingsschema.
- De variabele `[Virtualization Server Type]`, die wordt vervangen door 'vmwesx' als back-ups van virtuele machines worden gemaakt door Agent voor VMware, of door 'mshyperv' als back-ups van virtuele machines worden gemaakt door Agent voor Hyper-V.

Als er meerdere machines of postvakken worden geselecteerd voor een back-up, moet de naam van het back-upbestand een van de volgende variabelen bevatten: `[Machine Name]`, `[Unique ID]`, `[Mailbox ID]`, `[Resource Name]` of `[Resource Id]`.

Back-ups maken in een bestaand back-uparchief

U kunt configureren dat de back-ups van een workload worden toegevoegd aan een bestaand back-uparchief.

Deze optie kan bijvoorbeeld nuttig zijn wanneer een beschermingsschema wordt toegepast op slechts één machine en u deze machine moet verwijderen uit de Cyber Protect-console, of wanneer u de agent en de bijbehorende configuratie-instellingen moet verwijderen. Nadat u de machine opnieuw hebt toegevoegd of de agent opnieuw hebt geïnstalleerd, kunt u afdwingen dat het beschermingsschema nieuwe back-ups toevoegt aan het oorspronkelijke archief.



Configureren dat de back-ups van een workload worden toegevoegd aan een bestaand back-uparchief

Niet-cloud-to-cloud workloads

1. Open het scherm **Alle apparaten** en klik op de workload en vervolgens op **Beschermen**.
2. Ga naar de instellingen van het beschermingsschema en vouw de **Back-up**module uit.
3. Klik op **Back-upopties** en vervolgens op **Wijzigen**.
4. Ga naar het tabblad **Naam van back-upbestand** en klik op **Selecteren**.
   Met de knop **Selecteren** worden de back-ups weergegeven die te vinden zijn op de locatie die is geselecteerd in de sectie **Locatie van back-up** van het back-upschema.

   Opmerking
   De knop **Selecteren** is alleen beschikbaar voor beschermingsschema's die worden gemaakt voor en worden toegepast op een enkele workload.

5. Selecteer een archief en klik vervolgens op **Gereed**.
6. Klik op **Gereed** en vervolgens op **Toepassen**.

Cloud-to-cloud workloads

1. Ga naar het tabblad **Beheer** > **Back-up van cloudtoepassingen** en selecteer het schema.
2. Klik op **Bewerken** en klik vervolgens op het tandwielpictogram naast de naam van het schema.
3. Ga naar het tabblad **Naam van bestandsback-up** en klik op **Selecteren**.

   Opmerking
   De knop **Selecteren** is alleen beschikbaar voor beschermingsschema's die worden gemaakt voor en worden toegepast op slechts één workload.

4. Selecteer een back-uparchief en klik vervolgens op **Gereed**.
5. Klik op **Gereed** en vervolgens op **Wijzigingen opslaan**.

Back-upindeling

De optie **Back-upindeling** definieert de indeling van back-ups die met het beschermingsschema worden gemaakt. Deze optie is alleen beschikbaar voor beschermingsschema's die al gebruikmaken van de back-upindeling Versie 11. Als dit het geval is, kunt u de back-upindeling wijzigen in Versie 12. Nadat u de back-upindeling hebt bijgewerkt naar Versie 12, is de optie niet meer beschikbaar.

- **Versie 11**
  De verouderde indeling die behouden blijft voor achterwaartse compatibiliteit.

Opmerking
Het is niet mogelijk om de back-upindeling Versie 11 te gebruiken om back-ups te maken van databasebeschikbaarheidsgroepen (DAG). Back-ups van DAG worden alleen ondersteund in de indeling Versie 12.

- **Versie 12**
  De back-upindeling die is geïntroduceerd in Acronis Backup 12 en die snellere back-ups en herstel waarborgt. Elke back-upreeks (een volledige of differentiële back-up en alle incrementele back-ups die ervan afhankelijk zijn) wordt opgeslagen in één TIBX-bestand.

Back-upindeling en back-upbestanden

Voor back-uplocaties waarin u kunt bladeren met bestandsbeheer (zoals lokale mappen of netwerkmappen), bepaalt de back-upindeling het aantal bestanden en de extensie van deze bestanden. In de onderstaande tabel vindt u welke bestanden kunnen worden gemaakt per machine of postvak.

	Altijd incrementeel (één bestand)	**Andere back-upschema's**
Back-upindeling **Versie 11**	Eén TIB-bestand en één XML-metagegevensbestand	Meerdere TIB-bestanden en één XML-metagegevensbestand
Back-upindeling **Versie 12**	Eén TIBX-bestand per back-upreeks (een volledige of differentiële back-up en alle incrementele back-ups die ervan afhankelijk zijn). Als de grootte van een bestand dat is opgeslagen in een lokale of netwerkmap (SMB), groter is dan 200 GB, wordt het bestand standaard opgesplitst in bestanden van 200 GB.	

De back-upindeling wijzigen in versie 12 (TIBX)

Als u de back-upindeling wijzigt van versie 11 (TIB-indeling) in versie 12 (TIBX-indeling):

- De volgende back-up wordt uitgevoerd als volledige back-up.
- In back-uplocaties waarin u kunt bladeren met bestandsbeheer (zoals lokale mappen of netwerkmappen), wordt een nieuw TIBX-bestand gemaakt. Het nieuwe bestand krijgt de naam van het oorspronkelijke bestand, met het achtervoegsel **_v12A**.
- Bewaarregels en replicatie worden alleen toegepast op de nieuwe back-ups.
- De oude back-ups worden niet verwijderd en blijven beschikbaar op het tabblad **Back-upopslag**. U kunt ze handmatig verwijderen.
- Voor de oude cloudback-ups wordt geen **Cloudopslag** quota verbruikt.
- Voor de oude lokale back-ups wordt de quota van de **Lokale back-up** verbruikt tot u de back-ups handmatig verwijdert.

Deduplicatie in archief

De TIBX-back-upindeling van versie 12 ondersteunt deduplicatie in archief. Dit heeft de volgende voordelen:

- De back-ups zijn aanzienlijk kleiner, met ingebouwde deduplicatie op blokniveau voor elk type gegevens
- Efficiënte verwerking van vaste links waardoor er geen duplicaten in de opslag zijn
- Op hash gebaseerde chunks

Opmerking
Deduplicatie in archief is standaard ingeschakeld voor alle back-ups in TIBX-indeling. U hoeft deze optie niet in te schakelen in de back-upopties en u kunt deze niet uitschakelen.

Compatibiliteit van back-upindelingen in verschillende productversies

Zie Compatibiliteit van back-uparchieven in verschillende productversies (1689) voor informatie over de compatibiliteit van back-upindelingen.

Back-up valideren

Bij validatie wordt gecontroleerd of het mogelijk is gegevens te herstellen vanuit een back-up. Wanneer deze optie is ingeschakeld, wordt elke back-up die wordt gemaakt door het beschermingsschema, onmiddellijk na het maken gevalideerd met de controlesomverificatiemethode. Deze bewerking wordt uitgevoerd door de beveiligingsagent.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Zie "Controlesomverificatie" (p. 232) voor meer informatie over validatie via controlesomverificatie.

Opmerking
Validatie is mogelijk niet beschikbaar wanneer u een back-up maakt naar de cloudopslag. Dit hangt af van de instellingen die zijn gekozen door uw serviceprovider. Validatie is ook niet beschikbaar voor back-uplocaties in openbare clouds.

Changed Block Tracking (CBT, Gewijzigde blokken bijhouden)

Deze optie is effectief voor de volgende back-ups:

- Back-ups op schijfniveau van virtuele machines
- Back-ups op schijfniveau van fysieke machines met Windows
- Back-ups van Microsoft SQL Server-databases
- Back-ups van Microsoft Exchange Server-databases

De vooraf ingestelde waarde is: **Ingeschakeld**.

Met deze optie bepaalt u of Changed Block Tracking (CBT) wordt gebruikt bij incrementele of differentiële back-ups.

De CBT-technologie versnelt het back-upproces. Wijzigingen in de inhoud van de schijf of de database worden continu bijgehouden op blokniveau. Wanneer een back-up wordt gestart, worden de wijzigingen meteen opgeslagen in de back-up.

Clusterback-upmodus

Opmerking
Deze functie is alleen beschikbaar met het Advanced Backup-pakket.

Deze opties zijn beschikbaar voor Microsoft SQL Server- en Microsoft Exchange Server-back-ups op databaseniveau.

Deze opties zijn alleen beschikbaar als de cluster zelf (AlwaysOn-beschikbaarheidsgroepen (AAG) van Microsoft SQL Server of de databasebeschikbaarheidsgroep (DAG) van Microsoft Exchange Server) wordt geselecteerd voor een back-up, in plaats van de afzonderlijke knooppunten of databases binnen de cluster. Als u afzonderlijke items binnen de cluster selecteert, is de back-up zich niet bewust van het cluster en wordt alleen van de geselecteerde items een back-up gemaakt.

Microsoft SQL Server

Met deze optie wordt de back-upmodus ingesteld voor AlwaysOn-beschikbaarheidsgroepen (AAG) van SQL Server. Deze optie is alleen effectief als Agent voor SQL is geïnstalleerd op alle AAG-knooppunten. Voor meer informatie over het maken van back-ups van AlwaysOn-beschikbaarheidsgroepen raadpleegt u AlwaysOn-beschikbaarheidsgroepen (AAG) beschermen.

De vooraf ingestelde waarde is: **Indien mogelijk secundaire replica.**

U kunt een van de volgende opties selecteren:

- **Indien mogelijk secundaire replica**
  Als alle secundaire replica's offline zijn, wordt een back-up gemaakt van de primaire replica. Wanneer u een back-up maakt van de primaire replica, wordt de SQL-server mogelijk trager, maar de back-up bevat dan wel de meest actuele status van de gegevens.
- **Secundaire replica**
  Als alle secundaire replica's offline zijn, mislukt de back-up. Back-ups maken van secundaire replica's heeft geen invloed op de prestaties van de SQL-server en maakt het u mogelijk de back-upperiode te verlengen. Passieve replica's bevatten echter mogelijk informatie die niet actueel is, omdat voor deze replica's vaak wordt ingesteld dat deze asynchroon (met vertraging) worden bijgewerkt.
- **Primaire replica**
  Als de primaire replica offline is, mislukt de back-up. Wanneer u een back-up maakt van de primaire replica, wordt de SQL-server mogelijk trager, maar de back-up bevat dan wel de meest actuele status van de gegevens.

Wanneer de back-up start, slaat de software databases over die *niet* de status **GESYNCHRONISEERD** of **SYNCHRONISEREN** hebben, ongeacht de instelling van deze optie, zodat de database consistent blijft. Als alle databases worden overgeslagen, mislukt de back-up.

Microsoft Exchange Server

Deze optie bepaalt de back-upmodus voor databasebeschikbaarheidsgroepen van Exchange Server. Deze optie is alleen effectief als Agent voor Exchange is geïnstalleerd op alle DAG-knooppunten. Voor meer informatie over het maken van back-ups van databasebeschikbaarheidsgroepen raadpleegt u 'Databasebeschikbaarheidsgroepen (DAG) beschermen'.

De vooraf ingestelde waarde is: **Indien mogelijk passieve kopie.**

U kunt een van de volgende opties selecteren:

- **Indien mogelijk passieve kopie**
  Als alle passieve kopieën offline zijn, wordt een back-up gemaakt van de actieve kopie. Wanneer u een back-up maakt van de actieve kopie, wordt de Exchange-server mogelijk trager, maar de back-up bevat dan wel de meest actuele status van de gegevens.
- **Passieve kopie**
  Als alle passieve kopieën offline zijn, mislukt de back-up. Back-ups maken van passieve kopieën heeft geen invloed op de prestaties van de Exchange-server en maakt het u mogelijk de back-upperiode te verlengen. Passieve kopieën bevatten echter mogelijk informatie die niet actueel is, omdat voor deze kopieën vaak wordt ingesteld dat deze asynchroon (met vertraging) worden bijgewerkt.
- **Actieve kopie**
  Als de actieve kopie offline is, mislukt de back-up. Wanneer u een back-up maakt van de actieve kopie, wordt de Exchange-server mogelijk trager, maar de back-up bevat dan wel de meest actuele status van de gegevens.

Wanneer de back-up start, slaat de software databases over die *niet* de status **IN ORDE** of **ACTIEF** hebben, ongeacht de instelling van deze optie, zodat de database consistent blijft. Als alle databases worden overgeslagen, mislukt de back-up.

Compressieniveau

Opmerking
Deze optie is niet beschikbaar voor cloud-to-cloud back-ups. Compressie voor deze back-ups is standaard ingeschakeld met een vast niveau dat overeenkomt met het niveau **Normaal** hieronder.

Met deze optie definieert u het compressieniveau dat wordt toegepast op de gegevens waarvan een back-up wordt gemaakt. De beschikbare niveaus zijn: **Geen**, **Normaal**, **Hoog**, **Maximum**.

De vooraf ingestelde waarde is: **Normaal**.

Bij een hoger compressieniveau duurt het back-upproces langer, maar de resulterende back-up neemt minder ruimte in beslag. Het niveau **Hoog** en **Maximum** werken momenteel op dezelfde manier.

Het optimale niveau voor gegevenscompressie hangt af van het type gegevens waarvan een back-up wordt gemaakt. De omvang van de back-up kan bijvoorbeeld zelfs met maximale compressie niet sterk worden verkleind als de back-up voornamelijk bestaat uit gecomprimeerde bestanden zoals .jpg, .pdf of .mp3. Indelingen als .doc of .xls kunnen wel goed worden gecomprimeerd.

Foutafhandeling

Met deze opties kunt u opgeven hoe eventuele fouten worden afgehandeld tijdens een back-up.

Opnieuw proberen als er een fout optreedt

De vooraf ingestelde waarde is: **Ingeschakeld. Aantal pogingen: 10. Interval tussen pogingen: 30 seconden.**

Wanneer een herstelbare fout optreedt, wordt automatisch geprobeerd de mislukte bewerking opnieuw uit te voeren. U kunt het tijdsinterval en het aantal pogingen instellen. Er worden geen pogingen meer ondernomen zodra de bewerking lukt of wanneer het opgegeven aantal pogingen is bereikt, al naargelang van wat het eerste gebeurt.

Als de back-upbestemming op het netwerk bijvoorbeeld niet beschikbaar is of onbereikbaar is tijdens het uitvoeren van een back-up, dan wordt automatisch om de 30 seconden geprobeerd de bestemming te bereiken, met een maximaal aantal pogingen van 30. Er worden geen pogingen meer ondernomen zodra de verbinding wordt hervat of wanneer het opgegeven aantal pogingen is bereikt, al naargelang van wat het eerste gebeurt.

Als de back-upbestemming echter niet beschikbaar is wanneer de back-up start, worden slechts 10 pogingen ondernomen.

Geen berichten en dialoogvensters weergeven tijdens de verwerking (silent mode)

De vooraf ingestelde waarde is: **Ingeschakeld**.

Wanneer silent mode is ingeschakeld, worden automatisch alle situaties verwerkt waarvoor gebruikersinteractie is vereist (met uitzondering van de behandeling van beschadigde sectoren, want dit is als afzonderlijke optie gedefinieerd). Als een bewerking niet kan worden voortgezet zonder gebruikersinteractie, dan mislukt de bewerking. In het bewerkingslogboek worden de details van de bewerking weergegeven, met inbegrip van eventuele fouten.

Beschadigde sectoren negeren

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Wanneer deze optie is uitgeschakeld en er een beschadigde sector wordt gedetecteerd, krijgt de back-upactiviteit de status **Interactie vereist**. Als u een back-up wilt maken van de geldige gegevens op een schijf die snel vervalt, kunt u het negeren van beschadigde sectoren inschakelen. Er wordt een back-up gemaakt van de resterende gegevens en u kunt de resulterende schijfback-up koppelen en geldige bestanden uitpakken naar een andere schijf.

Opmerking
Het overslaan van beschadigde sectoren wordt niet ondersteund in Linux. In de offline modus kunt u een back-up maken van Linux-systemen met beschadigde sectoren door gebruik te maken van Bootable Media Builder in de on-premises versie van Cyber Protect. Voor het gebruik van de on-premises Bootable Media Builder is een afzonderlijke licentie vereist. Neem contact op met ondersteuning voor hulp.

Opnieuw proberen als er een fout optreedt tijdens het maken van een momentopname van een VM

De vooraf ingestelde waarde is: **Ingeschakeld. Aantal pogingen: 3. Interval tussen pogingen: 5 minuten.**

Wanneer de momentopname van een virtuele machine mislukt, wordt automatisch geprobeerd de mislukte bewerking opnieuw uit te voeren. U kunt het tijdsinterval en het aantal pogingen instellen. Er worden geen pogingen meer ondernomen zodra de bewerking lukt OF wanneer het opgegeven aantal pogingen is bereikt, al naar gelang van wat het eerste gebeurt.

Snelle incrementele/differentiële back-up

Deze optie is effectief voor incrementele en differentiële back-up op schijfniveau.

Deze optie is niet effectief (altijd uitgeschakeld) voor volumes die zijn geformatteerd met een JFS-, ReiserFS3-, ReiserFS4-, ReFS- of XFS-bestandssysteem.

De vooraf ingestelde waarde is: **Ingeschakeld**.

Bij incrementele of differentiële back-up worden alleen gegevenswijzigingen vastgelegd. Het back-upproces wordt versneld omdat aan de hand van de bestandsgrootte automatisch wordt bepaald of een bestand al dan niet is gewijzigd. De datum/tijd van de laatste wijziging wordt ook vermeld. Als u deze functie uitschakelt, wordt de hele bestandsinhoud vergeleken met de inhoud die is opgeslagen in de back-up.

Bestandsfilters (uitsluiten/opnemen)

Gebruik de bestandsfilters om alleen specifieke bestanden en mappen op te nemen in een back-up of uit te sluiten van een back-up.

Bestandsfilters zijn beschikbaar voor back-ups van volledige machines, back-ups op schijfniveau en back-ups op bestandsniveau, tenzij anders vermeld.

Bestandsfilters zijn niet beschikbaar voor de XFS-, JFS-, exFAT- en ReiserFS4-bestandssystemen. Voor meer informatie: zie "Ondersteunde bestandssystemen" (p. 54).

Bestandsfilters zijn niet van toepassing voor dynamische schijven (LVM- of LDM-volumes) van virtuele machines waarvan een back-up is gemaakt in de modus zonder agent, bijvoorbeeld met Agent voor VMware, Agent voor Hyper-V of Agent voor Scale Computing.

Bestandsfilters inschakelen

1. Breid de **Backup**-module uit in een beschermingsschema.
2. Klik in **Back-upopties** op **Wijzigen**.
3. Selecteer **Bestandsfilters (uitsluiten/opnemen)**.
4. Gebruik een van de hieronder beschreven opties.

Filters voor opnemen en uitsluiten

Er zijn twee filters: een filter voor opnemen en een filter voor uitsluiten.

- **Neem alleen de bestanden op die voldoen aan de volgende criteria**
  Als u `C:\File.exe` opgeeft in het filter voor opnemen, wordt alleen van dit bestand een back-up gemaakt, zelfs als u Back-up van volledige machine hebt geselecteerd.

  Opmerking
  Dit filter wordt niet ondersteund voor back-ups op bestandsniveau wanneer **Versie 11** is geselecteerd als back-upindeling en de back-upbestemming niet de cloudopslag is.

- **Sluit de bestanden uit die voldoen aan de volgende criteria**
  Als u `C:\File.exe` opgeeft in het filter voor uitsluiten, wordt dit bestand tijdens een back-up overgeslagen, zelfs als u Back-up van volledige machine hebt geselecteerd.

U kunt beide filters tegelijkertijd gebruiken. Het filter voor uitsluiten heeft meer prioriteit dab het filter voor opnemen. Dus als u bijvoorbeeld in beide velden `C:\File.exe` opgeeft, wordt dit bestand tijdens het back-upproces overgeslagen.

Filtercriteria

U bestands- en mapnamen en volledige paden naar bestanden en mappen gebruiken als filtercriteria of maskers met jokertekens gebruiken.

De filtercriteria zijn niet hoofdlettergevoelig. Als u bijvoorbeeld `C:\Temp` opgeeft, selecteert u ook `C:\TEMP` en `C:\temp`.

- Naam
  Geef de naam van het bestand of de map op, zoals `Document.txt`. Alle bestanden en mappen met die naam worden geselecteerd.
- Volledig pad

Geef het volledige pad naar het bestand of de map op. Het pad begint met de stationsletter (voor back-ups in Windows) of de hoofdmap (root directory) (voor back-ups in Linux of macOS). In Windows, Linux en macOS kunt u schuine strepen (slashes) gebruiken (zoals in `C:/Temp/Bestand.tmp`). In Windows kunt u ook de traditionele backslash gebruiken (zoals in `C:\Temp\Bestand.tmp`).

Belangrijk
Als het besturingssysteem van de machine waarvan een back-up is gemaakt, niet correct wordt gedetecteerd tijdens een back-up op schijfniveau, dan zullen de filters voor volledige padbestanden niet werken. Er wordt een waarschuwing weergegeven in het geval van een uitsluitingsfilter. De back-up mislukt in het geval van een filter voor het opnemen van bestanden.

Een volledig pad voor een bestand is bijvoorbeeld: `C:\Temp\Bestand.tmp`. Een filter voor een volledig pad, met de stationsletter of de root directory/hoofdmap, bijvoorbeeld `C:\Temp\Bestand.tmp` of `C:\Temp\*`, resulteert in een waarschuwing of fout.

Een filter zonder de stationsletter of de root directory/hoofdmap (bijvoorbeeld `Temp\*` of `Temp\Bestand.tmp`) of een filter dat begint met een sterretje (bijvoorbeeld `*C:\`) retourneert geen waarschuwing of fout. Als het besturingssysteem van de machine waarvan een back-up is gemaakt, niet correct wordt gedetecteerd, dan zullen deze filters ook niet werken.

- Masker

  U kunt de volgende jokertekens gebruiken voor de namen en volledige paden: sterretje (*), dubbel sterretje (**) en vraagteken (?).

  Het sterretje (*) staat voor nul of meer tekens. Het filtercriterium **Doc*.txt** komt bijvoorbeeld overeen met de bestanden `Doc.txt` en `Document.txt`.

  Het dubbele sterretje (**) staat voor nul of meer tekens, met inbegrip van de slash. ****/Docs/**.txt** komt bijvoorbeeld overeen met alle TXT-bestanden in alle submappen van alle mappen met de naam `Docs`. U kunt het jokerteken met dubbel sterretje (**) alleen gebruiken voor back-ups in de indeling Versie 12.

  Het vraagteken (?) staat voor één teken. **Doc?.txt** komt bijvoorbeeld overeen met de bestanden `Doc1.txt` en `Docs.txt`, maar niet met de bestanden `Doc.txt` of `Doc11.txt`.

Momentopname voor back-up op bestandsniveau

Deze optie is alleen effectief bij het maken van back-ups op bestandsniveau.

Met deze optie definieert u hoe back-ups worden gemaakt van bestanden: ofwel een voor een, ofwel door een directe momentopname van de gegevens.

Opmerking
Van bestanden die zijn opgeslagen op netwerkshares, worden back-ups altijd een voor een gemaakt.

De vooraf ingestelde waarde is:

- Als alleen machines met Linux worden geselecteerd voor back-up: **Geen momentopname maken.**
- Anders: **Indien mogelijk een momentopname maken**.

U kunt een van de volgende opties selecteren:

- **Indien mogelijk een momentopname maken**
  Maak altijd rechtstreeks een back-up van bestanden als het niet mogelijk is een momentopname te maken.
- **Altijd een momentopname maken**
  Via een momentopname kunt u een back-up maken van alle bestanden, inclusief bestanden die zijn geopend voor exclusieve toegang. Er wordt op hetzelfde tijdstip een back-up van de bestanden gemaakt. Kies deze instelling alleen als deze factoren kritiek zijn, dat wil zeggen als het geen zin heeft back-ups van bestanden te maken zonder momentopname. Als er geen momentopname kan worden gemaakt, mislukt de back-up.
- **Geen momentopname maken**
  Maak altijd rechtstreeks een back-up van bestanden. Pogingen om een back-up te maken van bestanden die zijn geopend voor exclusieve toegang, resulteren in een leesfout. Mogelijk is ook de tijd van de bestanden in de back-up niet consistent.

Forensische gegevens

Virussen, malware en ransomware kunnen schadelijke activiteiten uitvoeren, zoals het stelen of wijzigen van gegevens. Deze activiteiten moeten mogelijk worden onderzocht, maar dit kan alleen als u digitaal bewijsmateriaal kunt overleggen. Digitaal bewijsmateriaal, zoals bestanden of sporen van activiteiten, kunnen echter worden gewist of de machine waarop de schadelijke activiteit plaatsvond, kan niet meer beschikbaar zijn.

Met back-ups met forensische gegevens kunnen onderzoekers schijfgebieden analyseren die doorgaans niet zijn opgenomen in een gewone schijfback-up. Met de optie voor back-up met **forensische gegevens** kunt u digitaal bewijsmateriaal verzamelen dat u kunt gebruiken bij forensisch onderzoek: momentopnamen van ongebruikte schijfruimte, geheugendumps en momentopnamen van actieve processen.

Back-ups met forensische gegevens worden automatisch genotariseerd.

De optie **Forensische gegevens** is alleen beschikbaar voor volledige back-ups van Windows-machines met de volgende besturingssystemen:

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

Back-ups met forensische gegevens zijn niet beschikbaar voor de volgende machines:

- Machines die met uw netwerk zijn verbonden via VPN en geen directe toegang tot internet hebben
- Machines met schijven die zijn versleuteld met BitLocker

Opmerking
U kunt de instellingen voor forensische gegevens niet wijzigen nadat een beschermingsschema met ingeschakelde **Backup**-module wordt toegepast op een machine. Maak een nieuw beschermingsschema als u andere instellingen voor forensische gegevens wilt gebruiken.

U kunt back-ups met forensische gegevens opslaan op de volgende locaties:

- Cloudopslag
- Lokale map

  Opmerking
  De locatie van de lokale map wordt alleen ondersteund voor externe harde schijven die zijn verbonden via USB.
  Lokale dynamische schijven worden niet ondersteund als locatie voor back-ups met forensische gegevens.

- Netwerkmap

Het proces van forensische back-ups

Tijdens een forensische back-up worden de volgende processen uitgevoerd:

1. Een onbewerkte geheugendump en de lijst met actieve processen genereren.
2. Een machine automatisch opnieuw opstarten in de opstartmedia.
3. Een back-up maken die zowel de bezette als niet-toegewezen ruimte bevat.
4. De schijven notariseren waarvan een back-up is gemaakt.
5. Opnieuw opstarten in het live besturingssysteem en de uitvoering van het schema voortzetten (bijvoorbeeld replicatie, retentie, validatie enzovoort).

Forensische gegevensverzameling configureren

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**. Indien gewenst, kunt u het beschermingsschema ook maken vanaf het tabblad **Beheer**.
2. Selecteer het apparaat en klik op **Beschermen**.
3. Schakel in het beschermingsschema de **Back-up**-module in.
4. Selecteer **Volledige machine** in **Back-up maken van**.
5. Klik in **Back-upopties** op **Wijzigen**.
6. Zoek de optie **Forensische gegevens**.
7. Schakel **Forensische gegevens verzamelen** in. Er wordt automatisch een geheugendump gegenereerd en een momentopname van actieve processen gemaakt.

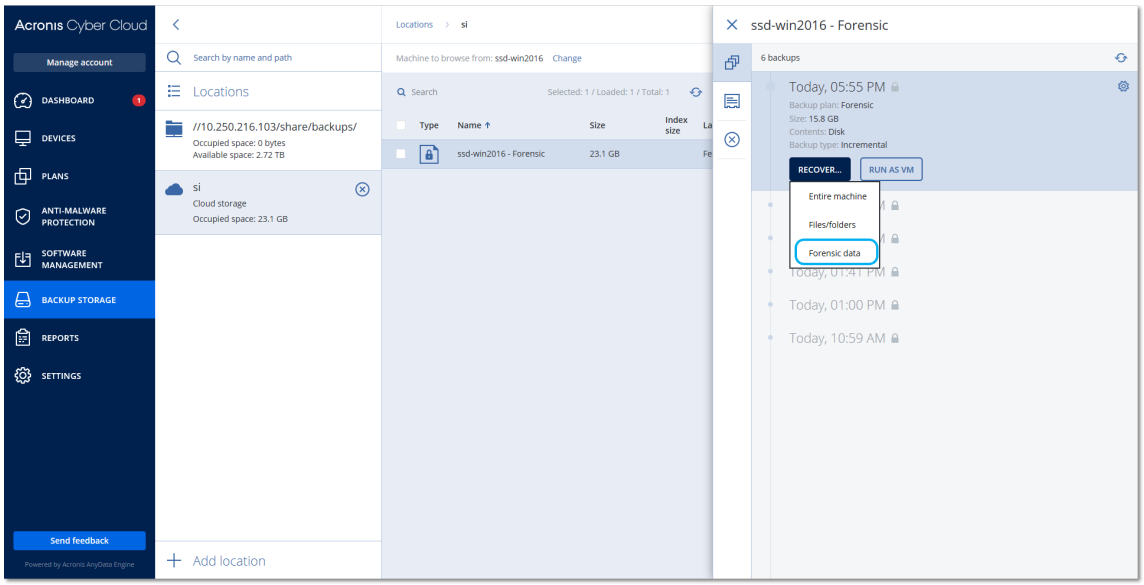
Opmerking
Volledige geheugendump kan gevoelige gegevens bevatten, zoals wachtwoorden.

8. Geef de locatie op.
9. Klik op **Nu uitvoeren** om meteen een back-up met forensische gegevens uit te voeren of wacht tot de back-up volgens het schema is gemaakt.
10. Ga naar **Controle** > **Activiteiten** en controleer of de back-up met forensische gegevens is gemaakt.

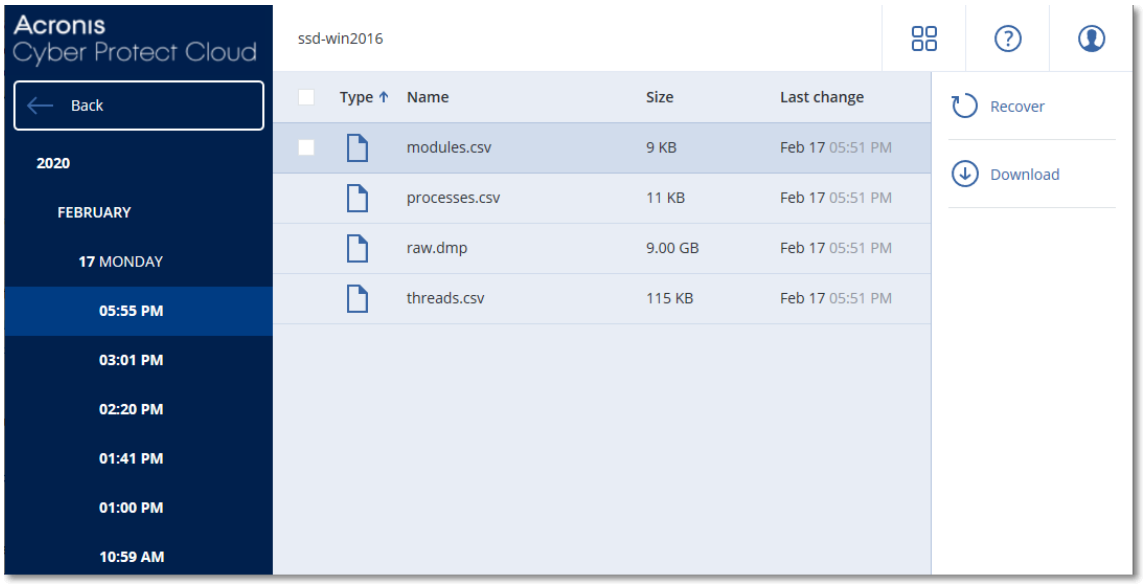
De back-ups zullen dan forensische gegevens bevatten en u kunt deze ophalen en analyseren. Back-ups met forensische gegevens worden gemarkeerd, zodat u hierop kunt filteren tussen andere back-ups in **Back-upopslag** > **Locaties** en de optie **Alleen met forensische gegevens**.

Hoe kan ik forensische gegevens ophalen uit een back-up?

1. Ga in de Cyber Protect-console naar **Back-upopslag** en selecteer de locatie met back-ups die forensische gegevens bevatten.
2. Selecteer de back-up met forensische gegevens en klik op **Back-ups weergeven**.
3. Klik op **Herstellen** voor de back-up met forensische gegevens.
   - Als u alleen de forensische gegevens wilt ophalen, klikt u op **Forensische gegevens**.



Er wordt een map met forensische gegevens weergegeven. Selecteer een geheugendumpbestand of een ander forensisch bestand en klik op **Downloaden**.



- Als u een volledige forensische back-up wilt herstellen, klikt u op **Volledige machine**. Het systeem herstelt de back-up zonder de opstartmodus. Het is dus mogelijk om te controleren of de schijf niet is gewijzigd.

U kunt de opgehaalde geheugendump gebruiken met verschillende forensische software van derden, zoals Volatility Framework op https://www.volatilityfoundation.org/ voor verdere geheugenanalyse.

Notarisatie van back-ups met forensische gegevens

Als u wilt controleren of een back-up met forensische gegevens precies de installatiekopie is die is gemaakt en of deze niet is aangetast, kunt u de back-upmodule gebruiken die notarisatie van back-ups met forensische gegevens bevat.

Zo werkt het

Met notarisatie kunt u bewijzen dat een schijf met forensische gegevens authentiek en ongewijzigd is sinds hiervan een back-up is gemaakt.

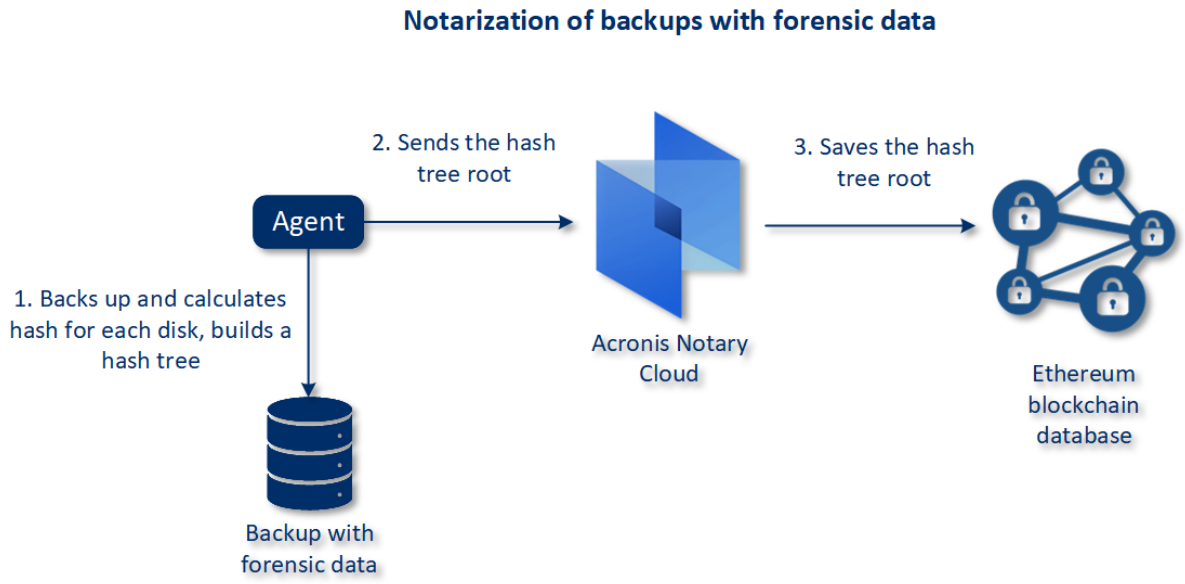
Tijdens een back-up berekent de agent de hashcodes van de schijven waarvan een back-up is gemaakt. Daarnaast wordt een hash-boom gemaakt, wordt de boom opgeslagen in de back-up en wordt de root van de hash-boom verzonden naar de Notary-service. De Notary-service slaat de root van de hash-boom op in de Ethereum-blockchaindatabase om te waarborgen dat deze waarde niet wordt gewijzigd.

Wanneer u de authenticiteit van de schijf met forensische gegevens verifieert, berekent de agent de hash van de schijf en vergelijkt deze met de hash die is opgeslagen in de hash-boom binnen de back-up. Als deze hashes niet overeenkomen, wordt de schijf beschouwd als niet-authentiek. In andere gevallen wordt de authenticiteit van de schijf gegarandeerd door de hash-boom.

De agent verzendt de root van de hash-boom naar de Notary-service om te verifiëren of de hash-boom niet zelf is aangetast. De Notary-service vergelijkt deze met de root die is opgeslagen in de

blockchaindatabase. Als de hashes overeenkomen, is de geselecteerde schijf gegarandeerd authentiek. Anders ziet u een bericht dat de schijf niet authentiek is.

Het onderstaande schema toont in het kort hoe het notarisatieproces voor back-ups met forensische gegevens verloopt.



Als u de genotariseerde schijfback-up handmatig wilt verifiëren, kunt u het certificaat hiervoor ophalen en de verificatieprocedure volgen met de tibxread-tool, zoals aangegeven bij het certificaat.

Certificaat voor back-ups met forensische gegevens ophalen

Ga als volgt te werk om het certificaat voor een back-up met forensische gegevens op te halen van de console:

1. Ga naar **Back-upopslag** en selecteer de back-up met forensische gegevens.
2. Herstel de volledige machine.
3. Het systeem opent de weergave **Schijftoewijzing**.
4. Klik op het pictogram **Certificaat ophalen** voor de schijf.
5. Het certificaat wordt gegenereerd en in de browser wordt een nieuw venster geopend met het certificaat. Onder het certificaat ziet u de instructie voor handmatige verificatie van genotariseerde schijfback-up.

De tool 'tibxread' voor het ophalen van back-upgegevens

De tool van Cyber Protection, `tibxread` genaamd, is bedoeld voor handmatige controle van de integriteit van de schijf waarvan een back-up is gemaakt. Met de tool kunt u gegevens ophalen van een back-up en de hash van de opgegeven schijf berekenen. De tool wordt automatisch geïnstalleerd met de volgende onderdelen: Agent voor Windows, Agent voor Linux en Agent voor Mac.

Het installatiepad: dezelfde map als de agent (bijvoorbeeld `C:\Program Files\BackupClient\BackupAndRecovery`).

De ondersteunde locaties zijn:

- De lokale schijf
- De netwerkmap (CIFS/SMB) die toegankelijk is zonder de referenties.
  In het geval van een netwerkmap die met een wachtwoord is beveiligd, kunt u de netwerkmap koppelen aan de lokale map met behulp van de OS-tools en vervolgens de lokale map als de bron voor deze tool.
- De cloudopslag
  U moet de URL, de poort en het certificaat opgeven. De URL en poort kunnen worden verkregen via de Windows-registersleutel of configuratiebestanden op Linux-/Mac-machines.
  Voor Windows:

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<gebruikersnaam_tenant>\FesUri
  ```

  Voor Linux:

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  Voor macOS:

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  Het certificaat is te vinden op de volgende locaties:
  Voor Windows:

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```

  Voor Linux:

  ```
  /var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

  Voor macOS:

  ```
  /Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

De tool biedt de volgende opdrachten:

- `list backups`
- `list content`
- `get content`
- `calculate hash`

list backups

Hiermee worden de herstelpunten in een back-up aangegeven.

SAMENVATTING:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Opties

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Uitvoersjabloon:
```

```
GUID   Datum   Datum-tijdstempel
----   ------ --------------
<guid> <datum> <tijdstempel>
```

<guid> – GUID van een back-up.

<date> – aanmaakdatum van de back-up. De indeling is 'DD.MM.JJJJ UU24:MM:SS'. De tijd is standaard de lokale tijdzone (u kunt deze instelling wijzigen met de optie --utc).

Voorbeeld van mogelijke uitvoer:

```
GUID   Datum   Datum-tijdstempel
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

Hiermee wordt de inhoud in een herstelpunt weergegeven.

SAMENVATTING:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

Opties

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
```

```
--raw
--log=PATH
```

Uitvoersjabloon:

```
Schijf     Grootte   Notarisatiestatus
-------- ------ --------------------
<nummer> <grootte> <notarisatiestatus>
```

<number> – identificatie van de schijf.

<size> – de grootte in bytes.

<notarization_status> – de notarisatiestatus, kan de volgende waarden hebben: Zonder notarisatie, Genotariseerd, Volgende back-up.

Voorbeeld van mogelijke uitvoer:

```
Schijf     Grootte   Notary-status
-------- ------ --------------
1        123123465798 Genotariseerd
2        123123465798 Genotariseerd
```

get content

Hiermee wordt inhoud van de opgegeven schijf in het herstelpunt geschreven naar de standaarduitvoer (stdout).

SAMENVATTING:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

Opties

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

Hiermee wordt de hash van de opgegeven schijf in het herstelpunt berekend met het SHA-2 (256-bits)-algoritme en naar de standaarduitvoer (stdout) geschreven.

SAMENVATTING:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Opties

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

Beschrijving van de opties

Optie	Beschrijving
--arc=NAAM_BACK-UP	De naam van het back-upbestand dat u kunt ophalen uit de back-upeigenschappen in de Cyber Protect-console. Het back-upbestand moet de extensie .tibx hebben.
--backup=HERSTELPUNT_ID	De id van het herstelpunt
--disk=SCHIJFNUMMER	Schijfnummer (hetzelfde nummer dat is geschreven als uitvoer van de opdracht 'get content')

--loc=URI	URI van een back-uplocatie. De mogelijke indelingen van de optie '--loc' zijn:
	• Naam van lokaal pad (Windows)
	`c:/upload/backups`
	• Naam van lokaal pad (Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• Cloudopslag
	`--loc=<IP-adres>:443 --cert=<pad_naar_certificaat> [--storage_path=/1]`
	`<IP-adres>` – kan worden gevonden in de registersleutel in Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<gebruikersnaam_tenant>\FesUri
	`<pad_naar_certificaat>` – een pad naar het certificaatbestand voor toegang tot Cyber Protect Cloud. In Windows kan dit certificaat bijvoorbeeld worden gevonden in `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<gebruikersnaam>.crt`, waarbij <gebruikersnaam> de naam van uw account is waarmee u toegang krijgt tot Cyber Protect Cloud.

--log=PAD	Hiermee kunnen de logboeken worden geschreven voor het opgegeven PAD (alleen lokaal pad, indeling is dezelfde als voor de parameter `--loc=URI`). Niveau van logboekregistratie is DEBUG.
--password=PASSWORD	Een versleutelingswachtwoord voor uw back-up. Als de back-up niet is versleuteld, laat u deze waarde leeg.

--raw	Hiermee worden de headers (2 eerste rijen) verborgen in de uitvoer van de opdracht. Wordt gebruikt wanneer de uitvoer van de opdracht moet worden geparseerd.
	Voorbeeld van uitvoer zonder '`raw`':
	`GUID Datum Datum-tijdstempel`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	Uitvoer met '`--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	Hiermee worden de datums weergegeven in UTC

--progress	Geeft de voortgang van de bewerking weer.
	Bijvoorbeeld:
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

Ingekort logboek

Deze optie is effectief voor back-ups van Microsoft SQL Server-databases en voor back-ups op schijfniveau waarbij Microsoft SQL Server-applicatieback-up is ingeschakeld.

Met deze optie wordt gedefinieerd of de SQL Server-transactielogboeken worden ingekort na een voltooide back-up.

De vooraf ingestelde waarde is: **Ingeschakeld**.

Wanneer deze optie is ingeschakeld, kan een database alleen worden hersteld naar een tijdstip van een back-up die met deze software is gemaakt. Schakel deze optie uit als u een back-up maakt van transactielogboeken via de systeemeigen back-upengine van Microsoft SQL Server. U kunt de transactielogboeken toepassen na een herstelbewerking en op die manier kunt u een database herstellen naar elk gewenst tijdstip.

LVM-momentopname maken

Deze optie is alleen effectief voor fysieke machines.

Deze optie is effectief voor back-ups op schijfniveau van volumes die worden beheerd met Linux Logical Volume Manager (LVM). Dergelijke volumes worden ook wel logische volumes genoemd.

Met deze optie definieert u hoe een momentopname van een logisch volume wordt gemaakt De back-upsoftware kan dit autonoom uitvoeren of gebruikmaken van Linux Logical Volume Manager (LVM).

De vooraf ingestelde waarde is: **Door de back-upsoftware**.

- **Door de back-upsoftware**. De momentopnamegegevens worden voornamelijk bewaard in het RAM-geheugen. De back-up wordt sneller gemaakt en er is geen niet-toegewezen ruimte voor de volumegroep vereist. We raden daarom aan om de vooraf ingestelde waarde alleen te wijzigen als u problemen ondervindt met de back-ups van logische volumes.
- **Door LVM**. De momentopname wordt opgeslagen op niet-toegewezen ruimte van de volumegroep. Als er geen niet-toegewezen ruimte is, wordt de momentopname gemaakt door de back-upsoftware.

De momentopname wordt alleen gebruikt tijdens de back-upbewerking en wordt automatisch verwijderd wanneer de back-upbewerking is voltooid. Er worden geen tijdelijke bestanden bewaard.

Koppelpunten

Deze optie is alleen effectief in Windows voor een back-up op bestandsniveau van een gegevensbron met gekoppelde volumes of gedeelde clustervolumes.

Deze optie is alleen effectief wanneer u voor de back-up een map selecteert die hoger in de maphiërarchie is dan het koppelpunt. (Een koppelpunt is een map waaraan een extra volume logisch is gekoppeld.)

- Als u een dergelijke map (een bovenliggende map) selecteert voor back-up en de optie **Koppelpunten** is ingeschakeld, wordt een back-up gemaakt van alle bestanden in het gekoppelde volume. Als de optie **Koppelpunten** is uitgeschakeld, is het koppelpunt in de back-up leeg.

  Of de inhoud van het koppelpunt wordt hersteld tijdens het herstel van een bovenliggende map, hangt af van de status van de hersteloptie voor **Koppelpunten**, namelijk of deze is ingeschakeld of uitgeschakeld.
- Als u het koppelpunt rechtstreeks selecteert, of een map in het gekoppelde volume selecteert, worden de geselecteerde mappen beschouwd als gewone mappen. Er wordt een back-up van deze mappen gemaakt, ongeacht de status van de optie **Koppelpunten** en de mappen worden hersteld, ongeacht de status van de hersteloptie voor **Koppelpunten**.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Opmerking
U kunt een back-up maken van virtuele Hyper-V-machines op een gedeeld clustervolume door een back-up te maken van de vereiste bestanden of door een back-up op bestandsniveau te maken van het hele volume. Schakel de virtuele machines van te voren uit om te waarborgen dat de back-up wordt gemaakt van de machines in een consistente status.

Voorbeeld

Stel dat de map **C:\Data1** een koppelpunt is voor het gekoppelde volume. Het volume bevat de mappen **Map1** en **Map2**. U maakt een beschermingsschema voor een back-up van uw gegevens op bestandsniveau.

Als u het selectievakje voor volume C inschakelt en vervolgens de optie **Koppelpunten** inschakelt, ziet u dat de map **C:\Data1** in uw back-up de mappen **Map1** en **Map2** bevat. Wanneer u de gegevens herstelt waarvan een back-up is gemaakt, moet u goed letten op de werking van de hersteloptie voor **Koppelpunten**.

Als u het selectievakje voor volume C inschakelt maar de optie **Koppelpunten** uitschakelt, zal de map **C:\Data1** in uw back-up leeg zijn.

Als u het selectievakje inschakelt voor de map **Data1**, **Map1** of **Map2**, worden de geselecteerde mappen beschouwd als gewone mappen en wordt er een back-up van gemaakt, ongeacht de status van de optie **Koppelpunten**.

Momentopname van meerdere volumes

Deze optie is effectief voor back-ups van fysieke machines met Windows of Linux.

Deze optie is van toepassing voor back-ups op schijfniveau. Deze optie is ook van toepassing voor back-ups op bestandsniveau wanneer de back-up op bestandsniveau wordt uitgevoerd door een momentopname te maken. (Met de optie 'Momentopname voor back-up op bestandsniveau' wordt bepaald of er een momentopname wordt gemaakt tijdens een back-up op bestandsniveau.)

Met deze optie wordt bepaald of momentopnamen van meerdere volumes gelijktijdig of een voor een worden gemaakt.

De vooraf ingestelde waarde is:

- Als er ten minste één machine met Windows is geselecteerd voor back-up: **Ingeschakeld**.
- Anders: **Uitgeschakeld**.

Wanneer deze optie is ingeschakeld, worden er gelijktijdig momentopnamen gemaakt van alle volumes waarvan een back-up wordt gemaakt. Gebruik deze optie als u een consistente back-up van gegevens uit meerdere volumes (spanned volumes) wilt maken, bijvoorbeeld voor een Oracle-database.

Wanneer deze optie is uitgeschakeld, worden de momentopnamen van de volumes achter elkaar gemaakt. Dus als de gegevens afkomstig zijn uit meerdere volumes (spanned volumes), is de resulterende back-up mogelijk niet consistent.

Herstel met één klik

Opmerking
Deze functie is alleen beschikbaar met het Advanced Backup-pakket.

Met Herstel met één klik kunt u automatisch een schijfback-up van uw Windows- of Linux-machine herstellen. Deze back-up kan een back-up zijn van de hele machine of een back-up van specifieke schijven of volumes op deze machine.

Herstel met één klik ondersteunt de volgende bewerkingen:

- Automatisch herstel van de meest recente back-up
- Herstel van een specifieke back-up (ook bekend als herstelpunt) binnen het back-uparchief

Herstel met één klik ondersteunt de volgende back-upopslagplaatsen:

- Secure Zone
- Lokale map
- Netwerkmap
- Cloudopslag

Belangrijk
Schort de BitLocker-versleuteling op tot de volgende herstart van uw machine wanneer u een van de volgende handelingen uitvoert:

- Secure Zone maken, wijzigen of verwijderen.
- Startup Recovery Manager in- of uitschakelen.
- [Alleen als Startup Recovery Manager nog niet was ingeschakeld] De eerste back-up uitvoeren nadat herstel met één klik is ingeschakeld in het beschermingsschema. Met deze bewerking wordt Startup Recovery Manager automatisch ingeschakeld.
- Startup Recovery Manager bijwerken, bijvoorbeeld door de beveiliging bij te werken.

Als de BitLocker-versleuteling niet is opgeschort tijdens deze bewerkingen, moet u uw Bitlocker-pincode opgeven nadat uw machine opnieuw is opgestart.

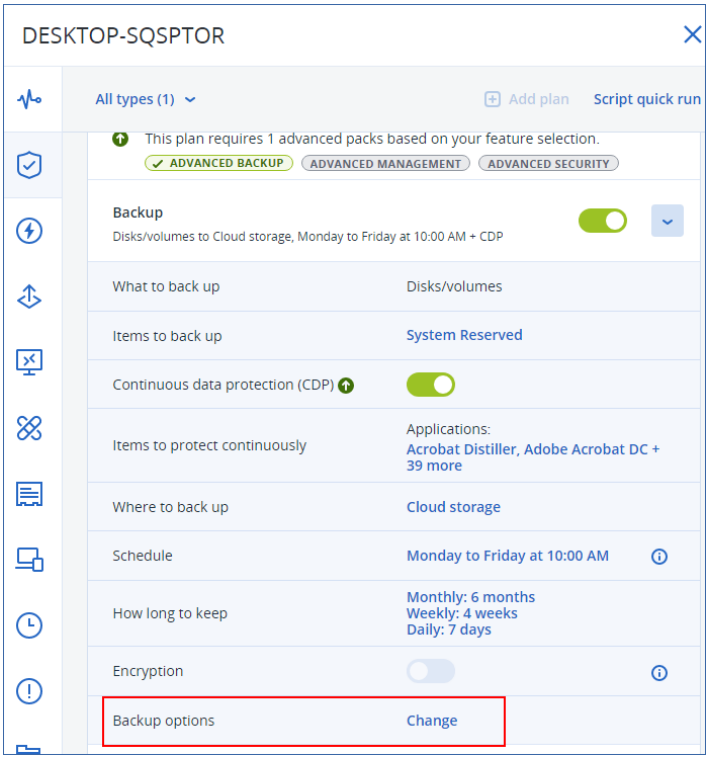
Herstel met één klik inschakelen

Herstel met één klik is een back-upoptie in het beschermingsschema. Voor meer informatie over het maken van een schema: zie "Een beschermingsschema maken" (p. 217).

Opmerking
Als u Herstel met één klik inschakelt, wordt ook Startup Recovery Manager ingeschakeld op de doelmachine. Als Startup Recovery Manager niet kan worden ingeschakeld, mislukt de back-upbewerking waarmee back-ups voor Herstel met één klik worden gemaakt. Voor meer informatie over Startup Recovery Manager: zie "Startup Recovery Manager" (p. 771).

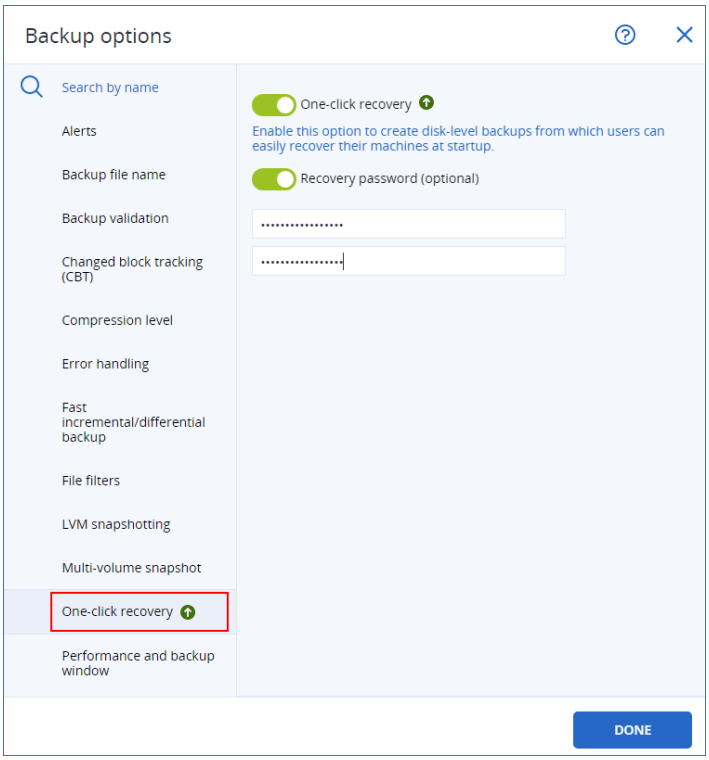
Herstel met één klik inschakelen

1. Vouw in het beschermingsschema de module **Back-up maken van** uit.
2. Selecteer in **Back-up maken van** de optie **Volledige machine** of **Schijf/volumes**.
3. [Als u **Schijf/volumes** hebt geselecteerd]. Geef in **Items waarvan een back-up moet worden gemaakt** de schijf of volumes op waarvan u een back-up wilt maken.
4. Klik in **Back-upopties** op **Wijzigen** en selecteer vervolgens **Herstel met één klik**.



5. Zet de schakelaar **Herstel met één klik** op 'aan'.
6. [Optioneel] Zet de schakelaar **Herstelwachtwoord** op 'aan' en geef vervolgens een wachtwoord op.

Belangrijk
We raden u sterk aan om een herstelwachtwoord op te geven. De gebruiker die herstel met één klik op de doelcomputer uitvoert, moet dit wachtwoord kennen.



7. Klik op **Gereed**.
8. Configureer de andere elementen van het beschermingsschema naar wens en sla het schema vervolgens op.

Het beschermingsschema wordt uitgevoerd en er wordt een back-up gemaakt. Herstel met één klik wordt toegankelijk voor de gebruikers van de beschermde machine.

Belangrijk
Herstel met één klik is tijdelijk niet beschikbaar wanneer u de beveiligingsagent bijwerkt. Voer een back-up uit om herstel met één klik opnieuw in te schakelen. Wanneer de back-up is voltooid, kunt u herstel met één klik opnieuw uitvoeren.

Herstel met één klik uitschakelen

U kunt Herstel met één klik uitschakelen voor een specifieke workload. Ga op een van de volgende manieren te werk:

- Schakel de optie **Herstel met één klik** uit in het beschermingsplan dat wordt toegepast voor de workload.
- Trek het beschermingsschema in waarin de optie **Herstel met één klik** is ingeschakeld.
- Verwijder het beschermingsschema waarin de optie **Herstel met één klik** is ingeschakeld.

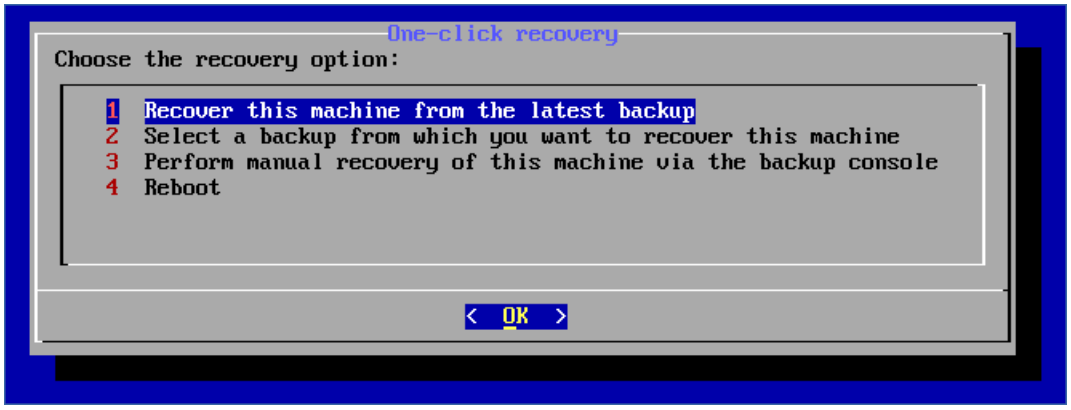
Herstel met één klik gebruiken om een machine te herstellen

Vereisten

- Er wordt een beschermingsschema met ingeschakelde back-upoptie **Herstel met één klik** toegepast op de machine.
- Er is ten minste één schijfback-up van de machine.

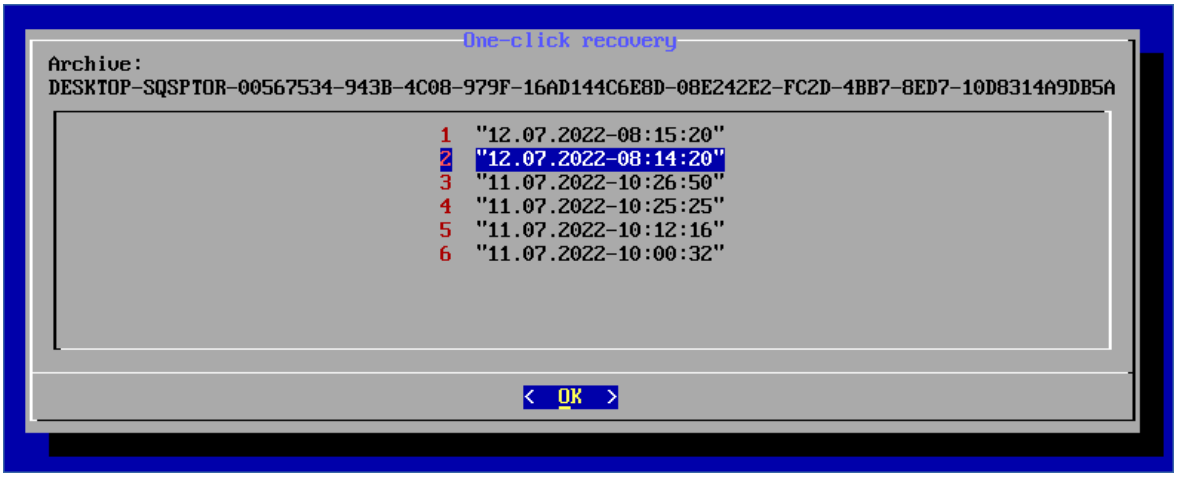
Een machine herstellen

1. Start de machine die u wilt herstellen, opnieuw op.
2. Druk tijdens het opnieuw opstarten op F11 om Startup Recovery Manager in te voeren.
   Het venster voor opstartmedia wordt geopend.
3. Selecteer **Acronis Cyber Protect**.
4. [Als een herstelwachtwoord is opgegeven in het beschermingsschema] Voer het herstelwachtwoord in en klik vervolgens op **OK**.
5. Selecteer een optie voor Herstel met één klik.
   - Als u de meest recente back-up automatisch wilt herstellen, selecteert u de eerste optie en klikt u vervolgens op **OK**.
   - Als u een andere back-up wilt herstellen binnen het back-uparchief, selecteert u de tweede optie en klikt u vervolgens op **OK**.

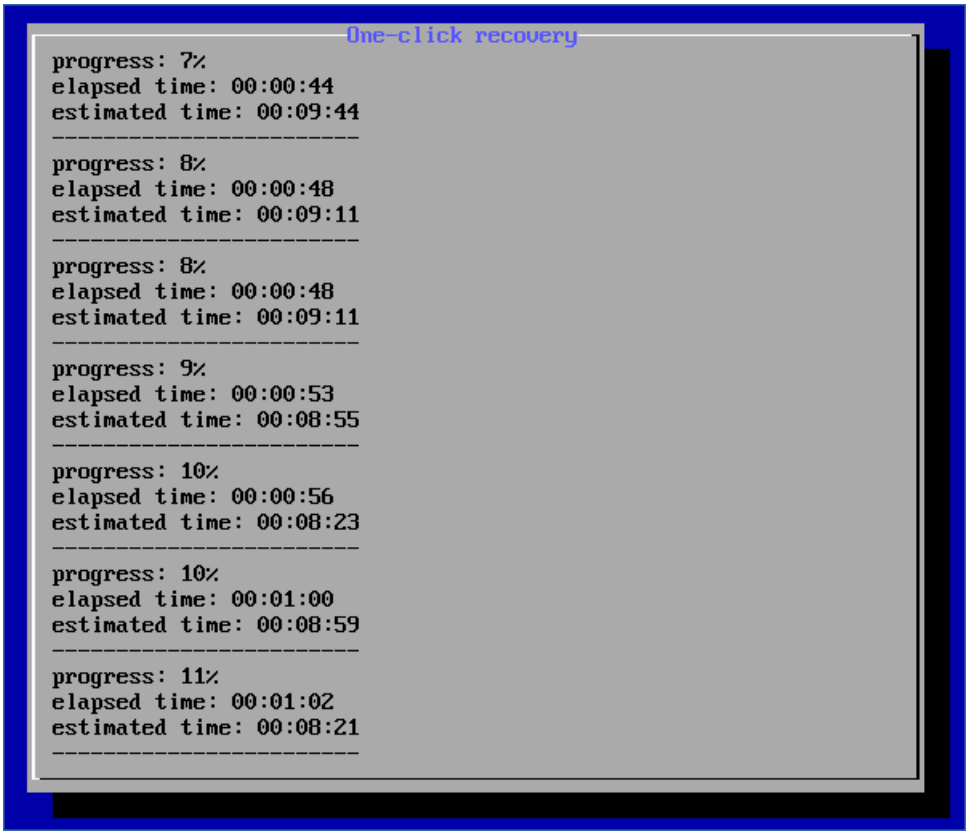


6. Bevestig uw keuze door te klikken op **Ja**.
   Het venster voor opstartmedia wordt geopend en verdwijnt vervolgens. De herstelprocedure gaat verder zonder dit venster.
7. [Als u ervoor kiest om een specifieke back-up te herstellen] Selecteer de back-up die u wilt

herstellen en klik vervolgens op **OK**.



Na een tijdje begint het herstel en wordt de voortgang weergegeven. Wanneer het herstel is voltooid, wordt de machine opnieuw opgestart.



Prestatie- en back-upvenster

Met deze optie kunt u een van de drie niveaus van back-upprestaties (hoog, laag, verboden) instellen voor elk uur binnen een week. Op deze manier kunt u een tijdvenster definiëren voor het starten en uitvoeren van back-ups. Met de prestatieniveaus 'hoog' en 'laag' kunt u de prioriteit van het proces en de uitvoersnelheid configureren.

Deze optie is niet beschikbaar voor back-ups die worden uitgevoerd door de cloudagenten, zoals back-ups van websites of back-ups van servers op de herstelsite in de cloud.

Deze optie is alleen effectief voor het back-up- en back-upreplicatieproces. Opdrachten na back-up en andere bewerkingen die zijn opgenomen in een beschermingsschema (bijvoorbeeld validatie), worden uitgevoerd ongeacht deze optie.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Wanneer deze optie is uitgeschakeld, kunnen back-ups op elk moment worden uitgevoerd met de volgende parameters (ongeacht of de parameters zijn gewijzigd ten opzichte van de vooraf ingestelde waarde):

- CPU-prioriteit: **Laag** (in Windows komt dit overeen met **Lager dan normaal**)
- Uitvoersnelheid: **Onbeperkt**

Wanneer deze optie is ingeschakeld, worden geplande back-ups toegestaan of geblokkeerd volgens de performance-parameters die zijn opgegeven voor het huidige uur. Aan het begin van een uur waarin back-ups zijn geblokkeerd, wordt een back-up proces automatisch gestopt en wordt er een waarschuwing gegenereerd. Zelfs als geplande back-ups zijn geblokkeerd, kan een back-up handmatig worden gestart. Hierbij worden de performance-parameters gebruiken van het meest recente uur waarin back-ups waren toegestaan.

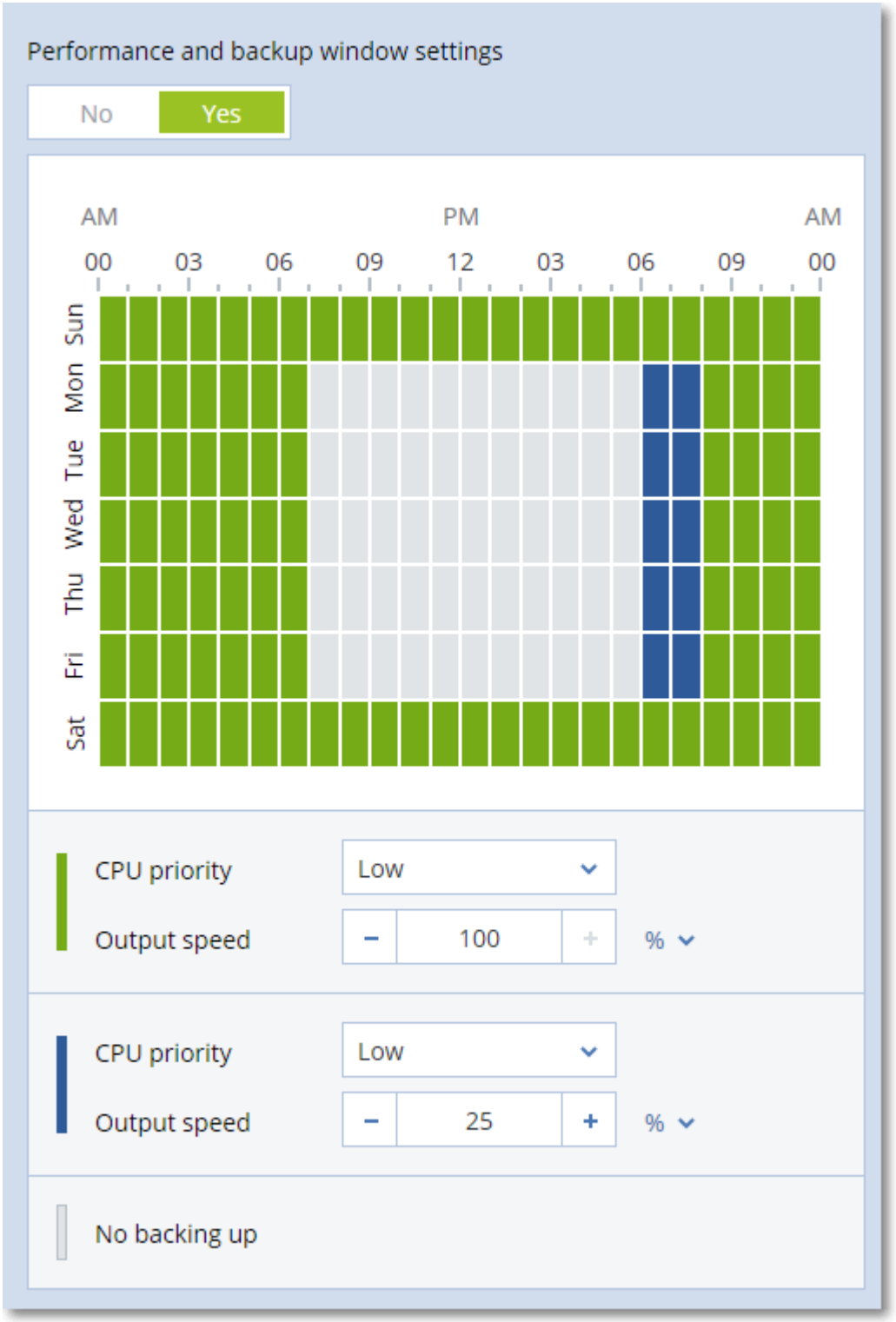
Opmerking
U kunt het performance- en back-upvenster voor elke replicatielocatie afzonderlijk configureren. Als u toegang wilt krijgen tot de instellingen van de replicatielocatie, klikt u in het beschermingsschema op het tandwielpictogram naast de naam van de locatie. Klik vervolgens op **Performance- en back-upvenster**.

Back-upvenster

Elke rechthoek geeft een uur van een weekdag weer. Klik op een rechthoek om de volgende statussen weer te geven:

- **Groen:** back-up is toegestaan met de parameters die zijn opgegeven in het groene gedeelte.
- **Blauw:** back-up is toegestaan met de parameters die zijn opgegeven in het blauwe gedeelte. Deze status is niet beschikbaar als de back-upindeling is ingesteld op **Versie 11**.
- **Grijs:** back-up is geblokkeerd.

U kunt klikken en slepen om de status van meerdere rechthoeken tegelijk te wijzigen.



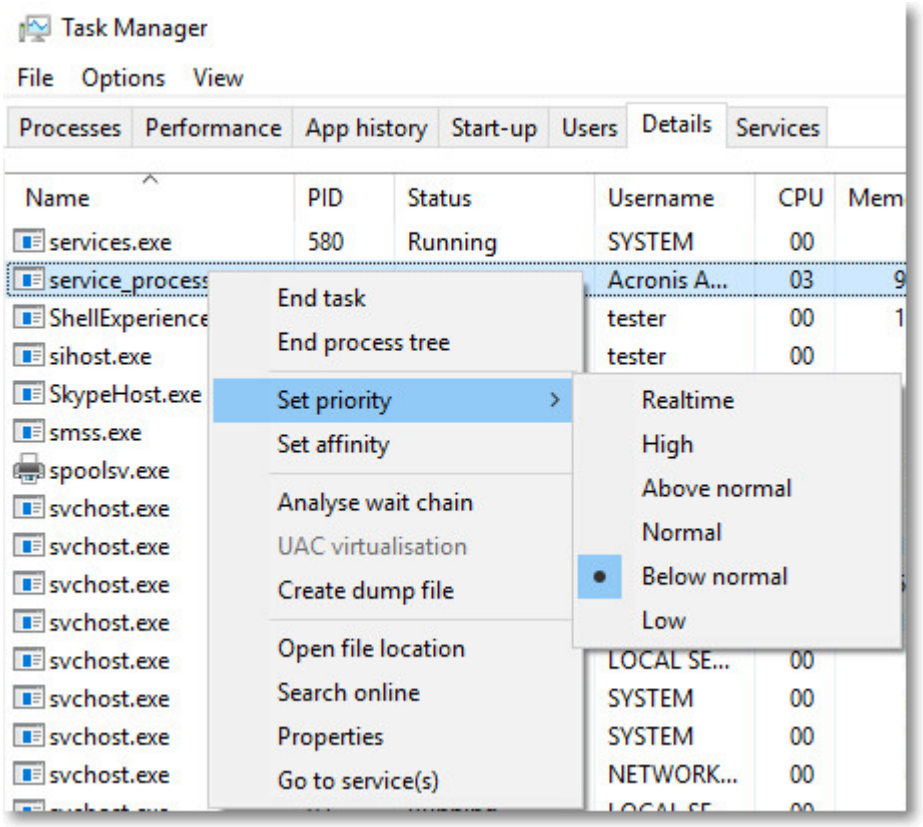
CPU-prioriteit

Met deze parameter definieert u de prioriteit van het back-upproces in het besturingssysteem.

De beschikbare instellingen zijn: **Laag**, **Normaal**, **Hoog**.

De prioriteit van een proces dat in een systeem wordt uitgevoerd, bepaalt hoeveel CPU- en systeembronnen aan het proces worden toegewezen. Als u de prioriteit voor back-ups verlaagt, komen er meer resources vrij voor andere applicaties. Als u de prioriteit voor back-ups verhoogt, wordt het back-upproces mogelijk versneld doordat het besturingssysteem wordt gevraagd meer resources, zoals de CPU, toe te wijzen aan de back-upapplicatie. Het resultaat hiervan hangt echter af van het totale CPU-gebruik en andere factoren zoals I/O-snelheid van de schijf of netwerkverkeer.

Met deze optie kunt u de prioriteit van het back-upproces (**service_process.exe)** in Windows en de 'niceness' van het back-upproces (**service_process)** in Linux en macOS instellen.



De onderstaande tabel bevat een overzicht van de toewijzing voor deze instelling in Windows, Linux en macOS.

Cyber Protection – prioriteit	Windows – prioriteit	Linux en macOS – 'niceness'
Laag	Lager dan normaal	10
Normaal	Normaal	0
Hoog	Hoog	-10

Uitvoersnelheid tijdens back-up

Met deze parameter kunt u een beperking instellen voor de schrijfsnelheid van de harde schijf (bij het maken van een back-up naar een lokale map) of de overdrachtsnelheid van back-upgegevens via het netwerk (bij het maken van een back-up naar een netwerkshare of cloudopslag).

Wanneer deze optie is ingeschakeld, kunt u de maximaal toegestane uitvoersnelheid opgeven:

- Als percentage van de geschatte schrijfsnelheid van de harde schijf van bestemming (bij het maken van een back-up naar een lokale map) of van de geschatte maximumsnelheid van de netwerkverbinding (bij het maken van een back-up naar een netwerkshare of cloudopslag).
  Deze instelling werkt alleen als de agent in Windows wordt uitgevoerd.
- In kB/seconde (voor alle bestemmingen).

Physical Data Shipping

Deze optie is beschikbaar als de back-up- of replicatiebestemming de cloudopslag is en de back-upindeling is ingesteld op **Versie 12**.

Deze optie is effectief voor back-ups op schijfniveau en bestandsback-ups die zijn gemaakt met Agent voor Windows, Agent voor Linux, Agent voor Mac, Agent voor VMware, Agent voor Hyper-V en Agent voor Virtuozzo.

Gebruik deze optie als u de Physical Data Shipping-service wilt gebruiken om de eerste volledige back-up die door een beschermingsschema wordt gemaakt, te verzenden naar de cloudopslag op een hardeschijfstation. De volgende incrementele back-ups kunnen via het netwerk worden uitgevoerd.

Voor lokale back-ups die worden gerepliceerd naar de cloud, worden incrementele back-ups voortgezet en lokaal opgeslagen totdat de oorspronkelijke back-up is geüpload naar de cloudopslag. Vervolgens worden alle incrementele wijzigingen gerepliceerd naar de cloud en wordt de replicatie voortgezet volgens het back-upschema.

De vooraf ingestelde waarde is: **Uitgeschakeld.**

Over de Physical Data Shipping-service

De webinterface van de Physical Data Shipping-service is alleen beschikbaar voor beheerders.

Raadpleeg de Beheerdershandleiding van Physical Data Shipping voor gedetailleerde instructies over het gebruik van de Physical Data Shipping-service en het hulpprogramma voor het maken van orders. Klik op het vraagtekenpictogram om dit document te openen in de webinterface van de Physical Data Shipping-service.

Overzicht van het Physical Data Shipping-proces

1. [Back-ups verzenden die cloudopslag als primaire back-uplocatie hebben]
   a. Maak een nieuw beschermingsschema met back-up naar de cloud.
   b. Klik in de rij **Back-upopties** op **Wijzigen**.
   c. Klik in de lijst met beschikbare opties op **Physical Data Shipping**.

   U kunt een back-up rechtstreeks naar een verwisselbaar station wegschrijven of een back-up maken in een lokale map of netwerkmap en de back-up(s) vervolgens naar het station kopiëren/verplaatsen.
2. [Lokale back-ups verzenden die worden gerepliceerd naar de cloud]

   Opmerking
   Deze optie wordt ondersteund met de versie van de beveiligingsagent vanaf release C21.06.

   a. Maak een nieuw beschermingsschema met back-up naar een lokale of netwerkopslag.
   b. Klik op **Locatie toevoegen** en selecteer **Cloudopslag**.
   c. Klik in de rij voor de locatie van de **Cloudopslag** op het tandwiel en selecteer **Physical Data Shipping**.
3. Klik onder **Physical Data Shipping gebruiken** op **Ja** en **Gereed**.
   De optie Versleuteling wordt automatisch ingeschakeld in het beschermingsschema omdat alle back-ups die worden verzonden, moeten worden versleuteld.
4. Klik in de rij **Versleuteling** op **Geef een wachtwoord op** en voer een wachtwoord voor de versleuteling in.
5. Selecteer in de rij **Physical Data Shipping** het verwisselbare station waar u eerste back-up wilt opslaan.
6. Klik op **Maken** om het beschermingsschema op te slaan.
7. Wanneer de eerste back-up is voltooid, gebruikt u de webinterface van de Physical Data Shipping-service om het hulpprogramma voor het maken van orders te downloaden en de order te maken.

   Voor toegang tot deze webinterface meldt u zich aan bij de beheerportal, klikt u op **Overzicht** > **Gebruik** en klikt u op **Service beheren** onder **Physical Data Shipping**.

   Belangrijk
   Zodra de eerste volledige back-up is voltooid, moeten de volgende back-ups worden uitgevoerd met hetzelfde beschermingsschema. Voor een ander beschermingsschema, zelfs met dezelfde parameters en voor dezelfde machine, is een andere Physical Data Shipping-cyclus vereist.

8. Verpak de stations en stuur ze naar het datacenter.

Belangrijk
Zorg ervoor dat u de verpakkingsinstructies volgt zoals beschreven in de Beheerdershandleiding van Physical Data Shipping.

9. Volg de orderstatus via de webinterface van de Physical Data Shipping-service. Houd er rekening mee dat de daaropvolgende back-ups mislukken totdat de eerste back-up is geüpload naar de cloudopslag.

Aangepaste opdrachten

Met deze optie kunt u definiëren welke opdrachten automatisch worden uitgevoerd vóór en na de back-upprocedure.

Het volgende schema geeft aan wanneer aangepaste opdrachten worden uitgevoerd.

Opdracht vóór back-up	Back-up	Opdracht na back-up

Voorbeelden van het gebruik van de aangepaste opdrachten:

- Verwijder enkele tijdelijke bestanden van de schijf voordat de back-up wordt gestart.
- Configureer een antivirusproduct van derden dat elke keer wordt gestart voordat de back-up begint.
- Selecteer enkele back-ups om te kopiëren naar een andere locatie. Deze optie kan nuttig zijn omdat bij de uitvoering van een replicatie die is geconfigureerd in een beschermingsschema, *elke* back-up naar opeenvolgende locaties wordt gekopieerd.

De agent voert de replicatie pas uit als *eerst* de opdracht na back-up is uitgevoerd.

Interactieve opdrachten worden niet ondersteund, dat wil zeggen opdrachten waarvoor gebruikersinvoer is vereist (bijvoorbeeld 'pause').

Opdracht vóór back-up

Een opdracht/batchbestand opgeven dat moet worden uitgevoerd voordat het back-upproces begint

1. Schakel de optie **Een opdracht uitvoeren voordat de back-up wordt gemaakt** in.
2. Ga naar het veld **Opdracht...** en typ een opdracht of blader naar een batchbestand. Interactieve opdrachten worden niet ondersteund, dat wil zeggen opdrachten waarvoor gebruikersinvoer is vereist (bijvoorbeeld 'pause').
3. Geef in het veld **Werkmap** een pad op naar een directory waar de opdracht/het batchbestand wordt uitgevoerd.
4. Geef in het veld **Argumenten** indien nodig de argumenten op voor het uitvoeren van de opdracht.
5. Afhankelijk van het resultaat dat u wilt verkrijgen, selecteert u de gewenste opties zoals

beschreven in de volgende tabel.

6. Klik op **Gereed**.

Selectievakje	Inschakelen			
De back-up afkeuren als het uitvoeren van de opdracht mislukt*	Ingeschakeld	Uitgeschakeld	Ingeschakeld	Uitgeschakeld
Geen back-up maken voordat de opdracht volledig is uitgevoerd	Ingeschakeld	Ingeschakeld	Uitgeschakeld	Uitgeschakeld
Resultaat				
	Vooraf ingesteld Voer de back-up alleen uit wanneer de opdracht is uitgevoerd. Keur de back-up af als het uitvoeren van de opdracht mislukt.	Voer de back-up uit wanneer de opdracht is uitgevoerd, ongeacht het resultaat van de uitvoering.	N.v.t.	Voer de back-up gelijktijdig uit met de uitvoering van de opdracht, ongeacht het resultaat van de uitvoering van de opdracht.

* Een opdracht wordt als mislukt beschouwd als de afsluitcode niet gelijk is aan nul.

Opmerking
Als een script mislukt door een conflict met betrekking tot een vereiste bibliotheekversie in Linux, dan sluit u de omgevingsvariabelen `LD_LIBRARY_PATH` en `LD_PRELOAD` uit door de volgende regels toe te voegen aan uw script:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Opdracht na back-up

Een opdracht/uitvoerbaar bestand opgeven om uit te voeren nadat de back-up is voltooid

1. Schakel de optie **Een opdracht uitvoeren nadat de back-up is gemaakt** in.
2. Ga naar het veld **Opdracht...** en typ een opdracht of blader naar een batchbestand.

3. Geef in het veld **Werkmap** een pad op naar een directory waar de opdracht/het batchbestand wordt uitgevoerd.
4. Geef in het veld **Argumenten** indien nodig de argumenten op voor het uitvoeren van de opdracht.
5. Schakel het selectievakje **De back-up afkeuren als het uitvoeren van de opdracht mislukt** in als een goede uitvoering van de opdracht essentieel voor u is. De opdracht wordt als mislukt beschouwd als de afsluitcode niet gelijk is aan nul. Als de opdracht niet correct wordt uitgevoerd, wordt de back-upstatus ingesteld op **Fout**.

   Wanneer het selectievakje niet is ingeschakeld, dan heeft het resultaat van de uitvoering van de opdracht geen invloed op de al dan niet correcte uitvoering van de back-up. U kunt het resultaat van de uitvoering van de opdracht bijhouden via het tabblad **Activiteiten**.
6. Klik op **Gereed**.

Aangepaste opdrachten voor gegevensvastlegging

Met deze optie kunt u definiëren welke opdrachten automatisch worden uitgevoerd vóór en na het vastleggen van gegevens (dat wil zeggen het maken van de momentopname). Gegevens worden vastgelegd aan het begin van de back-upprocedure.

Het volgende schema geeft aan wanneer aangepaste opdrachten voor gegevensvastlegging worden uitgevoerd.

	<---------- **Back-up** ---------->				
Opdracht vóór back-up	Opdracht vóór gegevensvastlegging	Gegevens vastleggen	Opdracht na gegevensvastlegging	Gegevens schrijven naar de back-upset	Opdracht na back-up

Interactie met andere back-upopties

Het uitvoeren van aangepaste opdrachten voor gegevensvastlegging kan worden gewijzigd door middel van andere back-upopties.

Als de optie **Momentopname van meerdere volumes** is ingeschakeld, worden de aangepaste opdrachten voor gegevensvastlegging slechts eenmaal uitgevoerd, omdat de momentopnamen voor alle volumes gelijktijdig worden gemaakt. Als de optie **Momentopname van meerdere volumes** is uitgeschakeld, worden de aangepaste opdrachten voor gegevensvastlegging uitgevoerd voor elk volume waarvan een back-up wordt gemaakt, omdat de momentopnamen voor de volumes een voor een worden gemaakt.

Als de optie **Volume Shadow Copy Service (VSS)** is ingeschakeld, worden de aangepaste opdrachten voor gegevensvastlegging en de Microsoft VSS-acties als volgt uitgevoerd:

Opdrachten vóór gegevensvastlegging > VSS onderbreken > Gegevens vastleggen > VSS hervatten > Opdrachten na gegevensvastlegging

Met de aangepaste opdrachten voor gegevensvastlegging kunt u een database of applicatie die niet compatibel is met VSS, onderbreken en hervatten. Aangezien het vastleggen van de gegevens slechts enkele seconden duurt, blijft de niet-actieve tijd van de database of applicatie tot het minimum beperkt.

Opdracht vóór gegevensvastlegging

Een opdracht/batchbestand opgeven om uit te voeren voordat gegevens worden vastgelegd

1. Schakel de optie **Een opdracht uitvoeren voordat de gegevens worden vastgelegd** in.
2. Ga naar het veld **Opdracht...** en typ een opdracht of blader naar een batchbestand. Interactieve opdrachten worden niet ondersteund, dat wil zeggen opdrachten waarvoor gebruikersinvoer is vereist (bijvoorbeeld 'pause').
3. Geef in het veld **Werkmap** een pad op naar een directory waar de opdracht/het batchbestand wordt uitgevoerd.
4. Geef in het veld **Argumenten** indien nodig de argumenten op voor het uitvoeren van de opdracht.
5. Afhankelijk van het resultaat dat u wilt verkrijgen, selecteert u de gewenste opties zoals beschreven in de volgende tabel.
6. Klik op **Gereed**.

Selectievakje	**Inschakelen**			
De back-up afkeuren als het uitvoeren van de opdracht mislukt*	Ingeschakeld	Uitgeschakeld	Ingeschakeld	Uitgeschakeld
Geen gegevens vastleggen voordat de opdracht volledig is uitgevoerd	Ingeschakeld	Ingeschakeld	Uitgeschakeld	Uitgeschakeld
Resultaat				
	Vooraf ingesteld Leg de gegevens alleen vast wanneer de opdracht is uitgevoerd. Keur de back-up af als	Leg de gegevens vast wanneer de opdracht is uitgevoerd, ongeacht het	N.v.t.	Leg de gegevens vast gelijktijdig met de opdracht, ongeacht het resultaat van de

	het uitvoeren van de opdracht mislukt.	resultaat van de uitvoering.		uitvoering van de opdracht.

* Een opdracht wordt als mislukt beschouwd als de afsluitcode niet gelijk is aan nul.

Opmerking
Als een script mislukt door een conflict met betrekking tot een vereiste bibliotheekversie in Linux, dan sluit u de omgevingsvariabelen `LD_LIBRARY_PATH` en `LD_PRELOAD` uit door de volgende regels toe te voegen aan uw script:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Opdracht na gegevensvastlegging

Een opdracht/batchbestand opgeven om uit te voeren nadat gegevens zijn vastgelegd

1. Schakel de optie **Een opdracht uitvoeren nadat de gegevens zijn vastgelegd** in.
2. Ga naar het veld **Opdracht...** en typ een opdracht of blader naar een batchbestand. Interactieve opdrachten worden niet ondersteund, dat wil zeggen opdrachten waarvoor gebruikersinvoer is vereist (bijvoorbeeld 'pause').
3. Geef in het veld **Werkmap** een pad op naar een directory waar de opdracht/het batchbestand wordt uitgevoerd.
4. Geef in het veld **Argumenten** indien nodig de argumenten op voor het uitvoeren van de opdracht.
5. Afhankelijk van het resultaat dat u wilt verkrijgen, selecteert u de gewenste opties zoals beschreven in de volgende tabel.
6. Klik op **Gereed**.

Selectievakje	**Inschakelen**			
De back-up afkeuren als het uitvoeren van de opdracht mislukt*	Ingeschakeld	Uitgeschakeld	Ingeschakeld	Uitgeschakeld
Geen back-up maken voordat de opdracht volledig is uitgevoerd	Ingeschakeld	Ingeschakeld	Uitgeschakeld	Uitgeschakeld

Resultaat				
	Vooraf ingesteld Zet de back-up alleen voort wanneer de opdracht is uitgevoerd.	Zet de back-up voort wanneer de opdracht is uitgevoerd, ongeacht het resultaat van de uitvoering.	N.v.t.	Zet de back-up voort gelijktijdig met de uitvoering van de opdracht en ongeacht het resultaat van de uitvoering van de opdracht.

* Een opdracht wordt als mislukt beschouwd als de afsluitcode niet gelijk is aan nul.

Plannen

Met deze optie definieert u of back-ups precies volgens de planning worden gestart of met een vertraging, en van hoeveel virtuele machines tegelijkertijd een back-up wordt gemaakt.

Zie "Een back-up uitvoeren volgens schema" (p. 447) voor meer informatie over het configureren van het back-upschema.

De vooraf ingestelde waarde is: **Starttijden van back-ups binnen een tijdvenster distribueren**. **Maximale vertraging**: **30 minuten**.

U kunt een van de volgende opties selecteren:

- **Alle back-ups precies volgens het schema starten**

  Back-ups van fysieke machines beginnen exact zoals gepland. Back-ups van virtuele machines worden een voor een gemaakt.
- **Starttijden binnen een tijdvenster distribueren**

  Back-ups van fysieke machines beginnen met een vertraging ten opzichte van de geplande tijd. De waarde van de vertraging voor elke machine wordt willekeurig geselecteerd in een bereik van nul tot de door u opgegeven maximumwaarde. U kunt deze instelling bijvoorbeeld gebruiken als u een te grote belasting van het netwerk wilt vermijden wanneer u back-ups van meerdere machines naar een netwerklocatie maakt. De waarde van de vertraging voor elke machine wordt bepaald op het moment dat het beschermingsschema wordt toegepast op de machine. Deze waarde verandert niet totdat u het beschermingsschema bewerkt en de maximumwaarde voor de vertraging wijzigt.

  Back-ups van virtuele machines worden een voor een gemaakt.
- **Gelijktijdig uitvoeren van aantal back-ups beperken tot**

  Gebruik deze optie voor het beheer van parallelle back-ups van virtuele machines waarvan een back-up wordt gemaakt op hypervisorniveau (back-up zonder agent).

  Beschermingsschema's waarvoor deze optie is geselecteerd, kunnen samen met andere beschermingsschema's worden uitgevoerd die tegelijkertijd door dezelfde agent worden verwerkt. Wanneer u deze optie selecteert, moet u het aantal parallelle back-ups per schema opgeven. Het totale aantal machines waarvan gelijktijdig een back-up wordt gemaakt door alle schema's, is beperkt tot 10 per agent. Zie "Beperkingen instellen voor het totale aantal virtuele

machines waarvan gelijktijdig een back-up kan worden gemaakt" (p. 743) voor meer informatie over het wijzigen van de standaardlimiet.

In beschermingsschema's waarvoor deze optie niet is geselecteerd, worden de back-upbewerkingen opeenvolgend uitgevoerd, d.w.z. de ene virtuele machine na de andere.

Back-up sector-voor-sector

De optie is alleen effectief bij het maken van back-ups op schijfniveau.

Met deze optie definieert u of een exacte kopie van een schijf of volume op fysiek niveau wordt gemaakt.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Als deze optie is ingeschakeld, wordt er een back-up gemaakt van alle sectoren van een schijf of volume, met inbegrip van niet-toegewezen ruimte en sectoren zonder gegevens. De resulterende back-up heeft dezelfde grootte als de schijf waarvan een back-up wordt gemaakt (als de optie 'Compressieniveau' is ingesteld op **Geen**). De software schakelt automatisch over naar de modus sector-voor-sector wanneer een back-up wordt gemaakt van stations met niet-herkende of niet-ondersteunde bestandssystemen.

Opmerking
Het is dan niet mogelijk om toepassingsgegevens te herstellen van de back-ups die zijn gemaakt in de modus sector-voor-sector.

Splitsen

Met deze optie selecteert u de methode voor het opsplitsen van grote back-ups in kleinere bestanden.

Opmerking
Splitsen is niet beschikbaar in beschermingsschema's die de cloudopslag als back-uplocatie gebruiken.

De vooraf ingestelde waarde is:

- Als de back-uplocatie een lokale of netwerkmap (SMB) is en de back-upindeling versie 12 is: **Vaste grootte - 200 GB**

  Met deze instelling kan de back-upsoftware grote hoeveelheden gegevens verwerken op het NTFS-bestandssysteem, zonder de negatieve effecten van bestandsfragmentatie.
- Anders: **Automatisch**

De volgende instellingen zijn beschikbaar:

- **Automatisch**

  Een back-up wordt opgesplitst als deze de maximale bestandsgrootte overschrijdt die door het bestandssysteem wordt ondersteund.

- **Vaste grootte**
  Voer de gewenste bestandsgrootte in of selecteer deze in het vervolgmenu.

Taakfout afhandelen

Deze optie bepaalt hoe het programma reageert wanneer een geplande uitvoering van een beschermingsschema mislukt of wanneer uw machine opnieuw wordt opgestart terwijl een back-up wordt uitgevoerd. Deze optie werkt niet wanneer een beschermingsschema handmatig wordt gestart.

Als deze optie is ingeschakeld, probeert het programma het beschermingsschema opnieuw uit te voeren. U kunt opgeven hoe vaak en om de hoeveel tijd dit wordt geprobeerd. Het programma probeert het niet meer zodra een poging lukt of wanneer het opgegeven aantal pogingen is bereikt, al naar gelang van wat het eerst gebeurt.

Als deze optie is ingeschakeld en uw machine opnieuw wordt opgestart terwijl er een back-up wordt uitgevoerd, dan zal de back-upbewerking niet mislukken. Enkele minuten na de herstart wordt de back-upbewerking automatisch voortgezet en wordt het back-upbestand aangevuld met de ontbrekende gegevens. In dit geval is de optie **Interval tussen pogingen** niet relevant.

De vooraf ingestelde waarde is: **Ingeschakeld**.

Opmerking
Deze optie is niet van toepassing voor forensische back-ups.

Startvoorwaarden voor taak

Deze optie is beschikbaar voor Windows- en Linux-besturingssystemen.

Deze optie bepaalt hoe het programma reageert als een taak op het punt staat te beginnen (de geplande tijd is bereikt of de in het schema opgegeven gebeurtenis vindt plaats), maar er niet is voldaan aan een of meer voorwaarden. Zie "Startvoorwaarden" (p. 454) voor meer informatie over de voorwaarden.

De vooraf ingestelde waarde is: **Wachten totdat aan de voorwaarden van het schema wordt voldaan.**

Wachten totdat aan de voorwaarden van het schema wordt voldaan

Met deze instelling begint de planner bij te houden of aan de voorwaarden wordt voldaan. Zodra dat het geval is, wordt de taak gestart. Als nooit aan de voorwaarden wordt voldaan, start de taak ook nooit.

Voor het geval dat er te lang niet aan de voorwaarden wordt voldaan en het te risicovol wordt om taak nog langer uit te stellen, kunt u een tijdinterval instellen waarna de taak wordt uitgevoerd, ongeacht of al dan niet aan de voorwaarden is voldaan. Schakel het selectievakje **De taak hoe dan ook uitvoeren na** in en geef het tijdinterval op. De taak start zodra aan de voorwaarden wordt voldaan OF zodra de maximale uitsteltijd is verlopen, afhankelijk van wat als eerste plaatsvindt.

Uitvoering van de taak overslaan

Het uitstellen van een taak is niet altijd acceptabel, bijvoorbeeld wanneer u een taak exact op een bepaald moment moet uitvoeren. Dan is het logischer om de taak over te slaan dan te wachten tot aan de voorwaarden wordt voldaan, vooral als de taken relatief vaak worden uitgevoerd.

Volume Shadow Copy Service (VSS)

Deze optie is alleen van toepassing op Windows-besturingssystemen.

Hiermee definieert u of een back-up kan worden uitgevoerd als een of meer VSS Writers (Volume Shadow Copy Service) niet werken en welke provider een melding moet versturen aan VSS-compatibele applicaties wanneer een back-up wordt gestart.

Als u de Volume Shadow Copy Service gebruikt, wordt de consistente status gewaarborgd van alle gegevens die door de applicaties worden gebruikt; met name wordt gewaarborgd dat alle databasetransacties zijn voltooid op het moment dat de momentopname van de gegevens wordt gemaakt door de back-upsoftware. Met gegevensconsistentie wordt er dan weer voor gezorgd dat de applicatie in de juiste status wordt hersteld en meteen na het herstel weer operationeel is.

De momentopname wordt alleen gebruikt tijdens de back-upbewerking en wordt automatisch verwijderd wanneer de back-upbewerking is voltooid. Er worden geen tijdelijke bestanden bewaard.

U kunt Aangepaste opdrachten voor gegevensvastlegging gebruiken als u er zeker van wilt zijn dat er back-ups worden gemaakt van gegevens met een consistente status. Voorbeeld: gebruik een aangepaste opdracht voordat u gegevens vastlegt om op te geven dat de database moet worden onderbroken en dat alle caches moeten worden geleegd, zodat u zeker weet dat alle transacties zijn voltooid; en gebruik een aangepaste opdracht nadat u de gegevens hebt vastgelegd om op te geven dat de databasebewerkingen moeten worden hervat nadat de momentopname is gemaakt.

Opmerking
Er wordt geen back-up gemaakt van bestanden en mappen die zijn opgegeven in de registersleutel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**. Met name offline Outlook-gegevensbestanden (.ost) worden niet ondersteund, omdat ze zijn opgegeven in de waarde **OutlookOST** van deze sleutel.

Mislukte VSS Writers negeren

U kunt een van de volgende opties selecteren:

- **Mislukte VSS Writers negeren**
  Met deze optie kunt u back-ups maken, zelfs als een of meer VSS Writers niet werken.

Belangrijk
Applicatiegerichte back-ups mislukken altijd als de applicatiespecifieke Writer niet werkt. Als u bijvoorbeeld een applicatiegerichte back-up maakt van SQL Server-gegevens en **SqlServerWriter** niet werkt, dan mislukt de back-upbewerking ook.

Wanneer deze optie is ingeschakeld, worden maximaal drie opeenvolgende pogingen gedaan om een VSS-momentopname te maken.

Bij de eerste poging zijn alle VSS Writers vereist. Als deze poging mislukt, wordt deze herhaald. Als de tweede poging ook mislukt, worden de niet-werkende VSS Writers uitgesloten van de back-upbewerking en wordt een derde poging ondernomen. Als de derde poging lukt, wordt de back-up voltooid met een waarschuwing over de mislukte VSS Writers. Als de derde poging mislukt, wordt de back-up niet uitgevoerd.

- **Volledig uitgevoerde verwerking vereisen voor alle VSS Writers**
  Als een van de VSS Writers niet werkt, mislukt ook de back-up.

De provider van momentopnamen selecteren

U kunt een van de volgende opties selecteren:

- **Automatisch provider van momentopnamen selecteren**
  Automatisch een selectie maken uit de providers voor momentopnamen van hardware, providers voor momentopnamen van software en Microsoft Software Shadow Copy Provider.
- **Microsoft Software Shadow Copy Provider gebruiken**
  Het wordt aanbevolen deze optie te kiezen wanneer u een back-up maakt van applicatieservers (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint of Active Directory).

Volledige VSS-back-up inschakelen

Als deze optie is ingeschakeld, worden de logboeken van Microsoft Exchange Server en andere VSS-compatibele toepassingen (met uitzondering van Microsoft SQL Server) ingekort na elke volledige incrementele of differentiële back-up op schijfniveau.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Laat deze optie uitgeschakeld in de volgende gevallen:

- Als u Agent voor Exchange of software van derden gebruikt voor back-ups van Exchange Server-gegevens. De reden is dat er problemen optreden met de achtereenvolgende back-ups van transactielogboeken omdat logboeken worden ingekort.
- Als u software van derden gebruikt voor back-ups van SQL Server-gegevens. De reden is dat de software van derden de resulterende back-up op schijfniveau beschouwt als een 'eigen' volledige back-up. Bijgevolg mislukt de volgende differentiële back-up van de SQL Server-gegevens. De back-ups blijven mislukken totdat de software van derden de volgende 'eigen' volledige back-up maakt.

- Als andere VSS-compatibele applicaties worden uitgevoerd op de machine en u de logboeken daarvan wilt bewaren.

Belangrijk
Als deze optie is ingeschakeld, worden Microsoft SQL Server-logboeken niet ingekort. Om de SQL Server-log na een back-up korter te maken, activeert u de optie Log afkorting.

Volume Shadow Copy Service (VSS) voor virtuele machines

Met deze optie definieert u of stilgelegde momentopnamen worden gemaakt van virtuele machines.

De vooraf ingestelde waarde is: **Ingeschakeld**.

Wanneer deze optie is uitgeschakeld, wordt er een niet-stilgelegde momentopname gemaakt. Er wordt een back-up gemaakt van de virtuele machine met een crashconsistente status.

Wanneer deze optie is ingeschakeld, worden de transacties van alle VSS-compatibele toepassingen in de virtuele machine voltooid voordat er een stilgelegde momentopname wordt gemaakt.

Als u geen stilgelegde momentopname hebt kunnen maken na het aantal pogingen dat is opgegeven in de optie 'Foutafhandeling' en back-ups van toepassingen is ingeschakeld, dan mislukt de back-up.

Als u geen stilgelegde momentopname hebt kunnen maken na het aantal pogingen dat is opgegeven in de optie 'Foutafhandeling' en back-ups van toepassingen is uitgeschakeld, dan wordt er een crashconsistente back-up gemaakt. Als u geen crashconsistente back-up wilt maken, kunt u de back-up laten mislukken via het selectievakje **Back-up laten mislukken als het niet mogelijk is een stilgelegde momentopname te maken**.

De volgende tabel bevat een overzicht van de instellingen en de gevolgen hiervan.

Instellingen	Stilgelegde momentopname gemaakt		Geen stilgelegde momentopname gemaakt	
	Back-up van toepassingen ingeschakeld	**Back-up van toepassingen uitgeschakeld**	**Back-up van toepassingen ingeschakeld**	**Back-up van toepassingen uitgeschakeld**
Volume Shadow Copy Service (VSS) voor virtuele machines ingeschakeld **Back-up laten mislukken als het niet mogelijk is een stilgelegde momentopname**	Er wordt een stilgelegde momentopname gemaakt. Er wordt een applicatieconsistente back-up gemaakt.	Er wordt een stilgelegde momentopname gemaakt. Er wordt een applicatieconsistente back-up gemaakt.	Back-up mislukt.	Er wordt een niet-stilgelegde momentopname gemaakt. Er wordt een crashconsistente back-up gemaakt.

Instellingen	Stilgelegde momentopname gemaakt		Geen stilgelegde momentopname gemaakt	
	Back-up van toepassingen ingeschakeld	**Back-up van toepassingen uitgeschakeld**	**Back-up van toepassingen ingeschakeld**	**Back-up van toepassingen uitgeschakeld**
te maken niet ingeschakeld				
Volume Shadow Copy Service (VSS) voor virtuele machines ingeschakeld **Back-up laten mislukken als het niet mogelijk is een stilgelegde momentopname te maken** ingeschakeld	Er wordt een stilgelegde momentopname gemaakt. Er wordt een applicatieconsistente back-up gemaakt.	Er wordt een stilgelegde momentopname gemaakt. Er wordt een applicatieconsistente back-up gemaakt.	Back-up mislukt.	Back-up mislukt.
Volume Shadow Copy Service (VSS) voor virtuele machines uitgeschakeld	Er wordt een niet-stilgelegde momentopname gemaakt. Er wordt een crashconsistente back-up gemaakt.	Er wordt een niet-stilgelegde momentopname gemaakt. Er wordt een crashconsistente back-up gemaakt.	Er wordt een niet-stilgelegde momentopname gemaakt. Er wordt een crashconsistente back-up gemaakt.	Er wordt een niet-stilgelegde momentopname gemaakt. Er wordt een crashconsistente back-up gemaakt.

Als u de optie **Volume Shadow Copy Service (VSS) voor virtuele machines** inschakelt, worden ook de scripts voorafgaand aan stilzetten en na afloop van reactivering gestart (mogelijk hebt u deze scripts gebruikt voor de virtuele machine waarvan een back-up is gemaakt). Zie "Automatisch uitvoeren van scripts voorafgaand aan stilzetten en na afloop van reactivering" (p. 733) voor meer informatie over deze scripts.

Als u een stilgelegde momentopname wilt maken, maakt de back-upsoftware respectievelijk gebruik van VMware Tools, Hyper-V Integration Services, Virtuozzo Guest Tools, Red Hat Virtualization Guest Tools of QEMU Guest Tools om VSS toe te passen in een virtuele machine.

Opmerking
Voor virtuele Red Hat Virtualization (oVirt) machines raden we aan dat u QEMU Guest Tools installeert in plaats van Red Hat Virtualization Guest Tools. Sommige versies van Red Hat Virtualization Guest Tools bieden geen ondersteuning voor applicatieconsistente momentopnamen.

Deze optie heeft geen invloed op virtuele Scale Computing HC3-machines. Stilleggen hangt in dit geval af van het feit of de Scale-tools zijn geïnstalleerd op de virtuele machine.

Wekelijkse back-up

Deze optie bepaalt welke back-ups in de bewaarregels en back-upschema's 'wekelijks' worden uitgevoerd. Een wekelijkse back-up is de eerste back-up die na het begin van de week wordt gemaakt.

De vooraf ingestelde waarde is: **Maandag**.

Windows-gebeurtenislogboek

Deze optie is alleen effectief in Windows-besturingssystemen.

Met deze optie definieert u of gebeurtenissen van de back-upbewerkingen door agenten worden geregistreerd in het Toepassingsgebeurtenislogboek van Windows (bekijk dit logboek door eventvwr.exe uit te voeren of selecteer **Configuratiescherm** > **Systeembeheer** > **Logboeken**). U kunt filteren welke gebeurtenissen u wilt laten registreren.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Herstel

Referentiemateriaal voor herstelbewerkingen

De volgende tabel bevat een overzicht van de beschikbare herstelmethoden. Gebruik de tabel om de beste herstelmethode voor uw behoeften te kiezen.

Opmerking
In de Cyber Protect-console kunt u geen back-ups herstellen voor tenants in de compliancemodus. Zie "Back-ups herstellen voor tenants in de compliancemodus" (p. 1167) voor meer informatie over het herstellen van dergelijke back-ups.

Te herstellen	Herstelmethode
Fysieke machine (Windows of Linux)	De Cyber Protect-console gebruiken Opstartmedia
Fysieke machine	Opstartmedia

(Mac)	
Virtuele machine (VMware, Hyper-V, Red Hat Virtualization (oVirt) of Scale Computing HC3)	De Cyber Protect-console gebruiken Opstartmedia
Virtuele machine of container (Virtuozzo, Virtuozzo Hybrid Server of Virtuozzo Hybrid Infrastructure)	De Cyber Protect-console gebruiken
ESXi-configuratie	Opstartmedia
Bestanden/mappen	De Cyber Protect-console gebruiken Bestanden downloaden uit de cloudopslag Opstartmedia Bestanden uitpakken vanuit lokale back-ups
Systeemstatus	De Cyber Protect-console gebruiken
SQL-databases	De Cyber Protect-console gebruiken
Exchange-databases	De Cyber Protect-console gebruiken
Exchange-postvakken	De Cyber Protect-console gebruiken
Websites	De Cyber Protect-console gebruiken
Microsoft 365	
Postvakken (lokale agent voor Microsoft 365)	De Cyber Protect-console gebruiken
Postvakken (cloudagent voor Microsoft 365)	De Cyber Protect-console gebruiken
Openbare mappen	De Cyber Protect-console gebruiken
OneDrive-bestanden	De Cyber Protect-console gebruiken
SharePoint Online-gegevens	De Cyber Protect-console gebruiken
Google Workspace	
Postvakken	De Cyber Protect-console gebruiken
Google Drive-bestanden	De Cyber Protect-console gebruiken
Gedeelde Drive-bestanden	De Cyber Protect-console gebruiken

Platformonafhankelijk herstel

Platformonafhankelijk herstel is beschikbaar voor back-ups van volledige machines en back-ups van schijven die een besturingssysteem bevatten.

Platformonafhankelijk herstel is vereist in de volgende gevallen:

- Een back-up wordt gemaakt door een bepaald type agent, maar hersteld door een ander type agent.
- Een back-up met agent wordt hersteld op hypervisorniveau (herstel zonder agent), of een back-up zonder agent wordt hersteld door een agent (herstel met agent).
- Een back-up wordt hersteld naar niet-vergelijkbare hardware (waaronder virtuele hardware).

Opmerking
Sommige randapparaten, zoals printers, worden mogelijk niet correct hersteld wanneer u een platformonafhankelijk herstel uitvoert.

De onderstaande tabel bevat enkele voorbeelden van platformonafhankelijk herstel.

Platformonafhankelijk herstel	
Back-up zonder agent	Herstel met agent
Back-up met agent	Herstel zonder agent
Back-up door Agent voor Windows	Herstel door Agent voor VMware
Back-up door Agent voor VMware	Herstel door Agent voor Hyper-V
Back-up door Agent voor Windows die is geïnstalleerd op een virtuele VMware ESXi-machine (met agent)	Herstel door Agent voor VMware (zonder agent) op dezelfde VMware ESXi-host
Back-up door Agent voor Windows	Herstel door Agent voor Windows geïnstalleerd op een machine met niet-vergelijkbare hardware
Back-up van een fysieke machine	Herstel als virtuele machine

Opmerking voor Mac-gebruikers

- Vanaf El Capitan 10.11 worden om beveiligingsredenen bepaalde systeembestanden, mappen en processen gemarkeerd met een uitgebreid bestandskenmerk (com.apple.rootless). Deze functie wordt System Integrity Protection (SIP) genoemd. De functie wordt bijvoorbeeld toegepast voor vooraf geïnstalleerde applicaties en de meeste mappen in /system, /bin, /sbin, /usr, die op deze manier worden beschermd.

  De beschermde mappen en bestanden kunnen niet worden overschreven tijdens een herstelbewerking met het besturingssysteem. Als u de beschermde bestanden wilt overschrijven, moet u de herstelbewerking uitvoeren met opstartmedia.

- Vanaf macOS Sierra 10.12 kunnen zelden gebruikte bestanden worden verplaatst naar iCloud door de functie voor opslaan in de cloud. Kleine voetafdrukken van deze bestanden worden bewaard in het bestandssysteem. De back-ups worden gemaakt van deze voetafdrukken en niet van de oorspronkelijke bestanden.

  Wanneer u een voetafdruk herstelt naar de oorspronkelijke locatie, wordt deze gesynchroniseerd met iCloud en het oorspronkelijke bestand wordt dan beschikbaar. Wanneer u een voetafdruk herstelt naar een andere locatie, kan deze niet worden gesynchroniseerd en het oorspronkelijke bestand is dan niet beschikbaar.

Veilig herstel

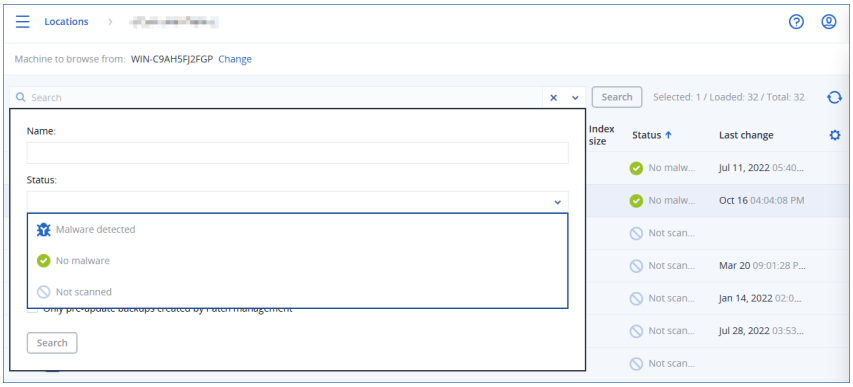
Gebruik veilig herstel met back-ups van **Volledige machine** of **Schijven/volumes** van Windows-workloads om te waarborgen dat u alleen gegevens zonder malware herstelt, zelfs als de back-up geïnfecteerde bestanden bevat.

Tijdens een veilige herstelbewerking wordt de back-up automatisch gescand op malware. Vervolgens wordt de back-up door de beveiligingsagent hersteld op de doelworkload en worden alle geïnfecteerde bestanden verwijderd. Hierdoor wordt een back-up zonder malware hersteld.

Daarnaast wordt een van de volgende statussen toegewezen aan de back-up:

- Malware gedetecteerd
- Geen malware
- Niet gescand

U kunt de status gebruiken om de back-uparchieven te filteren.



Beperkingen

- Veilig herstel wordt ondersteund voor fysieke en virtuele Windows-machines waarop een beveiligingsagent is geïnstalleerd.
- Veilig herstel wordt ondersteund voor back-ups van **Volledige machine** en **Schijven/volumes**.
- Alleen NTFS-volumes worden gescand op malware. Andere volumes dan NTFS-volumes worden hersteld zonder antimalwarescan.

- Veilig herstel wordt niet ondersteund voor de CDP-back-up (Continuous data protection) in het archief. Als u de gegevens uit de CDP-back-up wilt herstellen, voert u een extra herstelbewerking voor **Bestanden/mappen** uit. Zie "Continue gegevensbescherming (CDP)" (p. 435) voor meer informatie over de CDP-back-ups.

Een machine herstellen

Fysieke machines herstellen

In dit gedeelte wordt beschreven hoe u fysieke machines herstelt met behulp van de webinterface.

Gebruik in de volgende gevallen in plaats van de webinterface een opstartmedium:

- Een machine met macOS
- Een machine van een tenant in de compliancemodus
- Elk besturingssysteem naar bare metal of naar een offline machine
- De structuur van logische volumes (volumes die zijn gemaakt door Logical Volume Manager in Linux). Met de media kunt u de structuur van het logisch volume automatisch opnieuw maken.

Opmerking
Back-ups op schijfniveau van Macs met Intel naar Macs met een Apple Silicon-processor (en omgekeerd) kunnen niet worden hersteld. U kunt bestanden en mappen herstellen.

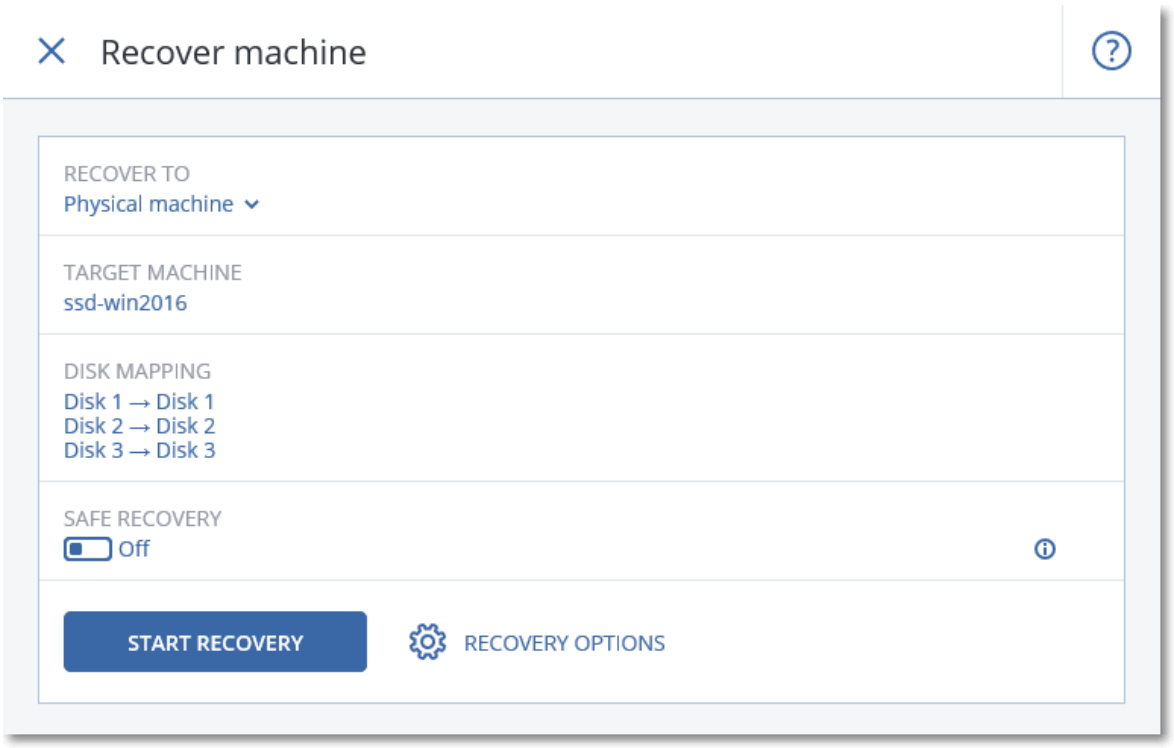
Een fysieke machine herstellen

1. Selecteer de machine waarvan een back-up is gemaakt.
2. Klik op **Herstel**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de machine offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:
   - Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een doelmachine die online is en selecteert u vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad Back-upopslag.
   - Herstel de machine zoals wordt beschreven in 'Schijven herstellen met opstartmedia'.
4. Klik op **Herstellen** > **Volledige machine**.

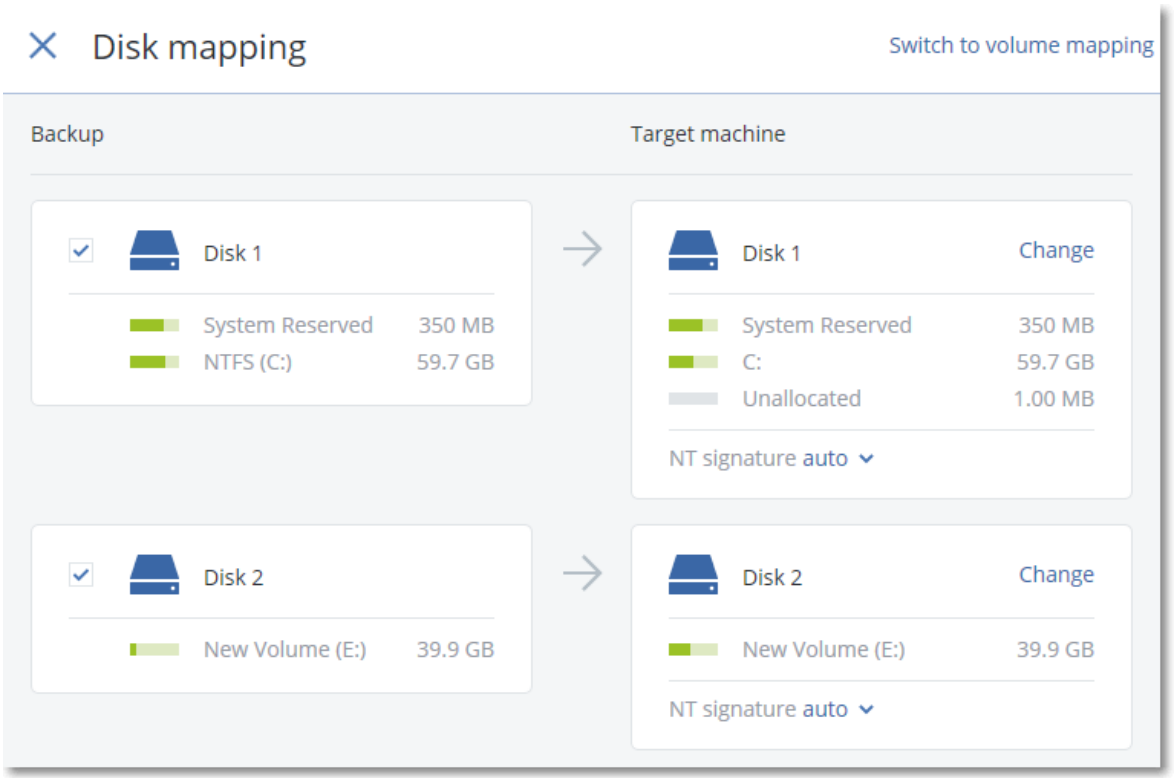
   De schijven uit de back-up worden automatisch toegewezen aan de schijven van de doelmachine.

   Als u wilt herstellen naar een andere fysieke machine, klikt u op **Doelmachine** en selecteert u vervolgens een doelmachine die online is.



5. Als u niet tevreden bent over het toewijzingsresultaat of als de schijftoewijzing mislukt, klikt u op **Volumetoewijzing** om de schijven handmatig opnieuw toe te wijzen.

   In het toewijzingsgedeelte kunt u ook afzonderlijke schijven of volumes kiezen die moeten worden hersteld. U kunt schakelen tussen het herstel van schijven en volumes met de koppeling **Overschakelen naar...** in de rechterbovenhoek.



6. [Alleen beschikbaar voor Windows-machines waarop een beveiligingsagent is geïnstalleerd] Gebruik de schakelaar om **Veilig herstel** in te schakelen zodat u zeker weet dat de herstelde gegevens geen malware bevatten. Zie "Veilig herstel" (p. 528) voor meer informatie over hoe veilig herstel werkt.
7. Klik op **Herstel starten**.
8. Bevestig dat u de schijven wilt overschrijven met de back-ups. Kies of u de machine automatisch opnieuw wilt opstarten.

De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**.

Fysieke machine naar virtueel

U kunt een fysieke machine herstellen naar een virtuele machine op een van de ondersteunde hypervisors. Dit is ook een mechanisme om een fysieke machine te migreren naar een virtuele machine. Ga voor meer informatie over ondersteunde P2V-migratiepaden naar 'Machinemigratie'.

In dit gedeelte wordt beschreven hoe u een fysieke machine herstelt als virtuele machine via de webinterface. Deze bewerking kan worden uitgevoerd als er ten minste één agent voor de betreffende hypervisor is geïnstalleerd en geregistreerd in Acronis Management Server. Voor herstel naar VMware ESXi is bijvoorbeeld ten minste één Agent voor VMware en voor herstel naar Hyper-V is ten minste één Agent voor Hyper-V vereist die in de omgeving is geïnstalleerd en geregistreerd.

Herstel via de webinterface is niet beschikbaar voor tenants in de compliancemodus.

Opmerking
U kunt geen virtuele macOS-machines herstellen naar Hyper-V-hosts, omdat Hyper-V geen ondersteuning biedt voor macOS. U kunt virtuele macOS-machines herstellen naar een VMware-host die op Mac-hardware is geïnstalleerd.

U kunt echter geen back-ups van fysieke macOS-machines herstellen als virtuele machines.

Een fysieke machine herstellen als virtuele machine

1. Selecteer de machine waarvan een back-up is gemaakt.
2. Klik op **Herstel**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de machine offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:
   - Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een machine die online is en selecteert u vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad Back-upopslag.
   - Herstel de machine zoals wordt beschreven in 'Schijven herstellen met opstartmedia'.

4. Klik op **Herstellen** > **Volledige machine**.
5. Selecteer bij **Herstellen naar** de optie **Virtuele machine**.
6. Klik op **Doelmachine**.
   a. Selecteer de hypervisor.

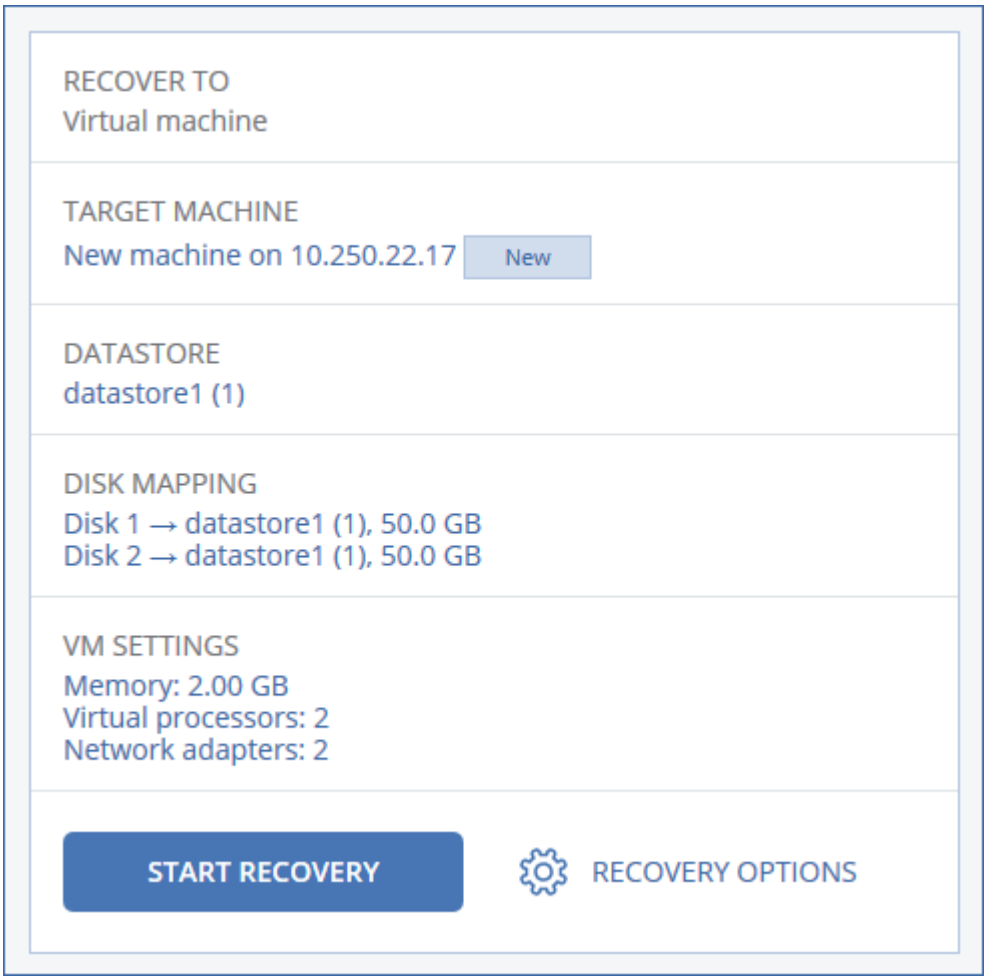
      Opmerking
      Er moet ten minste één agent voor die hypervisor zijn geïnstalleerd en geregistreerd in Acronis Management Server.

   b. Selecteer of u een naar een nieuwe of bestaande machine wilt herstellen. De optie voor een nieuwe machine heeft de voorkeur omdat de schijfconfiguratie van de doelmachine dan niet precies hoeft overeen te stemmen met de schijfconfiguratie in de back-up.
   c. Selecteer de host en geef de naam van de nieuwe machine op, of selecteer en bestaande doelmachine.
   d. Klik op **OK**.
7. [Voor Virtuozzo Hybrid Infrastructure] Klik op **VM-instellingen** om **Variant** te selecteren. Indien gewenst kunt u de geheugengrootte, het aantal processors en de netwerkverbindingen van de virtuele machine wijzigen.

   Opmerking
   Het selecteren van een variant is een vereiste stap voor Virtuozzo Hybrid Infrastructure.

8. [Optioneel] Aanvullende herstelopties configureren:
   - [Niet beschikbaar voor Virtuozzo Hybrid Infrastructure] Klik op **Gegevensopslag** voor ESXi of op **Pad** voor Hyper-V en selecteer vervolgens de gegevensopslag voor de virtuele machine.
   - Klik op **Schijftoewijzing** om de (gegevens)opslag, interface en inrichtingsmethode voor elke virtuele schijf te selecteren. In het toewijzingsgedeelte kunt u ook afzonderlijke schijven kiezen die moeten worden hersteld.

     Voor Virtuozzo Hybrid Infrastructure kunt u alleen het opslagbeleid voor de doelschijven selecteren. Selecteer hiervoor de gewenste doelschijf en klik vervolgens op Wijzigen. Klik in de geopende blade op het tandwielpictogram, selecteer het opslagbeleid en klik vervolgens op Gereed.
   - [Voor VMware ESXi, Hyper-V en Red Hat Virtualization/oVirt] Klik op **VM-instellingen** om de geheugengrootte, het aantal processors en de netwerkverbindingen van de virtuele machine te wijzigen.



9. [Alleen beschikbaar voor Windows-machines waarop een beveiligingsagent is geïnstalleerd] Gebruik de schakelaar om **Veilig herstel** in te schakelen zodat u zeker weet dat de herstelde gegevens geen malware bevatten. Zie "Veilig herstel" (p. 528) voor meer informatie over hoe veilig herstel werkt.
10. Klik op **Herstel starten**.
11. Wanneer u herstelt naar een bestaande virtuele machine, bevestigt u dat u de schijven wilt overschrijven.

De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**.

Een virtuele machine herstellen

U kunt virtuele machines herstellen vanuit de betreffende back-ups.

Opmerking
In de Cyber Protect-console kunt u geen back-ups herstellen voor tenants in de compliancemodus. Zie "Back-ups herstellen voor tenants in de compliancemodus" (p. 1167) voor meer informatie over het herstellen van dergelijke back-ups.

Vereisten

- Een virtuele machine moet worden gestopt tijdens de herstelbewerking naar deze machine. Standaard wordt de machine gestopt zonder dat u hoeft te bevestigen. Wanneer de herstelbewerking is voltooid, moet u de machine handmatig starten. U kunt dit standaardgedrag wijzigen via de hersteloptie van het energiebeheer van de VM (klik op **Herstelopties** > **Energiebeheer VM**).

Procedure

1. Voer een van de volgende handelingen uit:
   - Selecteer een machine waarvan een back-up is gemaakt, klik op **Herstel** en selecteer vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad Back-upopslag.
2. Klik op **Herstellen** > **Volledige machine**.
3. Als u wilt herstellen naar een fysieke machine, selecteert u **Fysieke machine** in **Herstellen naar**. Anders kunt u deze stap overslaan.

   Herstel naar een fysieke machine is alleen mogelijk als de schijfconfiguratie van de doelmachine precies overeenstemt met de schijfconfiguratie in de back-up.

   Als dit het geval is, gaat u verder naar stap 4 in 'Fysieke machine'. Zo niet, dan raden we u aan om de V2P-migratie uit te voeren met opstartmedia.
4. [Optioneel] Standaard wordt de oorspronkelijke machine automatisch geselecteerd als doelmachine. Als u wilt herstellen naar een andere virtuele machine, klit u op **Doelmachine** en doet u het volgende:
   a. Selecteer de hypervisor (**VMware ESXi**, **Hyper-V**, **Virtuozzo**, **Virtuozzo Hybrid Infrastructure**, **Scale Computing HC3** of **oVirt**).

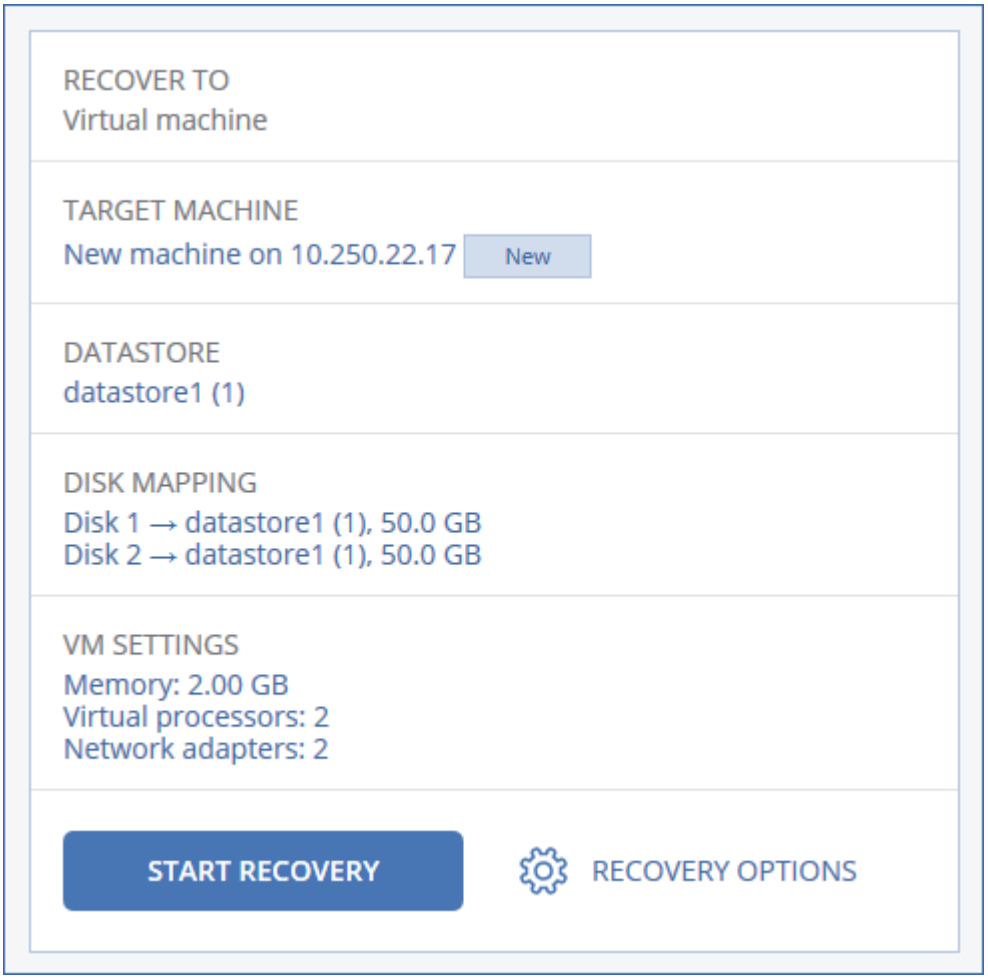
      Alleen virtuele Virtuozzo-machines kunnen worden hersteld naar Virtuozzo. Ga voor meer informatie over V2V-migratie naar 'Machinemigratie'.
   b. Selecteer of u een naar een nieuwe of bestaande machine wilt herstellen.
   c. Selecteer de host en geef de naam van de nieuwe machine op, of selecteer en bestaande doelmachine.
   d. Klik op **OK**.
5. Stel de extra herstelopties in die u nodig hebt.
   - [Optioneel] [Niet beschikbaar voor Virtuozzo Hybrid Infrastructure en Scale Computing HC3] Als u de gegevensopslag voor de virtuele machine wilt selecteren: klik op **Gegevensopslag** voor ESXi, of **Pad** voor Hyper-V en Virtuozzo, of **Opslagdomein** voor Red Hat Virtualization (oVirt) en selecteer vervolgens de (gegevens)opslag voor de virtuele machine.
   - [Optioneel] Als u de (gegevens)opslag, interface en de inrichtingsmethode voor elke virtuele schijf wilt bekijken, klikt u op **Schijftoewijzing**. U kunt deze instellingen wijzigen, tenzij u een Virtuozzo-container of een virtuele Virtuozzo Hybrid Infrastructure-machine herstelt.

     Voor Virtuozzo Hybrid Infrastructure kunt u alleen het opslagbeleid voor de doelschijven selecteren. Selecteer hiervoor de gewenste doelschijf en klik vervolgens op **Wijzigen**. Klik in de

geopende blade op het tandwielpictogram, selecteer het opslagbeleid en klik vervolgens op **Gereed**.

In het toewijzingsgedeelte kunt u ook afzonderlijke schijven kiezen die moeten worden hersteld.

- [Optioneel] [Beschikbaar voor VMware ESXi, Hyper-V en Virtuozzo] Klik op **VM-instellingen** om de geheugengrootte, het aantal processors en de netwerkverbindingen van de virtuele machine te wijzigen.
- [Voor Virtuozzo Hybrid Infrastructure] Selecteer **Variant** om de geheugengrootte en het aantal processors van de virtuele machine te wijzigen.



6. [Alleen beschikbaar voor Windows-machines waarop een beveiligingsagent is geïnstalleerd] Gebruik de schakelaar om **Veilig herstel** in te schakelen zodat u zeker weet dat de herstelde gegevens geen malware bevatten. Zie "Veilig herstel" (p. 528) voor meer informatie over hoe veilig herstel werkt.
7. Klik op **Herstel starten**.
8. Wanneer u herstelt naar een bestaande virtuele machine, bevestigt u dat u de schijven wilt overschrijven.

De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**.

Herstel met opnieuw opstarten

Herstel met opnieuw opstarten wordt ondersteund voor Windows- en Linux-machines.

U kunt kiezen of u de machine automatisch opnieuw wilt laten opstarten of u kunt de status **Interactie vereist** toewijzen. Het herstelde besturingssysteem gaat automatisch online.

Een herstart is vereist bij herstel van de volgende items:

- Een besturingssysteem
  Bijvoorbeeld wanneer u een volledige machine of het systeemvolume van een machine herstelt.
- Versleutelde volumes
  Bijvoorbeeld wanneer u volumes herstelt die zijn versleuteld met BitLocker of CheckPoint.

Belangrijk
Een back-up van versleutelde volumes wordt hersteld als niet-versleuteld.

Een herstelomgeving wordt automatisch voorbereid voor de herstelde machine. Wanneer de omgeving gereed is, start de machine opnieuw op en wordt de herstelomgeving geopend. Wanneer het herstel is voltooid, start het besturingssysteem.

Herstelomgeving

Herstel met opnieuw opstarten in een Linux-herstelomgeving.

Opmerking
Voor herstel van een machine met een versleuteld systeemvolume moet er ten minste één niet-versleuteld volume op dezelfde machine bestaan.

Vereisten voor schijfruimte

De herstelomgeving vereist schijfruimte voor tijdelijke bestanden. De vereisten variëren afhankelijk van de herstelde machine.

De onderstaande tabel bevat een overzicht van de beschikbare opties.

Opstartmodus	Machine met niet-versleuteld systeemvolume	Machine met versleuteld systeemvolume
BIOS	200 MB op het systeemvolume	400 MB op een niet-versleuteld volume
UEFI	200 MB op de EFI-systeempartitie (ESP)	Eén van het volgende: • 400 MB op de EFI-systeempartitie (ESP) • 200 MB op de EFI-systeempartitie (ESP) en 200 MB op een onversleutelde partitie die

Opstartmodus	Machine met niet-versleuteld systeemvolume	Machine met versleuteld systeemvolume
		toegankelijk is tijdens het opstartproces

Beperkingen

- Voordat u begint met het herstel, moet u alle versleutelde volumes die geen systeemvolume zijn, vergrendelen. U kunt een volume vergrendelen door een bestand binnen het volume te openen. Als het volume niet is vergrendeld, gaat het herstel door zonder opnieuw op te starten, en het besturingssysteem herkent het volume mogelijk niet.

  Een versleuteld systeemvolume hoeft u niet te vergrendelen.

Problemen oplossen

Als een herstel mislukt en de foutmelding `Kan bestand niet ophalen uit partitie` wordt weergegeven na het opnieuw starten, dan schakelt u Secure Boot uit. Voor meer informatie: zie Secure Boot uitschakelen in de Microsoft-documentatie.

Schijven herstellen met opstartmedia

Zie "Fysieke opstartmedia maken" (p. 750) voor informatie over het maken van opstartmedia.

Opmerking
Back-ups op schijfniveau van Macs met Intel naar Macs met een Apple Silicon-processor (en omgekeerd) kunnen niet worden hersteld. U kunt bestanden en mappen herstellen.

Schijven herstellen met opstartmedia

1. Start de doelmachine op met een opstartmedium.
2. [Alleen bij het herstellen van een Mac] Wanneer u als APFS geformatteerde schijven/volumes herstelt naar bare metal of een machine die niet de oorspronkelijke machine is, moet u de oorspronkelijke schijfconfiguratie handmatig opnieuw maken:
   a. Klik op **Hulpprogramma voor schijf**.
   b. Wis en formatteer de doelschijf naar APFS. Zie https://support.apple.com/en-us/HT208496#erasedisk voor instructies.
   c. Maak de oorspronkelijke schijfconfiguratie opnieuw aan. Zie https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15 voor instructies.
   d. Klik op **Hulpprogramma voor schijf** > **Hulpprogramma voor schijf afsluiten**.
3. Klik op **Deze machine lokaal beheren** of dubbelklik op **Opstartbaar herstelmedium**, afhankelijk van het type medium dat u gebruikt.

4. Als een proxyserver is ingeschakeld in uw netwerk, klikt u op **Extra** > **Proxyserver** en geeft u de hostnaam/het IP-adres, de poort en de referenties van de proxyserver op. Anders kunt u deze stap overslaan.
5. [Optioneel] Klik bij het herstellen van Windows of Linux op **Extra** > **Media registreren in de Cyber Protection-service** en geef vervolgens het registratietoken op dat u hebt verkregen bij het downloaden van de media. Als u dit doet, hoeft u geen referenties of registratiecode in te voeren voor toegang tot de cloudopslag, zoals beschreven in stap 8.
6. Klik in het welkomstscherm op **Herstellen**.
7. Klik op **Gegevens selecteren** en klik vervolgens op **Bladeren**.
8. Geef de back-uplocatie op:
   - Als u gegevens uit de cloudopslag wilt herstellen, selecteert u **Cloudopslag**. Geef de referenties op van het account waaraan de back-up van de machine is toegewezen.

     Wanneer u Windows of Linux herstelt, kunt u een registratiecode aanvragen en deze gebruiken in plaats van de referenties. Klik op **Registratiecode gebruiken** > **De code aanvragen**. Het programma geeft de registratielink en de registratiecode weer. U kunt deze kopiëren en de registratiestappen uitvoeren op een andere machine. De registratiecode is een uur geldig.
   - Als u gegevens uit een lokale map of een netwerkmap wilt herstellen, bladert u bij **Lokale mappen** of **Netwerkmappen** naar de desbetreffende map.
   - Als u wilt herstellen vanuit back-uplocaties op openbare cloudopslag zoals Microsoft Azure, Amazon S3, Wasabi of S3-compatibel, klikt u eerst op **Media registreren in de Cyber Protection-service** en vervolgens configureert u het herstel via de webinterface. Voor meer informatie over extern beheer van media via de webinterface raadpleegt u "Bewerkingen op afstand met opstartmedia" (p. 768).

   Klik op **OK** om uw selectie te bevestigen.
9. Selecteer de back-up waaruit u gegevens wilt herstellen. Geef desgevraagd het wachtwoord voor de back-up op.
10. Selecteer in **Back-upinhoud** de schijven die u wilt herstellen. Klik op **OK** om uw selectie te bevestigen.
11. In het gedeelte **Waar herstellen** worden de geselecteerde schijven automatisch door de software aan de doelschijven toegewezen.

    Als de toewijzing mislukt of als u niet tevreden bent over de toewijzingsresultaten, kunt u de schijven handmatig opnieuw toewijzen.

    Opmerking
    Als u de schijfindeling wijzigt, kan dit van invloed zijn op de opstartbaarheid van het besturingssysteem. Gebruik de oorspronkelijke schijfindeling van de machine, tenzij u zeker weet dat u ook een andere schijfindeling kunt gebruiken.
12. [Bij het herstellen van Linux] Als de machine waarvan een back-up is gemaakt, logische volumes (LVM) bevat en u de oorspronkelijke LVM-structuur wilt reproduceren:

a. Zorg ervoor dat het aantal doelmachineschijven en de capaciteit van de schijven minimaal gelijk is aan die van de oorspronkelijke machine en klik vervolgens op **RAID/LVM toepassen**.
b. Controleer de volumestructuur en klik vervolgens op **RAID/LVM toepassen** om de structuur te maken.

13. [Optioneel] Klik op **Herstelopties** om aanvullende instellingen op te geven.
14. Klik op **OK** om de herstelbewerking te starten.

Universal Restore gebruiken

De meest recente besturingssystemen blijven opstartbaar wanneer ze worden hersteld naar andere hardware, zoals de VMware- of Hyper-V-platformen. Als een hersteld besturingssysteem niet opstart, kunt u Universal Restore gebruiken om de stuurprogramma's en modules bij te werken die essentieel zijn om het besturingssysteem op te starten.

Universal Restore is beschikbaar voor Windows en Linux.

Universal Restore toepassen

1. Start de machine op vanaf de opstartmedia.
2. Klik op **Universal Restore toepassen**.
3. Als er meerdere besturingssystemen zijn op de machine, kiest u het systeem waarop u Universal Restore wilt toepassen.
4. [Alleen voor Windows] Configureer de aanvullende instellingen.
5. Klik op **OK**.

Universal Restore in Windows

Voorbereiding

Stuurprogramma's voorbereiden

Voordat u Universal Restore toepast op een Windows-besturingssysteem, controleert u of u de stuurprogramma's hebt voor de nieuwe HDD-controller en de chipset. Deze stuurprogramma's zijn essentieel om het besturingssysteem op te starten. Gebruik de door uw hardwareleverancier meegeleverde cd of dvd of download de stuurprogramma's van de website van de leverancier. De stuurprogrammabestanden moeten de extensie *.inf hebben. Als u de stuurprogramma's downloadt in de indeling *.exe, *.cab of *.zip, moet u ze uitpakken met een applicatie van derden.

Het beste kunt u de stuurprogramma's voor alle hardware die in uw organisatie wordt gebruikt, opslaan in één opslagplaats, gesorteerd op apparaattype of op hardwareconfiguratie. Ga als volgt te werk: bewaar een kopie van de opslagplaats op een dvd of flashstation; kies enkele stuurprogramma's en voeg deze toe aan de opstartmedia; maak de aangepaste opstartmedia met de nodige stuurprogramma's (en de nodige netwerkconfiguratie) voor elk van uw servers. Of u kunt gewoon het pad naar de opslagplaats opgeven telkens wanneer u Universal Restore gebruikt.

Toegang tot de stuurprogramma's controleren in een opstartbare omgeving

Controleer of u toegang hebt tot het apparaat met stuurprogramma's wanneer u met opstartmedia werkt. Gebruik WinPE-media als het apparaat beschikbaar is in Windows, maar niet wordt gedetecteerd door Linux-media.

Instellingen voor Universal Restore

Automatisch zoeken van stuurprogramma's

Geef op waar het programma moet zoeken naar de Hardware Abstraction Layer (HAL), het stuurprogramma voor de HDD-controller en het/de stuurprogramma('s) voor de netwerkadapter(s):

- Als de stuurprogramma's zich bevinden op een schijf van een leverancier of andere verwisselbare media, schakelt u **Verwisselbare media doorzoeken** in.
- Als de stuurprogramma's zich bevinden in een netwerkmap of op de opstartmedia, geeft u het pad naar de map op door te klikken op **Map toevoegen**.

Universal Restore doorzoekt ook de standaardopslagmap voor stuurprogramma's in Windows. Deze locatie wordt bepaald in de registerwaarde **DevicePath** in de registersleutel **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. De gebruikelijke opslagmap hiervoor is WINDOWS/inf.

Met Universal Restore worden de volgende acties uitgevoerd: recursief zoeken in alle submappen van de opgegeven map, meest geschikte HAL en stuurprogramma's voor de HDD-controller vinden van alle beschikbare opties, en deze installeren in het systeem. Universal Restore zoekt ook naar het stuurprogramma voor de netwerkadapter. Het pad naar het gevonden stuurprogramma wordt dan door Universal Restore doorgegeven aan het besturingssysteem. Als de hardware meerdere netwerkinterfacekaarten heeft, probeert Universal Restore alle stuurprogramma's voor de kaarten te configureren.

Stuurprogramma's voor massaopslag die moeten worden geïnstalleerd

Deze instelling hebt u nodig in de volgende gevallen:

- Als de hardware over een specifieke controller voor massaopslag beschikt, zoals RAID (met name NVIDIA RAID) of een Fibre Channel-adapter.
- Als u een systeem hebt gemigreerd naar een virtuele machine die een controller voor een harde SCSI-schijf gebruikt. Als u SCSI-stuurprogramma's gebruikt die zijn gebundeld met uw virtualisatiesoftware of als u de nieuwste versies van de stuurprogramma's downloadt vanaf de website van de softwarefabrikant.
- Als het systeem niet wordt opgestart na het automatisch zoeken van stuurprogramma's.

Geef de betreffende stuurprogramma's op door te klikken op **Stuurprogramma toevoegen**. De hier gedefinieerde stuurprogramma's worden geïnstalleerd, met de relevante waarschuwingen, zelfs als het programma een beter stuurprogramma vindt.

Werking van Universal Restore

Wanneer u de vereiste instellingen hebt opgegeven, klikt u op **OK**.

Als Universal Restore geen compatibel stuurprogramma vindt in de opgegeven locaties, wordt een prompt weergegeven over het apparaat met het probleem. Voer een van de volgende handelingen uit:

- Voeg het stuurprogramma toe aan een van de eerder opgegeven locaties en klik op **Opnieuw proberen**.
- Als u de locatie niet meer weet, klikt u op **Negeren** en gaat u verder met het proces. Als het resultaat niet is wat u verwacht, past u Universal Restore opnieuw toe. Wanneer u de bewerking configureert, geeft u het nodige stuurprogramma op.

Wanneer Windows opnieuw wordt opgestart, wordt de standaardprocedure voor de installatie van nieuwe hardware geïnitialiseerd. Het stuurprogramma voor de netwerkadapter wordt op de achtergrond geïnstalleerd (silent mode) als het de Microsoft Windows-handtekening heeft. Zo niet, dan vraagt Windows om bevestiging of het niet-ondertekende stuurprogramma moet worden geïnstalleerd.

Vervolgens kunt u de netwerkverbinding configureren en stuurprogramma's opgeven voor de videoadapter, USB en andere apparaten.

Universal Restore in Linux

Universal Restore kan worden toegepast op Linux-besturingssystemen met een kernel versie 2.6.8 of later.

Wanneer Universal Restore wordt toegepast op een Linux-besturingssysteem, wordt een update gemaakt van een tijdelijk bestandssysteem (ook wel de 'initial RAM disk' (initrd) genoemd). Hiermee wordt gewaarborgd dat het besturingssysteem kan worden opgestart op de nieuwe hardware.

Met Universal Restore worden modules voor de nieuwe hardware (onder andere apparaatstuurprogramma's) toegevoegd aan de initial RAM disk. Deze modules worden doorgaans opgehaald in de directory **/lib/modules**. Als Universal Restore een vereiste module niet kan vinden, wordt de bestandsnaam van de module geregistreerd in het logboek.

Universal Restore kan de configuratie van het GRUB-opstartlaadprogramma wijzigen. Dit kan bijvoorbeeld nodig zijn om ervoor te zorgen dat het systeem opstartbaar blijft wanneer de nieuwe machine een andere volume-indeling heeft dan de oorspronkelijke machine.

De Linux-kernel wordt nooit gewijzigd door Universal Restore.

Terugkeren naar de oorspronkelijke initial RAM disk

Indien nodig kunt u terugkeren naar de oorspronkelijke initial RAM disk

De initial RAM disk wordt opgeslagen in een bestand op de machine. Voordat de initial RAM disk voor het eerst wordt bijgewerkt door Universal Restore, wordt een kopie van deze schijf opgeslagen in dezelfde directory. De naam van de kopie is de naam van het bestand, gevolgd door het achtervoegsel **_acronis_backup.img**. Deze kopie wordt niet overschreven als u Universal Restore meer dan eens uitvoert (bijvoorbeeld wanneer u ontbrekende stuurprogramma's toevoegt).

Terugkeren naar de oorspronkelijke initial RAM disk:

- Geef de kopie een toepasselijke naam. Voer bijvoorbeeld een opdracht uit zoals deze:

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- Voeg een vermelding van de kopie toe op de **initrd**-regel in de configuratie van het GRUB-opstartlaadprogramma.

Bestanden herstellen

Bestanden herstellen in de Cyber Protect-console

Opmerking
In de Cyber Protect-console kunt u geen back-ups herstellen voor tenants in de compliancemodus. Zie "Back-ups herstellen voor tenants in de compliancemodus" (p. 1167) voor meer informatie over het herstellen van dergelijke back-ups.

1. Selecteer de oorspronkelijke machine met de gegevens die u wilt herstellen.
2. Klik op **Herstel**.
3. Selecteer het herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de geselecteerde machine een fysieke machine is die offline is, worden geen herstelpunten weergegeven. Voer een van de volgende handelingen uit:
   - [Aanbevolen] Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een doelmachine die online is en selecteert u vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad Back-upopslag.
   - Download bestanden uit de cloudopslag.
   - Gebruik opstartmedia.
4. Klik op **Herstellen** > **Bestanden/mappen**.
5. Blader naar de vereiste map of gebruik de zoekbalk om de lijst met de vereiste bestanden en mappen op te halen.

   Zoekopdrachten zijn taalonafhankelijk.

   U kunt een of meer jokertekens (* en ?) gebruiken. Zie "Masker" (p. 490) voor meer informatie over jokers.

Opmerking
Zoeken is niet beschikbaar voor back-ups op schijfniveau die in de cloudopslag zijn opgeslagen.

6. Selecteer de bestanden die u wilt herstellen.
7. Als u de bestanden wilt opslaan als ZIP-bestand, klikt u op **Downloaden**, selecteert u de locatie waar u de gegevens wilt opslaan en klikt u op **Opslaan**. Anders kunt u deze stap overslaan.
   U kunt niet downloaden als u mappen hebt geselecteerd of als de totale grootte van de geselecteerde bestanden meer is dan 100 MB. Als u grotere hoeveelheden gegevens uit de cloud wilt ophalen, gebruikt u de procedure "Bestanden downloaden uit de cloudopslag" (p. 544).
8. Klik op **Herstellen**.
   Ga naar **Herstellen naar** en selecteer het doel voor de herstelbewerking. U kunt ook het standaardwaarde voor het doel gebruiken. Het standaarddoel is afhankelijk van de bron van de back-up.
   De volgende doelen zijn beschikbaar:
   - De bronmachine (als hierop een beveiligingsagent is geïnstalleerd).
     Dit is de oorspronkelijke machine met de bestanden die u wilt herstellen.
   - Andere machines waarop een beveiligingsagent is geïnstalleerd: fysieke machines, virtuele machines en virtualisatiehosts waarop een beveiligingsagent is geïnstalleerd, of virtuele toepassingen.
     U kunt bestanden herstellen naar fysieke machines, virtuele machines en virtualisatiehosts waarop een beveiligingsagent is geïnstalleerd. U kunt geen bestanden herstellen naar virtuele machines waarop geen beveiligingsagent is geïnstalleerd (behalve voor virtuele Virtuozzo-machines).
   - Virtuozzo-containers of virtuele Virtuozzo-machines.
     U kunt met enkele beperkingen bestanden herstellen naar Virtuozzo-containers en virtuele Virtuozzo-machines. Zie "Beperkingen voor het herstellen van bestanden in de Cyber Protect-console" (p. 548) voor meer informatie hierover.
9. Ga naar **Pad** en selecteer de herstelbestemming. U kunt een van de volgende opties selecteren:
   - [Bij herstel naar de oorspronkelijke machine] De oorspronkelijke locatie.
   - Een lokale map of lokaal gekoppelde opslag op de doelmachine.

     Opmerking
     Symbolische links worden niet ondersteund.

   - Een netwerkmap die toegankelijk is vanuit de doelmachine.
10. Klik op **Herstel starten**.
11. Selecteer een van de opties voor het overschrijven van bestanden:
    - **Bestaande bestanden overschrijven**
    - **Een bestaand bestand overschrijven als dit ouder is**
    - **Bestaande bestanden niet overschrijven**

De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**.

Bestanden downloaden uit de cloudopslag

In de Webherstel-console kunt u in de cloudopslag bladeren, de inhoud van back-ups bekijken en de back-ups van bestanden en mappen downloaden.

Opmerking
U kunt alleen toegang krijgen tot de Web Restore-console als u een Cyber Protection-beheerder of tenantgebruiker van de klant bent. De gebruikersrollen op partnerniveau zijn niet toegestaan.

Beperkingen

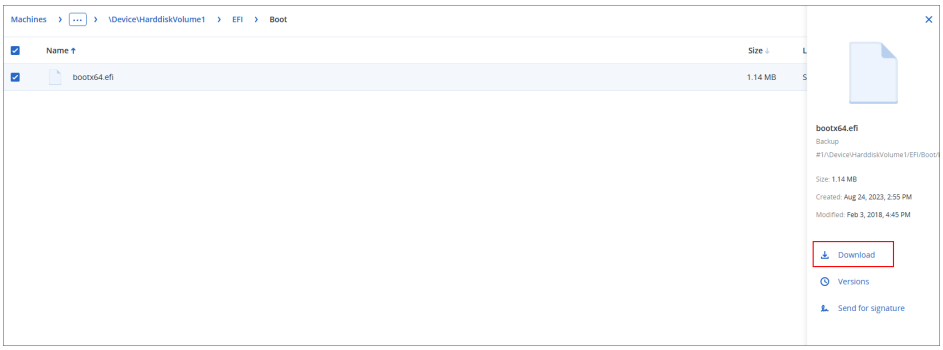
- U kunt geen back-ups van schijven, volumes of volledige herstelpunten downloaden.
- Wanneer u back-ups op schijfniveau doorzoekt, worden logische volumes (zoals LVM en LDM) niet weergegeven.
- U kunt niet bladeren in back-ups van systeemstatus, SQL-databases en Exchange-databases.

Bestanden en mappen downloaden uit de cloudopslag

1. Open de Cyber Protection-console, selecteer de gewenste workload en klik op **Herstel**.
2. [Als er meerdere back-uplocaties beschikbaar zijn] Selecteer de back-uplocatie en klik vervolgens op **Meer herstelbewerkingen**.
3. Klik op **Bestanden downloaden**.
4. Ga naar **Machines**, klik op de naam van de workload en klik op het back-uparchief.
   Een back-uparchief bevat een of meer back-ups (herstelpunten).
5. Klik op het nummer van de back-up (herstelpunt) van waaruit u bestanden of mappen wilt downloaden, en navigeer vervolgens naar de vereiste items.
6. Schakel de selectievakjes in naast de items die u wilt downloaden.

   Opmerking
   Als u meerdere items selecteert, worden ze gedownload als zipbestand.

7. Klik op **Downloaden**.



De authenticiteit van bestanden verifiëren met de Notary-service

Als notarisatie is ingeschakeld tijdens het maken van een back-up, kunt u de authenticiteit verifiëren van een bestand waarvan een back-up is gemaakt.

De authenticiteit van bestanden verifiëren

1. Selecteer het bestand zoals beschreven in stap 1-6 van het gedeelte 'Bestanden herstellen via de webinterface', of stap 1-5 van het gedeelte 'Bestanden downloaden uit de cloudopslag'.
2. Controleer of het geselecteerde bestand is gemarkeerd met het volgende pictogram:  . Dit betekent dat het bestand is genotariseerd.
3. Voer een van de volgende handelingen uit:
   - Klik op **Verifiëren**.
     De software controleert de authenticiteit van het bestand en geeft het resultaat weer.
   - Klik op **Certificaat ophalen**.
     Een certificaat dat bevestigt dat het bestand is genotariseerd, wordt geopend in een browservenster. Het venster bevat ook instructies voor het handmatig verifiëren van de authenticiteit van het bestand.

Een bestand ondertekenen met ASign

Opmerking
Deze functie is alleen beschikbaar met het Advanced Backup-pakket.

ASign is een service die meerdere mensen in staat stelt om de back-up van een bestand elektronisch te ondertekenen. Deze functie is alleen beschikbaar voor back-ups op bestandsniveau die zijn opgeslagen in de cloudopslag.

Er kan slechts één bestandsversie tegelijk worden ondertekend. Als er meerdere keren een back-up is gemaakt van het bestand, moet u kiezen welke versie u wilt ondertekenen. Alleen deze versie wordt dan ondertekend.

ASign kan bijvoorbeeld worden gebruikt voor het elektronisch ondertekenen van de volgende bestanden:

- Huur- of leaseovereenkomsten
- Verkoopcontracten
- Koopovereenkomsten van activa
- Leningsovereenkomsten
- Toestemmingsstrookjes
- Financiële documenten
- Verzekeringsdocumenten

- Vrijstellingen van aansprakelijkheid
- Gezondheidszorgdocumenten
- Onderzoeksdocumenten
- Certificaten van echtheid van een product
- Geheimhoudingsverklaringen
- Offertebrieven
- Vertrouwelijkheidsovereenkomsten
- Overeenkomsten voor zelfstandig ondernemers

Een bestandsversie ondertekenen

1. Selecteer het bestand zoals beschreven in stap 1-6 van het gedeelte 'Bestanden herstellen via de webinterface', of stap 1-5 van het gedeelte 'Bestanden downloaden uit de cloudopslag'.
2. Controleer of de juiste datum en tijd zijn geselecteerd in het linkerdeelvenster.
3. Klik op **Deze bestandsversie ondertekenen**.
4. Geef het wachtwoord op voor het cloudopslagaccount waar de back-up is opgeslagen. De gebruikersnaam van het account wordt weergegeven in het opdrachtpromptvenster.
   De interface van de ASign-service wordt geopend in een browservenster.
5. Voeg andere ondertekenaars toe door hun e-mailadressen op te geven. U kunt geen ondertekenaars toevoegen of verwijderen nadat u uitnodigingen hebt verzonden. Controleer dus of in de lijst alle personen worden vermeld van wie de handtekening is vereist.
6. Klik op **Uitnodigen om te ondertekenen** om de uitnodigingen te verzenden naar de ondertekenaars.
   Elke ondertekende ontvangt een e-mailbericht met het ondertekeningsverzoek. Wanneer alle ondertekenaars het bestand hebben ondertekend, wordt het genotariseerd en ondertekend via de Notary-service.
   U ontvangt meldingen wanneer elke ondertekenaar het bestand ondertekent en wanneer het hele proces is voltooid. U kunt de ASign-webpagina openen door te klikken op **Details weergeven** in een van de e-mailberichten die u ontvangt.
7. Wanneer het proces is voltooid, gaat u naar de ASign-webpagina en klikt u op **Document ophalen** om een PDF-document te downloaden. Dit document bevat:
   - De pagina Signature Certificate met de verzamelde ondertekeningen.
   - De pagina Audit Trail met geschiedenis van activiteiten: wanneer de uitnodiging is verzonden naar de ondertekenaars, wanneer elke ondertekenaar het bestand heeft ondertekend, enzovoort.

Bestanden herstellen met opstartmedia

Zie het gedeelte 'Opstartmedia maken' voor meer informatie over het maken van opstartmedia.

Bestanden herstellen met opstartmedia

1. Start de doelmachine op met de opstartmedia.
2. Klik op **Deze machine lokaal beheren** of dubbelklik op **Opstartbaar herstelmedium**, afhankelijk van het type medium dat u gebruikt.
3. Als een proxyserver is ingeschakeld in uw netwerk, klikt u op **Extra** > **Proxyserver** en geeft u de hostnaam/het IP-adres, de poort en de referenties van de proxyserver op. Anders kunt u deze stap overslaan.
4. [Optioneel] Klik bij het herstellen van Windows of Linux op **Extra** > **Media registreren in de Cyber Protection-service** en geef vervolgens het registratietoken op dat u hebt verkregen bij het downloaden van de media. Als u dit doet, hoeft u geen referenties of registratiecode in te voeren voor toegang tot de cloudopslag, zoals beschreven in stap 7.
5. Klik in het welkomstscherm op **Herstellen**.
6. Klik op **Gegevens selecteren** en klik vervolgens op **Bladeren**.
7. Geef de back-uplocatie op:
   - Als u gegevens uit de cloudopslag wilt herstellen, selecteert u **Cloudopslag**. Geef de referenties op van het account waaraan de back-up van de machine is toegewezen.

     Wanneer u Windows of Linux herstelt, kunt u een registratiecode aanvragen en deze gebruiken in plaats van de referenties. Klik op **Registratiecode gebruiken** > **De code aanvragen**. Het programma geeft de registratielink en de registratiecode weer. U kunt deze kopiëren en de registratiestappen uitvoeren op een andere machine. De registratiecode is een uur geldig.
   - Als u gegevens uit een lokale map of een netwerkmap wilt herstellen, bladert u bij **Lokale mappen** of **Netwerkmappen** naar de desbetreffende map.
   - Als u wilt herstellen vanuit back-uplocaties op openbare cloudopslag zoals Microsoft Azure, Amazon S3, Wasabi of S3-compatibel, klikt u eerst op **Media registreren in de Cyber Protection-service** en vervolgens configureert u het herstel via de webinterface. Voor meer informatie over extern beheer van media via de webinterface raadpleegt u "Bewerkingen op afstand met opstartmedia" (p. 768).

   Klik op **OK** om uw selectie te bevestigen.
8. Selecteer de back-up waaruit u gegevens wilt herstellen. Geef desgevraagd het wachtwoord voor de back-up op.
9. Selecteer bij **Back-upinhoud** de optie **Mappen/bestanden**.
10. Selecteer de gegevens die u wilt herstellen. Klik op **OK** om uw selectie te bevestigen.
11. Geef bij **Waar herstellen** een map op. U kunt eventueel voorkomen dat nieuwere versies van bestanden worden overschreven of bepaalde bestanden uitsluiten voor de herstelbewerking.
12. [Optioneel] Klik op **Herstelopties** om aanvullende instellingen op te geven.
13. Klik op **OK** om de herstelbewerking te starten.

Bestanden uitpakken vanuit lokale back-ups

U kunt door de inhoud van back-ups bladeren en de nodige bestanden uitpakken.

Vereisten

- Deze functionaliteit is alleen beschikbaar via Verkenner in Windows.
- Het bestandssysteem waarvan u een back-up maakt, moet een van de volgende systemen zijn: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS, of HFS+.

Vereisten

- Er moet een beveiligingsagent zijn geïnstalleerd op de machine waar u bladert naar een back-up.
- De back-up moet zijn opgeslagen in een lokale map of op een netwerkshare (SMB/CIFS).

Bestanden uitpakken vanuit een back-up

1. Gebruik Verkenner om naar de locatie van de back-up te bladeren.
2. Dubbelklik op het back-upbestand. De bestandsnamen zijn gebaseerd op de volgende sjabloon:
   `<naam machine> - <GUID beschermingsschema>`
3. Als de back-up is versleuteld, voert u het versleutelingswachtwoord in. Anders kunt u deze stap overslaan.
   De herstelpunten worden weergegeven in Verkenner.
4. Dubbelklik op het herstelpunt.
   De gegevens waarvan een back-up is gemaakt, worden weergegeven in Verkenner.
5. Blader naar de vereiste map.
6. Kopieer de vereiste bestanden naar een willekeurige map in het bestandssysteem.

Beperkingen voor het herstellen van bestanden in de Cyber Protect-console

Tenants in de compliancemodus

In de Cyber Protect-console kunt u geen back-ups herstellen voor tenants in de compliancemodus. Zie "Back-ups herstellen voor tenants in de compliancemodus" (p. 1167) voor meer informatie over het herstellen van dergelijke back-ups.

Herstel naar Virtuozzo-containers of virtuele Virtuozzo-machines

- QEMU Guest Agent moet zijn geïnstalleerd op de virtuele doelmachine.
- [Alleen van toepassing bij herstel naar containers] Koppelpunten in containers kunnen niet worden gebruikt als doel voor herstel. U kunt bijvoorbeeld geen bestanden herstellen naar een tweede harde schijf of naar een NFS-share die is gekoppeld aan een container.
- Bij het herstellen van bestanden naar een virtuele Windows-machine en als de hersteloptie "Beveiliging op bestandsniveau" (p. 554) is ingeschakeld, wordt het archiefbitkenmerk ingesteld op de herstelde bestanden.
- Bestanden waarvan de naam niet-ANSI-tekens bevat, worden hersteld met onjuiste namen op machines met Windows Server 2012 of ouder en machines met Windows 7 of ouder.

- Als u bestanden wilt herstellen naar virtuele CentOS- of Red Hat Enterprise Linux-machines met Virtuozzo Hybrid Server, moet u het bestand `qemu-ga` als volgt bewerken:
  - Navigeer op de virtuele doelmachine naar `/etc/sysconfig/` en open vervolgens het bestand `qemu-ga` om het te bewerken.
  - Navigeer naar de volgende regel en verwijder alles achter het isgelijkteken (=):

    ```
    BLACKLIST_RPC=
    ```

  - Start QEMU Guest Agent opnieuw op via de volgende opdracht:

    ```
    systemctl restart qemu-guest-agent
    ```

Systeemstatus herstellen

Opmerking
In de Cyber Protect-console kunt u geen back-ups herstellen voor tenants in de compliancemodus. Zie "Back-ups herstellen voor tenants in de compliancemodus" (p. 1167) voor meer informatie over het herstellen van dergelijke back-ups.

1. Selecteer de machine waarvan u de systeemstatus wilt herstellen.
2. Klik op **Herstel**.
3. Selecteer een herstelpunt voor de systeemstatus. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.
4. Klik op **Systeemstatus herstellen**.
5. Bevestig dat u de systeemstatus wilt overschrijven met de back-upversie.

De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**.

ESXi-configuratie herstellen

Als u een ESXi-configuratie wilt herstellen, hebt u Linux-opstartmedia nodig. Zie "Fysieke opstartmedia maken" (p. 750) voor informatie over het maken van opstartmedia.

Als u een ESXi-configuratie herstelt naar een niet-oorspronkelijke host terwijl de oorspronkelijke ESXi-host nog is verbonden met vCenter Server, dan moet u de verbinding met deze host verbreken en deze host verwijderen van vCenter Server om onverwachte problemen tijdens het herstel te vermijden. Als u de oorspronkelijke host wilt behouden naast de herstelde host, dan moet u deze opnieuw toevoegen nadat het herstel is voltooid.

De virtuele machines die op de host worden uitgevoerd, worden niet inbegrepen in back-ups van een ESXi-configuratie. Back-up en herstel hiervan kunnen afzonderlijk worden uitgevoerd.

Een ESXi-configuratie herstellen

1. Start de doelmachine op met de opstartmedia.
2. Klik op **Deze machine lokaal beheren**.

3. Klik in het welkomstscherm op **Herstellen**.
4. Klik op **Gegevens selecteren** en klik vervolgens op **Bladeren**.
5. Geef de back-uplocatie op:
   - Blader naar de map onder **Lokale mappen** of **Netwerkmappen**.

   Klik op **OK** om uw selectie te bevestigen.
6. Ga naar **Weergeven** en selecteer **ESXi-configuraties**.
7. Selecteer de back-up waaruit u gegevens wilt herstellen. Geef desgevraagd het wachtwoord voor de back-up op.
8. Klik op **OK**.
9. Ga naar **Schijven voor gebruik in nieuwe gegevensopslag** en voer een van de volgende handelingen uit:
   - Ga naar **ESXi herstellen naar** en selecteer de schijf waar de hostconfiguratie wordt hersteld. Als u de configuratie herstelt naar de oorspronkelijke host, wordt standaard de oorspronkelijke schijf geselecteerd.
   - [Optioneel] Ga naar **Gebruiken voor nieuwe gegevensopslag** en selecteer de schijven waar de nieuwe gegevensopslag wordt gemaakt. Let op: alle gegevens op de geselecteerde schijven gaan verloren. Als u de virtuele machines in de bestaande gegevensopslag wilt behouden, selecteert u geen enkele schijf.
10. Als er schijven zijn geselecteerd voor nieuwe gegevensopslag, selecteert u welke methode moet worden gebruikt voor het maken van de gegevensopslag. De gewenste methode kunt u kiezen in de optie **Nieuwe gegevensopslag maken**: **Eén gegevensopslag maken per schijf** of **Eén gegevensopslag maken op alle geselecteerde hardeschijfstations**.
11. [Optioneel] In **Netwerktoewijzing** wijzigt u het resultaat van de automatische toewijzing van de virtuele switches in de back-up en stelt u deze in op fysieke netwerkadapters.
12. [Optioneel] Klik op **Herstelopties** om aanvullende instellingen op te geven.
13. Klik op **OK** om de herstelbewerking te starten.

Herstelopties

Als u de herstelopties wilt wijzigen, klikt u op **Herstelopties** wanneer u de herstelbewerking configureert.

Beschikbaarheid van de herstelopties

Welke herstelopties beschikbaar zijn, hangt af van het volgende:

- De omgeving van de agent waarmee de herstelbewerking wordt uitgevoerd (Windows, Linux, macOS of opstartmedia).
- Het type gegevens dat wordt hersteld (schijven, bestanden, virtuele machines, applicatiegegevens).

De volgende tabel bevat een overzicht van de beschikbare herstelopties.

	Schijven			Bestanden				Virtuele machines	SQL en Exchange
	Windows	Linux	Opstartmedia	Windows	Linux	macOS	Opstartmedia	ESXi, Hyper-V en Virtuozzo	Windows
Back-up valideren	+	+	+	+	+	+	+	+	+
Opstartmodus	+	-	-	-	-	-	-	+	-
Datum en tijd voor bestanden	-	-	-	+	+	+	+	-	-
Foutafhandeling	+	+	+	+	+	+	+	+	+
Uitgesloten bestanden	-	-	-	+	+	+	+	-	-
Beveiliging op bestandsniveau	-	-	-	+	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-
Volledig pad herstellen	-	-	-	+	+	+	+	-	-
Koppelpunten	-	-	-	+	-	-	-	-	-
Prestaties	+	+	-	+	+	+	-	+	+
Aangepaste opdrachten	+	+	-	+	+	+	-	+	+
SID wijzigen	+	-	-	-	-	-	-	-	-
Energiebeheer van VM's	-	-	-	-	-	-	-	+	-
Windows-gebeurtenislogboek	+	-	-	+	-	-	-	Alleen Hyper-V	+

Back-up valideren

Met deze optie definieert u of u een back-up wilt laten valideren voordat u gegevens van de back-up gaat herstellen, zodat u zeker weet dat de back-up niet is beschadigd. Deze bewerking wordt uitgevoerd door de beveiligingsagent.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Zie "Controlesomverificatie" (p. 232) voor meer informatie over validatie via controlesomverificatie.

Opmerking
Validatie is mogelijk niet beschikbaar wanneer u een back-up maakt naar de cloudopslag. Dit hangt af van de instellingen die zijn gekozen door uw serviceprovider.

Opstartmodus

Deze optie is effectief bij het herstellen van een fysieke of een virtuele machine vanaf een back-up op schijfniveau die een Windows-besturingssysteem bevat.

Met deze optie kunt u de opstartmodus (BIOS of UEFI) selecteren die u voor Windows wilt gebruiken na het herstel. Als de opstartmodus van de oorspronkelijke machine verschilt van de geselecteerde opstartmodus, gebeurt het volgende:

- De schijf waarnaar u het systeemvolume wilt herstellen, wordt geïnitialiseerd volgens de geselecteerde opstartmodus (MBR voor BIOS, GPT voor UEFI).
- Het Windows-besturingssysteem wordt aangepast voor gebruik van de geselecteerde opstartmodus.

De vooraf ingestelde waarde is: **Zoals op de doelmachine.**

U kunt een van de volgende opties selecteren:

- **Zoals op de doelmachine**
  De agent die op de doelmachine wordt uitgevoerd, detecteert de opstartmodus die momenteel door Windows wordt gebruikt en voert de aanpassingen uit volgens de gedetecteerde opstartmodus.
  Dit is de veiligste waarde die automatisch resulteert in een opstartbaar systeem, tenzij de onderstaande beperkingen van toepassing zijn. Aangezien de optie **Opstartmodus** ontbreekt voor opstartmedia, gedraagt de agent op media zich altijd alsof deze waarde is gekozen.
- **Zoals op de machine waarvan een back-up is gemaakt**
  De agent die op de doelmachine wordt uitgevoerd, leest de opstartmodus vanaf de back-up en voert de aanpassingen uit volgens deze opstartmodus. Hierdoor kunt u een systeem herstellen op een andere machine (zelfs als deze machine een andere opstartmodus gebruikt) en vervolgens de schijf vervangen in de machine waarvan een back-up is gemaakt.
- **BIOS**

De agent die op de doelmachine wordt uitgevoerd, voert de aanpassingen voor het gebruik van BIOS uit.

- **UEFI**

  De agent die op de doelmachine wordt uitgevoerd, voert de aanpassingen voor het gebruik van UEFI uit.

Wanneer een instelling wordt gewijzigd, wordt de procedure voor het toewijzen van schijven herhaald. Dit kan enige tijd duren.

Aanbevelingen

Als u Windows wilt overzetten tussen UEFI en BIOS:

- Herstel de volledige schijf waar het systeemvolume zich bevindt. Als u alleen het systeemvolume boven op een bestaand volume herstelt, kan de agent de doelschijf niet correct initialiseren.
- Vergeet niet dat BIOS niet meer dan 2 TB aan schijfruimte toelaat.

Beperkingen

- Overzetten tussen UEFI en BIOS wordt ondersteund voor:
  - 64-bits Windows-besturingssystemen vanaf Windows 7
  - 64-bits Windows Server-besturingssystemen vanaf Windows Server 2008 SP1
- Het overzetten tussen UEFI en BIOS wordt niet ondersteund als de back-up is opgeslagen op een tapeapparaat.

Wanneer het overzetten van een systeem tussen UEFI en BIOS niet wordt ondersteund, gedraagt de agent zich alsof de instelling **Zoals op de machine waarvan een back-up is gemaakt** is geselecteerd. Als de doelmachine zowel UEFI als BIOS ondersteunt, moet u de opstartmodus die overeenkomt met de oorspronkelijke machine, handmatig inschakelen. Anders start het systeem niet op.

Datum en tijd voor bestanden

Deze optie is alleen effectief bij het herstellen van bestanden.

Met deze optie bepaalt u of de datum en tijd van de bestanden in de back-up wordt hersteld of dat de huidige datum en tijd aan de bestanden worden toegewezen.

Als deze optie is ingeschakeld, worden de huidige datum en tijd toegewezen aan de bestanden.

De vooraf ingestelde waarde is: **Ingeschakeld**.

Foutafhandeling

Met deze opties kunt u opgeven hoe eventuele fouten worden afgehandeld tijdens een herstelbewerking.

Opnieuw proberen als er een fout optreedt

De vooraf ingestelde waarde is: **Ingeschakeld. Aantal pogingen: 30. Interval tussen pogingen: 30 seconden.**

Wanneer een herstelbare fout optreedt, wordt automatisch geprobeerd de mislukte bewerking opnieuw uit te voeren. U kunt het tijdsinterval en het aantal pogingen instellen. Er worden geen pogingen meer ondernomen zodra de bewerking lukt OF wanneer het opgegeven aantal pogingen is bereikt, al naar gelang van wat het eerste gebeurt.

Geen berichten en dialoogvensters weergeven tijdens de verwerking (silent mode)

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Wanneer silent mode is ingeschakeld, worden waar mogelijk automatisch alle situaties verwerkt waarvoor gebruikersinteractie is vereist. Als een bewerking niet kan worden voortgezet zonder gebruikersinteractie, dan mislukt de bewerking. In het bewerkingslogboek worden de details van de bewerking weergegeven, met inbegrip van eventuele fouten.

Systeeminformatie opslaan als opnieuw opstarten mislukt

Deze optie is effectief voor herstel van een schijf of volume naar een fysieke machine met Windows of Linux.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Wanneer deze optie is ingeschakeld, kunt u een map opgeven op de lokale schijf (inclusief flashstations of HDD-stations die zijn verbonden met de doelmachine) of op een netwerkshare waar de logbestanden, systeeminformatiebestanden en crashdump-bestanden worden opgeslagen. Dit bestand kan door medewerkers van technische ondersteuning worden gebruikt om het probleem te identificeren.

Uitgesloten bestanden

Deze optie is alleen effectief bij het herstellen van bestanden.

Met deze optie definieert u welke bestanden en mappen worden overgeslagen tijdens het herstelproces en dus niet worden vermeld in de lijst met herstelde items.

Opmerking
Met uitsluitingen overschrijft u de selectie van gegevensitems die moeten worden hersteld. Als u bijvoorbeeld het bestand MyFile.tmp selecteert om te herstellen maar alle .tmp-bestanden uitsluit, wordt het bestand MyFile.tmp niet hersteld.

Beveiliging op bestandsniveau

Deze optie is effectief bij het herstellen van bestanden uit back-ups van met NTFS geformatteerde volumes op schijf- en bestandsniveau.

Met deze optie definieert u of NTFS-machtigingen voor bestanden worden hersteld samen met de bestanden.

De vooraf ingestelde waarde is: **Ingeschakeld**.

U kunt kiezen of u de machtigingen wilt herstellen of dat de bestanden de NTFS-machtigingen overnemen van de map waarin ze zijn hersteld.

Flashback

Deze optie werkt wanneer u schijven en volumes herstelt op fysieke en virtuele machines, behalve voor Mac.

Deze optie werkt alleen als volume-indeling van de schijf die wordt hersteld, precies overeenkomt met die van de doelschijf.

Als de optie is ingeschakeld, worden alleen de verschillen tussen de gegevens in de back-up en de gegevens op de doelschijf hersteld. Hierdoor worden fysieke en virtuele machines sneller hersteld. De gegevens worden vergeleken op blokniveau.

Wanneer u een fysieke machine herstelt, is de vooraf ingestelde waarde: **Uitgeschakeld**.

Wanneer u een virtuele machine herstelt, is de vooraf ingestelde waarde: **Ingeschakeld**.

Volledig pad herstellen

Deze optie is alleen effectief wanneer u gegevens herstelt vanaf een back-up op bestandsniveau.

Als deze optie is ingeschakeld, wordt het volledige pad naar het bestand opnieuw gemaakt op de doellocatie.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Koppelpunten

Deze optie is alleen effectief in Windows voor het herstellen van gegevens vanaf een back-up op bestandsniveau.

Schakel deze optie in als u bestanden en mappen wilt herstellen die zijn opgeslagen op de gekoppelde volumes en waarvan een back-up is gemaakt met de ingeschakelde optie Koppelpunten.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Deze optie is alleen effectief wanneer u voor de herstelbewerking een map selecteert die hoger in de maphiërarchie is dan het koppelpunt. Als u voor de herstelbewerking mappen binnen het koppelpunt of het koppelpunt zelf selecteert, worden de geselecteerde items hersteld, ongeacht de waarde van de optie **Koppelpunten**.

Opmerking
Let op: als het volume niet is gekoppeld op het moment van herstel, worden de gegevens rechtstreeks hersteld naar de map die het koppelpunt was op het moment van de back-up.

Prestaties

Met deze optie definieert u de prioriteit van het herstelproces in het besturingssysteem.

De beschikbare instellingen zijn: **Laag**, **Normaal**, **Hoog**.

De vooraf ingestelde waarde is: **Normaal**.

De prioriteit van een proces dat in een systeem wordt uitgevoerd, bepaalt hoeveel CPU- en systeembronnen aan het proces worden toegewezen. Als u de prioriteit voor herstelbewerkingen verlaagt, komen er meer resources vrij voor andere applicaties. Als u de prioriteit voor herstelbewerkingen verhoogt, wordt het herstelproces mogelijk versneld doordat het besturingssysteem wordt gevraagd meer resources toe te wijzen aan de applicatie waarmee de herstelbewerking wordt uitgevoerd. Het resultaat hiervan hangt echter af van het totale CPU-gebruik en andere factoren zoals I/O-snelheid van de schijf of netwerkverkeer.

Aangepaste opdrachten

Met deze optie kunt u definiëren welke opdrachten automatisch worden uitgevoerd vóór en na het gegevensherstel.

Voorbeeld van het gebruik van de aangepaste opdrachten:

- Start de opdracht **Checkdisk** voor het vinden en verhelpen van fouten van het logische bestandssysteem, fysieke fouten en beschadigde sectoren die moeten worden gestart voordat de herstelbewerking begint of nadat het herstel is voltooid.

Interactieve opdrachten worden niet ondersteund, dat wil zeggen opdrachten waarvoor gebruikersinvoer is vereist (bijvoorbeeld 'pause').

Een opdracht na herstel wordt niet uitgevoerd als de herstelbewerking wordt voortgezet door opnieuw op te starten.

Opdracht vóór herstel

Een opdracht/batchbestand opgeven dat moet worden uitgevoerd voordat het herstelproces begint

1. Schakel de optie **Een opdracht uitvoeren vóór de herstelbewerking** in.
2. Ga naar het veld **Opdracht...** en typ een opdracht of blader naar een batchbestand. Interactieve opdrachten worden niet ondersteund, dat wil zeggen opdrachten waarvoor gebruikersinvoer is vereist (bijvoorbeeld 'pause').
3. Geef in het veld **Werkmap** een pad op naar een directory waar de opdracht/het batchbestand wordt uitgevoerd.

4. Geef in het veld **Argumenten** indien nodig de argumenten op voor het uitvoeren van de opdracht.
5. Afhankelijk van het resultaat dat u wilt verkrijgen, selecteert u de gewenste opties zoals beschreven in de volgende tabel.
6. Klik op **Gereed**.

Selectievakje	**Inschakelen**			
De herstelbewerking afkeuren als het uitvoeren van de opdracht mislukt*	Ingeschakeld	Uitgeschakeld	Ingeschakeld	Uitgeschakeld
Geen herstelbewerking uitvoeren voordat de opdracht volledig is uitgevoerd	Ingeschakeld	Ingeschakeld	Uitgeschakeld	Uitgeschakeld
Resultaat				
	Vooraf ingesteld Voer de herstelbewerking alleen uit wanneer de opdracht is uitgevoerd. Keur de herstelbewerking af als het uitvoeren van de opdracht is mislukt.	Voer de herstelbewerking uit wanneer de opdracht is uitgevoerd, ongeacht het resultaat van de uitvoering.	N.v.t.	Voer de herstelbewerking gelijktijdig uit met de uitvoering van de opdracht, ongeacht het resultaat van de uitvoering van de opdracht.

* Een opdracht wordt als mislukt beschouwd als de afsluitcode niet gelijk is aan nul.

Opdrachten na herstel

Een opdracht/uitvoerbaar bestand opgeven om uit te voeren nadat de herstelbewerking is voltooid

1. Schakel de optie **Een opdracht uitvoeren na de herstelbewerking** in.
2. Ga naar het veld **Opdracht...** en typ een opdracht of blader naar een batchbestand.
3. Geef in het veld **Werkmap** een pad op naar een directory waar de opdracht/het batchbestand wordt uitgevoerd.
4. Geef in het veld **Argumenten** indien nodig de argumenten op voor het uitvoeren van de opdracht.

5. Schakel het selectievakje **De herstelbewerking afkeuren als het uitvoeren van de opdracht mislukt** in als een goede uitvoering van de opdracht essentieel voor u is. De opdracht wordt als mislukt beschouwd als de afsluitcode niet gelijk is aan nul. Als de opdracht niet correct wordt uitgevoerd, wordt de herstelstatus ingesteld op **Fout**.

   Wanneer het selectievakje niet is ingeschakeld, dan heeft het resultaat van de uitvoering van de opdracht geen invloed op de al dan niet correcte uitvoering van de herstelbewerking. U kunt het resultaat van de uitvoering van de opdracht bijhouden via het tabblad **Activiteiten**.
6. Klik op **Gereed**.

Opmerking
Een opdracht na herstel wordt niet uitgevoerd als de herstelbewerking wordt voortgezet door opnieuw op te starten.

SID wijzigen

Deze optie is effectief wanneer u Windows 8.1/Windows Server 2012 R2 of eerder herstelt.

Deze optie werkt niet wanneer het herstel naar een virtuele machine wordt uitgevoerd met Agent voor VMware, Agent voor Hyper-V of Agent voor Scale Computing HC3 of Agent voor oVirt.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

De software kan een unieke beveiligings-id (computer-SID) voor het herstelde besturingssysteem genereren. Deze optie is alleen nodig om de goede werking te waarborgen voor software van derden de afhangen van de computer SID.

Het wijzigen van een SID op een geïmplementeerd of hersteld systeem wordt niet officieel ondersteund door Microsoft. U gebruikt deze optie dus op eigen risico.

Energiebeheer van VM's

Deze opties werken alleen wanneer het herstel naar een virtuele machine wordt uitgevoerd met Agent voor VMware, Agent voor Hyper-V, Agent voor Virtuozzo, Agent voor Scale Computing HC3 of Agent voor oVirt.

Virtuele doelmachines uitschakelen wanneer het herstelproces wordt gestart

De vooraf ingestelde waarde is: **Ingeschakeld**.

Herstel naar een bestaande virtuele machine is niet mogelijk als de machine online is, dus de machine wordt automatisch uitgeschakeld wanneer het herstel begint. De verbinding van gebruikers met de machine wordt verbroken en niet-opgeslagen gegevens gaan verloren.

Schakel het selectievakje voor deze optie uit als u virtuele machines liever handmatig uitschakelt voordat het herstel begint.

De virtuele doelmachine inschakelen wanneer de herstelbewerking is voltooid

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Wanneer een machine vanaf een back-up wordt hersteld naar een andere machine, wordt mogelijk de replica van de bestaande machine weergegeven op het netwerk. De veiligste methode is om de herstelde virtuele machine handmatig in te schakelen, maar u moet wel de nodige voorzorgsmaatregelen nemen.

Windows-gebeurtenislogboek

Deze optie is alleen effectief in Windows-besturingssystemen.

Met deze optie definieert u of gebeurtenissen van de herstelbewerkingen door agenten worden geregistreerd in het Toepassingsgebeurtenislogboek van Windows (bekijk dit logboek door eventvwr.exe uit te voeren of selecteer **Configuratiescherm** > **Systeembeheer** > **Logboeken**). U kunt filteren welke gebeurtenissen u wilt laten registreren.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Bewerkingen met back-ups

Het tabblad Back-upopslag

Het tabblad **Back-upopslag** biedt toegang tot alle back-ups, waaronder back-ups van offline machines, back-ups van machines die niet meer zijn geregistreerd in de Cyber Protection-service, back-ups in openbare clouds zoals Microsoft Azure en zwevende back-ups[1].

Back-ups gemaakt via `acrocmd`, worden gemarkeerd als zwevend. Back-ups gemaakt in versie 12.5 van het product worden ook aangeduid als zwevend.

Opmerking
Let op: voor zwevende back-ups worden ook kosten in rekening gebracht.

Back-ups die zijn opgeslagen in een gedeelde locatie (zoals een SMB- of NFS-share), zijn zichtbaar voor alle gebruikers met leesmachtiging voor de locatie.

In Windows worden de toegangsrechten voor back-upbestanden overgenomen van de bovenliggende map. Daarom raden we aan om de leesrechten voor deze map te beperken.

In de cloudopslag hebben gebruikers alleen toegang tot hun eigen back-ups.

Door de cloudopslag te selecteren voor een account kunnen beheerders back-ups naar de cloud bekijken namens elk account dat hoort bij de betreffende eenheid of het betreffende bedrijf en de onderliggende groepen daarvan. Klik op **Wijzigen** in de rij **Machine waarmee u wilt bladeren** om het apparaat te selecteren dat u wilt gebruiken om gegevens op te halen uit de cloud. Op het tabblad **Back-upopslag** worden de back-ups weergegeven van alle machines die ooit zijn geregistreerd voor het geselecteerde account.

[1] Een zwevende back-up is een back-up die niet meer is gekoppeld aan een beschermingsschema.

Back-ups gemaakt met Agent voor Microsoft 365 in de *cloud* en back-ups van Google Workspace-gegevens worden niet weergegeven in de **Cloudopslag** locatie, maar in een afzonderlijk gedeelte dat **Back-ups van cloudtoepassingen** wordt genoemd.

Back-uplocaties die worden gebruikt in beschermingsschema's, worden automatisch toegevoegd aan het tabblad **Back-upopslag**. Als u een aangepaste map (bijvoorbeeld een verwisselbaar USB-apparaat) wilt toevoegen aan de lijst met back-uplocaties, klikt u op **Bladeren** en geeft u het pad naar de map op.

Als u enkele back-ups hebt toegevoegd of verwijderd met behulp van bestandsbeheer, klikt u op het tandwielpictogram naast de naam van de locatie en klikt u vervolgens op **Vernieuwen**.

Waarschuwing!
Probeer de back-upbestanden niet handmatig te bewerken, omdat dit kan leiden tot beschadiging van bestanden en de back-ups onbruikbaar kan maken. Ook raden wij u aan om de back-upreplicatie te gebruiken in plaats van back-upbestanden handmatig te verplaatsen.

Een back-uplocatie (met uitzondering van de cloudopslag) wordt niet meer weergegeven op het tabblad **Back-upopslag** als alle machines waarvan ooit een back-up is gemaakt op die locatie, worden verwijderd uit de Cyber Protection-service. Op die manier hoeft u niet te betalen voor de back-ups die op deze locatie zijn opgeslagen. Zodra een back-up wordt gemaakt naar deze locatie, wordt de locatie opnieuw toegevoegd, samen met alle back-ups die erin zijn opgeslagen.

Op het tabblad **Back-upopslag** kunt u back-ups in de lijst filteren met behulp van de volgende criteria:

- **Alleen met forensische gegevens**: alleen back-ups met forensische gegevens worden weergegeven.
- **Alleen back-ups vóór update gemaakt met patchbeheer**: alleen back-ups die zijn gemaakt tijdens patchbeheer voordat de patch is geïnstalleerd, worden weergegeven.

Een herstelpunt selecteren via het tabblad Back-upopslag:

1. Selecteer op het tabblad **Back-upopslag** de locatie waar de back-ups worden opgeslagen.
   Alle back-ups die uw account mag bekijken in de geselecteerde locatie, worden weergegeven. De back-ups zijn gecombineerd in groepen. De namen van de groepen zijn gebaseerd op de volgende sjabloon:
   `<naam machine> – <naam beschermingsschema>`
2. Selecteer een groep waaruit u gegevens wilt herstellen.
3. [Optioneel] Klik op **Wijzigen** naast **Machine waarmee u wilt bladeren** en selecteer vervolgens een andere machine. Voor het bladeren door bepaalde back-ups zijn specifieke agenten vereist. Als u wilt bladeren door de back-ups van Microsoft SQL Server-databases moet u bijvoorbeeld een machine met Agent voor SQL selecteren.

Belangrijk
De **Machine waarmee u wilt bladeren** wordt gebruikt als standaardbestemming voor herstel vanaf back-ups van een fysieke machine. Wanneer u een herstelpunt selecteert en op **Herstellen** klikt, controleer dan goed of **Doelmachine** correct is ingesteld en of u zeker weet dat u naar deze specifieke machine wilt herstellen. Als u de herstelbestemming wilt wijzigen, geeft u een andere machine op in **Machine waarmee u wilt bladeren**.

4. Klik op **Back-ups weergeven**.
5. Selecteer het herstelpunt.

Een locatie voor een back-up toevoegen

Opmerking
Deze bewerking is alleen beschikbaar als u een online agent hebt.

Ga naar het tabblad **Back-upopslag** en klik op **Locatie toevoegen**.

Selecteer een locatie in een van de volgende locatietypen en klik vervolgens op **Gereed**:

- Lokale map
- Netwerkmap
- Secure Zone
- NFS-map
- Openbare cloud

Volumes koppelen vanaf een back-up

Als u volumes koppelt vanaf een back-up op schijfniveau, kunt u de volumes op dezelfde manier openen als fysieke schijven.

Als u volumes koppelt in de modus lezen/schrijven, kunt u de back-upinhoud wijzigen. U kunt dan bestanden en mappen opslaan, verplaatsen, maken en verwijderen en u kunt uitvoerbare bestanden bestaande uit één bestand uitvoeren. In deze modus wordt een incrementele back-up gemaakt van de wijzigingen die u aanbrengt in de back-upinhoud. Geen enkele van de daaropvolgende back-ups zal deze wijzigingen bevatten.

Vereisten

- Deze functionaliteit is alleen beschikbaar via Verkenner in Windows.
- Agent voor Windows moet zijn geïnstalleerd op de machine waarop de koppelingsbewerking wordt uitgevoerd.
- Het bestandssysteem waarvan u een back-up maakt, moet worden ondersteund door de Windows-versie op de machine.

- De back-up moet zijn opgeslagen in een lokale map op een netwerkshare (SMB/CIFS) of in Secure Zone.

Gebruiksscenario's

- Gegevens delen

  Gekoppelde volumes kunnen gemakkelijk worden gedeeld via het netwerk.
- Snelle oplossing tijdens databaseherstel

  Koppel een volume met een SQL-database van een machine die recentelijk een foutstatus had. Hierdoor krijgt u toegang tot de database totdat de machine met de foutstatus is hersteld. Deze procedure kan ook worden gebruikt voor gedetailleerd herstel van Microsoft SharePoint-gegevens met SharePoint Explorer.
- Virus offline verwijderen

  Als een machine is geïnfecteerd, kunt u de back-up van die machine koppelen, deze opschonen met een antivirusprogramma (of de meest recente, niet-geïnfecteerde back-up zoeken) en de machine dan herstellen vanaf deze back-up.
- Controleren op fouten

  Als herstel met formaatwijziging van het volume mislukt, is de oorzaak mogelijk een fout in het bestandssysteem waarvan de back-up is gemaakt. Koppel de back-up in de modus lezen/schrijven. Gebruik vervolgens de opdracht `chkdsk /r` om het gekoppelde volume te controleren op fouten. Wanneer de fouten zijn verholpen en er een nieuwe, incrementele back-up is gemaakt, herstelt u het systeem vanaf deze back-up.

Een volume koppelen vanaf een back-up

1. Gebruik Verkenner om naar de locatie van de back-up te bladeren.
2. Dubbelklik op het back-upbestand. De bestandsnamen zijn gebaseerd op de volgende sjabloon:

   `<naam machine> - <GUID beschermingsschema>`
3. Als de back-up is versleuteld, voert u het versleutelingswachtwoord in. Anders kunt u deze stap overslaan.

   De herstelpunten worden weergegeven in Verkenner.
4. Dubbelklik op het herstelpunt.

   De volumes waarvan een back-up is gemaakt, worden weergegeven in Verkenner.

   Opmerking
   Dubbelklik op een volume om door de inhoud te bladeren. Bestanden en mappen van de back-up kunt u kopiëren naar elke map in het bestandssysteem.
5. Klik met de rechtermuisknop op een volume dat u wilt koppelen en selecteer een van de volgende opties:

a. **Koppelen**

Opmerking
Alleen de laatste back-up in het archief (back-upketen) kan in de lees- en schrijfmodus worden gekoppeld.

b. **Koppelen in de modus alleen-lezen**.

6. Als de back-up is opgeslagen op een netwerkshare, geeft u de toegangsreferenties op. Anders kunt u deze stap overslaan.
   Het geselecteerde volume wordt gekoppeld. De eerste ongebruikte letter wordt toegewezen aan het volume.

Een volume ontkoppelen

1. Gebruik Verkenner om te bladeren naar **Computer** (**Deze pc** in Windows 8.1 en later).
2. Klik met de rechtermuisknop op het gekoppelde volume.
3. Klik op **Ontkoppelen**.
4. [Optioneel] Als het volume is gekoppeld in de modus lezen/schrijven, en de inhoud is gewijzigd, selecteert u of u een incrementele back-up met de wijzigingen wilt maken. Anders kunt u deze stap overslaan.

Het geselecteerde volume wordt ontkoppeld.

Back-ups valideren ...

Door een back-up te valideren verifieert u dat u de gegevens ervan kunt herstellen. Zie "Validatie" (p. 228) voor meer informatie over deze bewerking.

Opmerking
Deze functionaliteit is beschikbaar in klanttenants voor wie het quotum **Advanced Backup - Servers** of **Advanced Backup - NAS** is ingeschakeld als onderdeel van het Advanced Backup-pakket.

Een back-up valideren

1. Selecteer de workload waarvan een back-up is gemaakt.
2. Klik op **Herstel**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.
   Als de workload offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:
   - Als de back-uplocatie cloudopslag of gedeelde opslag is (dat wil zeggen dat andere agents hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een doelworkload die online is en selecteert u vervolgens een herstelpunt.

- Selecteer een herstelpunt op het tabblad Back-upopslag. Zie "Het tabblad Back-upopslag" (p. 559) voor meer informatie over de back-ups daar.

4. Klik op het tandwielpictogram en klik vervolgens op **Valideren**.
5. Selecteer de agent die de validatie gaat uitvoeren.
6. Selecteer de validatiemethode.
7. Als de back-up is versleuteld, geeft u het versleutelingswachtwoord op.
8. Klik op **Starten**.

Back-ups exporteren

Met de exportbewerking wordt een zelfvoorzienende kopie van een back-up gemaakt op de door u opgegeven locatie. De oorspronkelijke back-up blijft onveranderd. U kunt de exportfunctie voor back-ups gebruiken om een specifieke back-up te scheiden van een reeks incrementele en differentiële back-ups als u bijvoorbeeld een snel herstel wilt uitvoeren of wilt schrijven op verwisselbare of afneembare media, of voor andere doeleinden.

Opmerking
Deze functionaliteit is beschikbaar in klanttenants voor wie het quotum **Advanced Backup - Servers** of **Advanced Backup - NAS** is ingeschakeld als onderdeel van het Advanced Backup-pakket.

Een exportbewerking resulteert is altijd in een volledige back-up. Als u de hele back-upreeks naar een andere locatie wilt repliceren en meerdere herstelpunten wilt behouden, gebruikt u een back-upreplicatieschema. Zie "Back-upreplicatie" (p. 225) voor meer informatie over dit schema.

Het geëxporteerde back-upbestand krijgt dezelfde naam als de oorspronkelijke back-up, behalve het volgnummer. Als meerdere back-ups van dezelfde back-upreeks naar dezelfde locatie worden geëxporteerd, wordt een viercijferig volgnummer toegevoegd aan de bestandsnamen van alle back-ups, met uitzondering van de eerste.

De versleutelingsinstellingen en het wachtwoord van de oorspronkelijke back-up worden overgenomen in de geëxporteerde back-up. Wanneer u een versleutelde back-up exporteert, moet u het wachtwoord opgeven.

Een back-up exporteren

1. Selecteer de workload waarvan een back-up is gemaakt.
2. Klik op **Herstel**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de workload offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:
   - Als de back-uplocatie cloudopslag of gedeelde opslag is (dat wil zeggen dat andere agents hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een doelworkload die

online is en selecteert u vervolgens een herstelpunt.
- Selecteer een herstelpunt op het tabblad Back-upopslag. Zie "Het tabblad Back-upopslag" (p. 559) voor meer informatie over de back-ups daar.

4. Klik op het tandwielpictogram en klik vervolgens op **Exporteren**.
5. Selecteer de agent die de exportbewerking uitvoert.
6. Als de back-up is versleuteld, geeft u het versleutelingswachtwoord op. Anders kunt u deze stap overslaan.
7. Geef de bestemming op voor de export.
8. Klik op **Starten**.

Back-ups verwijderen

Een back-uparchief bevat een of meer back-ups. U kunt specifieke back-ups (herstelpunten) in een archief verwijderen of het hele archief.

Als u het back-uparchief verwijdert, worden alle back-ups in het archief ook verwijderd. Als u alle back-ups van een workload verwijdert, worden ook de back-uparchieven verwijderd die deze back-ups bevatten.

U kunt back-ups verwijderen via de Cyber Protect-console (tabblad **Apparaten** en tabblad **Back-upopslag**). U kunt back-ups ook verwijderen uit de cloudopslag via de Webherstel-console.

Waarschuwing!
Als onveranderbare opslag is uitgeschakeld, worden de back-ups van gegevens permanent verwijderd en kunnen deze niet worden hersteld.

Back-ups of back-uparchieven verwijderen

Op het tabblad Apparaten

Deze procedure is alleen van toepassing op online workloads.

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de workloadback-ups die u wilt verwijderen.
3. Klik op **Herstel**.
4. [Als er meerdere back-uplocaties beschikbaar zijn] Selecteer de back-uplocatie.
5. [Als u alle back-ups van de workload wilt verwijderen] Klik op **Alles verwijderen**.
   Als u alle back-ups verwijdert, worden ook de back-uparchieven verwijderd die deze back-ups bevatten.
6. [Als u een specifieke back-up wilt verwijderen] Selecteer de back-up (herstelpunt) die u wilt verwijderen en klik vervolgens op **Acties** > **Verwijderen**.
7. [Bij het verwijderen van alle back-ups] Schakel het selectievakje in en klik vervolgens op **Verwijderen** om te bevestigen.
8. [Als u een specifieke back-up wilt verwijderen] Klik op **Verwijderen** om te bevestigen.

Op het tabblad Back-upopslag

Deze procedure is van toepassing op online en offline workloads.

1. Ga in de Cyber Protect-console naar **Back-upopslag**.
2. Selecteer de locatie waaruit u back-ups wilt verwijderen.
3. Selecteer het back-uparchief waaruit u back-ups wilt verwijderen.
   Voor de archiefnaam wordt de volgende sjabloon gebruikt:
   - Niet-cloud-naar-cloud back-uparchieven: <naam workload> - <naam beschermingsschema>
   - Cloud-naar-cloud back-uparchieven: <gebruikersnaam> of <stationsnaam> of <teamnaam> - <cloudservice> - <naam beschermingsschema>
4. [Als u het volledige back-uparchief wilt verwijderen] Klik op **Verwijderen**.
   Als u een back-uparchief verwijdert, worden alle back-ups in dat archief ook verwijderd.
5. [Als u een specifieke back-up in het back-uparchief wilt verwijderen] Klik op **Back-ups weergeven**.
   a. Selecteer de back-up (herstelpunt) die u wilt verwijderen.
   b. Klik op **Acties** > **Verwijderen**.
6. [Als u een back-uparchief wilt verwijderen] Schakel het selectievakje in en klik vervolgens op **Verwijderen** om te bevestigen.
7. [Als u een specifieke back-up wilt verwijderen] Klik op **Verwijderen** om te bevestigen.

In de Webherstel-console

Deze procedure is alleen van toepassing op back-uparchieven in de cloudopslag.

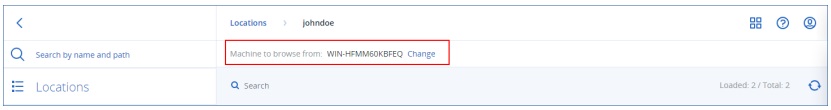
1. In de Cyber Protection-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de workloadback-ups die u wilt verwijderen en klik vervolgens op **Herstel**.
3. [Als er meerdere back-uplocaties beschikbaar zijn] Selecteer de back-uplocatie en klik vervolgens op **Meer herstelbewerkingen**.
4. Klik op **Bestanden downloaden**.
   U wordt omgeleid naar de Webherstel-console.
5. Open de Webherstel-console, ga naar **Machines** en klik op de naam van de workload.
6. Klik onder **Laatste versie** op de datum en klik vervolgens op **Verwijderen**.
   Deze actie is alleen beschikbaar op het niveau van het back-uparchief. U kunt niet inzoomen in het archief en u kunt geen specifieke back-ups uit het archief verwijderen.
7. Klik op **Verwijderen** om te bevestigen.

Back-ups verwijderen buiten de Cyber Protect-console

We raden aan dat u back-ups verwijdert via de Cyber Protect-console. Als u back-ups uit de cloudopslag verwijdert via de Webherstel-console of lokale back-ups verwijdert via bestandsbeheer, moet u de back-uplocatie vernieuwen om de wijzigingen te synchroniseren met de Cyber Protect-console.

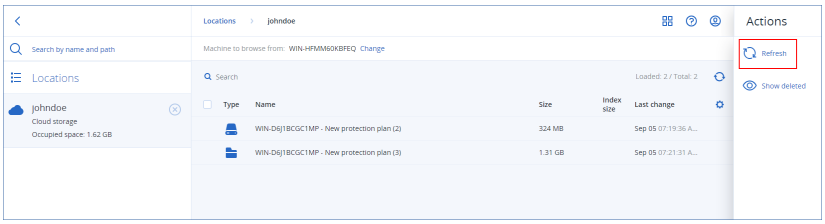
Voorwaarde

- Een online agent die toegang heeft tot de back-uplocatie, moet worden geselecteerd als **Machine waarmee u wilt bladeren** in de Cyber Protect-console.



Een back-uplocatie vernieuwen

1. Ga in de Cyber Protect-console naar **Back-upopslag**.
2. Selecteer de back-uplocatie waarin de verwijderde back-ups waren opgeslagen.
3. Klik in het deelvenster **Acties** op **Vernieuwen**.



De detectie van knelpunten begrijpen

De functie voor knelpuntdetectie helpt u te begrijpen waar u de prestaties kunt verbeteren doordat u ziet welk onderdeel van uw systeem het langzaamst was tijdens een back-up- of herstelproces.

Er zijn *altijd* knelpunten bij elke gegevensoverdracht, maar soms hoeven deze niet te worden opgelost. Uw back-ups zijn misschien al snel genoeg en voldoen perfect aan uw back-upvensters en uw SLA's, dus er is vaak niets dat u daadwerkelijk hoeft op te lossen.

U kunt knelpunten eenvoudig bekijken en volgen op het tabblad **Activiteitgegevens**. Ga in de Cyber Protect-console naar **Controle > Activiteiten** en klik vervolgens op de betreffende activiteit. Zie "Knelpuntdetails weergeven" (p. 569) en "Voor welke workloads, agents en back-uplocaties worden knelpunten weergegeven?" (p. 571) voor meer informatie over het bekijken van knelpunten.

Wat is een knelpunt?

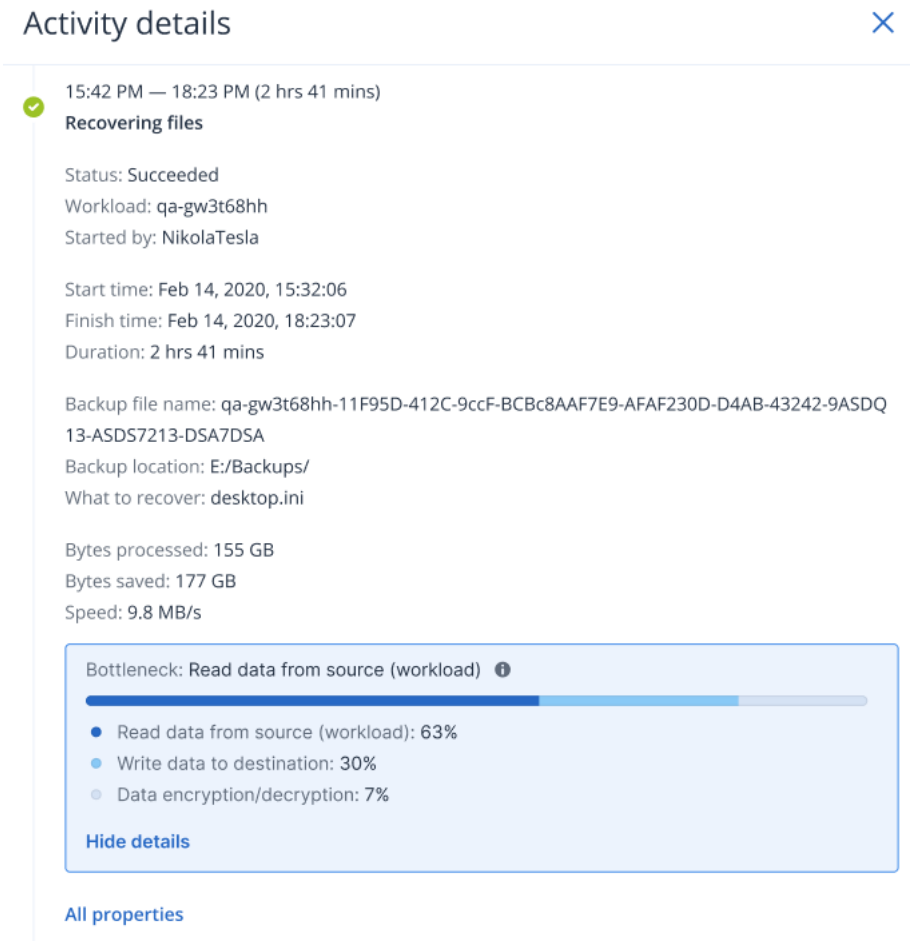
Knelpunten worden doorgaans veroorzaakt door een traag onderdeel in de verwerkingsketen, dat wil zeggen een onderdeel waarop de andere onderdelen wachten.

Met de functie voor knelpuntdetectie kunt u deze trage onderdelen volgen tijdens het back-up- en herstelproces, zodat u begrijpt welke van de volgende typen onderdelen het langzaamst is:

- **Bron**: In één oogopslag kunt u vaststellen of de leessnelheid van de back-up-/herstelbron een knelpunt veroorzaakt.
- **Bestemming**: Krijg inzicht of de schrijfsnelheid naar de bestemming van de back-up-/herstelbewerking van invloed is op de prestaties.
- **Agent**: Zie of de agent de gegevens snel genoeg verwerkt.

Het type knelpunt, of het nu gaat om de bron, de bestemming of de agent, kan op verschillende momenten tijdens de back-up-/herstelactiviteit veranderen. De percentages die worden weergegeven in het gedeelte **Knelpunt** van het tabblad **Activiteitgegevens** hieronder (bijvoorbeeld **Gegevens uit bron lezen (workload): 63%**), vertegenwoordigen het percentage van de tijd waarin dit type knelpunten zijn aangetroffen. In dit geval werd het knelpunt gedurende 63% van de herstelactiviteit veroorzaakt door het lezen van gegevens, dat wil zeggen de lage snelheid waarmee de agent gegevens uit het back-uparchief las.

Verder was het knelpunt gedurende 30% van de tijd te wijten aan de lage snelheid waarmee gegevens naar de herstelbestemming werden geschreven (**Gegevens schrijven naar doel: 30%**).



Opmerking
Het is normaal om knelpuntstatistieken te zien op het tabblad **Activiteitgegevens**. Deze statistieken zijn alleen beschikbaar voor taken die langer dan een minuut duren.

Knelpunten verminderen

Zoals hierboven vermeld, geeft de functie voor knelpuntdetectie inzicht in de gegevensstromen voor *lezen* en *schrijven* tussen de onderdelen van de back-up. De statistieken voor *lezen* hebben betrekking op de gegevensstroom van de gegevensbron naar de agent die de back-up-

/herstelbewerking uitvoert, en de statistieken voor *schrijven* op de gegevensstroom tussen de agent en het back-uparchief (de bestemming).

Als u knelpunten wilt verminderen en de prestaties van de gegevensstroom voor lezen/schrijven wilt verbeteren, moet u het kanaal tussen de agent en de gegevensbron/het back-uparchief analyseren. U kunt bijvoorbeeld proberen een benchmark voor uw harde schijven te definiëren als de agent een back-up van lokale bestanden maakt.

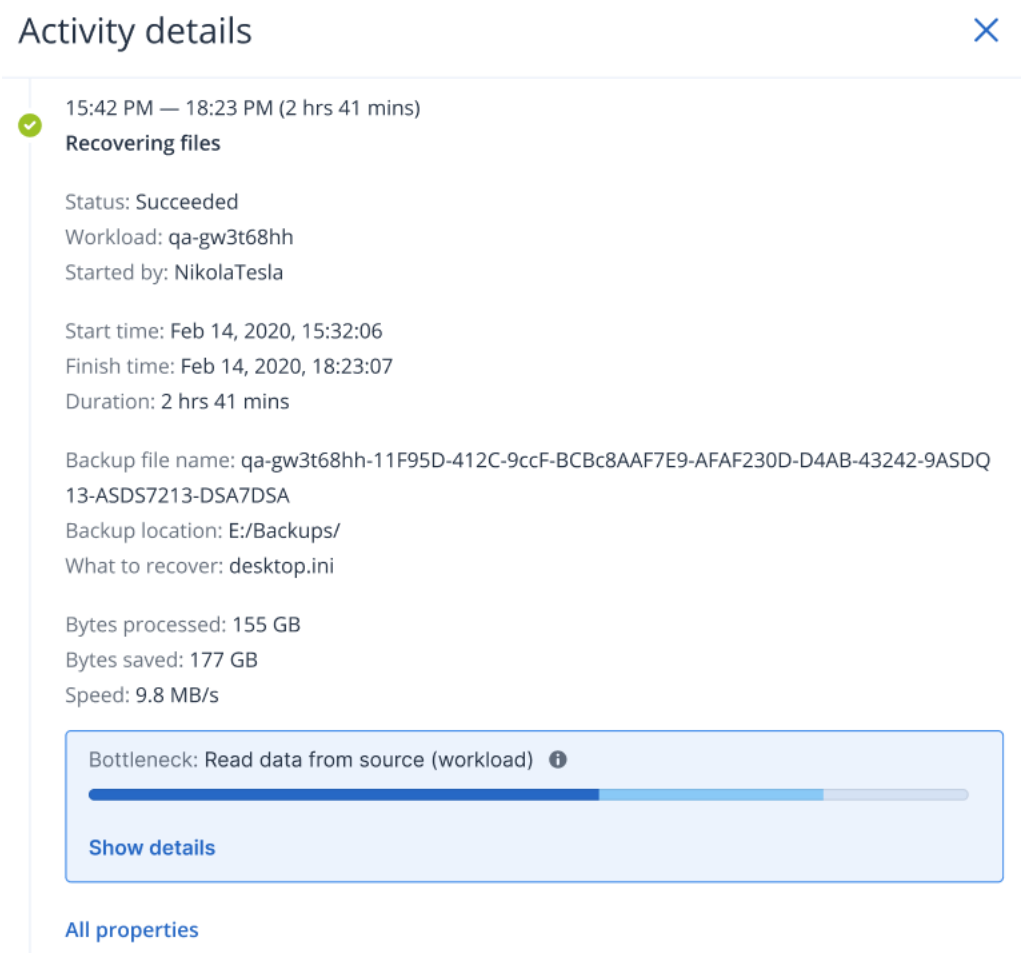
Knelpuntdetails weergeven

U kunt gedetecteerde knelpunten bekijken voor elk type back-up-, back-upreplicatie- of herstelproces (naar elk type doelmap of locatie), inclusief back-ups van (virtuele) machines en back-ups van bestanden/mappen. U kunt ook knelpunten bekijken voor replicatie- en failbackactiviteiten van virtuele machines.

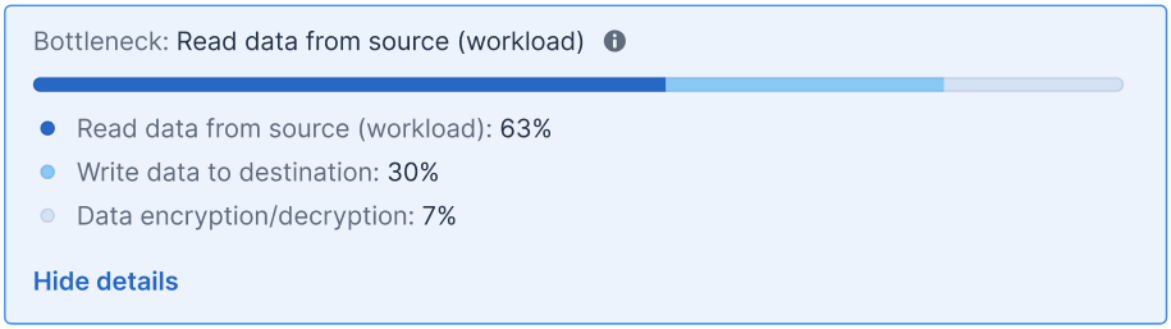
Zie "De detectie van knelpunten begrijpen" (p. 567) voor meer informatie over de definitie en kernconcepten van knelpunttypen.

De knelpuntdetails bekijken:

1. Ga in de Cyber Protect-console naar **Controle > Activiteiten**.
2. Klik op de betreffende activiteit.
   Op het tabblad **Activiteitgegevens** wordt het gedeelte **Knelpunt** in het blauw weergegeven.



3. Klik op **Details weergeven** om de meest voorkomende knelpunten te bekijken tijdens de back-up- en herstelbewerking.
   Het gedeelte **Knelpunt** kan worden uitgevouwen om een samenvatting van de betreffende knelpunttypen te zien.



   In het bovenstaande voorbeeld werd het knelpunt, dat 63% van de totale tijd van de bewerking in beslag nam, veroorzaakt door de bewerking *Lezen* (uitgevoerd door de agent).

Opmerking
De knelpuntwaarden worden elke minuut dynamisch bijgewerkt zolang de betreffende activiteit wordt uitgevoerd.

Voor welke workloads, agents en back-uplocaties worden knelpunten weergegeven?

De detectie van knelpunten is beschikbaar voor de volgende typen workloads, agents en back-uplocaties:

- Back-ups op schijf/imageniveau, uitgevoerd door:
  - Agent voor Azure
  - Agent voor Windows
  - Agent voor Linux
  - Agent voor MAC
  - Agent voor VMware (zowel Virtual Appliance als Windows, inclusief VM-replicatie en failback van replica-activiteiten (herstel vanaf replica))
  - Agent voor Hyper-V
  - Agent voor Scale Computing
  - Agent voor oVirt (KVM)
  - Agent voor Virtuozzo Infrastructure Platform
  - Agent voor Virtuozzo
  - Agent voor VMware Cloud Director (vCD-BA)
- Back-ups op bestandsniveau
  - Agent voor Windows
  - Agent voor Linux
  - Agent voor MAC
- Back-ups op toepassingsniveau
  - Agent voor SQL
  - Agent voor Exchange
  - Agent voor MySQL/MariaDB
  - Agent voor Oracle
  - Agent voor SAP HANA
- Back-uplocaties
  - Acronis Cloud Storage (inclusief gehoste opslag van partner)
  - Openbare cloudopslag
  - Netwerkshares (SMB + NFS)
  - Lokale mappen
  - Locaties gedefinieerd door een script
  - Acronis Secure Zone

Back-ups van workloads maken in openbare clouds

Opmerking
Deze functie maakt deel uit van het Advanced Backup-pakket (een onderdeel van de Cyber Protection-service). Let op: wanneer u deze functionaliteit toevoegt aan een beschermingsschema, worden er mogelijk extra kosten in rekening gebracht.

U kunt openbare cloudservices, zoals Microsoft Azure en Amazon S3 (Simple Storage Service), selecteren als back-upbestemming in de Cyber Protect-console.

Als u back-uplocaties in openbare clouds wilt configureren, moet u een bedrijfbeheerder of eenheidbeheerder zijn, of moet u een van de volgende rollen hebben zoals gedefinieerd in de Cyber Protection-service: Cyberbeheerder, Beheerder of Gebruiker.

Een back-uplocatie in Microsoft Azure definiëren

Opmerking
Als u back-uplocaties op Microsoft Azure wilt configureren, moet u een van de volgende rollen hebben gedefinieerd in de Cyber Protection-service: Bedrijfbeheerder, Gebruiker, Cyberbeheerder.

Als u een back-up van een workload wilt maken in Microsoft Azure, moet u de Microsoft Azure-back-uplocatie definiëren in de Cyber Protect-console en verbinding maken met het betreffende Microsoft Azure-abonnement. Dit kunt u op de volgende manieren doen:

- Een beschermingsschema maken of bewerken.
- Back-upopslaglocaties definiëren en beheren.

Belangrijk
Zowel beheerders als gebruikers zonder beheerdersrechten kunnen een back-up maken van workloads naar Microsoft Azure.

Gebruikers zonder beheerdersrechten kunnen toegang toevoegen aan een Microsoft Azure-abonnement (zie "Toegang tot Microsoft Azure-abonnementen beheren" (p. 583)), maar kunnen alleen beschermingsschema's toepassen waarvan de back-uplocatie is verbonden met het Microsoft Azure-abonnement dat ze zelf hebben toegevoegd, en voor workloads die onder hun naam zijn geregistreerd in de Cyber Protect-console.

Beheerders kunnen beschermingsschema's toepassen waarvan de back-uplocatie is verbonden met Microsoft Azure-abonnementen die ze zelf hebben toegevoegd of met abonnementen die door een andere beheerder zijn toegevoegd, en voor workloads die onder de naam van een willekeurige gebruiker zijn geregistreerd in de Cyber Protect-console.

Een back-uplocatie in Microsoft Azure definiëren:

1. Voer een van de volgende handelingen uit in de Cyber Protect-console:
   - Als u een beschermingsschema maakt of bewerkt, gaat u naar **Apparaten** en selecteert u de betreffende workload waarvan u een back-up wilt maken naar Microsoft Azure. Ga naar het gedeelte **Back-up** van het beschermingsschema van de geselecteerde workload en klik op de link in de rij **Locatie van back-up**.

     Zie "Beschermingsschema's en -modules" (p. 216) voor meer informatie over het werken met beschermingsschema's.
   - Als u uw back-upopslaglocaties beheert en Microsoft Azure als nieuwe locatie wilt toevoegen, gaat u naar **Back-upopslag**.

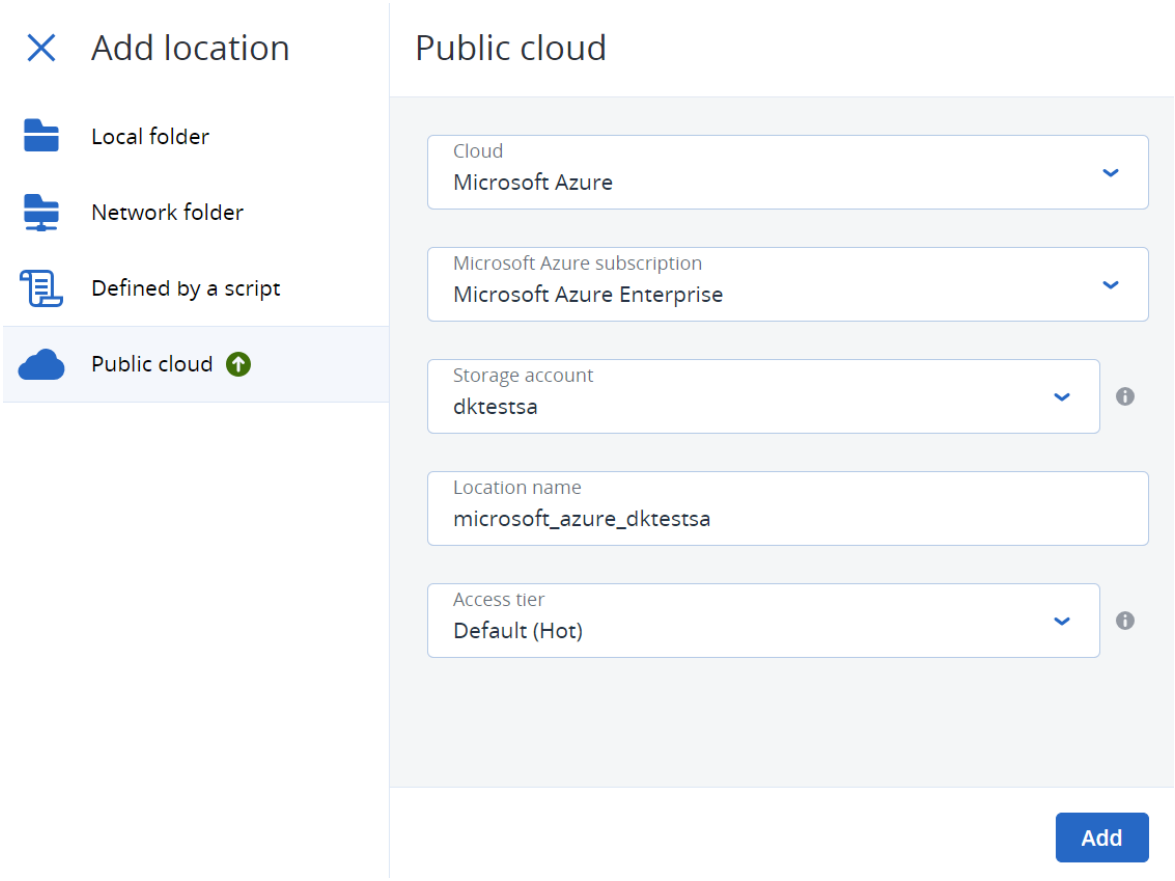
     Zie "Het tabblad Back-upopslag" (p. 559) voor meer informatie over het beheren van back-upopslaglocaties.
2. Klik op **Locatie toevoegen**.
3. Open de de vervolgkeuzelijst **Openbare clouds** en selecteer **Microsoft Azure**.
4. Als het betreffende Microsoft Azure-abonnement al is geregistreerd in de Cyber Protect-console, selecteert u dit in de lijst met abonnementen.

   Als het betreffende abonnement niet is geregistreerd in de Cyber Protect-console, klikt u op **Toevoegen** en klikt u in het weergegeven dialoogvenster op **Aanmelden**. U wordt omgeleid naar de aanmeldingspagina van Microsoft. Zie "Toegang tot een Microsoft Azure-abonnement toevoegen" (p. 584) voor meer informatie over het toevoegen en definiëren van toegang tot een Microsoft Azure-abonnement.
5. Ga naar het veld **Opslagaccount** en selecteer het betreffende account.

   Opmerking
   Momenteel wordt er alleen ondersteuning geboden voor Microsoft Azure-opslagaccounts met reguliere eindpuntachtervoegsels die `core.windows.net` bevatten. Bovendien moet het geselecteerde opslagaccount een account van het type StorageV2 zijn.

   De velden **Locatienaam** en **Toegangsniveau** worden standaard automatisch ingevuld, afhankelijk van het geselecteerde opslagaccount. De weergegeven locatienaam is `microsoft_azure_[opslagaccount]` en het geselecteerde toegangsniveau is **Standaard (Hot)**. Beide velden kunnen indien nodig worden gewijzigd.

   Opmerking
   Wanneer u de locatienaam wijzigt, voert u een unieke locatienaam in (de naam moet uniek zijn voor de klanttenant). Als de door u toevoegde naam al bestaat in het opslagaccount, wordt er door Acronis een achtervoegselnummer toegevoegd aan de naam. Als **Microsoft Azure Storage** bijvoorbeeld al bestaat, wordt de naam automatisch bijgewerkt naar **Microsoft Azure Storage_01**.



6. Klik op **Toevoegen**.

   Als u een beschermingsschema maakt of bewerkt, wordt de Microsoft Azure-back-uplocatie ingesteld als de locatie in de rij **Locatie van back-up**. Wanneer de back-up wordt uitgevoerd (handmatig of gepland), wordt de back-up opgeslagen op de gedefinieerde locatie.

   Als u uw back-upopslaglocaties beheert, kunt u de locatiegegevens indien nodig bekijken en bijwerken. De Microsoft Azure-locatie is ook beschikbaar wanneer u een back-uplocatie voor workloads definieert. Zie "Back-uplocaties in de openbare cloud bekijken en bijwerken" (p. 579) voor meer informatie.

Een back-uplocatie definiëren in Amazon S3

Opmerking
Als u back-uplocaties op Amazon S3 wilt configureren, moet u een van de volgende rollen hebben gedefinieerd in de Cyber Protection-service: Bedrijfbeheerder, Gebruiker, Cyberbeheerder.

Als u een back-up wilt maken van een workload naar Amazon S3, moet u de back-uplocatie in Amazon S3 definiëren in de Cyber Protect-console, en vervolgens verbinden met de relevante betreffende Amazon S3-verbinding. Dit kan op de volgende manieren:

- Een beschermingsschema maken of bewerken.
- Back-upopslaglocaties definiëren en beheren.

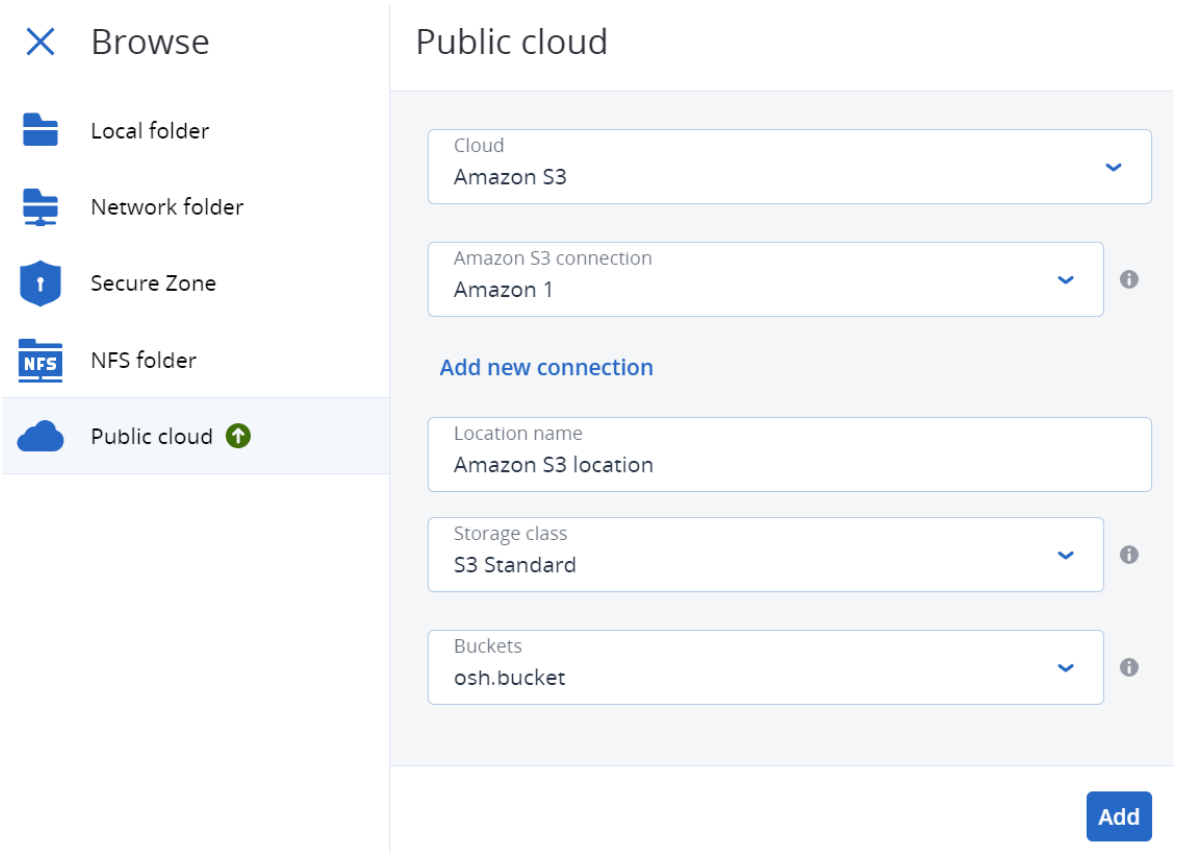
Belangrijk
Zowel beheerders als gebruikers zonder beheerdersrechten kunnen een back-up maken van workloads naar Amazon S3.

Gebruikers zonder beheerdersrechten kunnen toegang toevoegen voor een Amazon S3-verbinding (zie "Toegang tot andere services voor openbare cloudopslag beheren" (p. 587)), maar kunnen alleen beschermingsplannen toepassen waarvan de back-uplocatie is verbonden met de Amazon S3-verbinding die ze zelf hebben toegevoegd, en voor workloads die onder hun naam zijn geregistreerd in de Cyber Protect-console.

Beheerders kunnen beschermingsplannen toepassen waarvan de back-uplocatie is verbonden met Amazon S3-verbindingen die ze zelf hebben toegevoegd of met abonnementen die door een andere beheerder zijn toegevoegd, en voor workloads die onder de naam van een willekeurige gebruiker zijn geregistreerd in de Cyber Protect-console.

Een back-uplocatie definiëren in Amazon S3:

1. Voer een van de volgende handelingen uit in de Cyber Protect-console:
   - Als u een beschermingsplan maakt of bewerkt, gaat u naar **Apparaten** en selecteert u de workload waarvan u een back-up wilt maken naar Amazon S3. Ga naar het gedeelte **Back-up** van het beschermingsplan van de geselecteerde workload en klik op de link in de rij **Locatie van back-up**.
     Zie "Beschermingsschema's en -modules" (p. 216) voor meer informatie over het werken met beschermingsschema's.
   - Als u uw back-upopslaglocaties beheert en Amazon S3 als nieuwe locatie wilt toevoegen, gaat u naar **Back-upopslag**.
     Zie "Het tabblad Back-upopslag" (p. 559) voor meer informatie over het beheren van back-upopslaglocaties.
2. Klik op **Locatie toevoegen**.
3. Open de vervolgkeuzelijst **Openbare clouds** en selecteer **Amazon S3**.
4. Als de betreffende Amazon S3-verbinding al is geregistreerd in de Cyber Protect-console, selecteert u deze in de lijst.
   Als de betreffende verbinding niet is geregistreerd in de Cyber Protect-console, klikt u op **Nieuwe verbinding toevoegen**. Zie "Toegang tot een verbinding met openbare clouds toevoegen" (p. 587) voor meer informatie over het toevoegen en definiëren van toegang tot een Amazon S3-verbinding. Wanneer de verbinding is toegevoegd, gaat u door naar de volgende stap.



5. Definieer het volgende:
   - Ga naar het veld **Locatienaam** en voer de naam van de back-uplocatie in.

     Opmerking
     De locatienaam moet uniek zijn voor de klanttenant. Als de naam die u toevoegt, al bestaat in de verbinding, voegt Acronis een achtervoegselnummer toe aan de naam. Bijvoorbeeld: als **Amazon S3-opslag** al bestaat, wordt de naam automatisch bijgewerkt naar **Amazon S3-opslag 1**.

   - Ga naar het veld **Opslagklasse** en selecteer een van de volgende ondersteunde opslagklassen:
     - S3 Standard
     - Standard - Onregelmatige toegang (S3 Standard-IA)
     - One Zone - Onregelmatige toegang (S3 One Zone-IA)
     - S3 Intelligent Tiering
   - Ga naar het veld **Bucket** en selecteer de betreffende Amazon S3-bucket.
6. Klik op **Toevoegen**.

   Als u een beschermingsplan maakt of bewerkt, wordt de Amazon S3-back-uplocatie ingesteld als de locatie in de rij **Locatie van back-up**. Wanneer de back-up wordt uitgevoerd (handmatig of gepland), wordt de back-up opgeslagen op de gedefinieerde locatie.

Als u uw back-upopslaglocaties beheert, kunt u de locatiegegevens indien nodig bekijken en bijwerken. De Amazon S3-locatie is ook beschikbaar wanneer u een back-uplocatie voor workloads definieert. Zie "Back-uplocaties in de openbare cloud bekijken en bijwerken" (p. 579) voor meer informatie.

Een back-uplocatie definiëren in Wasabi

Opmerking
Als u back-uplocaties in Wasabi wilt configureren, moet u een van de volgende rollen hebben gedefinieerd in de Cyber Protection-service: Bedrijfbeheerder, Gebruiker, Cyberbeheerder.

Als u een back-up wilt maken van een workload naar Wasabi, moet u de back-uplocatie in Wasabi definiëren in de Cyber Protect-console, en vervolgens verbinden met de betreffende Wasabi-verbinding. Dit kan op de volgende manieren:

- Een beschermingsschema maken of bewerken.
- Back-upopslaglocaties definiëren en beheren.

Belangrijk
Zowel beheerders als gebruikers zonder beheerdersrechten kunnen een back-up maken van workloads naar Wasabi.

Gebruikers zonder beheerdersrechten kunnen toegang toevoegen voor een Wasabi-verbinding (zie "Toegang tot andere services voor openbare cloudopslag beheren" (p. 587)), maar kunnen alleen beschermingsplannen toepassen waarvan de back-uplocatie is verbonden met de Wasabi-verbinding die ze zelf hebben toegevoegd, en voor workloads die onder hun naam zijn geregistreerd in de Cyber Protect-console.

Beheerders kunnen beschermingsplannen toepassen waarvan de back-uplocatie is verbonden met Wasabi-verbindingen die ze zelf hebben toegevoegd of met abonnementen die door een andere beheerder zijn toegevoegd, en voor workloads die onder de naam van een willekeurige gebruiker zijn geregistreerd in de Cyber Protect-console.

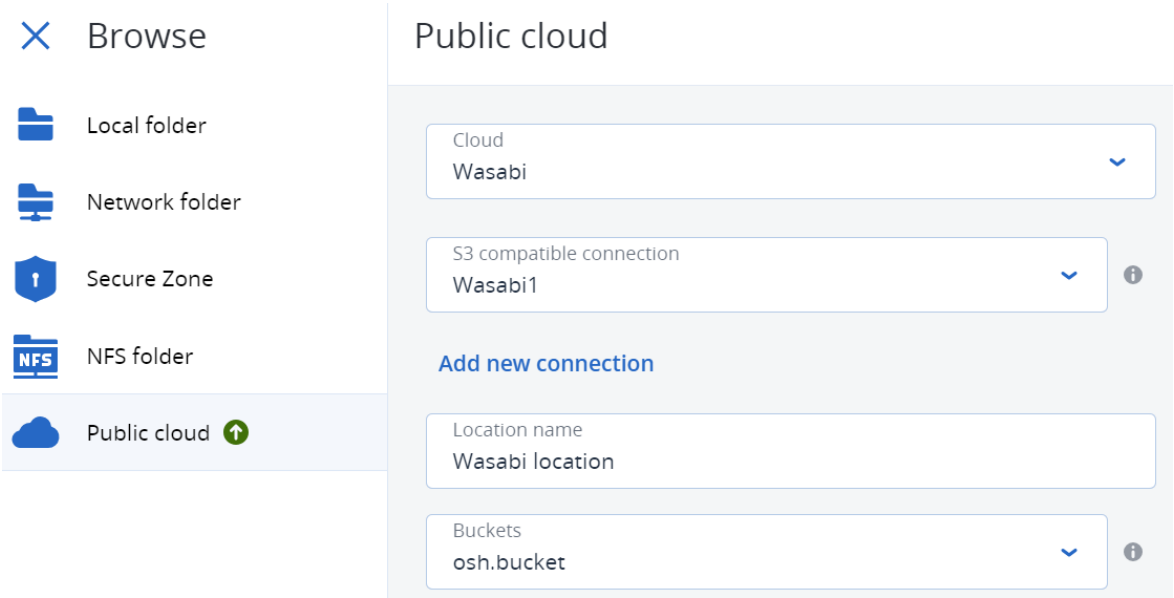
Een back-uplocatie definiëren in Wasabi:

1. Voer een van de volgende handelingen uit in de Cyber Protect-console:
   - Als u een beschermingsplan maakt of bewerkt, gaat u naar **Apparaten** en selecteert u de workload waarvan u een back-up wilt maken naar Wasabi. Ga naar het gedeelte **Back-up** van het beschermingsplan van de geselecteerde workload en klik op de link in de rij **Locatie van back-up**.
     Zie "Beschermingsschema's en -modules" (p. 216) voor meer informatie over het werken met beschermingsschema's.
   - Als u uw back-upopslaglocaties beheert en Wasabi als nieuwe locatie wilt toevoegen, gaat u naar **Back-upopslag**.

Zie "Het tabblad Back-upopslag" (p. 559) voor meer informatie over het beheren van back-upopslaglocaties.

2. Klik op **Locatie toevoegen**.
3. Open de de vervolgkeuzelijst **Openbare clouds** en selecteer **Wasabi**.
4. Als de betreffende Wasabi-verbinding al is geregistreerd in de Cyber Protect-console, selecteert u deze in de lijst.

   Als de betreffende verbinding niet is geregistreerd in de Cyber Protect-console, klikt u op **Nieuwe verbinding toevoegen**. Zie "Toegang tot een verbinding met openbare clouds toevoegen" (p. 587) voor meer informatie over het toevoegen en definiëren van toegang tot een Wasabi-verbinding. Wanneer de verbinding is toegevoegd, gaat u door naar de volgende stap.



5. Definieer het volgende:
   - Ga naar het veld **Locatienaam** en voer de naam van de back-uplocatie in.

     Opmerking
     De locatienaam moet uniek zijn voor de klanttenant. Als de naam die u toevoegt, al bestaat in de verbinding, voegt Acronis een achtervoegselnummer toe aan de naam. Bijvoorbeeld: als **Wasabi-opslag** al bestaat, wordt de naam automatisch bijgewerkt naar **Wasabi-opslag 1**.

   - Ga naar het veld **Bucket** en selecteer de betreffende Wasabi-bucket.
6. Klik op **Toevoegen**.

   Als u een beschermingsplan maakt of bewerkt, wordt de Wasabi-back-uplocatie ingesteld als de locatie in de rij **Locatie van back-up**. Wanneer de back-up wordt uitgevoerd (handmatig of gepland), wordt de back-up opgeslagen op de gedefinieerde locatie.

   Als u uw back-upopslaglocaties beheert, kunt u de locatiegegevens indien nodig bekijken en bijwerken. De Wasabi-locatie is ook beschikbaar wanneer u een back-uplocatie voor workloads definieert. Zie "Back-uplocaties in de openbare cloud bekijken en bijwerken" (p. 579) voor meer informatie.

Back-uplocaties in de openbare cloud bekijken en bijwerken

U kunt de door u gedefinieerde Microsoft Azure-, Amazon-S3- en Wasabi-back-uplocaties bekijken en bijwerken in de module **Back-upopslag** of wanneer u een beschermingsplan maakt of bewerkt.

Voor informatie over het verwijderen van toegang tot een Microsoft Azure-abonnement vanuit de Cyber Protect-console, zie "Toegang tot een Microsoft Azure-abonnement verwijderen" (p. 586). Voor informatie over het verwijderen van toegang tot andere openbare-cloudverbindingen, zie "Toegang tot andere services voor openbare cloudopslag beheren" (p. 587).

Opmerking
U kunt een back-uplocatie in de openbare cloud niet handmatig vernieuwen of verwijderen in de module **Back-upopslag**. De inhoud van de back-uplocatie wordt automatisch bijgewerkt na elke back-up of herstelbewerking.

Back-uplocaties in de openbare cloud bekijken

1. Ga in de Cyber Protect-console naar **Back-upopslag**.
   Een lijst met back-uplocaties wordt weergegeven, met details over de opslagcapaciteit en het aantal back-ups dat aan elke locatie is toegewezen.
   Zie "Het tabblad Back-upopslag" (p. 559) voor meer informatie over het werken met de vermelde back-uplocaties.
2. Selecteer de betreffende locatie.
   Alle huidige back-ups voor de geselecteerde locatie worden vermeld.
3. (Optioneel) Klik op een back-up om meer details over de back-up te bekijken.

Een back-uplocatie in de openbare cloud bijwerken in een beschermingsplan

1. Ga naar het betreffende beschermingsschema en selecteer **Bewerken**.
2. Klik op de link in de rij **Locatie van back-up**.
3. Maak een keuze uit de lijst met bestaande back-uplocaties of klik op **Locatie toevoegen** om een nieuwe locatie toe te voegen.
   Als het betreffende Microsoft Azure-abonnement of de verbinding met de openbare cloud al is geregistreerd in de Cyber Protect-console, kunt u deze selecteren in de weergegeven lijst.
   Als u een nieuw Microsoft Azure-abonnement toevoegt, wordt u gevraagd om uw Microsoft-accountgegevens te verifiëren (zie "Toegang tot een Microsoft Azure-abonnement toevoegen" (p. 584)). Voor meer informatie over de vereiste machtigingen wanneer u verbinding maakt met Microsoft Azure, raadpleegt u het artikel Microsoft Azure-verbindingsbeveiliging en -audit (72684).

Toegang tot het openbare cloud-account beheren

Als u de Acronis Cyber Protection-services op openbare cloud-platforms wilt inschakelen, moet de toegang tot de betreffende openbare cloud-accounts worden geconfigureerd.

Wanneer u bijvoorbeeld met Microsoft Azure werkt, is toegang tot uw Microsoft Azure-abonnement vereist. Zodra het abonnement is toegevoegd in de Cyber Protect-console, kunt u dit abonnement selecteren wanneer u een directe back-up naar Microsoft Azure configureert. En als u met Amazon S3 of Wasabi werkt, zijn de betreffende toegangssleutels vereist die zijn gekoppeld aan specifieke beleidsregels voor back-ups.

De toegang tot openbare clouds wordt beheerd via het menu **Infrastructuur** in de Cyber Protect-console.

Belangrijk
Back-upvalidatie is uitgeschakeld voor back-ups in een openbare cloudopslag, om overmatige kosten voor uitgaand verkeer te voorkomen. Bovendien is het momenteel niet mogelijk om een back-uplocatie op een openbare cloud 'opnieuw te koppelen' aan dezelfde of een andere klanttenant als de locatie eerder is verwijderd. Voor meer informatie kunt u contact opnemen met het ondersteuningsteam.

Toegangsvereisten nodig om een back-up te maken naar openbare cloudopslag

Wanneer u direct back-ups maakt naar services voor openbare cloudopslag, moet u rekening houden met enkele toegangsvereisten voor de verschillende platforms:

- Microsoft Azure
- Amazon S3
- Wasabi

Back-ups maken naar Microsoft Azure

Als u verbinding wilt maken met een Microsoft Azure-abonnement, moet u over verschillende machtigingen beschikken. Voor meer informatie hierover raadpleegt u artikel Microsoft Azure-verbindingsbeveiliging en -audit (72684).

Opmerking
U kunt de verbinding met het abonnement alleen tot stand brengen als u een van de volgende rollen hebt in Microsoft Azure AD: Cloudtoepassingsbeheerder, Toepassingsbeheerder of Globale beheerder. Voor elk geselecteerd abonnement moet ook de rol Eigenaar aan u worden toegewezen.

Een back-up maken naar Amazon S3

Wanneer u een back-up maakt naar Amazon S3, zijn er verschillende vereisten voor het definiëren van back-uplocaties in Amazon S3:

- Ondersteunde opslagklassen
- Beleidsmachtigingen

- Toegangssleutels
- Bucket-instellingen

Ondersteunde opslagklassen

De volgende Amazon S3-opslagklassen worden momenteel ondersteund:

- S3 Standard
- Standard - Onregelmatige toegang (S3 Standard-IA)
- One Zone - Onregelmatige toegang (S3 One Zone-IA)
- S3 Intelligent Tiering

Beleidsmachtigingen

Wanneer u een back-up maakt in Amazon S3, moeten de minimale machtigingen zijn toegepast op uw Amazon-account, zodat Acronis een back-up van de betreffende workloads kan maken in Amazon S3. Dit betekent dat de betreffende gebruikers toegang moeten hebben tot de AWS-beheerconsole en dat het relevante beleid moet zijn toegepast op de groep(en) waaraan ze zijn toegewezen.

Voorbeelden

Het volgende voorbeeldbeleid toont de minimale set van machtigingen voor verscheidene resources. * betekent alle resources.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource": "*" },
{ "Effect": "Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, {
"Effect": "Allow", "Action": [ "s3:GetBucketLocation", "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:ListBucket" ], "Resource": "*" } ] }
```

Het volgende voorbeeldbeleid toont de minimale machtigingen voor een specifieke bucket. Let op: `[BUCKETNAME]` moet worden vervangen door de naam van de bucket.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource":
"arn:aws:s3:::[BUCKETNAAM]" }, { "Effect": "Allow", "Action":
"sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:PutObject", "s3:GetObject", "s3:DeleteObject" ],
"Resource": "arn:aws:s3:::[BUCKETNAAM]/*" }, { "Effect": "Allow", "Action": [
"s3:ListBucket" ], "Resource": "arn:aws:s3:::[BUCKETNAAM]" } ] }
```

Toegangssleutels

Toegangssleutels zijn vereist door Acronis voor elke Amazon S3-verbinding. De sleutels worden gebruikt bij het definiëren van de Amazon S3-verbinding. Voor meer informatie over het genereren van toegangssleutels en toegangssleutel-ID's raadpleegt u de Amazon S3-documentatie.

Bucket-instellingen

Bij het gebruik van Amazon S3-buckets als back-uplocatie, moet de bucket geconfigureerd zijn met de standaardinstellingen, inclusief het blokkeren van alle openbare toegang (standaard is dit ingesteld op **Aan**). Voor meer informatie over het werken met buckets raadpleegt u de Amazon S3-documentatie.

Opmerking
Acronis ondersteunt momenteel geen bucketversiebeheer en objectvergrendeling in Amazon S3, zelfs niet wanneer dit is ingeschakeld voor de bucket.

Back-up maken naar Wasabi

Wanneer u een back-up maakt naar Wasabi, moet u rekening houden met enkele vereisten bij het definiëren van back-uplocaties:

- Beleidsmachtigingen
- Toegangssleutels
- Bucket-instellingen

Beleidsmachtigingen

Wanneer u een back-uplocatie in Wasabi definieert, moet u controleren of de relevante beleidsregels worden toegepast op de betreffende groepen en gebruikers in Wasabi.

Voorbeelden

Het volgende voorbeeldbeleid toont de minimale set van machtigingen voor verscheidene resources. * betekent een willekeurige resource.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "*" }, { "Effect": "Allow", "Action": [
"iam:CreateRole", "iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole"
], "Resource": "*" }, { "Effect": "Allow", "Action": [ "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": "s3:ListBucket", "Resource": "*" } ] }
```

Het volgende voorbeeldbeleid toont beperkte machtigingen met een beperkte reikwijdte van resources. Let op: `[BUCKETNAME]` moet worden vervangen door de naam van de bucket en `[ACCOUNTID]` door de ID van het Wasabi-account.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "iam:CreateRole", "iam:AttachRolePolicy",
"sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "arn:aws:iam::
[ACCOUNTID]:*" }, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject" ], "Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect":
"Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Toegangssleutels

Acronis vereist toegangssleutels voor elke Wasabi-verbinding. De toegangssleutels worden gebruikt tijdens het definiëren van de Wasabi-verbinding.

Let op: toegangssleutels voor hoofdgebruikersaccounts op Wasabi kunnen niet worden gebruikt omdat AssumeRole niet kan worden aangeroepen door hoofdgebruikers. U moet een afzonderlijke niet-hoofdgebruiker maken en toegangssleutels voor die gebruiker genereren.

Voor meer informatie over het genereren van toegangssleutels en toegangssleutel-ID's: zie de Wasabi-documentatie.

Bucket-instellingen

Bij het gebruik van Wasabi-buckets als back-uplocatie, moet de bucket zijn geconfigureerd met de standaardinstellingen. Voor meer informatie over het werken met buckets, raadpleegt u de Wasabi-documentatie.

Opmerking
Acronis ondersteunt momenteel geen bucketversiebeheer en objectvergrendeling in Wasabi, zelfs niet wanneer dit is ingeschakeld voor de bucket.

Toegang tot Microsoft Azure-abonnementen beheren

Als u verbinding maakt met de betreffende Microsoft Azure-abonnementen in de Cyber Protect-console, kunt u een back-up van de gewenste workloads rechtstreeks in Microsoft Azure maken.

De verbinding met een abonnement kan worden geconfigureerd wanneer u een back-uplocatie maakt via het menu **Apparaten** of **Back-upopslag**, zoals beschreven in "Een back-uplocatie in Microsoft Azure definiëren" (p. 572).

U kunt er ook voor kiezen de volgende Microsoft Azure-abonnementen te configureren op het scherm **Openbare clouds** (ga naar **Infrastructuur > Openbare clouds**). Hier kunt u ook uw abonnementen beheren, waaronder de toegang tot het abonnement verlengen, de eigenschappen en activiteiten van het abonnement bekijken of het abonnement verwijderen.

Afhankelijk van de aan u toegewezen beheerdersrol kunt u mogelijk Microsoft Azure-abonnementen beheren die door andere gebruikers binnen uw organisatie zijn toegevoegd. Als u bijvoorbeeld een bedrijfbeheerder of eenheidbeheerder bent, of als u de rol Cyberbeheerder of Beheerder hebt in de Cyber Protection-service, kunt u Microsoft Azure-abonnementen bekijken en beheren die zijn toegevoegd door andere beheerders, en abonnementen die zijn toegevoegd door gebruikers zonder beheerdersrechten. Gebruikers zonder beheerdersrechten kunnen alleen Microsoft Azure-abonnementen bekijken en openen die ze zelf aan de Cyber Protect-console hebben toegevoegd.

Opmerking
Partners kunnen de Microsoft Azure-abonnementen beheren van klanten op een lager niveau dan hun eigen niveau in de hiërarchie. Wanneer een partner echter **Alle klanten** selecteert, is het menu **Infrastructuur** in de Cyber Protect-console niet beschikbaar.

Belangrijk
Wanneer u verbinding maakt met een Microsoft Azure-abonnement, zijn de minimale machtigingen voor Acronis vereist om verbinding te maken met het abonnement. Zie het artikel Microsoft Azure-verbindingsbeveiliging en -audit (72684) voor meer informatie over de vereiste machtigingen.

Toegang tot een Microsoft Azure-abonnement toevoegen

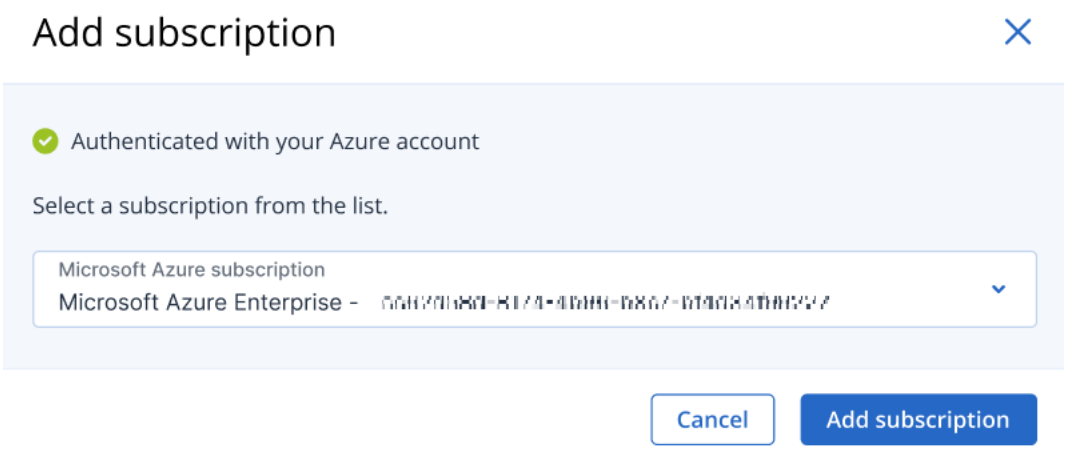
Als u een Microsoft Azure-abonnement toevoegt in de Cyber Protect-console, heeft Acronis veilig toegang tot uw abonnement en kunt u een back-up van de gewenste workloads rechtstreeks in Microsoft Azure maken.

Toegang tot een Microsoft Azure-abonnement toevoegen:

1. Ga in de Cyber Protect-console naar **Infrastructuur > Openbare clouds**.
2. Klik op **Toevoegen** en selecteer **Microsoft Azure** in de weergegeven lijst met opties.
3. In het weergegeven dialoogvenster klikt u op **Aanmelden**. U wordt omgeleid naar de aanmeldingspagina van Microsoft.

   Opmerking
   U kunt de verbinding met het abonnement alleen tot stand brengen als u een van de volgende rollen hebt in Microsoft Azure AD: Cloudtoepassingsbeheerder, Toepassingsbeheerder of Globale beheerder. Voor elk geselecteerd abonnement moet ook de rol Eigenaar aan u worden toegewezen.

4. Ga naar het Microsoft-aanmeldingsscherm, voer uw referenties in en accepteer de gevraagde machtigingen. De verbinding wordt tot stand gebracht, een ogenblik geduld...
   Zie het artikel Microsoft Azure-verbindingsbeveiliging en -audit (72684) voor meer informatie over veilige toegang tot uw Microsoft Azure en abonnement.
5. Wanneer de verbinding tot stand is gebracht, selecteert u het gewenste abonnement in de vervolgkeuzelijst in het weergegeven dialoogvenster en klikt u op **Abonnement toevoegen**.



Het abonnement wordt toegevoegd aan de lijst met openbare clouds.

Zie "Toegang tot een Microsoft Azure-abonnement verlengen" (p. 585) om het jaarlijkse toegangscertificaat voor het abonnement te verlengen.

Zie "Toegang tot een Microsoft Azure-abonnement verwijderen" (p. 586) als u de toegang tot het abonnement wilt verwijderen.

Opmerking
Als het Microsoft Azure-account waarbij u bent aangemeld, toegang biedt tot meerdere Microsoft Azure AD's, inclusief AD's waarvoor u bent uitgenodigd als gastgebruiker, wordt alleen de standaardgebruikersmap geselecteerd. Als u een map wilt gebruiken waarin u een gastgebruiker bent, moet u een nieuwe gebruiker maken in die specifieke Microsoft Azure AD. Vervolgens kunt u zich aanmelden bij dat account om verbinding te maken met het betreffende abonnement.

Toegang tot een Microsoft Azure-abonnement verlengen

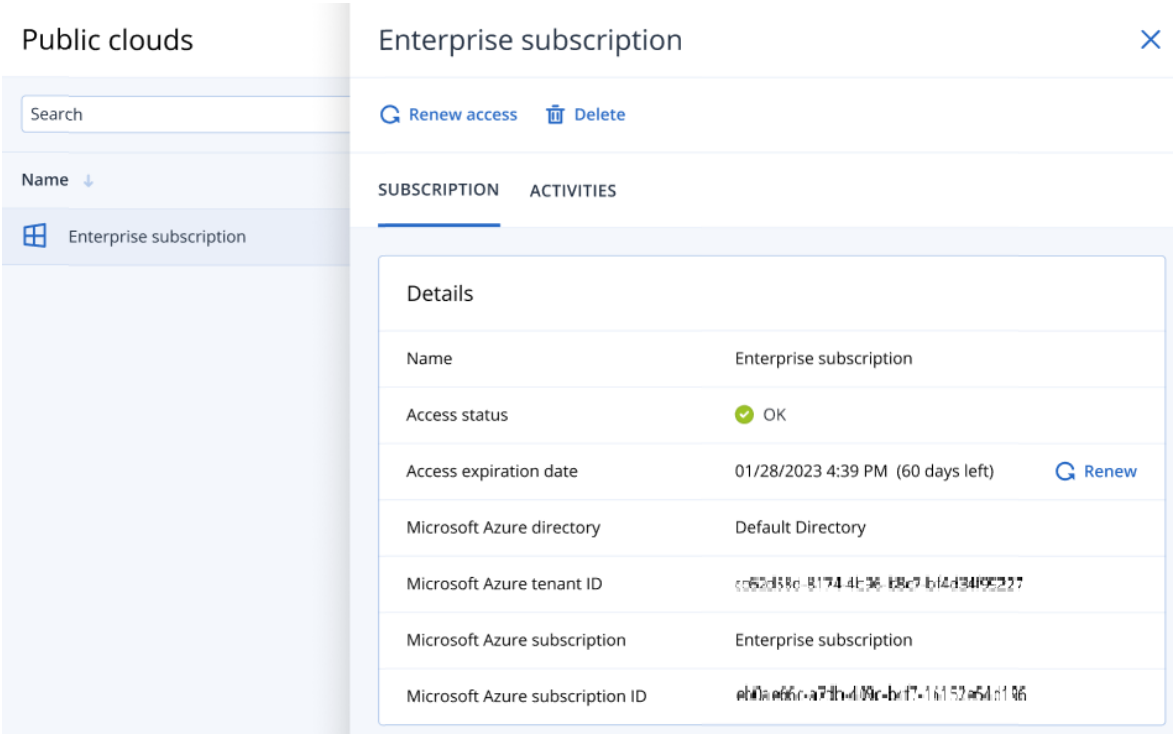
Wanneer toegang tot een Microsoft Azure-abonnement is geregistreerd in de Cyber Protect-console, wordt deze door Acronis automatisch ingesteld voor één jaar met een gratis en uniek toegangscertificaat. Wanneer de vervaldatum van het certificaat nadert, kunt u het certificaat snel en eenvoudig verlengen.

Het toegangscertificaat voor uw Microsoft Azure-abonnement verlengen:

1. Ga in de Cyber Protect-console naar **Infrastructuur > Openbare clouds**.
2. Selecteer het betreffende abonnement in de weergegeven lijst.

   Opmerking
   De kolom **Toegangsstatus** geeft de huidige status van het toegangscertificaat voor elk abonnement weer, samen met een van twee mogelijke statussen: **OK** of **Verlopen**.

3. Klik in het rechterdeelvenster op **Toegang verlengen**.
   U kunt ook op het tabblad **Abonnement** klikken en vervolgens klikken op **Verlengen** in het veld **Vervaldatum van de toegang**.



4. Ga naar het Microsoft-aanmeldingsscherm, voer uw referenties in en accepteer de gevraagde machtigingen. De verbinding wordt tot stand gebracht, een ogenblik geduld...
   Wanneer de verificatie lukt, wordt de toegang automatisch voor een jaar verlengd.
   Zie het artikel Microsoft Azure-verbindingsbeveiliging en -audit (72684) voor meer informatie over de vereiste machtigingen.

Toegang tot een Microsoft Azure-abonnement verwijderen

U moet de toegang tot het Microsoft Azure-abonnement verwijderen als u niet van plan bent back-ups van workloads op te slaan in Microsoft Azure.

Toegang tot een Microsoft Azure-abonnement verwijderen:

Belangrijk
U kunt een abonnement niet verwijderen als het momenteel wordt gebruikt om back-ups te maken voor opslag in Microsoft Azure.

1. Ga in de Cyber Protect-console naar **Infrastructuur > Openbare clouds**.
2. Selecteer het betreffende abonnement in de weergegeven lijst.
3. Klik in het rechterdeelvenster op **Verwijderen**.

   Opmerking
   U kunt alleen een abonnement verwijderen dat u zelf hebt toegevoegd. U kunt een abonnement ook verwijderen als u een bedrijfbeheerder of eenheidbeheerder bent, of als u de rol van cyberbeheerder of beheerder hebt in de Cyber Protection-service.

4. Klik in het weergegeven bevestigingsbericht op **Verwijderen**.

Toegang tot andere services voor openbare cloudopslag beheren

Opmerking
Dit gedeelte verwijst naar het beheren van toegang voor alle services voor openbare cloudopslag behalve Microsoft Azure (apart beschreven in "Toegang tot Microsoft Azure-abonnementen beheren" (p. 583)).

Door verbinding te maken met het betreffende openbare cloud-account in de Cyber Protect-console kunt u direct back-ups maken in de betreffende openbare cloudopslag.

U kunt verbindingen met openbare cloudopslag-accounts configureren wanneer u een back-uplocatie maakt via het menu **Apparaten** of **Back-upopslag**. U kunt verbindingen met openbare clouds ook configureren via het scherm **Openbare clouds** (ga naar **Infrastructuur > Openbare clouds**). Hier kunt u uw verbinding ook beheren, bijvoorbeeld de toegang tot de verbinding verlengen, verbindingskenmerken en -activiteiten bekijken of de verbinding verwijderen.

Afhankelijk van de aan u toegewezen beheerdersrol kunt u mogelijk verbindingen met openbare clouds beheren die door andere gebruikers binnen uw organisatie zijn toegevoegd. Als u bijvoorbeeld een bedrijfbeheerder of eenheidbeheerder bent, of als u de rol Cyberbeheerder of Beheerder hebt in de Cyber Protection-service, kunt u door andere beheerders toegevoegde verbindingen met openbare clouds bekijken en beheren, evenals verbindingen die zijn toegevoegd door gebruikers zonder beheerdersrechten. Gebruikers zonder beheerdersrechten kunnen alleen verbindingen met openbare clouds bekijken en openen die ze zelf aan de Cyber Protect-console hebben toegevoegd.

Opmerking
Partners kunnen de verbindingen met openbare clouds beheren van klanten op een lager niveau dan hun eigen niveau in de hiërarchie. Wanneer een partner echter **Alle klanten** selecteert, is het menu **Infrastructuur** in de Cyber Protect-console niet beschikbaar.

Belangrijk
In Acronis zijn er enkele machtigingen vereist voor verbinding met een openbare cloud. Zie "Toegangsvereisten nodig om een back-up te maken naar openbare cloudopslag" (p. 580) voor meer informatie .

Toegang tot een verbinding met openbare clouds toevoegen

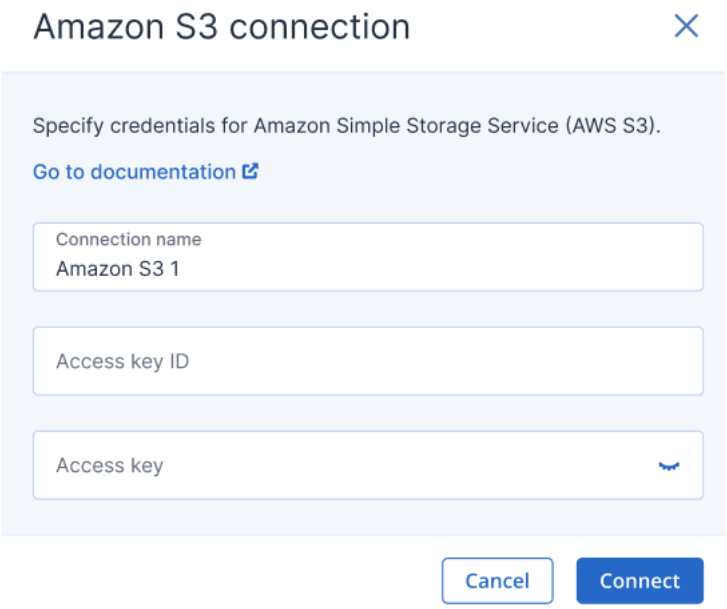
Nadat u een verbinding met een openbare cloud (zoals Amazon S3 of Wasabi) hebt toegevoegd in de Cyber Protect-console, kan Acronis veilig toegang krijgen tot uw cloudresources en direct een back-up van workloads maken in de betreffende openbare cloudopslag.

Toegang tot een verbinding met openbare clouds toevoegen:

1. Ga in de Cyber Protect-console naar **Infrastructuur > Openbare clouds**.
2. Klik op **Toevoegen** en selecteer een van de volgende opties:
   - **Amazon S3**

     Definieer het volgende in het weergegeven dialoogvenster:
     - **Verbindingsnaam**: de naam van de Amazon S3-verbinding.
     - **Toegangssleutel-ID**: de toegangssleutel-ID voor de gebruiker van de Amazon S3-service.
     - **Toegangssleutel**: de toegangssleutel voor de gebruiker van de Amazon S3-service.

       Via de toegangssleutel en toegangssleutel-ID kan Acronis toegang krijgen tot de opslagklassen en buckets voor de betreffende verbinding. Zie "Toegangsvereisten nodig om een back-up te maken naar openbare cloudopslag" (p. 580) voor meer informatie over de vereiste toegangssleutels en machtigingen voor Acronis.

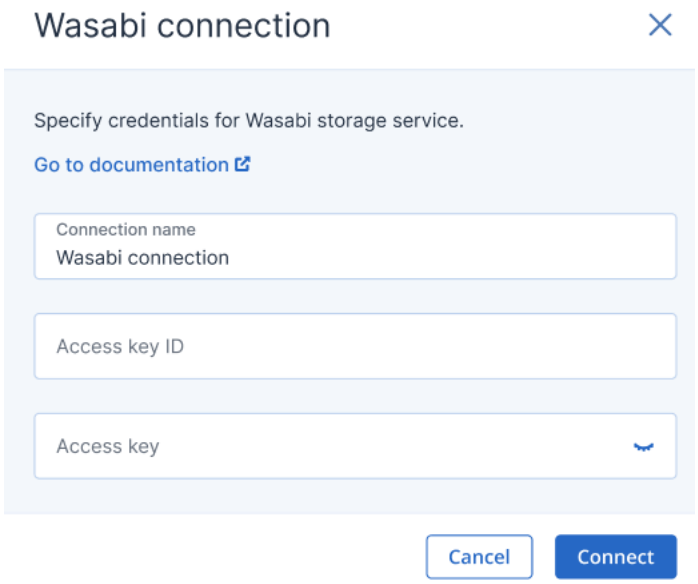
     

   - **Wasabi**

     Definieer het volgende in het weergegeven dialoogvenster:
     - **Verbindingsnaam**: de naam van de Wasabi-verbinding.
     - **Toegangssleutel-ID**: de toegangssleutel-ID voor de gebruiker van de Wasabi-service.
     - **Toegangssleutel**: de toegangssleutel voor de gebruiker van de Wasabi-service.

       Via de toegangssleutel en toegangssleutel-ID kan Acronis toegang krijgen tot de opslagklassen en buckets voor de betreffende verbinding. Zie "Toegangsvereisten nodig om een back-up te maken naar openbare cloudopslag" (p. 580) voor meer informatie over

de vereiste toegangssleutels en machtigingen voor Acronis.



3. Klik op **Verbinden**.

   Het verbindingsproces begint en kan enkele minuten duren. Wanneer het klaar is, wordt de verbinding toegevoegd aan de lijst met openbare clouds.

   Zie "Toegang tot een verbinding met openbare clouds verlengen" (p. 589) als u het jaarlijkse toegangscertificaat voor de verbinding wilt vernieuwen.

   Zie "Toegang tot een verbinding met openbare clouds verwijderen" (p. 590) als u de toegang tot de verbinding wilt verwijderen.

Toegang tot een verbinding met openbare clouds verlengen

Wanneer een openbare cloudverbinding is geregistreerd in de Cyber Protect-console, wijst Acronis automatisch een gratis en uniek toegangscertificaat toe dat toegang tot de verbinding met de openbare cloud mogelijk maakt. Het certificaat is één jaar geldig. Wanneer het certificaat bijna verloopt, kunt u het verlengen.

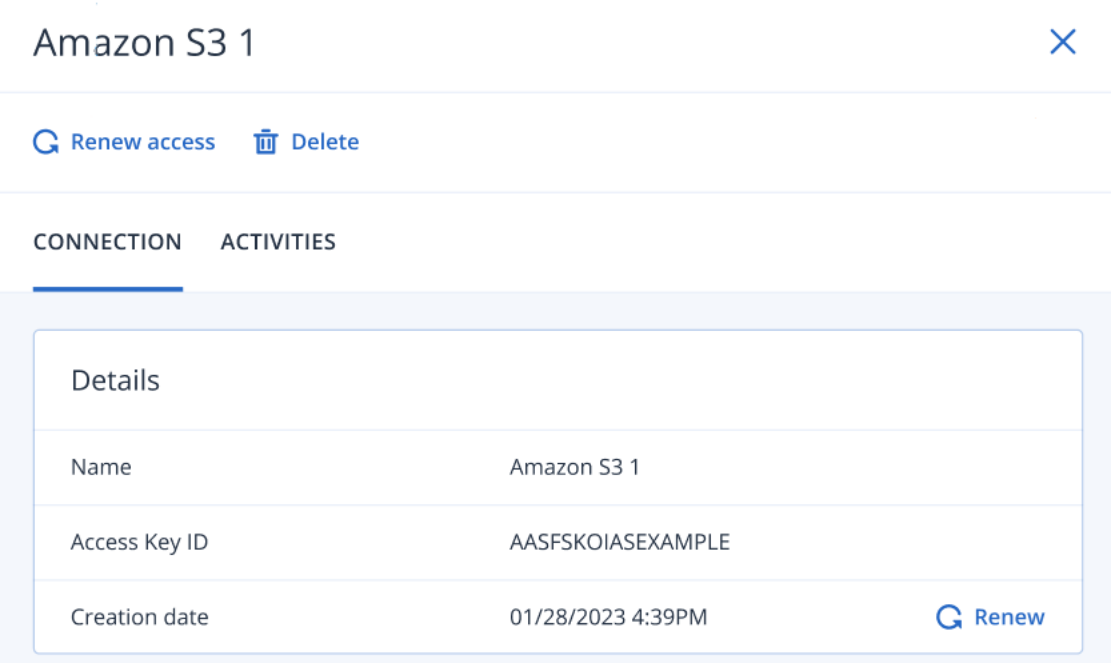
Het toegangscertificaat voor verbinding met een openbare cloud verlengen:

1. Ga in de Cyber Protect-console naar **Infrastructuur > Openbare clouds**.
2. Selecteer de betreffende verbinding in de lijst.

   Opmerking
   De kolom **Toegangsstatus** geeft de huidige status van het toegangscertificaat voor elke verbinding weer, samen met een van twee mogelijke statussen: **OK** of **Verlopen**.

3. Klik in het rechterdeelvenster op **Toegang verlengen**.

   U kunt ook op het tabblad **Verbinding** klikken en vervolgens klikken op **Verlengen** in de rij **Aanmaakdatum**.



Wanneer de verificatie lukt, wordt de toegang automatisch voor een jaar verlengd.

Toegang tot een verbinding met openbare clouds verwijderen

U moet toegang tot verbindingen met een openbare cloud verwijderen als u geen back-ups van workloads maakt in een openbare cloud.

Toegang tot een verbinding met openbare clouds verwijderen:

Belangrijk
U kunt een verbinding niet verwijderen als deze momenteel wordt gebruikt voor back-ups naar een openbare cloud.

1. Ga in de Cyber Protect-console naar **Infrastructuur > Openbare clouds**.
2. Selecteer de verbinding in de lijst.
3. Klik in het rechterdeelvenster op **Verwijderen**.

   Opmerking
   U kunt alleen een verbinding verwijderen die u zelf hebt toegevoegd. U kunt een verbinding ook verwijderen als u een bedrijfbeheerder of eenheidbeheerder bent, of als u de rol van cyberbeheerder of beheerder hebt in de Cyber Protection-service.

4. Klik in het weergegeven bevestigingsbericht op **Verwijderen**.

Microsoft-toepassingen beschermen

Microsoft SQL Server en Microsoft Exchange Server beschermen

Opmerking
Microsoft SQL-back-up wordt alleen ondersteund voor databases die worden uitgevoerd op NFTS-, REFS- en FAT32-bestandssystemen. ExFat wordt niet ondersteund.

Er zijn twee methoden om Microsoft-applicaties te beschermen:

- **Databaseback-up**
  Dit is een back-up op bestandsniveau van de databases en de bijbehorende metagegevens. De databases kunnen worden hersteld naar een live applicatie of als bestanden.
- **Applicatiegerichte back-up**
  Dit is een back-up op schijfniveau, waarbij ook de metagegevens van de applicaties worden verzameld. Dankzij deze metagegevens is het mogelijk de applicatiegegevens te doorzoeken en te herstellen, zonder de hele schijf of het hele volume te herstellen. De schijf of het volume kan ook als geheel worden hersteld. Dit betekent dat een enkele oplossing en een enkel beschermingsschema kunnen worden gebruikt voor zowel noodherstel als gegevensbeveiliging.

Voor Microsoft Exchange Server kunt u kiezen voor **Back-up van postvak**. Dit is een back-up van afzonderlijke postvakken via het Exchange-webservices-protocol. De postvakken of postvakitems kunnen worden hersteld naar een live Exchange-server of naar Microsoft 365. Het maken van back-ups van postvakken wordt ondersteund voor Microsoft Exchange Server 2010 Service Pack 1 (SP1) en later.

Microsoft SharePoint beveiligen

Een Microsoft SharePoint-farm bestaat uit front-endservers met SharePoint-services, databaseservers met Microsoft SQL Server en (optionele) applicatieservers voor offloading van bepaalde SharePoint-services vanaf de front-endservers. Bepaalde front-end- en applicatieservers kunnen identiek zijn.

Een hele SharePoint-farm beveiligen:

- Maak een back-up van alle databaseservers via een applicatiegerichte back-up.
- Maak een back-up van alle unieke front-endservers en applicatieservers via de gebruikelijke back-up op schijfniveau.

De back-ups van alle servers moeten volgens hetzelfde schema worden gedaan.

Als u alleen de inhoud wilt beveiligen, kunt u afzonderlijke back-ups van de inhoudsdatabases maken.

Een domeincontroller beveiligen

Een machine met Active Directory Domain Services kan worden beveiligd met een applicatiegerichte back-up. Als een domein meer dan een domeincontroller bevat en u een van deze controllers herstelt, wordt een niet-bindende herstelbewerking uitgevoerd en vindt er geen USN-terugdraaiactie plaats na het herstel.

Applicaties herstellen

De volgende tabel bevat een overzicht van de beschikbare herstelmethoden voor applicaties.

	Vanaf een databaseback-up	**Vanaf een applicatiegerichte back-up**	**Vanaf een schijfback-up**
Microsoft SQL Server	Databases naar een live SQL Server-exemplaar Databases als bestanden	Volledige machine Databases naar een live SQL Server-exemplaar Databases als bestanden	Volledige machine
Microsoft Exchange Server	Databases naar een live Exchange Databases als bestanden Gedetailleerd herstel naar live Exchange of naar Microsoft 365*	Volledige machine Databases naar een live Exchange Databases als bestanden Gedetailleerd herstel naar live Exchange of naar Microsoft 365*	Volledige machine
Microsoft SharePoint-databaseservers	Databases naar een live SQL Server-exemplaar Databases als bestanden Gedetailleerd herstel met SharePoint Explorer	Volledige machine Databases naar een live SQL Server-exemplaar Databases als bestanden Gedetailleerd herstel met SharePoint Explorer	Volledige machine
Microsoft SharePoint-front-endwebservers	-	-	Volledige machine
Active Directory Domain Services	-	Volledige machine	-

*Gedetailleerd herstel is ook beschikbaar via een back-up van een postvak. Herstel van Exchange-gegevensitems naar Microsoft 365, en vice versa, wordt ondersteund indien Agent voor Microsoft 365 lokaal is geïnstalleerd.

Vereisten

Voordat u de applicatieback-up configureert, controleert u of wordt voldaan aan de volgende vereisten.

Gebruik de opdracht `vssadmin list writers` om de status van VSS Writers te controleren.

Algemene vereisten

Voor Microsoft SQL Server controleert u het volgende:

- Er is ten minste één Microsoft SQL Server-exemplaar gestart.
- De SQL-writer voor VSS is ingeschakeld.

Voor Microsoft Exchange Server controleert u het volgende:

- De Microsoft Exchange Information Store-service is gestart.
- Windows PowerShell is geïnstalleerd. Voor Exchange 2010 of later is ten minste Windows PowerShell versie 2.0 vereist.
- Microsoft .NET Framework is geïnstalleerd.
  Voor Exchange 2007 of later is ten minste Microsoft .NET Framework versie 2.0 vereist.
  Voor Exchange 2010 of later is ten minste Microsoft .NET Framework versie 3.5 vereist.
- De Exchange-writer voor VSS is ingeschakeld.

Opmerking
Voor een goede werking van Agent voor Exchange is tijdelijke opslag vereist. De tijdelijke bestanden zijn standaard te vinden in `%ProgramData%\Acronis\Temp`. Controleer of het volume met de map `%ProgramData%` net zoveel vrije schijfruimte beschikbaar heeft als 15 procent van de omvang van een Exchange-database. U kunt ook de locatie van de tijdelijke bestanden wijzigen voordat u Exchange-back-ups maakt, zoals beschreven in De locatie van tijdelijke bestanden en mappen wijzigen (40040).

Op een domeincontroller controleert u het volgende:

- De Active Directory-writer voor VSS is ingeschakeld.

Bij het maken van een beschermingsschema moet aan het volgende zijn voldaan:

- Voor fysieke machines en machines met geïnstalleerde agent is de back-upoptie Volume Shadow Copy Service (VSS) ingeschakeld.
- Voor virtuele machines is de back-upoptie Volume Shadow Copy Service (VSS) voor virtuele machines ingeschakeld.

Aanvullende vereisten voor applicatiegerichte back-ups

Wanneer u een beschermingsschema maakt, controleert u of **Volledige machine** is geselecteerd voor de back-up. De back-upoptie **Sector-voor-sector** moet worden uitgeschakeld in een beschermingsschema, anders is het onmogelijk om toepassingsgegevens van dergelijke back-ups te herstellen. Als het schema wordt uitgevoerd in de modus **sector-voor-sector** omdat automatisch wordt overgeschakeld naar deze modus, dan kunnen de toepassingsgegevens ook niet worden hersteld.

Vereisten voor virtuele ESXi-machines

Als de toepassing wordt uitgevoerd op een virtuele machine waarvan back-ups worden gemaakt met Agent voor VMware, controleert u het volgende:

- De virtuele machine waarvan u een back-up maakt, voldoet aan de vereisten voor applicatieconsistente back-up en herstel, zoals vermeld in het artikel 'Windows Backup Implementations' in de VMware-documentatie: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html.
- VMware Tools is geïnstalleerd en up-to-date op de machine.
- Gebruikersaccountbeheer is uitgeschakeld op de machine. Als u UAC niet wilt uitschakelen, moet u de referenties van de ingebouwde domeinbeheerder (DOMAIN\Administrator) opgeven wanneer u back-ups van toepassingen inschakelt.
  Als u UAC niet wilt uitschakelen, moet u de referenties van de ingebouwde domeinbeheerder (DOMAIN\Administrator) opgeven wanneer u back-ups van toepassingen inschakelt.

  Opmerking
  Gebruik het ingebouwde account van de domeinbeheerder dat is geconfigureerd als onderdeel van het domein toen dit werd gemaakt. Later gemaakte accounts worden niet ondersteund.

Vereisten voor virtuele Hyper-V-machines

Als de toepassing wordt uitgevoerd op een virtuele machine waarvan back-ups worden gemaakt met Agent voor Hyper-V, controleert u het volgende:

- Het gastbesturingssysteem is Windows Server 2008 of later.
- For Hyper-V 2008 R2: het gastbesturingssysteem is Windows Server 2008/2008 R2/2012.
- De virtuele machine heeft geen dynamische schijven.
- Er bestaat en netwerkverbinding tussen de Hyper-V-host en het gastbesturingssysteem. Dit is vereist voor het uitvoeren van WMI-query's op afstand in de virtuele machine.
- Gebruikersaccountbeheer is uitgeschakeld op de machine. Als u UAC niet wilt uitschakelen, moet u de referenties van de ingebouwde domeinbeheerder (DOMAIN\Administrator) opgeven wanneer u back-ups van toepassingen inschakelt.
  Als u UAC niet wilt uitschakelen, moet u de referenties van de ingebouwde domeinbeheerder (DOMAIN\Administrator) opgeven wanneer u back-ups van toepassingen inschakelt.

Opmerking
Gebruik het ingebouwde account van de domeinbeheerder dat is geconfigureerd als onderdeel van het domein toen dit werd gemaakt. Later gemaakte accounts worden niet ondersteund.

- De configuratie van de virtuele machine voldoet aan de volgende criteria:
  - Hyper-V-integratieservices zijn geïnstalleerd en up-to-date op de machine. De kritieke update is https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - De optie **Beheer** > **Integratieservices** > **Back-up (controlepunt van volume)** is ingeschakeld in de instellingen van de virtuele machine.
  - Voor Hyper-V 2012 en later: de virtuele machine heeft geen controlepunten.
  - Voor Hyper-V 2012 R2 en later: de virtuele machine heeft een SCSI-controller (zie **Instellingen** > **Hardware**).

Databaseback-up

Voordat u een back-up maakt van databases, moet u controleren of wordt voldaan aan de vereisten zoals vermeld in 'Vereisten'.

Selecteer de databases zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

SQL-databases selecteren

Een back-up van een SQL-database bevat de databasebestanden (.mdf, .ndf), logboekbestanden (.ldf) en andere bijbehorende bestanden. Er wordt een back-up van de bestanden gemaakt met behulp van de SQL Writer-service. De service moet worden uitgevoerd op het moment dat de VSS-service (Volume Shadow Copy) een back-up- of herstelbewerking aanvraagt.

De SQL-transactielogboeken worden na elke geslaagde back-up ingekort. Het inkorten van het SQL-logboek kan worden uitgeschakeld in de opties van het beschermingsschema.

SQL-databases selecteren

1. Klik op **Apparaten** > **Microsoft SQL**.
   De software toont de structuur van AlwaysOn-beschikbaarheidsgroepen (AAG) in SQL Server, machines met Microsoft SQL Server, SQL Server-exemplaren en databases.
2. Blader naar de gegevens waarvan u een back-up wilt maken.
   Vouw de structuurknooppunten uit of dubbelklik op items in de lijst rechts van de structuur.
3. Selecteer de gegevens waarvan u een back-up wilt maken. U kunt AAG's, machines met SQL Server, SQL Server-exemplaren of individuele databases selecteren.
   - Als u een AAG selecteert, wordt er een back-up gemaakt van alle databases die zijn opgenomen in de geselecteerde AAG. Zie 'AlwaysOn-beschikbaarheidsgroepen (AAG) beschermen' voor meer informatie over het maken van back-ups van AAG's of afzonderlijke AAG-databases.

- Als u een machine selecteert met een SQL-server, wordt er een back-up gemaakt van alle databases die zijn gekoppeld aan alle SQL Server-exemplaren die worden uitgevoerd op de geselecteerde machine.
- Als u een SQL Server-exemplaar selecteert, wordt er een back-up gemaakt van alle databases die zijn gekoppeld aan het geselecteerde exemplaar.
- Als u de databases rechtstreeks selecteert, wordt er alleen een back-up gemaakt van de geselecteerde databases.

4. Klik op **Beschermen**. Geef desgevraagd de referenties voor toegang tot de SQL Server op.

   Als u Windows-verificatie gebruikt, moet het account lid zijn van de groep **Back-upoperators** of **Beheerders** op de machine en lid zijn van de rol **sysadmin** op elk van de exemplaren waarvan u een back-up wilt maken.

   Als u SQL Server-verificatie gebruikt, moet het account lid zijn van de rol **sysadmin** op elk van de exemplaren waarvan u een back-up wilt maken.

Exchange Server-gegevens selecteren

De volgende tabel bevat een overzicht van de Microsoft Exchange Server-gegevens die u voor een back-upbewerking kunt selecteren en van de gebruikersrechten die u minimaal nodig hebt om een back-up van de gegevens te maken.

Exchange-versie	Gegevensitems	Gebruikersrechten
2007	Opslaggroepen	Lid van de rolgroep **Beheerders van de Exchange-organisatie**.
2010/2013/2016/2019	Databases, Databasebeschikbaarheidsgroepen (DAG)	Lid van de rolgroep **Serverbeheer**.

Een volledige back-up bevat alle geselecteerde Exchange Server-gegevens.

Een incrementele back-up bevat de gewijzigde blokken van de databasebestanden, de controlepuntbestanden en een klein aantal logboekbestanden dat recenter is dan de bijbehorende controlepunt van de database. Aangezien de wijzigingen in de databasebestanden worden opgenomen in de back-up, hoeft er geen back-up worden gemaakt van alle transactielogboekrecords sinds de vorige back-up. Alleen het logboek dat recenter is dan de controlepunt moet na de herstelbewerking worden herhaald. Dit zorgt ervoor dat de herstelbewerking sneller wordt uitgevoerd en dat de back-up van de database lukt, zelfs wanneer de functie voor circulaire logboekregistratie is ingeschakeld.

De transactielogbestanden worden na elke geslaagde back-up afgebroken.

Exchange Server-gegevens selecteren

1. Klik op **Apparaten** > **Microsoft Exchange**.

   Automatisch wordt de structuur weergegeven van de Databasebeschikbaarheidsgroepen (DAG) in Exchange Server, de machines met Microsoft Exchange Server en de Exchange Server-

databases. Als u Agent voor Exchange hebt geconfigureerd zoals beschreven in "Back-up van postvak" (p. 604), worden er ook postvakken weergegeven in deze structuur.

2. Blader naar de gegevens waarvan u een back-up wilt maken.

   Vouw de structuurknooppunten uit of dubbelklik op items in de lijst rechts van de structuur.

3. Selecteer de gegevens waarvan u een back-up wilt maken.
   - Als u een DAG selecteert, wordt een back-up gemaakt van elk exemplaar van een geclusterde database. Zie "Databasebeschikbaarheidsgroepen (DAG) beveiligen" (p. 599) voor meer informatie over het maken van back-ups van DAG's.
   - Als u een machine selecteert met Microsoft Exchange Server, wordt er een back-up gemaakt van alle databases die zijn gekoppeld aan de Exchange Server die wordt uitgevoerd op de geselecteerde machine.
   - Als u de databases rechtstreeks selecteert, wordt er alleen een back-up gemaakt van de geselecteerde databases.
   - Als u Agent voor Exchange hebt geconfigureerd zoals beschreven in "Back-up van postvak" (p. 604), kunt u postvakken selecteren voor back-up.

   Als uw selectie meerdere databases bevat, worden deze met twee tegelijk verwerkt. Wanneer de back-up van de eerste groep is voltooid, begint de back-up van de volgende groep.

4. Geef desgevraagd de referenties voor toegang tot de gegevens op.

5. Klik op **Beschermen**.

AlwaysOn-beschikbaarheidsgroepen (AAG) beschermen

Opmerking
Deze functie is alleen beschikbaar met het Advanced Backup-pakket.

Overzicht van SQL Server-oplossingen met hoge beschikbaarheid

Met de functionaliteit Failoverclustering van Windows Server (WSFC) kunt u een SQL Server met hoge beschikbaarheid configureren via redundantie op exemplaarniveau (failoverclusterexemplaar, FCI) of op databaseniveau (AlwaysOn-beschikbaarheidsgroep, AAG). Het is ook mogelijk om beide methoden te combineren.

In een failoverclusterexemplaar bevinden SQL-databases zich op een gedeelde opslag. Deze opslag is alleen toegankelijk via het actieve clusterknooppunt. Als het actieve knooppunt mislukt, vindt er een failover plaats en wordt er een ander knooppunt actief.

In een beschikbaarheidsgroep bevindt elke databasereplica zich op een ander knooppunt. Als de primaire replica niet meer beschikbaar is, wordt er een secundaire replica die zich op een ander knooppunt bevindt aan de primaire rol toegewezen.

De clusters functioneren dus zelf al als noodhersteloplossing. Er zijn echter mogelijk situaties waarin clusters geen gegevensbescherming kunnen bieden, bijvoorbeeld in het geval van logische beschadiging van een database of als het gehele cluster niet beschikbaar is. Clusteroplossingen

bieden eveneens geen bescherming tegen schadelijke inhoudswijzigingen, aangezien deze onmiddellijk worden gerepliceerd naar alle clusterknooppunten.

Ondersteunde clusterconfiguraties

Deze back-upsoftware biedt *alleen* ondersteuning voor de AlwaysOn- beschikbaarheidsgroep (AAG) voor SQL Server 2012 of later. Andere clusterconfiguraties, zoals failoverclusterexemplaren, databasespiegeling en back-ups van logboekbestanden, worden *niet* ondersteund.

Hoeveel agents zijn vereist voor back-up en herstel van clustergegevens?

Voor back-up en herstel van de gegevens van een cluster dient Agent voor SQL op elk knooppunt van het WSFC-cluster te zijn geïnstalleerd.

Back-ups van databases in een AAG maken

1. Installeer Agent voor SQL op elk knooppunt van het WSFC-cluster.
2. Selecteer de AAG waarvan u een back-up wilt maken zoals wordt beschreven in "SQL-databases selecteren".

   U moet de AAG zelf selecteren om een back-up te maken van alle databases van de AAG. Als u een back-up wilt maken van een set databases, moet u deze set databases definiëren in alle knooppunten van de AAG.

   Waarschuwing!
   De set databases moet in alle knooppunten exact hetzelfde zijn. Als ook maar één set verschillend is, of niet op alle knooppunten is gedefinieerd, zal de clusterback-up niet correct werken.
3. Configureer de back-upoptie "Clusterback-upmodus".

Herstel van databases in een AAG

1. Selecteer de databases die u wilt herstellen en selecteer vervolgens het herstelpunt waarvandaan u de databases wilt herstellen.

   Als u een geclusterde database selecteert onder **Apparaten** > **Microsoft SQL** > **Databases** en vervolgens op **Herstellen** klikt, worden alleen de herstelpunten weergegeven die overeenkomen met de tijden waarop er een back-up is gemaakt van de geselecteerde kopie van de database.

   De eenvoudigste manier om alle herstelpunten van een geclusterde database weer te geven, is om de back-up van de gehele AAG te selecteren op het tabblad Back-upopslag. De namen van de AAG-back-ups zijn gebaseerd op de sjabloon `<naam van AAG> - <naam van beschermingsschema>` en zijn voorzien van een speciaal pictogram.
2. Als u het herstel wilt configureren, volgt u de stappen die worden beschreven in 'SQL-databases herstellen', vanaf stap 5.

Er wordt automatisch een clusterknooppunt gedefinieerd waarnaar de gegevens worden hersteld. De naam van het knooppunt wordt weergegeven in het veld **Herstellen naar**. U kunt het doelknooppunt handmatig wijzigen.

Belangrijk
Een database in een AlwaysOn-beschikbaarheidsgroep kan tijdens herstel niet worden overschreven, omdat Microsoft SQL Server dit verhindert. U dient de doeldatabase vóór het herstel van de AAG uit te sluiten. U kunt de database ook herstellen als nieuwe database buiten AAG. Wanneer de herstelbewerking is voltooid, kunt u de oorspronkelijke AAG-configuratie reconstrueren.

Databasebeschikbaarheidsgroepen (DAG) beveiligen

Opmerking
Deze functie is alleen beschikbaar met het Advanced Backup-pakket.

Overzicht van Exchange Server-clusters

Exchange-clusters worden met name gebruikt om te zorgen voor hoge beschikbaarheid van databases met een snelle failover zonder gegevensverlies. Doorgaans wordt dit bereikt door een of meer exemplaren van databases of opslag op de leden van het cluster (clusterknooppunten) te gebruiken. Als het clusterknooppunt dat functioneert als host van de actieve databasekopie of van de actieve databasekopie zelf mislukt, neemt het andere knooppunt dat functioneert als host voor de passieve kopie de bewerkingen automatisch over van het mislukte knooppunt en biedt dit met minimale downtime toegang tot Exchange-services. De clusters functioneren dus zelf al als noodhersteloplossing.

Er zijn echter mogelijk situaties waarin failoverclusteroplossingen geen gegevensbescherming kunnen bieden, bijvoorbeeld in het geval van logische beschadiging van een database of als een bepaalde database in een cluster geen kopie (replica) heeft of het gehele cluster niet beschikbaar is. Clusteroplossingen bieden eveneens geen bescherming tegen schadelijke inhoudswijzigingen, aangezien deze onmiddellijk worden gerepliceerd naar alle clusterknooppunten.

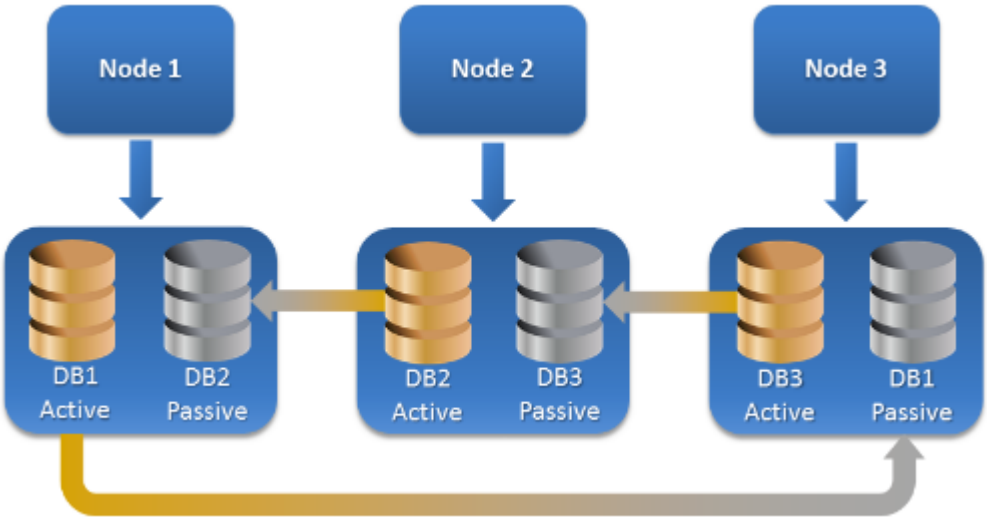
Clustergerichte back-up

Met clustergerichte back-up maakt u een back-up van slechts één exemplaar van de geclusterde gegevens. Als de plaats van de gegevens binnen het cluster wordt gewijzigd (vanwege een switchover of failover), worden alle verplaatsingen van deze gegevens bijgehouden en wordt hiervan een veilige back-up gemaakt.

Ondersteunde clusterconfiguraties

Clustergerichte back-ups worden *alleen* ondersteund voor Databasebeschikbaarheidsgroep (DAG) in Exchange Server 2010 of later. Andere clusterconfiguraties, zoals cluster met enkele opslaggroep (SCC) en continue replicatie in een cluster (CCR) voor Exchange 2007, worden *niet* ondersteund.

DAG is een groep die bestaat uit maximaal 16 Exchange-postvakservers. Elk knooppunt kan functioneren als een host voor een kopie van een postvakdatabase van elk ander knooppunt. Elk knooppunt kan functioneren als host voor passieve en actieve databasekopieën. Van elke database kunnen maximaal 16 kopieën worden gemaakt.



Hoeveel agenten zijn vereist voor clustergerichte back-ups en herstel van clustergegevens?

Voor back-up en herstel van geclusterde databases moet Agent voor Exchange zijn geïnstalleerd op elk knooppunt van het Exchange-cluster.

Opmerking
Wanneer u de agent op een van de knooppunten hebt geïnstalleerd, worden de DAG en de bijbehorende knooppunten weergegeven in de Cyber Protect-console onder **Apparaten** > **Microsoft Exchange** > **Databases**. Als u Agent voor Exchange wilt installeren op de rest van de knooppunten, selecteert u de DAG, klikt u op **Details** en klikt u vervolgens op **Agent installeren** naast elk knooppunt.

Een back-up van de Exchange-clustergegevens maken

1. Wanneer u een beschermingsschema maakt, selecteert u de DAG, zoals beschreven in "Exchange Server-gegevens selecteren" (p. 596).
2. Configureer de back-upoptie voor "Clusterback-upmodus" (p. 485).
3. Geef naar wens de andere instellingen van het beschermingsschema op.

Belangrijk
Voor clustergerichte back-ups moet u de DAG zelf selecteren. Als u afzonderlijke knooppunten of databases selecteert binnen de DAG, wordt er geen back-up gemaakt van de geselecteerde items en wordt de optie **Clusterback-upmodus** genegeerd.

De Exchange-clustergegevens herstellen

1. Selecteer het herstelpunt voor de databases die u wilt herstellen. Het is niet mogelijk een volledige cluster te selecteren voor herstel.

   Wanneer u een exemplaar van een geclusterde database selecteert onder **Apparaten** > **Microsoft Exchange** > **Databases** > <clusternaam> > <knooppuntnaam> en vervolgens op **Herstellen** klikt, worden alleen de herstelpunten weergegeven die overeenkomen met de tijden waarop een back-up is gemaakt van dit exemplaar.

   De eenvoudigste manier om alle herstelpunten van een geclusterde database weer te geven, is om de back-up te selecteren op het tabblad Back-upopslag.
2. Volg de stappen die worden beschreven in "Exchange-databases herstellen" (p. 614), te beginnen bij stap 5.

   Er wordt automatisch een clusterknooppunt gedefinieerd waarnaar de gegevens worden hersteld. De naam van het knooppunt wordt weergegeven in het veld **Herstellen naar**. U kunt het doelknooppunt handmatig wijzigen.

Applicatiegerichte back-up

Applicatiegerichte back-up op schijfniveau is beschikbaar voor fysieke machines, virtuele ESXi-machines en virtuele Hyper-V-machines.

Wanneer u een back-up maakt van een machine waarop Microsoft SQL Server, Microsoft Exchange Server of Active Directory Domain Services wordt uitgevoerd, schakelt u **Back-up van toepassing** in voor extra bescherming van de gegevens van deze toepassingen.

Waarom applicatiegerichte back-up gebruiken?

Applicatiegerichte back-up biedt de volgende voordelen:

- De back-ups van de applicaties worden gemaakt in een consistente status en deze zijn dus onmiddellijk beschikbaar nadat de machine is hersteld.
- U kunt de SQL- en Exchange-databases, postvakken en postvakitems herstellen zonder de volledige machine te herstellen.
- De SQL-transactielogboeken worden na elke geslaagde back-up ingekort. Het inkorten van het SQL-logboek kan worden uitgeschakeld in de opties van het beschermingsschema. De Exchange-transactielogboeken worden alleen ingekort op virtuele machines. U kunt de optie Volledige VSS-back-up inschakelen als u Exchange-transactielogboeken wilt inkorten op een fysieke machine.
- Als een domein meer dan een domeincontroller bevat en u een van deze controllers herstelt, wordt een niet-bindende herstelbewerking uitgevoerd en vindt er geen USN-terugdraaiactie plaats na het herstel.

Wat is er nodig voor applicatiegerichte back-ups?

Op een fysieke machine moeten naast Agent voor Windows ook Agent voor SQL en/of Agent voor Exchange zijn geïnstalleerd.

Op een virtuele machine hoeven geen agenten te worden geïnstalleerd; er wordt van uitgegaan dat back-ups van de machine worden gemaakt met Agent voor VMware (Windows) of Agent voor Hyper-V.

Opmerking
Voor virtuele Hyper-V- en VMware ESXi-machines waarop Windows Server 2022 wordt uitgevoerd, wordt applicatiegerichte back-up niet ondersteund in de modus zonder agent, dat wil zeggen wanneer de back-up wordt uitgevoerd door Agent voor Hyper-V of Agent voor VMware. Als u Microsoft-toepassingen wilt beschermen op deze machines, installeert u Agent voor Windows binnen het gastbesturingssysteem.

Met Agent voor VMware (Virtual Appliance) kunnen applicatiegerichte back-ups worden gemaakt, maar hiervan kunnen geen toepassingsgegevens worden hersteld. Als u toepassingsgegevens wilt herstellen van back-ups die door deze agent zijn gemaakt, hebt u Agent voor VMware (Windows), Agent voor SQL of Agent voor Exchange nodig op een machine die toegang heeft tot de locatie waar de back-ups zijn opgeslagen. Wanneer u herstel van toepassingsgegevens configureert, selecteert u het herstelpunt op het tabblad **Back-upopslag** en selecteert u vervolgens de machine in **Machine waarmee u wilt bladeren**.

Zie de gedeelten 'Vereisten' en 'Vereiste gebruikersrechten' voor andere vereisten.

Opmerking
Applicatiegerichte back-ups van virtuele Hyper-V-machines kunnen mislukken met de foutmelding 'WMI 'ExecQuery' failed executing query.' (WMI ExecQuery kan query niet uitvoeren) of 'Failed to create a new process via WMI' (kan geen nieuw proces maken via WMI) als de back-ups worden uitgevoerd op een host met zware belasting, omdat er geen of een vertraagde reactie van Windows Management Instrumentation is. Probeer deze back-ups opnieuw uit te voeren op een tijdstip waarop de host minder zwaar is belast.

Vereiste gebruikersrechten voor applicatiegerichte back-ups

Een applicatiegerichte back-up bevat metagegevens van VSS-compatibele applicaties die aanwezig zijn op de schijf. Als u wilt dat de agent toegang heeft tot deze metagegevens, hebt u een account met de juiste rechten nodig, zoals aangegeven in de lijst die u hier kunt vinden. U wordt gevraagd dit account op te geven wanneer u een applicatieback-up inschakelt.

- Voor SQL Server:
  Het account moet lid zijn van de groep **Back-upoperators** of **Beheerders** op de machine en lid zijn van de **sysadmin**-rol voor elk van de exemplaren waarvan u een back-up gaat maken.

Opmerking
Alleen Windows-verificatie wordt ondersteund.

- Voor Exchange Server:
  Exchange 2007: Het account moet lid zijn van de groep **Beheerders** op de machine en van de groep **Beheerdersrol voor Exchange (Organisatie)**.
  Exchange 2010 en later: Het account moet lid zijn van de groep **Beheerders** op de machine en van de rolgroep **Organisatiebeheer**.
- Voor Active Directory:
  Het account moet een domeinbeheerder zijn.

Aanvullende vereisten voor virtuele machines

Als de toepassing wordt uitgevoerd op een virtuele machine waarvan back-ups worden gemaakt met Agent voor VMware of Agent voor Hyper-V, controleert u of Gebruikersaccountbeheer (UAC) is uitgeschakeld op de machine.

Als u UAC niet wilt uitschakelen, moet u de referenties van de ingebouwde domeinbeheerder (DOMAIN\Administrator) opgeven wanneer u back-ups van toepassingen inschakelt.

Opmerking
Gebruik het ingebouwde account van de domeinbeheerder dat is geconfigureerd als onderdeel van het domein toen dit werd gemaakt. Later gemaakte accounts worden niet ondersteund.

Aanvullende vereisten voor machines met Windows

Voor alle Windows-versies moet u het beleid voor gebruikersaccountbeheer (UAC) uitschakelen om applicatiegerichte back-ups toe te staan.

Als u UAC niet wilt uitschakelen, moet u de referenties van de ingebouwde domeinbeheerder (DOMAIN\Administrator) opgeven wanneer u back-ups van toepassingen inschakelt.

Opmerking
Gebruik het ingebouwde account van de domeinbeheerder dat is geconfigureerd als onderdeel van het domein toen dit werd gemaakt. Later gemaakte accounts worden niet ondersteund.

Het UAC-beleid uitschakelen in Windows:

1. Zoek de volgende registersleutel in de Register-editor:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. Stel de waarde van **EnableLUA** in op **0**.
3. Start de machine opnieuw op.

Back-up van postvak

Het maken van back-ups van postvakken wordt ondersteund voor Microsoft Exchange Server 2010 Service Pack 1 (SP1) en later.

Het maken van een back-up van het postvak is beschikbaar als ten minste één Agent voor Exchange is geregistreerd op de beheerserver. De agent moet zijn geïnstalleerd op een machine die behoort tot hetzelfde Active Directory-forest als Microsoft Exchange Server.

Voordat u een back-up kunt maken van postvakken, moet u Agent voor Exchange verbinden met de machine met de serverrol **Clienttoegang** (CAS) van Microsoft Exchange Server. In Exchange 2016 en later is de CAS-rol niet beschikbaar als afzonderlijke installatieoptie. Deze wordt automatisch geïnstalleerd als onderdeel van de postvakserverfunctie. U kunt de agent dan verbinden met elke server waarop de **postvakfunctie** wordt uitgevoerd.

Opmerking
U kunt postvakken en postvakitems ook herstellen vanuit databaseback-ups en applicatiegerichte back-ups. Zie "Exchange-postvakken en postvakitems herstellen" (p. 617) voor meer informatie. Met databaseback-ups en applicatiegerichte back-ups kunt u geen beschermingsschema's maken voor afzonderlijke postvakken.

Agent voor Exchange verbinden met CAS

1. Klik op **Apparaten** > **Toevoegen**.
2. Klik op **Microsoft Exchange Server**.
3. Klik op **Exchange-postvakken**.
   Als er geen Agent voor Exchange is geregistreerd op de beheerserver, wordt u gevraagd om een agent te installeren. Na de installatie herhaalt u deze procedure vanaf stap 1.
4. [Optioneel] Als meerdere agenten voor Exchange zijn geregistreerd op de beheerserver, klikt u op **Agent** en wijzigt u de agent die de back-up gaat uitvoeren.
5. Geef in **Server voor clienttoegang** de FQDN (Fully Qualified Domain Name) op van de machine waarop de rol **Clienttoegang** van Microsoft Exchange Server is ingeschakeld.
   In Exchange 2016 en later worden de services voor clienttoegang automatisch geïnstalleerd als onderdeel van de postvakserverfunctie. U kunt dan elke server opgeven waarop de **postvakfunctie** wordt uitgevoerd. Verderop in dit gedeelte wordt deze server aangeduid als CAS.
6. Selecteer in **Authenticatietype** het authenticatietype dat wordt gebruikt door de CAS. U kunt **Kerberos** (standaard) of **Standaard** selecteren.
7. [Uitsluitend voor standaardauthenticatie] Selecteer welk protocol zal worden gebruikt. U kunt **HTTPS** (standaard) of **HTTP** selecteren.
8. [Alleen voor standaardverificatie met het HTTPS-protocol] Als CAS gebruikmaakt van een SSL-certificaat dat is verkregen van een certificeringsinstantie en als u wilt dat de software het

certificaat controleert bij het maken van een verbinding met CAS, schakelt u het selectievakje **SSL-certificaat controleren** in. Anders kunt u deze stap overslaan.

9. Geef de referenties op van een account dat wordt gebruikt om toegang te krijgen tot CAS. De vereisten voor dit account worden vermeld in 'Vereiste gebruikersrechten'.
10. Klik op **Toevoegen**.

Hierdoor worden de postvakken weergegeven onder **Apparaten** > **Microsoft Exchange** > **Postvakken**.

Postvakken van Exchange Server selecteren

Selecteer de postvakken zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

Exchange-postvakken selecteren

1. Klik op **Apparaten** > **Microsoft Exchange**.
   De software toont de structuur van Exchange-databases en -postvakken.
2. Klik op **Postvakken** en selecteer vervolgens de postvakken waarvan u een back-up wilt maken.
3. Klik op **Beschermen**.

Vereiste gebruikersrechten

Als u wilt dat Agent voor Exchange toegang heeft tot postvakken, hebt u een account met de juiste rechten nodig. U wordt gevraagd dit account op te geven bij de configuratie van diverse bewerkingen met postvakken.

Het lidmaatschap van het account in de rolgroep **Organisatiebeheer** geeft toegang tot elk postvak, inclusief postvakken die in de toekomst worden gemaakt.

De minimaal vereiste gebruikersrechten zijn als volgt:

- Het account moet lid zijn van de rolgroepen **Server Management** en **Recipient Management**.
- In het account moet de beheerrol **ApplicationImpersonation** zijn ingeschakeld voor alle gebruikers of groepen gebruikers van wie de postvakken toegankelijk zijn voor de agent.
  Raadpleeg het volgende Microsoft Knowledge Base-artikel voor informatie over het configureren van de beheerrol **ApplicationImpersonation**: https: //msdn.microsoft.com/en-us/library/office/dn722376.aspx.

SQL-databases herstellen

U kunt SQL- en Exchange-databases herstellen vanaf databaseback-ups en applicatiegerichte back-ups. Raadpleeg "Microsoft SQL Server en Microsoft Exchange Server beschermen" (p. 591) voor meer informatie over het verschil tussen de twee typen back-ups.

U kunt SQL-databases herstellen naar het oorspronkelijke exemplaar, naar een ander exemplaar op de oorspronkelijke machine of naar een exemplaar op een andere machine dan de oorspronkelijke

machine. Wanneer u herstelt naar een andere machine dan de oorspronkelijke machine, moet Agent voor SQL zijn geïnstalleerd op de doelmachine.

U kunt databases ook herstellen als bestanden.

Als u Windows-verificatie gebruikt voor het SQL-exemplaar, moet u de referenties opgeven voor een account dat lid is van de groep **Back-upoperators** of **Beheerders** op de machine en dat lid is van de rol **sysadmin** op het doelexemplaar. Als u SQL Server-verificatie gebruikt, moet u de referenties opgeven voor een account dat lid is van de rol **sysadmin** op het doelexemplaar.

Systeemdatabases worden hersteld als gebruikersdatabases, met enkele verschillen. Raadpleeg "Systeemdatabases herstellen" (p. 613) voor meer informatie over deze verschillen.

Tijdens een herstel kunt u de voortgang van de bewerking controleren in de Cyber Protect-console, op het tabblad **Controle** > **Activiteiten**.

SQL-databases herstellen naar de oorspronkelijke machine

U kunt SQL-databases herstellen naar het oorspronkelijke exemplaar, naar een ander exemplaar op de oorspronkelijke machine of naar een exemplaar op een andere doelmachine.

SQL-databases herstellen naar de oorspronkelijke machine:

Vanaf een databaseback-up

1. Ga in de Cyber Protect-console naar **Apparaten** > **Microsoft SQL**.
2. Selecteer het SQL Server-exemplaar of klik op de naam van het exemplaar om specifieke databases te selecteren die u wilt herstellen en klik vervolgens op **Herstel**.
   Als de machine offline is, worden de herstelpunten niet weergegeven. Raadpleeg "SQL-databases herstellen naar een andere machine dan de oorspronkelijke machine" (p. 608) voor meer informatie over hoe u gegevens kunt herstellen naar een andere machine dan de oorspronkelijke machine.
3. Selecteer een herstelpunt.
   De herstelpunten worden gefilterd op locatie.
4. Klik op **Herstellen** > **Databases naar een exemplaar**.
   Het exemplaar en de databases worden standaard hersteld naar de oorspronkelijke items. U kunt een oorspronkelijke database ook herstellen als nieuwe database.
5. [Bij herstel naar een niet-oorspronkelijk exemplaar op dezelfde machine] Klik op **SQL Server-doelexemplaar**, selecteer het doelexemplaar en klik vervolgens op **Gereed**.
6. [Bij herstel van een database naar een nieuwe database] Klik op de naam van de database, ga naar **Herstellen naar** en selecteer **Nieuwe database**.
   - Geef een naam voor de nieuwe database op.
   - Geef het pad voor de nieuwe database op.
   - Geef het pad naar het logboek op.
7. [Optioneel] [Niet beschikbaar voor herstel van een database als nieuwe database] Als u de status van de database na de herstelbewerking wilt wijzigen, klikt u op de naam van de database, kiest

u een van de volgende statusopties en klikt u op **Gereed**.

- **Klaar voor gebruik (RESTORE WITH RECOVERY)** (standaard)

  Nadat de herstelbewerking is voltooid, is de database klaar voor gebruik. De database is volledig toegankelijk voor gebruikers. Alle niet-doorgevoerde transacties van de herstelde database die zijn opgeslagen in de transactielogboeken, worden door de software teruggedraaid. U kunt geen aanvullende transactielogboeken uit de systeemeigen Microsoft SQL-back-ups herstellen.
- **Niet-operationeel (RESTORE WITH NORECOVERY)**

  Nadat de herstelbewerking is voltooid, is de database niet-operationeel. Gebruikers hebben geen toegang tot de database. Alle niet-doorgevoerde transacties van de herstelde database worden door de software behouden. U kunt aanvullende transactielogboeken uit de systeemeigen Microsoft SQL-back-ups herstellen en dus het benodigde herstelpunt bereiken.
- **Alleen-lezen (RESTORE WITH STANDBY)**

  Nadat de herstelbewerking is voltooid, kunnen gebruikers de database alleen lezen. De software maakt alle niet-doorgevoerde transacties ongedaan. Deze bewerkingen worden echter opgeslagen in een tijdelijk stand-bybestand zodat de hersteleffecten kunnen worden teruggedraaid.

  Deze waarde wordt voornamelijk gebruikt om te bepalen op welk punt in de tijd zich een SQL Server-fout voordeed.

8. Klik op **Herstel starten**.

Vanaf een applicatiegerichte back-up

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de oorspronkelijke machine met de gegevens die u wilt herstellen en klik vervolgens op **Herstel**.

   Als de machine offline is, worden de herstelpunten niet weergegeven. Raadpleeg "SQL-databases herstellen naar een andere machine dan de oorspronkelijke machine" (p. 608) voor meer informatie over hoe u gegevens kunt herstellen naar een andere machine dan de oorspronkelijke machine.
3. Selecteer een herstelpunt.

   De herstelpunten worden gefilterd op locatie.
4. Klik op **Herstellen** > **SQL-databases**.
5. Selecteer het SQL Server-exemplaar of klik op de naam van het exemplaar om specifieke databases te selecteren die u wilt herstellen en klik vervolgens op **Herstellen**.

   Het exemplaar en de databases worden standaard hersteld naar de oorspronkelijke items. U kunt een oorspronkelijke database ook herstellen als nieuwe database.
6. [Bij herstel naar een niet-oorspronkelijk exemplaar op dezelfde machine] Klik op **SQL Server-doelexemplaar**, selecteer het doelexemplaar en klik vervolgens op **Gereed**.
7. [Bij herstel van een database naar een nieuwe database] Klik op de naam van de database, ga naar **Herstellen naar** en selecteer **Nieuwe database**.

- Geef een naam voor de nieuwe database op.
- Geef het pad voor de nieuwe database op.
- Geef het pad naar het logboek op.

8. [Optioneel] [Niet beschikbaar voor herstel van een database als nieuwe database] Als u de status van de database na de herstelbewerking wilt wijzigen, klikt u op de naam van de database, kiest u een van de volgende statusopties en klikt u op **Gereed**.
   - **Klaar voor gebruik (RESTORE WITH RECOVERY)** (standaard)

     Nadat de herstelbewerking is voltooid, is de database klaar voor gebruik. De database is volledig toegankelijk voor gebruikers. Alle niet-doorgevoerde transacties van de herstelde database die zijn opgeslagen in de transactielogboeken, worden door de software teruggedraaid. U kunt geen aanvullende transactielogboeken uit de systeemeigen Microsoft SQL-back-ups herstellen.
   - **Niet-operationeel (RESTORE WITH NORECOVERY)**

     Nadat de herstelbewerking is voltooid, is de database niet-operationeel. Gebruikers hebben geen toegang tot de database. Alle niet-doorgevoerde transacties van de herstelde database worden door de software behouden. U kunt aanvullende transactielogboeken uit de systeemeigen Microsoft SQL-back-ups herstellen en dus het benodigde herstelpunt bereiken.
   - **Alleen-lezen (RESTORE WITH STANDBY)**

     Nadat de herstelbewerking is voltooid, kunnen gebruikers de database alleen lezen. De software maakt alle niet-doorgevoerde transacties ongedaan. Deze bewerkingen worden echter opgeslagen in een tijdelijk stand-bybestand zodat de hersteleffecten kunnen worden teruggedraaid.

     Deze waarde wordt voornamelijk gebruikt om te bepalen op welk punt in de tijd zich een SQL Server-fout voordeed.
9. Klik op **Herstel starten**.

SQL-databases herstellen naar een andere machine dan de oorspronkelijke machine

U kunt zowel applicatiegerichte back-ups als databaseback-ups herstellen naar SQL Server-exemplaren op andere doelmachines waarop Agent voor SQL is geïnstalleerd. De back-ups moeten zich bevinden in de cloudopslag of in een gedeelde opslag waartoe de doelmachine toegang heeft.

De versie van de SQL Server op de doelmachine moet gelijk zijn aan of nieuwer zijn dan de versie van de bronmachine.

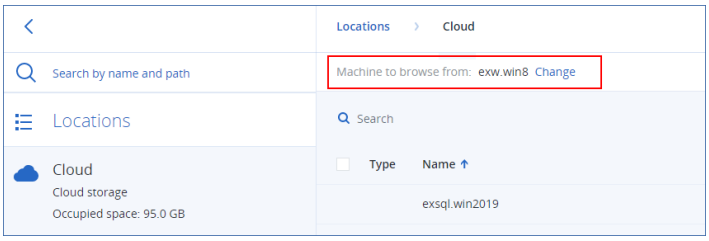
SQL-databases herstellen naar een andere machine dan de oorspronkelijke machine:

Vanuit back-upopslag

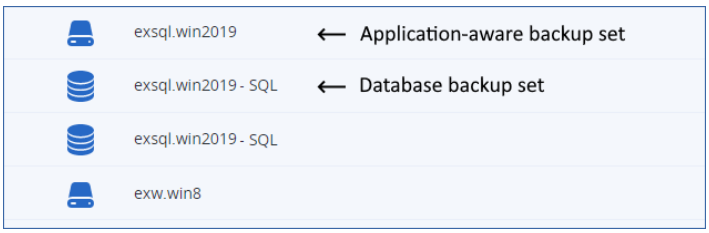
Deze procedure is van toepassing op applicatiegerichte back-ups en databaseback-ups.

1. Ga in de Cyber Protect-console naar **Back-upopslag**.
2. Selecteer de locatie van de back-upset waaruit u gegevens wilt herstellen.

3. Ga naar **Machine waarmee u wilt bladeren** en selecteer de doelmachine.
   Dit is de machine waarop u gegevens wilt herstellen. De doelmachine moet online zijn.



4. Selecteer de back-upset en klik vervolgens in het deelvenster **Acties** op **Back-ups weergeven**.
   Applicatiegerichte back-upsets en databaseback-upsets hebben een verschillend pictogram.



5. Selecteer het herstelpunt waaruit u gegevens wilt herstellen.
6. [Voor databaseback-ups] Klik op **SQL-databases herstellen**.
7. [Voor applicatiegerichte back-ups] Klik op **Herstellen** > **SQL-databases**.
8. Selecteer het SQL Server-exemplaar of klik op de naam van het exemplaar om specifieke databases te selecteren die u wilt herstellen en klik vervolgens op **Herstellen**.
9. [Als er meer dan één SQL-exemplaar is op de doelmachine] Klik op **SQL Server-doelexemplaar**, selecteer het doelexemplaar en klik vervolgens op **Gereed**.
10. Klik op de naam van de database, geef het pad naar de nieuwe database en het pad naar het logboek op en klik vervolgens op **Gereed**.
    U kunt in beide velden hetzelfde pad opgeven, bijvoorbeeld:

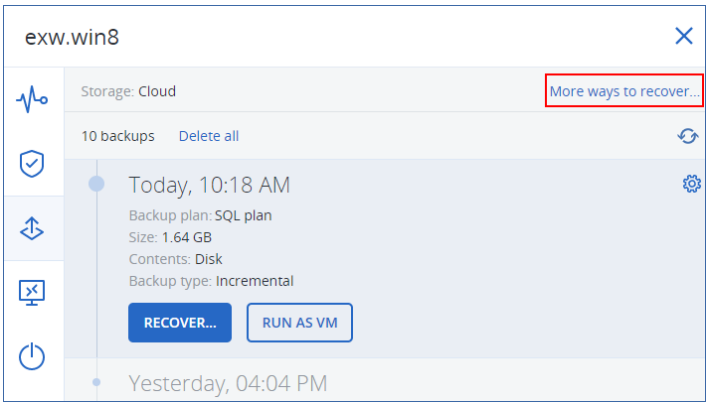
```
C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
```

11. Klik op **Herstel starten**.

Vanaf apparaten

Deze procedure is alleen van toepassing op applicatiegerichte back-ups.

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de oorspronkelijke machine met de gegevens die u wilt herstellen en klik vervolgens op **Herstel**.
3. [Als de bronmachine online is] Klik op **Meer herstelbewerkingen**.



4. Klik op **Machine selecteren** om de doelmachine te selecteren en klik vervolgens op **OK**.
   Dit is de machine waarop u gegevens wilt herstellen. De doelmachine moet online zijn.
5. Selecteer een herstelpunt.
   De herstelpunten worden gefilterd op locatie.
6. Klik op **Herstellen** > **SQL-databases**.
7. Selecteer het SQL Server-exemplaar of klik op de naam van het exemplaar om specifieke databases te selecteren die u wilt herstellen en klik vervolgens op **Herstellen**.
8. [Als er meer dan één SQL-exemplaar is op de doelmachine] Klik op **SQL Server-doelexemplaar**, selecteer het doelexemplaar en klik vervolgens op **Gereed**.
9. Klik op de naam van de database, geef het pad naar de nieuwe database en het pad naar het logboek op en klik vervolgens op **Gereed**.
   U kunt in beide velden hetzelfde pad opgeven, bijvoorbeeld:
   ```
   C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
   ```
10. Klik op **Herstel starten**.

SQL-databases herstellen als bestanden

U kunt databases herstellen als bestanden. Deze optie kan handig zijn wanneer u gegevens moet uitpakken voor gegevensanalyse, controledoeleinden of verdere verwerking door hulpprogramma's van derden. Raadpleeg "SQL Server-databases koppelen" (p. 613) voor meer informatie over hoe u de SQL-databasebestanden kunt koppelen aan een SQL Server-exemplaar.

U kunt databases als bestanden herstellen naar de oorspronkelijke machine of naar andere doelmachines waarop Agent voor SQL is geïnstalleerd. Wanneer u gegevens herstelt op andere machines dan de oorspronkelijke machine, moeten de back-ups zich bevinden in de cloudopslag of in een gedeelde opslag waartoe de doelmachine toegang heeft.

Opmerking
Als u Agent voor VMware (Windows) gebruikt, is het herstellen van databases als bestanden de enige herstelmogelijkheid. Herstellen van databases met Agent voor VMware (Virtual Appliance) is niet mogelijk.

SQL-databases herstellen als bestanden

Vanaf een databaseback-up

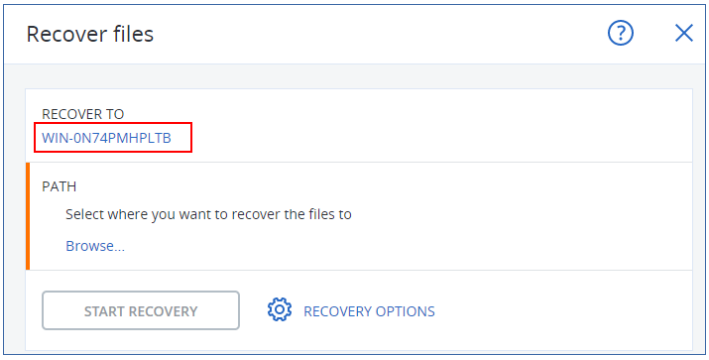
Deze procedure is van toepassing op online bronmachines.

1. Ga in de Cyber Protect-console naar **Apparaten** > **Microsoft SQL**.
2. Selecteer de databases die u wilt herstellen en klik vervolgens op **Herstel**.
3. Selecteer een herstelpunt.

   De herstelpunten worden gefilterd op locatie.
4. Klik op **Herstellen** > **Databases als bestanden**.
5. [Bij herstel naar een andere machine dan de oorspronkelijke machine] Ga naar **Herstellen naar** en selecteer de doelmachine.

   Dit is de machine waarop u gegevens wilt herstellen. De doelmachine moet online zijn.

   Als u de selectie wilt wijzigen, klikt u op de naam van de machine, selecteert u een andere machine en klikt u vervolgens op **OK**.



6. Ga naar **Pad**, klik op **Bladeren**, selecteer een lokale map of netwerkmap waarin u de bestanden wilt opslaan en klik vervolgens op **Gereed**.
7. Klik op **Herstel starten**.

Vanaf een applicatiegerichte back-up

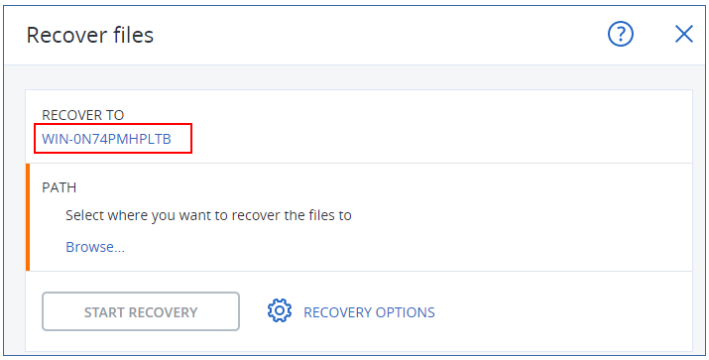
Deze procedure is van toepassing op online bronmachines.

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de oorspronkelijke machine met de gegevens die u wilt herstellen en klik vervolgens op **Herstel**.
3. Selecteer een herstelpunt.

   De herstelpunten worden gefilterd op locatie.
4. Klik op **Herstellen** > **SQL-databases**, selecteer de databases die u wilt herstellen en klik vervolgens op **Herstellen als bestanden**.
5. [Bij herstel naar een andere machine dan de oorspronkelijke machine] Ga naar **Herstellen naar** en selecteer de doelmachine.

   Dit is de machine waarop u gegevens wilt herstellen. De doelmachine moet online zijn.

   Als u de selectie wilt wijzigen, klikt u op de naam van de machine, selecteert u een andere machine en klikt u vervolgens op **OK**.

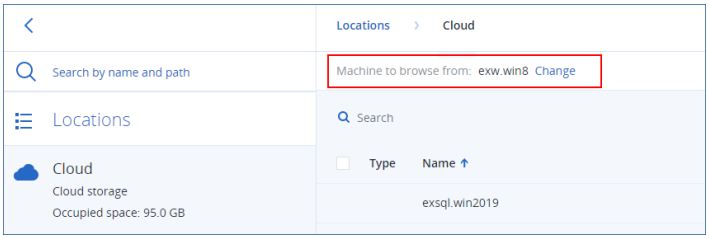


6. Ga naar **Pad**, klik op **Bladeren**, selecteer een lokale map of netwerkmap waarin u de bestanden wilt opslaan en klik vervolgens op **Gereed**.
7. Klik op **Herstel starten**.

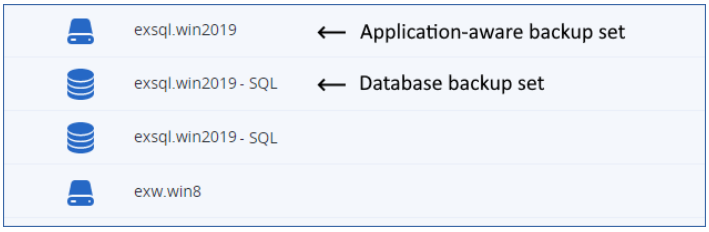
Vanaf een back-up op een offline machine

Deze procedure is van toepassing op applicatiegerichte back-ups en databaseback-ups op bronmachines die offline zijn.

1. Ga in de Cyber Protect-console naar **Back-upopslag**.
2. Selecteer de locatie van de back-upset waaruit u gegevens wilt herstellen.
3. Ga naar **Machine waarmee u wilt bladeren** en selecteer de doelmachine.
   Dit is de machine waarop u gegevens wilt herstellen. De doelmachine moet online zijn.



4. Selecteer de back-upset en klik vervolgens in het deelvenster **Acties** op **Back-ups weergeven**.
   Applicatiegerichte back-upsets en databaseback-upsets hebben een verschillend pictogram.



5. Selecteer het herstelpunt waaruit u gegevens wilt herstellen.
6. [Voor databaseback-ups] Klik op **SQL-databases herstellen**.
7. [Voor applicatiegerichte back-ups] Klik op **Herstellen** > **SQL-databases**.
8. Selecteer het SQL Server-exemplaar of klik op de naam van het exemplaar om specifieke databases te selecteren die u wilt herstellen en klik vervolgens op **Herstellen als bestanden**.
9. Ga naar **Pad**, klik op **Bladeren**, selecteer een lokale map of netwerkmap waarin u de bestanden

wilt opslaan en klik vervolgens op **Gereed**.

10. Klik op **Herstel starten**.

Systeemdatabases herstellen

Alle systeemdatabases van een exemplaar worden in één keer hersteld. Wanneer er een systeemdatabase wordt hersteld, zorgt de software ervoor dat het bestemmingsexemplaar automatisch opnieuw wordt opgestart in de modus voor één gebruiker. Nadat de herstelbewerking is voltooid, wordt het exemplaar opnieuw door de software opgestart en worden vervolgens de andere databases (indien aanwezig) hersteld.

Overige aandachtspunten voor het herstellen van systeemdatabases:

- Systeemdatabases kunnen alleen worden hersteld naar een exemplaar van dezelfde versie als het oorspronkelijke exemplaar.
- Systeemdatabases worden altijd hersteld naar de status 'klaar voor gebruik'.

De hoofddatabase herstellen

Systeemdatabases bevatten de **hoofddatabase**. De **hoofddatabase** registreert informatie over alle databases van het exemplaar. Daarom bevat de **hoofddatabase** in een back-up informatie over databases die zich op het moment van de back-up in het exemplaar bevonden. Nadat de **hoofddatabase** is hersteld, moet u mogelijk het volgende doen:

- Databases die aan het exemplaar zijn toegevoegd nadat de back-up is uitgevoerd, zijn niet zichtbaar voor het exemplaar. Om deze databases weer in productie te brengen, koppelt u ze handmatig aan het exemplaar door gebruik te maken van SQL Server Management Studio.
- Databases die zijn verwijderd nadat de back-up is uitgevoerd, worden in het exemplaar weergegeven als offline. Verwijder deze databases met SQL Server Management Studio.

SQL Server-databases koppelen

In dit gedeelte wordt beschreven hoe u een database koppelt in SQL Server via SQL Server Management Studio. U kunt slechts één database tegelijk koppelen.

Als u een database wilt koppelen, moet u beschikken over de volgende machtigingen: **CREATE DATABASE**, **CREATE ANY DATABASE** of **ALTER ANY DATABASE**. Deze machtigingen worden doorgaans toegekend aan de rol **sysadmin** van het exemplaar.

Een database koppelen

1. Voer Microsoft SQL Server Management Studio uit.
2. Maak verbinding met het vereiste SQL Server-exemplaar en vouw het exemplaar uit.
3. Klik met de rechtermuisknop op **Databases** en klik op **Koppelen**.
4. Klik op **Toevoegen**.

5. Ga naar het dialoogvenster **Databasebestanden zoeken** en zoek en selecteer het MDF-bestand van de database.
6. Controleer in het gedeelte **Databasedetails** of er andere databasebestanden (NDF- en LDF-bestanden) zijn gevonden.

   Details. SQL Server-databasebestanden worden mogelijk niet automatisch gevonden in de volgende gevallen:
   - Ze bevinden zich niet in de standaardlocatie of niet in dezelfde map als het primaire databasebestand (.mdf). Oplossing: Geef het pad naar de vereiste bestanden handmatig op in de kolom **Huidig bestandspad**.
   - U hebt een onvolledige set bestanden uit de database hersteld. Oplossing: Herstel de ontbrekende SQL Server-databasebestanden vanaf de back-up.
7. Wanneer alle bestanden zijn gevonden, klikt u op **OK**.

Exchange-databases herstellen

In dit gedeelte wordt beschreven hoe u herstelbewerkingen uitvoert vanaf databaseback-ups en applicatiegerichte back-ups.

U kunt gegevens van een Exchange-server herstellen naar een live Exchange-server. Dit kan de oorspronkelijke Exchange-server of een Exchange-server van dezelfde versie zijn die wordt uitgevoerd op de machine met dezelfde FQDN. Agent voor Exchange moet zijn geïnstalleerd op de doelmachine.

De volgende tabel bevat een overzicht van de Exchange Server-gegevens die u voor een herstelbewerking kunt selecteren en van de gebruikersrechten die u minimaal nodig hebt om de gegevens te herstellen.

Exchange-versie	Gegevensitems	Gebruikersrechten
2007	Opslaggroepen	Lid van de rolgroep **Beheerders van de Exchange-organisatie**.
2010/2013/2016/2019	Databases	Lid van de rolgroep **Serverbeheer**.

U kunt de databases (opslaggroepen) eventueel ook herstellen als bestanden. De databasebestanden in de back-up worden samen met de transactielogbestanden uitgepakt naar een map die u opgeeft. Dit kan handig zijn wanneer u gegevens moet uitpakken voor controledoeleinden, verdere verwerking met hulpprogramma's van derden of wanneer de herstelbewerking om de een of andere reden mislukt en u een tijdelijke oplossing zoekt om de de databases handmatig te koppelen.

Als u alleen Agent voor VMware (Windows) gebruikt, kunt u databases alleen als bestanden herstellen. Herstellen van databases met Agent voor VMware (Virtual Appliance) is niet mogelijk.

Voor onderstaande procedures wordt met term 'databases' zowel naar databases als naar opslaggroepen verwezen.

Exchange-databases herstellen naar een live Exchange-server

1. Voer een van de volgende handelingen uit:
   - Wanneer u herstelt vanaf een applicatiegerichte back-up: selecteer onder **Apparaten** de oorspronkelijke machine met de gegevens die u wilt herstellen.
   - Wanneer u herstelt vanaf een databaseback-up, klikt u op **Apparaten** > **Microsoft Exchange** > **Databases**, en selecteert u vervolgens de databases die u wilt herstellen.
2. Klik op **Herstel**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de machine offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:
   - [Alleen bij het herstellen vanaf een applicatiegerichte back-up] Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een online machine met Agent voor SQL of voor Agent voor Exchange en selecteert u vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad Back-upopslag.

   De machine die u hebt gekozen om te bladeren via een van de genoemde acties, wordt een doelmachine voor het herstel van de Exchange-gegevens.
4. Voer een van de volgende handelingen uit:
   - Wanneer u herstelt vanaf een applicatiegerichte back-up, klikt u op **Herstellen** > **SQL-databases**, selecteert u de databases die u wilt herstellen en klikt u vervolgens op **Herstellen**.
   - Wanneer u herstelt vanaf een databaseback-up, klikt u op **Herstellen** > **Databases naar een Exchange-server**.
5. De databases worden standaard hersteld naar de oorspronkelijke databases. Als de oorspronkelijke database niet bestaat, wordt deze opnieuw gemaakt.

   Een database herstellen als een andere database:
   a. Klik op de naam van de database.
   b. Selecteer bij **Herstellen naar** de optie **Nieuwe database**.
   c. Geef een naam voor de nieuwe database op.
   d. Geef het pad naar de nieuwe database en het pad naar het logboek op. De map die u opgeeft, moet de oorspronkelijke database en logboekbestanden bevatten.
6. Klik op **Herstel starten**.

De voortgang van de herstelbewerking wordt weergegeven op het tabblad Activiteiten.

Exchange-databases herstellen als bestanden

1. Voer een van de volgende handelingen uit:
   - Wanneer u herstelt vanaf een applicatiegerichte back-up: selecteer onder **Apparaten** de oorspronkelijke machine met de gegevens die u wilt herstellen.
   - Wanneer u herstelt vanaf een databaseback-up, klikt u op **Apparaten** > **Microsoft Exchange** > **Databases**, en selecteert u vervolgens de databases die u wilt herstellen.

2. Klik op **Herstel**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de machine offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:

   - [Alleen bij het herstellen vanaf een applicatiegerichte back-up] Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een online machine met Agent voor Exchange of Agent voor VMware en selecteert u vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad Back-upopslag.

   De machine die u hebt gekozen om te bladeren via een van de genoemde acties, wordt een doelmachine voor het herstel van de Exchange-gegevens.
4. Voer een van de volgende handelingen uit:
   - Wanneer u herstelt vanaf een applicatiegerichte back-up, klikt u op **Herstellen** > **Exchange-databases**, selecteert u de databases die u wilt herstellen en klikt u vervolgens op **Herstellen als bestanden**.
   - Wanneer u herstelt vanaf een databaseback-up, klikt u op **Herstellen** > **Databases als bestanden**.
5. Klik op **Bladeren** en selecteer vervolgens een lokale map of netwerkmap waarnaar u de gegevens wilt opslaan.
6. Klik op **Herstel starten**.

De voortgang van de herstelbewerking wordt weergegeven op het tabblad Activiteiten.

Exchange Server-databases koppelen

Nadat u de databasebestanden hebt hersteld, kunt u de databases online brengen door ze te koppelen. Voor de koppeling kunt u Exchange Management Console, Exchange System Manager of Exchange Management Shell gebruiken.

De herstelde databases hebben de status Onverwacht afgesloten. Een database met de status Onverwacht afgesloten kan door het systeem worden gekoppeld als deze is hersteld naar de originele locatie (oftewel, de informatie over de originele database is aanwezig in Active Directory). Wanneer een database naar een alternatieve locatie wordt hersteld (zoals een nieuwe database of als de hersteldatabase), kan de database pas worden gekoppeld nadat de database foutloos is gesloten met de opdracht `Eseutil /r <Enn>`. `<Enn>` geeft het logbestandsvoorvoegsel voor de database aan (of de opslaggroep die de database bevat) waarin u de transactielogbestanden moet toepassen.

Het account dat u gebruikt om een database te koppelen, moet de rol van Exchange Server-beheerder vervullen en de doelserver moet deel uitmaken van de lokale groep Administrators.

Raadpleeg de volgende artikelen voor meer informatie over het koppelen van databases:

- Exchange 2010 of later: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

Exchange-postvakken en postvakitems herstellen

U kunt Exchange-postvakken en -postvakitems herstellen vanuit de volgende back-ups:

- Databaseback-ups
- Applicatiegerichte back-ups
- Back-ups van postvakken

U kunt de volgende items herstellen:

- Postvakken (behalve archiefpostvakken)
- Openbare mappen

> **Opmerking**
> Alleen beschikbaar in databaseback-ups. Zie "Exchange Server-gegevens selecteren" (p. 596).

- Items uit openbare mappen
- E-mailmappen
- E-mailberichten
- Agendagebeurtenissen
- Taken
- Contacten
- Logboekvermeldingen
- Notities

U kunt een zoekopdracht gebruiken om de items te vinden.

De postvakken of postvakitems kunnen worden hersteld naar een live Exchange-server of naar Microsoft 365.

Herstel naar een Exchange-server

Gedetailleerd herstel kan worden uitgevoerd voor Microsoft Exchange Server 2010 Service Pack 1 (SP1) en later. De bronback-up kan databases of postvakken van elke ondersteunde Exchange-versie bevatten.

Gedetailleerd herstel kan alleen worden uitgevoerd met Agent voor Exchange of Agent voor VMware (Windows). De Exchange-server van bestemming en de machine waarop de agent wordt uitgevoerd, moeten behoren tot hetzelfde Active Directory-forest.

Wanneer een postvak wordt hersteld naar een bestaand postvak, worden de bestaande items met overeenkomende id's overschreven.

Bij het herstel van postvakitems worden geen items overschreven. In plaats daarvan wordt het volledige pad naar een postvakitem opnieuw gemaakt in de doelmap.

Vereisten voor gebruikersaccounts

Als een postvak wordt hersteld vanaf een back-up, moet het zijn gekoppeld aan een gebruikersaccount in Active Directory.

Postvakken van gebruikers en de inhoud daarvan kunnen alleen worden hersteld als de bijbehorende gebruikersaccounts zijn *ingeschakeld*. Gedeelde postvakken en postvakken voor vergaderruimten en apparatuur kunnen alleen worden hersteld als de bijbehorende gebruikersaccounts zijn *uitgeschakeld*.

Als een postvak niet voldoet aan de vermelde voorwaarden, wordt het overgeslagen bij het herstel.

Als sommige postvakken worden overgeslagen, wordt de herstelbewerking voltooid met waarschuwingen. Als alle postvakken worden overgeslagen, mislukt de herstelbewerking.

Herstel naar Microsoft 365

Herstel van Exchange-gegevensitems naar Microsoft 365, en vice versa, wordt ondersteund indien Agent voor Microsoft 365 lokaal is geïnstalleerd.

Herstel kan worden uitgevoerd vanaf back-ups van Microsoft Exchange Server 2010 en later.

Wanneer een postvak wordt hersteld naar een bestaand Microsoft 365-postvak, blijven de bestaande items intact en worden de herstelde items daarnaast geplaatst.

Wanneer u slechts één postvak herstelt, moet u het Microsoft 365-doelpostvak selecteren. Wanneer u in één bewerking meerdere postvakken herstelt, wordt geprobeerd elk postvak te herstellen naar het postvak van de gebruiker met dezelfde naam. Als de gebruiker niet wordt gevonden, wordt het postvak overgeslagen. Als sommige postvakken worden overgeslagen, wordt de herstelbewerking voltooid met waarschuwingen. Als alle postvakken worden overgeslagen, mislukt de herstelbewerking.

Zie "Microsoft 365-gegevens beschermen" (p. 632) voor meer informatie over herstel naar Microsoft 365.

Postvakken herstellen

Postvakken herstellen vanaf een applicatiegerichte back-up of een databaseback-up

1. [Alleen bij het herstellen vanaf een databaseback-up naar Microsoft 365] Als Agent voor Office 365 niet is geïnstalleerd op de machine met Exchange Server waarvan een back-up is gemaakt, voert u een van de volgende handelingen uit:
   - Als u niet beschikt over Agent voor Microsoft 365 in uw organisatie, installeert u Agent voor Microsoft 365 op de machine waarvan een back-up is gemaakt (of op een andere machine met dezelfde Microsoft Exchange Server-versie).
   - Als u Agent voor Microsoft 365 al hebt in uw organisatie, kopieert u bibliotheken van de machine waarvan een back-up is gemaakt (of van een andere machine met dezelfde Microsoft

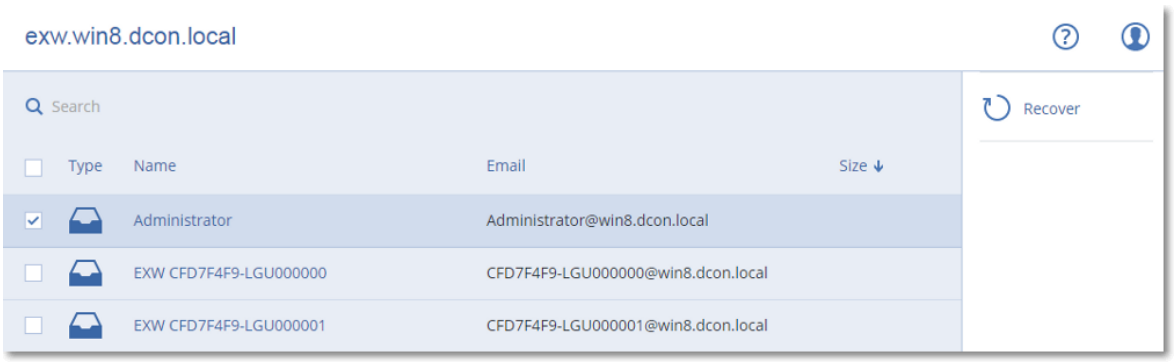
Exchange Server-versie), naar de machine met Agent voor Microsoft 365, zoals beschreven in 'Microsoft Exchange-bibliotheken kopiëren'.

2. Voer een van de volgende handelingen uit:
   - Wanneer u herstelt vanaf een applicatiegerichte back-up: selecteer onder **Apparaten** de oorspronkelijke machine met de gegevens die u wilt herstellen.
   - Wanneer u herstelt vanaf een databaseback-up, klikt u op **Apparaten** > **Microsoft Exchange** > **Databases** en selecteert u vervolgens de oorspronkelijke database met de gegevens die u wilt herstellen.
3. Klik op **Herstel**.
4. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de machine offline is, worden de herstelpunten niet weergegeven. Andere manieren gebruiken om te herstellen:
   - [Alleen bij het herstellen vanaf een applicatiegerichte back-up] Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een online machine met Agent voor Exchange of Agent voor VMware en selecteert u vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad Back-upopslag.

   De herstelbewerking wordt uitgevoerd door de machine die u kiest voor het bladeren bij een van de genoemde acties, en niet door de oorspronkelijke machine die offline is.
5. Klik op **Herstellen** > **Exchange-postvakken**.
6. Selecteer de postvakken die u wilt herstellen.

   U kunt postvakken zoeken op naam. Jokers worden niet ondersteund.



7. Klik op **Herstellen**.
8. [Alleen bij herstel naar Microsoft 365]:
   a. Ga naar **Herstellen naar** en selecteer **Microsoft 365**.
   b. [Als u slechts één postvak hebt geselecteerd in stap 6] Ga naar **Doelpostvak** en geef het doelpostvak op.
   c. Klik op **Herstel starten**.

   De andere stappen van deze procedure zijn niet vereist.

Klik op **Doelmachine met Microsoft Exchange Server** om de doelmachine te selecteren of te wijzigen. Via deze stap kunt u herstellen naar een machine waarop Agent voor Exchange niet wordt uitgevoerd.

Geef de FQDN (Fully Qualified Domain Name) op van een machine waarop de rol **Clienttoegang** (in Microsoft Exchange Server 2010/2013) of **Postvak** (in Microsoft Exchange Server 2016 of later) is ingeschakeld. De machine moet deel uitmaken van hetzelfde Active Directory-forest als de machine die de herstelbewerking uitvoert.

9. Geef desgevraagd de referenties op van een account dat wordt gebruikt om toegang te krijgen tot de machine. De vereisten voor dit account worden vermeld in 'Vereiste gebruikersrechten'.
10. [Optioneel] Klik op **Database voor het opnieuw maken van ontbrekende postvakken** om de automatisch geselecteerde database te wijzigen.
11. Klik op **Herstel starten**.

De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**.

Een postvak vanaf een postvakback-up herstellen

1. Klik op **Apparaten** > **Microsoft Exchange** > **Postvakken**.
2. Selecteer het postvak dat u wilt herstellen en klik vervolgens op **Herstel**.

   U kunt postvakken zoeken op naam. Jokers worden niet ondersteund.

   Als het postvak is verwijderd, selecteert u dit op het tabblad Back-upopslag en klikt u vervolgens op **Back-ups weergeven**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.
4. Klik op **Herstellen** > **Postvak**.
5. Voer de stappen 8-11 van de eerder beschreven procedure uit.

Postvakitems herstellen

Postvakitems herstellen vanaf een applicatiegerichte back-up of een databaseback-up

1. [Alleen bij het herstellen vanaf een databaseback-up naar Microsoft 365] Als Agent voor Office 365 niet is geïnstalleerd op de machine met Exchange Server waarvan een back-up is gemaakt, voert u een van de volgende handelingen uit:
   - Als u niet beschikt over Agent voor Microsoft 365 in uw organisatie, installeert u Agent voor Microsoft 365 op de machine waarvan een back-up is gemaakt (of op een andere machine met dezelfde Microsoft Exchange Server-versie).
   - Als u Agent voor Microsoft 365 al hebt in uw organisatie, kopieert u bibliotheken van de machine waarvan een back-up is gemaakt (of van een andere machine met dezelfde Microsoft Exchange Server-versie), naar de machine met Agent voor Microsoft 365, zoals beschreven in 'Microsoft Exchange-bibliotheken kopiëren'.
2. Voer een van de volgende handelingen uit:
   - Wanneer u herstelt vanaf een applicatiegerichte back-up: selecteer onder **Apparaten** de oorspronkelijke machine met de gegevens die u wilt herstellen.

- Wanneer u herstelt vanaf een databaseback-up, klikt u op **Apparaten** > **Microsoft Exchange** > **Databases** en selecteert u vervolgens de oorspronkelijke database met de gegevens die u wilt herstellen.

3. Klik op **Herstel**.
4. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de machine offline is, worden de herstelpunten niet weergegeven. Andere manieren gebruiken om te herstellen:

   - [Alleen bij het herstellen vanaf een applicatiegerichte back-up] Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een online machine met Agent voor Exchange of Agent voor VMware en selecteert u vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad Back-upopslag.

   De herstelbewerking wordt uitgevoerd door de machine die u kiest voor het bladeren bij een van de genoemde acties, en niet door de oorspronkelijke machine die offline is.
5. Klik op **Herstellen** > **Exchange-postvakken**.
6. Klik op het postvak dat oorspronkelijk de items bevatte die u wilt herstellen.
7. Selecteer de items die u wilt herstellen.

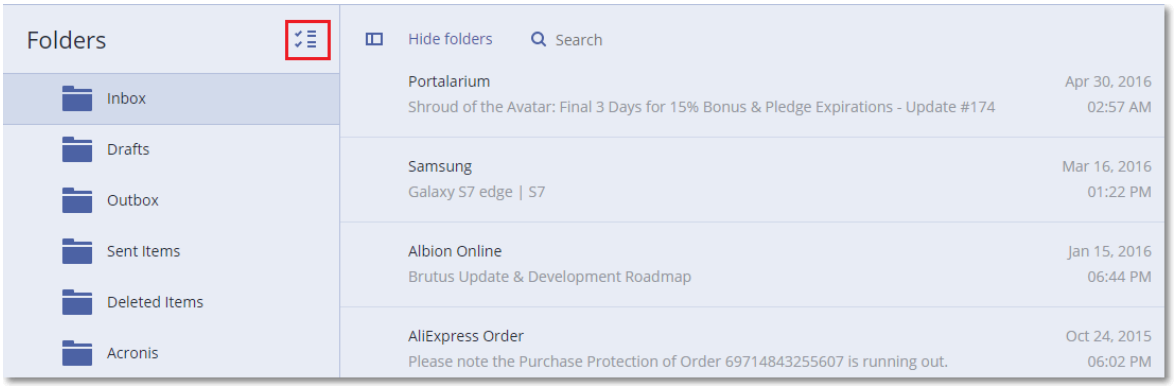
   De volgende zoekopties zijn beschikbaar. Jokers worden niet ondersteund.

   - E-mailberichten: u kunt zoeken op onderwerp, afzender, ontvanger en datum.
   - Gebeurtenissen: u kunt zoeken op titel en datum.
   - Taken: u kunt zoeken op onderwerp en datum.
   - Contacten: u kunt zoeken op naam, e-mailadres en telefoonnummer.

   Wanneer een e-mailbericht is geselecteerd, kunt u klikken op **Inhoud weergeven** om de inhoud weer te geven, met inbegrip van bijlagen.

   Opmerking
   Klik op de naam van een bijgevoegd bestand om het te downloaden.

   Als u mappen wilt selecteren, klikt u op het pictogram 'Mappen herstellen'.



8. Klik op **Herstellen**.

9. Als u wilt herstellen naar Microsoft 365, selecteert u **Microsoft 365** in **Herstellen naar**.

   Als u een Exchange-server wilt herstellen, behoudt u de standaardwaarde **Microsoft Exchange** in **Herstellen naar**.

   [Alleen bij het herstellen naar een Exchange-server] Klik op **Doelmachine met Microsoft Exchange Server** om de doelmachine te selecteren of te wijzigen. Via deze stap kunt u herstellen naar een machine waarop Agent voor Exchange niet wordt uitgevoerd.

   Geef de FQDN (Fully Qualified Domain Name) op van een machine waarop de rol **Clienttoegang** (in Microsoft Exchange Server 2010/2013) of **Postvak** (in Microsoft Exchange Server 2016 of later) is ingeschakeld. De machine moet deel uitmaken van hetzelfde Active Directory-forest als de machine die de herstelbewerking uitvoert.
10. Geef desgevraagd de referenties op van een account dat wordt gebruikt om toegang te krijgen tot de machine. De vereisten voor dit account worden vermeld in 'Vereiste gebruikersrechten'.
11. In **Doelpostvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.

    Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat of als een niet-oorspronkelijke doelmachine is geselecteerd, moet u het doelpostvak opgeven.
12. [Alleen bij het herstellen van e-mailberichten] Kies in **Doelmap** of u de doelmap in het doelpostvak wilt weergeven of wijzigen. Standaard wordt de map **Herstelde items** geselecteerd. Vanwege Microsoft Exchange-beperkingen worden gebeurtenissen, taken, notities en contacten hersteld naar hun oorspronkelijke locatie, ongeacht de **Doelmap** die wordt opgegeven.
13. Klik op **Herstel starten**.

De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**.

Een postvakitem vanaf een postvakback-up herstellen

1. Klik op **Apparaten** > **Microsoft Exchange** > **Postvakken**.
2. Selecteer het postvak dat oorspronkelijk de items bevatte die u wilt herstellen en klik vervolgens op **Herstel**.

   U kunt postvakken zoeken op naam. Jokers worden niet ondersteund.

   Als het postvak is verwijderd, selecteert u dit op het tabblad Back-upopslag en klikt u vervolgens op **Back-ups weergeven**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.
4. Klik op **Herstellen** > **E-mailberichten**.
5. Selecteer de items die u wilt herstellen.

   De volgende zoekopties zijn beschikbaar. Jokers worden niet ondersteund.

   - E-mailberichten: u kunt zoeken op onderwerp, afzender, ontvanger en datum.
   - Gebeurtenissen: u kunt zoeken op titel en datum.
   - Taken: u kunt zoeken op onderwerp en datum.
   - Contacten: u kunt zoeken op naam, e-mailadres en telefoonnummer.

   Wanneer een e-mailbericht is geselecteerd, kunt u klikken op **Inhoud weergeven** om de inhoud weer te geven, met inbegrip van bijlagen.

Opmerking
Klik op de naam van een bijgevoegd bestand om het te downloaden.

Wanneer een e-mailbericht is geselecteerd, kunt u klikken op **Versturen als e-mail** om het bericht naar een e-mailadres te verzenden. Het bericht wordt verzonden vanaf het e-mailadres van uw beheerdersaccount.

Als u mappen wilt selecteren, klikt u op het pictogram Mappen herstellen: 

6. Klik op **Herstellen**.
7. Voer de stappen 9-13 van de eerder beschreven procedure uit.

Microsoft Exchange Server-bibliotheken kopiëren

Wanneer u de optie Exchange-postvakken of -postvakitems herstellen naar Microsoft 365 gebruikt, moet u mogelijk de volgende bibliotheken kopiëren van de machine waarvan een back-up is gemaakt (of van een andere machine met dezelfde versie van Microsoft Exchange Server), naar de machine met Agent voor Microsoft 365.

Kopieer de volgende bestanden, afhankelijk van de versie van Microsoft Exchange Server waarvan een back-up is gemaakt.

Versie van Microsoft Exchange Server	Bibliotheken	Standaardlocatie

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`

De bibliotheken moeten worden geplaatst in de map `%ProgramData%\Acronis\ese`. Als deze map niet bestaat, maakt u deze handmatig.

De toegangsreferenties voor SQL Server of Exchange Server wijzigen

U kunt de toegangsreferenties voor SQL Server of Exchange Server wijzigen zonder dat u de agent opnieuw hoeft te installeren.

De toegangsreferenties voor SQL Server of Exchange Server wijzigen

1. Klik op **Apparaten** en vervolgens op **Microsoft SQL** of **Microsoft Exchange**.
2. Selecteer de AlwaysOn-beschikbaarheidsgroep, de databasebeschikbaarheidsgroep, het SQL Server-exemplaar of de Exchange-server waarvan u de toegangsreferenties wilt wijzigen.
3. Klik op **Referenties opgeven**.
4. Geef de nieuwe toegangsreferenties op en klik vervolgens op **OK**.

De toegangsreferenties voor Exchange Server voor postvakback-ups wijzigen

1. Klik op **Apparaten** > **Microsoft Exchange** en vouw **Postvakken** uit.
2. Selecteer de Exchange Server waarvan u de toegangsreferenties wilt wijzigen.
3. Klik op **Instellingen**.
4. Geef bij **Exchange-beheerdersaccount** de nieuwe toegangsreferenties op en klik vervolgens op **Opslaan**.

Mobiele apparaten beschermen

Met de Acronis Cyber Protect-app kunt u een back-up van uw mobiele gegevens maken in de cloudopslag en deze vervolgens herstellen in geval van verlies of beschadiging. Let op: voor back-ups naar de cloudopslag zijn een account en een cloudabonnement vereist.

Ondersteunde mobiele apparaten

U kunt de Cyber Protect-app installeren op een mobiel apparaat met een van de volgende besturingssystemen:

- iOS 15 tot iOS 17 (iPhone, iPod, iPad)
- Android 10 tot Android 14

Van welke items kunt u een back-up maken

- Contactgegevens (naam, telefoonnummer en e-mailadres)
- Foto's (de oorspronkelijke grootte en indeling van uw foto's blijven behouden)
- Video's
- Kalenders
- Herinneringen (alleen op iOS-apparaten)

Wat u moet weten

- Een back-up van de gegevens kan alleen worden opgeslagen in de cloudopslag.
- Telkens wanneer u de app opent, ziet u een overzicht van gegevenswijzigingen en kunt u handmatig een back-up starten.

- De functionaliteit **Continue back-up** is standaard ingeschakeld. Als deze instelling is ingeschakeld, worden nieuwe gegevens direct gedetecteerd door de Cyber Protect-app en automatisch geüpload naar de cloud.
- De optie **Alleen wifi gebruiken** is standaard ingeschakeld in de app-instellingen. Als deze instelling is ingeschakeld, maakt de Cyber Protect-app alleen een back-up van uw gegevens wanneer er een wifiverbinding beschikbaar is. Als de wifiverbinding wordt verbroken, worden er geen back-upprocessen gestart. Schakel deze optie uit als u wilt dat de app ook een mobiele verbinding kan gebruiken.
- De batterijoptimalisatie op uw apparaat kan de goede werking van de Cyber Protect-app belemmeren. Als u back-ups op tijd wilt laten uitvoeren, moet u de batterijoptimalisatie voor de app stoppen.
- U hebt twee manieren om energie te besparen:
  - De functie **Back-up maken tijdens het opladen** is standaard uitgeschakeld. Als deze instelling is ingeschakeld, maakt de Cyber Protect-app alleen een back-up van uw gegevens wanneer uw apparaat is aangesloten op een stroombron. Wanneer het apparaat wordt losgekoppeld van een stroombron tijdens een continu back-upproces, wordt de back-up gepauzeerd.
  - De **Energiebesparende modus** is standaard ingeschakeld. Als deze instelling is ingeschakeld, maakt de Cyber Protect-app geen back-up van uw gegevens wanneer de batterij van uw apparaat bijna leeg is. Wanneer de batterij van het apparaat bijna leeg is, wordt de continue back-up gepauzeerd.
- U kunt de gegevens waarvan een back-up is gemaakt, openen vanaf elk mobiel apparaat dat onder uw account is geregistreerd. Op die manier kunt u de gegevens van een oud mobiel apparaat overzetten naar een nieuw mobiel apparaat. Contacten en foto's van een Android-apparaat kunnen worden hersteld naar een iOS-apparaat en vice versa. U kunt ook een foto, video of contact naar een apparaat downloaden via de Cyber Protect-console.
- Gegevens waarvan een back-up wordt gemaakt vanaf een mobiel apparaat dat is geregistreerd onder uw account, zijn alleen beschikbaar onder dit account. Niemand anders kan uw gegevens weergeven of herstellen.
- In de Cyber Protect-app kunt u alleen de meest recente gegevensversies herstellen. Als u wilt herstellen vanaf een specifieke back-upversie, moet u de Cyber Protect-console op een tablet of computer gebruiken.
- Er worden geen bewaarregels toegepast op back-ups van mobiele apparaten.
- [Alleen voor Android-apparaten] Als een SD-kaart aanwezig is tijdens een back-up, worden de gegevens op deze kaart ook opgenomen in de back-up. De gegevens worden hersteld naar een SD-kaart, naar de map **Hersteld door back-up** als deze aanwezig is tijdens herstel, of anders wordt u gevraagd om een andere locatie op te geven waar u de gegevens wilt terugzetten.

Waar kunt u de Cyber Protect-app downloaden

U kunt de app installeren vanuit de App Store of Google Play, afhankelijk van uw mobiele apparaat.

Hoe kunt u een back-up van uw gegevens starten

1. Open de app.
2. Meld u aan met uw account.
3. Tik op **Instellen** om uw back-up te maken. Let op: deze knop wordt alleen weergegeven wanneer u geen back-up van uw mobiele apparaat hebt.
4. Selecteer de gegevenscategorieën waarvan u een back-up wilt maken. Standaard zijn alle categorieën geselecteerd.
5. [optionele stap] Schakel **Back-up coderen** in om uw back-up te beschermen met versleuteling. In dit geval moet u ook het volgende doen:
   a. Voer tweemaal een versleutelingswachtwoord in.

      Opmerking
      Onthoud het wachtwoord, want een vergeten wachtwoord kan niet worden hersteld of gewijzigd.

   b. Tik op **Coderen**.
6. Tik op **Back-up**.
7. Geef de app toegang tot uw persoonlijke gegevens. Als u geen toegang verleent tot bepaalde gegevenscategorieën, wordt hiervan geen back-up gemaakt.

De back-up begint.

Hoe kunt u gegevens herstellen naar een mobiel apparaat

Waarschuwing!
Als u mobiele gegevens wilt herstellen, moet u het eindgebruikersaccount gebruiken.

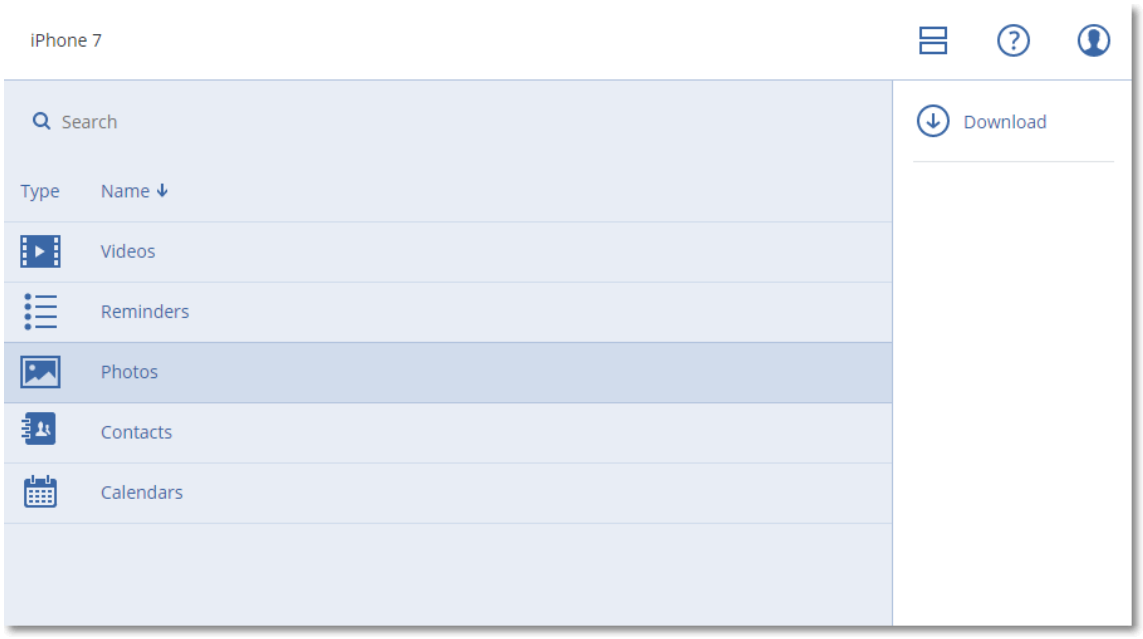
1. Open de Cyber Protect-app.
2. Tik op **Bladeren**.
3. Tik op de naam van het apparaat:
4. Voer een van de volgende handelingen uit:
   - Als u alle gegevens wilt herstellen waarvan een back-up is gemaakt, tikt u op **Alles herstellen**. U hoeft geen verdere actie te ondernemen.
   - Als u een of meer gegevenscategorieën wilt herstellen, tikt u op **Selecteren** en tikt u vervolgens op de selectievakjes voor de betreffende gegevenscategorieën. Tik op **Herstellen**. U hoeft geen verdere actie te ondernemen.
   - Als u een of meer gegevensitems uit dezelfde gegevenscategorie wilt herstellen, tikt u op de gegevenscategorie. Ga verder met de volgende stappen.
5. Voer een van de volgende handelingen uit:

- Als u slechts één gegevensitem wilt herstellen, tikt u op dit item.
- Als u meerdere gegevensitems wilt herstellen, tikt u op **Selecteren** en tikt u vervolgens op de selectievakjes voor de betreffende gegevensitems.

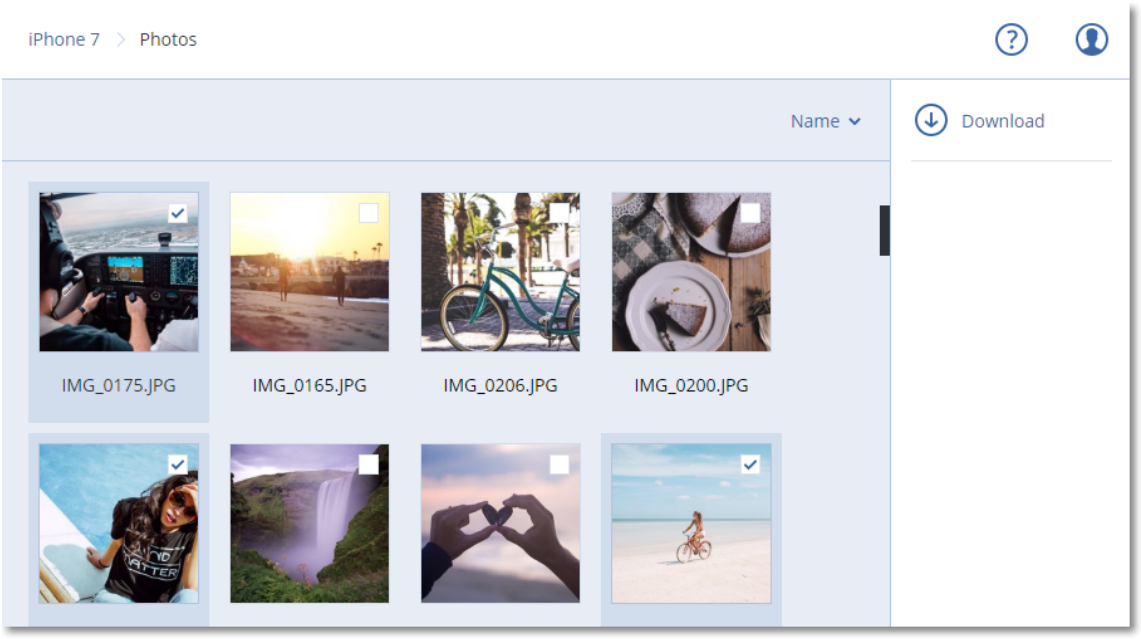
6. Tik op **Herstellen**.

Gegevens bekijken via de Cyber Protect-console

1. Open een browser op een computer en typ de URL van de Cyber Protect-console.
2. Meld u aan met uw account.
3. Ga naar **Alle apparaten** en klik op **Herstellen** onder de naam van uw mobiele apparaat.
4. Voer een van de volgende handelingen uit:
   - Als u alle foto's, video's, contacten, agenda's of herinneringen wilt downloaden, selecteert u de betreffende gegevenscategorie. Klik op **Downloaden**.



   - Als u afzonderlijke foto's, video's, contacten, agenda's of herinneringen wilt downloaden, klikt u op de naam van de betreffende gegevenscategorie en schakelt u de selectievakjes in voor de gewenste gegevensitems. Klik op **Downloaden**.



- Als u een voorbeeld van een foto of contact wilt weergeven, klikt u op de naam van de betreffende gegevenscategorie en klikt u vervolgens op het gewenste gegevensitem.

Gehoste Exchange-gegevens beschermen

Van welke items kan een back-up worden gemaakt?

U kunt een back-up maken van gebruikerspostvakken, gedeelde postvakken en groepspostvakken. U kunt er ook voor kiezen een back-up te maken van de archiefpostvakken (**in-place archief**) van de geselecteerde postvakken.

Welke items kunnen worden hersteld?

De volgende items kunnen worden hersteld vanuit een back-up van een postvak:

- Postvakken
- E-mailmappen
- E-mailberichten
- Agendagebeurtenissen
- Taken
- Contacten
- Logboekvermeldingen
- Notities

U kunt een zoekopdracht gebruiken om de items te vinden.

Wanneer u postvakken, postvakitems, openbare mappen en items uit openbare mappen herstelt, kunt u selecteren of u de items op de doellocatie wilt overschrijven.

Wanneer een postvak wordt hersteld naar een bestaand postvak, worden de bestaande items met overeenkomende id's overschreven.

Bij het herstel van postvakitems worden geen items overschreven. In plaats daarvan wordt het volledige pad naar een postvakitem opnieuw gemaakt in de doelmap.

Exchange Online-postvakken selecteren

Selecteer de postvakken zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

Exchange Online-postvakken selecteren

1. Klik op **Apparaten > Gehoste Exchange**.
2. Als meerdere Gehoste Exchange-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gebruikersgegevens waarvan u een back-up wilt maken. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u een back-up wilt maken van de postvakken van alle gebruikers en van alle gedeelde postvakken (inclusief postvakken die in de toekomst worden gemaakt), vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers** en klikt u vervolgens op **Back-up van groep**.
   - Als u een back-up wilt maken van de postvakken van afzonderlijke gebruikers of van gedeelde postvakken, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u de gebruikers met de postvakken waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.
   - Als u een back-up wilt maken van alle postvakken van een groep (inclusief postvakken van groepen die in de toekomst worden gemaakt), vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen** en klikt u vervolgens op **Back-up van groep**.
   - Als u een back-up wilt maken van afzonderlijke postvakken van een groep, vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen**, selecteert u de groepen met de postvakken waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.

Postvakken en postvakitems herstellen

Postvakken herstellen

1. Klik op **Apparaten > Gehoste Exchange**.
2. Als meerdere Gehoste Exchange-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie waarvan u de back-upgegevens wilt herstellen. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:

- Als u een gebruikerspostvak wilt herstellen, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u de gebruiker van wie u het postvak wilt herstellen en klikt u vervolgens op **Herstel**.
- Als u een gedeeld postvak wilt herstellen, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u het gedeelde postvak dat u wilt herstellen en klikt u vervolgens op **Herstel**.
- Als u een groepspostvak wilt herstellen, vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen**, selecteert u de groep waarvan u het postvak wilt herstellen en klikt u vervolgens op **Herstel**.
- Als de gebruiker, de groep of het gedeelde postvak is verwijderd, selecteert u het gewenste item in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-ups en klikt u vervolgens op **Back-ups weergeven**.

U kunt gebruikers en groepen zoeken op naam. Jokers worden niet ondersteund.

4. Selecteer een herstelpunt.
5. Klik op **Herstellen** > **Volledig postvak**.
6. Als meerdere Gehoste Exchange-organisaties worden toegevoegd aan de Cyber Protection-service, klikt u op **Gehoste Exchange-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
7. In **Herstellen naar postvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.

   Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u het doelpostvak opgeven.
8. Klik op **Herstel starten**.
9. Selecteer een van de opties voor overschrijven:
   - **Bestaande items overschrijven**
   - **Bestaande items niet overschrijven**
10. Klik op **Doorgaan** om uw beslissing te bevestigen.

Postvakitems herstellen

1. Klik op **Apparaten > Gehoste Exchange**.
2. Als meerdere Gehoste Exchange-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie waarvan u de back-upgegevens wilt herstellen. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u items uit een gebruikerspostvak wilt herstellen, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u de gebruiker van het postvak met de oorspronkelijke items die u wilt herstellen en klikt u vervolgens op **Herstel**.

- Als u items uit een gedeeld postvak wilt herstellen, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u het gedeelde postvak dat oorspronkelijk de items bevatte die u wilt herstellen en klikt u vervolgens op **Herstel**.
- Als u items uit een groepspostvak wilt herstellen, vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen**, selecteert u de groep van het postvak met de oorspronkelijke items die u wilt herstellen en klikt u vervolgens op **Herstel**.
- Als de gebruiker, de groep of het gedeelde postvak is verwijderd, selecteert u het gewenste item in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-ups en klikt u vervolgens op **Back-ups weergeven**.

U kunt gebruikers en groepen zoeken op naam. Jokers worden niet ondersteund.

4. Selecteer een herstelpunt.
5. Klik op **Herstellen** > **E-mailberichten**.
6. Blader naar de vereiste map of gebruik de zoekfunctie om de lijst met vereiste items weer te geven.

   De volgende zoekopties zijn beschikbaar. Jokers worden niet ondersteund.
   - E-mailberichten: u kunt zoeken op onderwerp, afzender, ontvanger, naam van bijlage en datum.
   - Gebeurtenissen: u kunt zoeken op titel en datum.
   - Taken: u kunt zoeken op onderwerp en datum.
   - Contacten: u kunt zoeken op naam, e-mailadres en telefoonnummer.
7. Selecteer de items die u wilt herstellen. Als u mappen wilt selecteren, klikt u op het pictogram 'Mappen herstellen': 

   U kunt ook een van de volgende handelingen uitvoeren:
   - Wanneer een item is geselecteerd, klikt u op **Inhoud weergeven** om de inhoud ervan te bekijken, inclusief bijlagen. Klik op de naam van een bijgevoegd bestand om het te downloaden.
   - Wanneer een e-mailbericht of agenda-item is geselecteerd, kunt u klikken op **Versturen als e-mail** om het bericht naar een e-mailadres te verzenden. U kunt de afzender selecteren en een tekst schrijven die u wilt toevoegen aan het doorgestuurde artikel.
   - Alleen als de back-up niet is versleuteld, u de zoekfunctie hebt gebruikt en één item in de zoekresultaten hebt geselecteerd: klik op **Versies weergeven** om de itemversie te selecteren die u wilt herstellen. U kunt elke versie selecteren waarvan een back-up is gemaakt, ongeacht of deze eerder of later is dan het geselecteerde herstelpunt.
8. Klik op **Herstellen**.
9. Als meerdere Gehoste Exchange-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Gehoste Exchange-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.

10. In **Herstellen naar postvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.
    Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u het doelpostvak opgeven.
11. [Alleen bij het herstellen naar een gebruikerspostvak of gedeeld postvak] Open **Pad** en bekijk of wijzig de doelmap in het doelpostvak. Standaard wordt de map **Herstelde items** geselecteerd.
    Items van groepspostvakken worden altijd hersteld naar de map **Postvak IN**.
12. Klik op **Herstel starten**.
13. Selecteer een van de opties voor overschrijven:
    - **Bestaande items overschrijven**
    - **Bestaande items niet overschrijven**
14. Klik op **Doorgaan** om uw beslissing te bevestigen.

Microsoft 365-gegevens beschermen

Waarom een back-up maken van Microsoft 365-gegevens?

Microsoft 365 is een set cloudservices, maar regelmatige back-ups bieden een extra beveiligingslaag tegen gebruikersfouten en opzettelijke kwaadwillende acties. U kunt verwijderde items herstellen vanaf een back-up, zelfs wanneer de Microsoft 365-retentieperiode is verstreken. U kunt ook een lokaal exemplaar van de Exchange Online-postvakken bewaren als dit is vereist voor naleving van de regelgeving.

Back-upgegevens worden automatisch gecomprimeerd en nemen op de back-uplocatie minder ruimte in beslag dan op de oorspronkelijke locatie. Het compressieniveau voor cloud-to-cloud back-ups kan niet worden veranderd. Het niveau komt overeen met het niveau **Normaal** voor niet-cloud-to-cloud back-ups. Zie "Compressieniveau" (p. 486) voor meer informatie over deze niveaus.

Cloudagent en lokale agent

Voor Microsoft 365-workloads zijn twee agents beschikbaar:

- Cloudagent
  De cloudagent biedt uitgebreide back-upfunctionaliteit die direct toegankelijk is in de Cyber Protect-console. Er is geen installatie vereist. Zie "De cloudagent voor Microsoft 365 gebruiken" (p. 642) voor meer informatie.
- Lokale agent
  De lokale agent biedt alleen een back-up van Exchange Online-postvakken. Deze agent moet zijn geïnstalleerd op een machine met Windows en een verbinding met internet. Zie "Lokale Agent voor Office 365 gebruiken" (p. 637) voor meer informatie.

Azure Information Protection (AIP) wordt ondersteund met beide agents.

Opmerking

Voor tenants in de compliancemodus is alleen de lokale agent beschikbaar. Deze tenants kunnen alleen een back-up maken van Microsoft 365-postvakken. Ze kunnen geen gebruik maken van de uitgebreide functionaliteit van de cloudagent.

De volgende tabel bevat een overzicht van de functies van de agents.

	Lokale agent	Cloudagent
Gegevensitems waarvan een back-up kan worden gemaakt	**Exchange Online:** gebruikers- en gedeelde postvakken (inclusief postvakken van gebruikers met een Kiosk-abonnement en postvakken waarvan de gegevens worden bewaard vanwege juridische procedures)	• **Exchange Online**: ◦ gebruikers- en gedeelde postvakken (inclusief postvakken van gebruikers met een Kiosk-abonnement en postvakken waarvan de gegevens worden bewaard vanwege juridische procedures) ◦ groepspostvakken ◦ openbare mappen • **OneDrive**: gebruikersbestanden en -mappen • **SharePoint Online**: ◦ klassieke siteverzamelingen ◦ groeps(team)sites ◦ communicatiesites ◦ afzonderlijke gegevensitems • **Microsoft 365 Teams**: ◦ volledige teams ◦ teamkanalen ◦ kanaalbestanden ◦ teampostvakken ◦ bestanden en e-mailberichten in teampostvakken ◦ vergaderingen ◦ teamsites • **OneNote-notitieblokken**: als onderdeel van back-ups van OneDrive, SharePoint Online en Microsoft 365 Teams
Back-up van	Nee	Ja

	Lokale agent	Cloudagent
archiefpostvakken (**in-place archief**)		
Back-upschema	Door gebruiker gedefinieerd	Tot zes keer per dag*
Back-uplocaties	Cloudopslag, lokale map, netwerkmap	Alleen Cloudopslag (inclusief door partner gehoste opslag)
Automatische bescherming van nieuwe Microsoft 365-gebruikers, -groepen, -sites en -teams	Nee	Ja, door een beschermingsschema toe te passen op de groepen **Alle gebruikers**, **Alle groepen**, **Alle sites** en **Alle teams**
Meer dan één Microsoft 365-organisatie beschermen	Nee	Ja
Granulair herstel	Ja	Ja
Herstel naar een andere gebruiker binnen één organisatie	Ja	Ja
Herstel naar een andere organisatie	Nee	Ja
Herstel naar een on-premises Microsoft Exchange-server	Nee	Nee
Maximaal aantal items waarvan een back-up kan worden gemaakt zonder verminderde prestaties	Bij back-ups naar de cloudopslag: 5000 postvakken per bedrijf Bij back-ups naar andere bestemmingen: 2000 postvakken per beschermingsschema (geen beperking voor het aantal postvakken per bedrijf)	10 000 beschermde items (postvakken, OneDrives of sites) per bedrijf**
Maximum aantal handmatige back-ups	Nee	10 handmatige back-ups in één uur
Maximum aantal gelijktijdige herstelbewerkingen	Nee	10 bewerkingen, waaronder Google Workspace-herstelbewerkingen

* De standaardoptie is **Eén keer per dag**. Met het Advanced Backup-pakket kunt u tot zes back-ups per dag plannen. De back-ups worden gestart met een interval dat afhangt van de huidige belasting van de cloudagent, die wordt gebruikt voor meerdere klanten in een datacenter. Zo wordt de belasting gelijkmatig verdeeld gedurende de dag en krijgen alle klanten eenzelfde serviceniveau.

Opmerking
Het beschermingsschema kan worden beïnvloed door de werking van externe services, bijvoorbeeld de toegankelijkheid van Microsoft 365-servers, beperkingsinstellingen op de Microsoft-servers, enzovoort. Zie ook https://docs.microsoft.com/en-us/graph/throttling.

** We raden aan om geleidelijk back-ups te maken van uw beschermde items, in deze volgorde:

1. Postvakken.
2. Wanneer u een back-up van alle postvakken hebt gemaakt, gaat u verder met OneDrives.
3. Wanneer de back-ups van OneDrives zijn voltooid, gaat u verder met de SharePoint Online-sites.

De eerste volledige back-up kan enkele dagen duren, afhankelijk van het aantal beschermde items en hun grootte.

Vereiste gebruikersrechten

In Cyber Protection

De lokale agent moet zijn geregistreerd voor een bedrijfbeheerdersaccount en worden gebruikt op het niveau van een klanttenant. Bedrijfbeheerders die werken op eenheidniveau, eenheidbeheerders en gebruikers kunnen geen back-up- en herstelbewerkingen uitvoeren voor Microsoft 365-gegevens.

De cloudagent kan zowel op het niveau van een klanttenant als op het niveau van een eenheid worden gebruikt. Zie "Microsoft 365 organisaties beheren die zijn toegevoegd op verschillende niveaus" (p. 643) voor meer informatie over deze niveaus en de respectievelijke beheerders.

In Microsoft 365

Aan uw account moet de rol van globale beheerder in Microsoft 365 zijn toegewezen.

Als u een detectie-, back-up- en herstelbewerking wilt uitvoeren voor openbare Microsoft 365-mappen, moet ten minste een van uw Microsoft 365-beheerdersaccounts een postvak en lees-/schrijfrechten hebben voor de openbare mappen waarvan u een back-up wilt maken.

- De lokale agent meldt zich bij Microsoft 365 aan met dit account. Aan dit account wordt de beheerrol **ApplicationImpersonation** toegewezen, zodat de agent toegang heeft tot de inhoud van alle postvakken. Als u het wachtwoord van het account wilt wijzigen, werkt u het wachtwoord bij in de Cyber Protect-console, zoals beschreven in "De Microsoft 365-toegangsreferenties wijzigen" (p. 639).
- De cloudagent meldt zich niet aan bij Microsoft 365. U moet u eenmalig als globale beheerder aanmelden bij Microsoft 365 om de cloudagent de machtigingen te geven die nodig zijn om goed te werken.

  De volgende machtigingen zijn vereist in Microsoft 365:

- Aanmelden en gebruikersprofielen lezen
- Bestanden lezen en schrijven in alle siteverzamelingen
- De volledige profielen van alle gebruikers lezen en schrijven
- Alle groepen lezen en schrijven
- Gegevens in mappen lezen
- Alle kanaalberichten lezen
- Beheerde metagegevens lezen en schrijven
- Items en lijsten lezen en schrijven in alle siteverzamelingen
- Volledig beheer hebben voor alle siteverzamelingen
- Items lezen en schrijven in alle siteverzamelingen
- Exchange-webservices gebruiken met volledige toegang tot alle postvakken

- De cloudagent slaat uw accountreferenties niet op en gebruikt deze niet om back-up of herstel uit te voeren. De werking van de cloudagent wordt niet beïnvloed als u de referenties wijzigt, het account uitschakelt of het account verwijdert.

Beperkingen

- Met de lokale agent kunt u tot 5000 workloads beschermen. Met de cloud agent kunt u tot 50000 workloads beschermen.
- Alle gebruikers met een postvak of OneDrive worden weergegeven in de Cyber Protect-console, inclusief gebruikers zonder Microsoft 365-licentie en gebruikers die zich niet kunnen aanmelden bij de Microsoft 365-services.
- Een back-up van een postvak bevat alleen mappen die zichtbaar zijn voor gebruikers. De map **Herstelbare items** met de bijbehorende submappen (**Verwijderingen**, **Versies**, **Leegmakingen**, **Audits**, **DiscoveryHold**, **Kalenderregistratie**) worden niet opgenomen in een postvakback-up.
- Het automatisch maken van gebruikers, openbare mappen, groepen of sites is niet mogelijk tijdens een herstelbewerking. Als u bijvoorbeeld een verwijderde SharePoint Online-site wilt herstellen, maakt u eerst handmatig een nieuwe site en geeft u deze tijdens de herstelbewerking op als de doelsite.
- U kunt niet gelijktijdig items van verschillende herstelpunten herstellen, maar u kunt dergelijke items wel selecteren in de zoekresultaten.
- Tijdens een back-up zullen alle gevoeligheidslabels die op de inhoud zijn toegepast, bewaard blijven. Gevoelige inhoud wordt dus mogelijk niet weergegeven als deze wordt teruggezet naar een niet-oorspronkelijke locatie en de gebruiker andere machtigingen heeft.
- U kunt niet meer dan één afzonderlijk back-upschema toepassen op dezelfde workload.
- Wanneer een afzonderlijk back-upschema en een groepsback-upschema op dezelfde workload worden toegepast, hebben de instellingen in het afzonderlijke schema voorrang.

Rapport Licenties voor Microsoft 365-seats

Bedrijfbeheerders kunnen een rapport downloaden over de beschermde Microsoft 365-seats en bijbehorende licenties. Het rapport is in CSV-indeling en bevat informatie over de licentiestatus van een seat en de reden waarom een licentie wordt gebruikt. Het rapport bevat ook de naam van de beschermde seat, het bijbehorende e-mailadres, de groep, de Microsoft 365-organisatie, de naam en het type van de beschermde workload.

Dit rapport is alleen beschikbaar voor tenants waarin een Microsoft 365-organisatie is geregistreerd.

Het licentierapport voor Microsoft 365-seats downloaden

1. Meld u als bedrijfbeheerder aan bij de Cyber Protect-console.
2. Klik op het accountpictogram in de rechterbovenhoek.
3. Klik op **Rapport Licenties voor Microsoft 365-seats**.

Aanmelden

Acties met cloud-to-cloud resources kunnen de privacy van de gebruiker schenden, bijvoorbeeld door het bekijken van de inhoud van e-mails in de back-up, het downloaden van bijlagen of bestanden, het herstellen van e-mails naar andere postvakken dan het oorspronkelijke postvak of het versturen van de resources als e-mail. Deze acties worden vastgelegd in **Controle** > **Auditlogboek** in de beheerportal.

Lokale Agent voor Office 365 gebruiken

Een Microsoft 365-organisatie toevoegen

Een Microsoft 365-organisatie toevoegen

1. Meld u als bedrijfbeheerder aan bij de Cyber Protect-console.
2. Klik op het accountpictogram in de rechterbovenhoek en klik vervolgens op **Downloads** > **Agent voor Office 365**.
3. Download en installeer de agent op een machine met Windows en een verbinding met internet.
4. Ga in de Cyber Protect-console naar **Apparaten** > **Microsoft Office 365 (lokale agent)**.
5. Geef uw toepassings-id en toepassingsgeheim en de Microsoft 365-tenant-id op in het venster dat wordt geopend. Zie "Toepassings-id en -geheim ophalen" (p. 638) voor meer informatie over hoe u deze kunt vinden.
6. Klik op **OK**.

Hierdoor worden de gegevensitems van uw organisatie in de Cyber Protect-console weergegeven op het tabblad **Microsoft Office 365 (lokale agent)**.

Belangrijk
Er kan slechts één Agent voor Office 365 lokaal worden geïnstalleerd binnen een organisatie (bedrijfsgroep).

Toepassings-id en -geheim ophalen

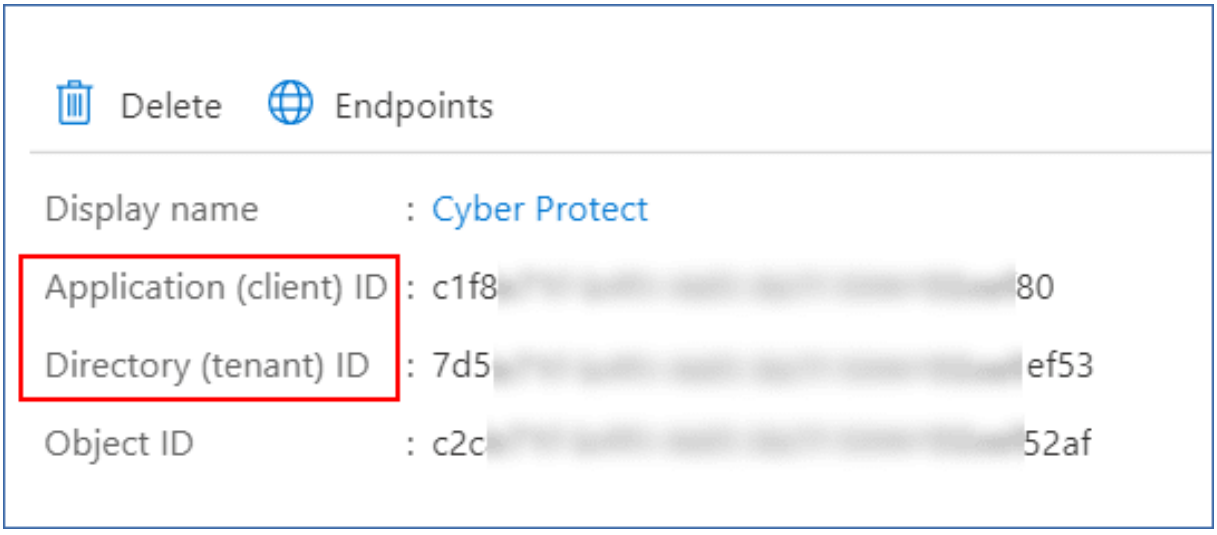
Als u de moderne verificatie voor Office 365 wilt gebruiken, moet u een aangepaste applicatie maken in het Entra-beheercentrum en hieraan specifieke API-machtigingen verlenen. Zo verkrijgt u de **applicatie-id**, het **applicatiegeheim** en de **directory (tenant)-id** die u moet invoeren in de Cyber Protect-console.

Opmerking
Op de machine waarop Agent voor Office 365 is geïnstalleerd, moet u toegang tot graph.microsoft.com verlenen via poort 443.

Een applicatie maken in Entra-beheercentrum

1. Meld u als beheerder aan bij het Entra-beheercentrum.
2. Navigeer naar **Azure Active Directory** > **App-registraties** en klik vervolgens op **Nieuwe registratie**.
3. Geef een naam op voor uw aangepaste toepassing, bijvoorbeeld Cyber Protection.
4. Selecteer in **Ondersteunde Accounttypen** de optie **Alleen accounts in deze organisatiedirectory**.
5. Klik op **Registreren**.

Uw applicatie is nu gemaakt. Navigeer in het Entra-beheercentrum naar de **Overzicht**pagina van de applicatie en controleer uw applicatie (client)-id en directory (tenant)-id.



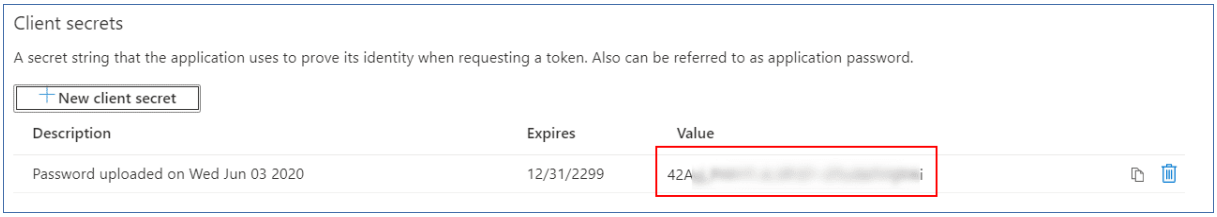
Voor meer informatie over het maken van een applicatie in het Entra-beheercentrum raadpleegt u de Microsoft-documentatie.

De nodige API-machtigingen verlenen aan uw toepassing

1. In het Entra-beheercentrum navigeert u naar de **API-machtigingen** van de applicatie en klikt u vervolgens op **Een machtiging toevoegen**.
2. Selecteer het tabblad **Door mijn organisatie gebruikte API's** en zoek **Office 365 Exchange Online**.
3. Klik op **Office 365 Exchange Online** en klik vervolgens op **Toepassingsmachtigingen**.
4. Schakel het selectievakje **full_access_as_app** in en klik op **Machtigingen toevoegen**.
5. Klik in **API-machtigingen** op **Een machtiging toevoegen**.
6. Selecteer **Microsoft Graph**.
7. Selecteer **Toepassingsmachtigingen**.
8. Breid het tabblad **Directory** uit en schakel het selectievakje **Directory.Read.All** in. Klik op **Machtigingen toevoegen**.
9. Controleer alle machtigingen en klik vervolgens op **Toestemming beheerder verlenen voor <naam van uw toepassing>**.
10. Bevestig uw keuze door te klikken op **Ja**.

Een toepassingsgeheim maken

1. In het Entra-beheercentrum navigeert u naar **Certificaten en geheimen** > **Nieuw klantgeheim** voor de applicatie.
2. Selecteer in het dialoogvenster dat wordt geopend, de optie Verloopt: **Nooit** en klik vervolgens op **Toevoegen**.
3. Controleer uw toepassingsgeheim in het veld **Waarde** en zorg ervoor dat u dit onthoudt.



Raadpleeg de Microsoft-documentatie voor meer informatie over het toepassingsgeheim.

De Microsoft 365-toegangsreferenties wijzigen

U kunt de toegangsreferenties voor Microsoft 365 wijzigen zonder dat u de agent opnieuw hoeft te installeren.

De Microsoft 365-toegangsreferenties wijzigen

1. Klik op **Apparaten** > **Microsoft Office 365 (lokale agent)**.
2. Selecteer de Microsoft 365-organisatie.
3. Klik op **Referenties opgeven**.
4. Voer uw toepassings-id en toepassingsgeheim en de Microsoft 365-tenant-id in. Zie

"Toepassings-id en -geheim ophalen" (p. 638) voor meer informatie over hoe u deze kunt vinden.

5. Klik op **OK**.

Exchange Online-postvakken beveiligen

Van welke items kan een back-up worden gemaakt?

U kunt een back-up maken van gebruikerspostvakken en gedeelde postvakken. Er kan geen back-up worden gemaakt van groepspostvakken en archiefpostvakken (**in-place archief**).

Welke items kunnen worden hersteld?

De volgende items kunnen worden hersteld vanuit een back-up van een postvak:

- Postvakken
- E-mailmappen
- E-mailberichten
- Agendagebeurtenissen
- Taken
- Contacten
- Logboekvermeldingen
- Notities

U kunt een zoekopdracht gebruiken om de items te vinden.

Wanneer een postvak wordt hersteld naar een bestaand postvak, worden de bestaande items met overeenkomende id's overschreven.

Bij het herstel van postvakitems worden geen items overschreven. In plaats daarvan wordt het volledige pad naar een postvakitem opnieuw gemaakt in de doelmap.

Microsoft 365-postvakken selecteren

Selecteer de postvakken zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

Postvakken selecteren

1. Klik op **Microsoft Office 365 (lokale agent)**.
2. Selecteer de postvakken waarvan u een back-up wilt maken.
3. Klik op **Back-up**.

Postvakken en postvakitems herstellen

Postvakken herstellen

1. Klik op **Microsoft Office 365 (lokale agent)**.
2. Selecteer het postvak dat u wilt herstellen en klik vervolgens op **Herstel**.
   U kunt postvakken zoeken op naam. Jokers worden niet ondersteund.
   Als het postvak is verwijderd, selecteert u dit op het tabblad Back-upopslag en klikt u vervolgens op **Back-ups weergeven**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.
4. Klik op **Herstellen** > **Postvak**.
5. In **Doelpostvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.
   Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat, moet u het doelpostvak opgeven.
6. Klik op **Herstel starten**.

Postvakitems herstellen

1. Klik op **Microsoft Office 365 (lokale agent)**.
2. Selecteer het postvak dat oorspronkelijk de items bevatte die u wilt herstellen en klik vervolgens op **Herstel**.
   U kunt postvakken zoeken op naam. Jokers worden niet ondersteund.
   Als het postvak is verwijderd, selecteert u dit op het tabblad Back-upopslag en klikt u vervolgens op **Back-ups weergeven**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.
4. Klik op **Herstellen** > **E-mailberichten**.
5. Selecteer de items die u wilt herstellen.
   De volgende zoekopties zijn beschikbaar. Jokers worden niet ondersteund.
   - E-mailberichten: u kunt zoeken op onderwerp, afzender, ontvanger, naam van bijlage en datum.
   - Gebeurtenissen: u kunt zoeken op titel en datum.
   - Taken: u kunt zoeken op onderwerp en datum.
   - Contacten: u kunt zoeken op naam, e-mailadres en telefoonnummer.

   Wanneer een e-mailbericht is geselecteerd, kunt u klikken op **Inhoud weergeven** om de inhoud weer te geven, met inbegrip van bijlagen.

Opmerking
Klik op de naam van een bijgevoegd bestand om het te downloaden.

Wanneer een e-mailbericht is geselecteerd, kunt u klikken op **Versturen als e-mail** om het bericht naar een e-mailadres te verzenden. Het bericht wordt verzonden vanaf het e-mailadres van uw beheerdersaccount.

Als u mappen wilt selecteren, klikt u op het pictogram 'Mappen herstellen': 

6. Klik op **Herstellen**.
7. In **Doelpostvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.
   Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat, moet u het doelpostvak opgeven.
8. Klik op **Herstel starten**.
9. Bevestig uw beslissing.

De postvakitems worden altijd hersteld naar de map **Herstelde items** van het doelpostvak.

De cloudagent voor Microsoft 365 gebruiken

Een Microsoft 365-organisatie toevoegen

Een beheerder kan een of meer Microsoft 365-organisaties toevoegen aan een klanttenant of eenheid.

Bedrijfbeheerders voegen organisaties toe aan klanttenants. Eenheidbeheerders en klantbeheerders die werken op eenheidniveau, voegen organisaties toe aan eenheden.

Een Microsoft 365-organisatie toevoegen

1. Meld u aan bij de Cyber Protect-console als bedrijfbeheerder of eenheidbeheerder, afhankelijk van waar u de organisatie wilt toevoegen.
2. [Voor bedrijfbeheerders die werken op eenheidniveau] Navigeer in de beheerportal naar de gewenste eenheid.
3. Klik op **Apparaten** > **Toevoegen** > **Microsoft 365 Business**.
   U wordt automatisch doorgestuurd naar de aanmeldingspagina van Microsoft 365.
4. Meld u aan met de referenties van de globale beheerder van Microsoft 365.
   In Microsoft 365 wordt een lijst weergegeven met machtigingen die nodig zijn voor het maken van back-ups en het herstellen van de gegevens van uw organisatie.
5. Bevestig dat u deze machtigingen toekent aan de Cyber Protection-service.

Uw Microsoft 365-organisatie wordt dan weergegeven op het tabblad **Apparaten** in de Cyber Protect-console.

Nuttige tips

- De cloudagent wordt om de 24 uur gesynchroniseerd met Microsoft 365, te beginnen vanaf het moment dat de organisatie wordt toegevoegd aan de Cyber Protection-service. Als u een gebruiker, groep of site toevoegt of verwijdert, is deze wijziging niet onmiddellijk zichtbaar in de Cyber Protect-console. Als u de wijziging onmiddellijk wilt synchroniseren, selecteert u de organisatie op de pagina **Microsoft 365** en klikt u op **Vernieuwen**.

  Voor meer informatie over het synchroniseren van de resources van een Microsoft 365-organisatie en de Cyber Protect-console raadpleegt u "Microsoft 365-resources detecteren" (p. 645).
- Als u een beschermingsschema hebt toegepast op de groep **Alle gebruikers**, **Alle groepen** of **Alle sites**, worden de nieuw toegevoegde items pas na de synchronisatie opgenomen in de back-up.
- Volgens het Microsoft-beleid blijft een gebruiker, groep of site die is verwijderd uit de gebruikersinterface van Microsoft 365, nog enkele dagen beschikbaar via een API. Tijdens deze periode is het verwijderde item inactief (grijs weergegeven) in de Cyber Protect-console en worden hiervan geen back-ups gemaakt. Wanneer het verwijderde item niet meer beschikbaar is via de API, wordt het niet meer weergegeven in de Cyber Protect-console. Eventuele back-ups vindt u in **Back-upopslag** > **Back-ups van cloudtoepassingen**.

Microsoft 365 organisaties beheren die zijn toegevoegd op verschillende niveaus

Bedrijfbeheerders hebben volledige toegang tot de Microsoft 365-organisaties die zijn toegevoegd aan het klanttenantniveau.

Bedrijfbeheerders hebben beperkte toegang tot de organisaties die zijn toegevoegd aan een eenheid. In deze organisaties, weergegeven met de naam van de eenheid tussen haakjes, kunnen bedrijfbeheerders het volgende doen:

- Gegevens herstellen vanaf back-ups.

  Bedrijfbeheerders kunnen gegevens herstellen voor alle organisaties in de tenant, ongeacht het niveau waarop deze organisaties zijn toegevoegd.
- Bladeren in back-ups en herstelpunten in back-ups.
- Back-ups en herstelpunten in back-ups verwijderen.
- Waarschuwingen en activiteiten bekijken.

Bedrijfbeheerders kunnen, wanneer ze werken op klanttenantniveau, niet het volgende doen:

- Microsoft 365-organisaties toevoegen aan eenheden.
- Microsoft 365-organisaties verwijderen uit eenheden.
- Microsoft 365-organisaties synchroniseren die zijn toegevoegd aan een eenheid.

- Beschermingsschema's bekijken, maken, bewerken, verwijderen, toepassen, uitvoeren of intrekken voor gegevensitems in de Microsoft 365-organisaties die zijn toegevoegd aan een eenheid.

Eenheidbeheerders en bedrijfbeheerders die werken op eenheidniveau, hebben volledige toegang tot de organisaties die zijn toegevoegd aan een eenheid. Ze hebben echter geen toegang tot de resources van de bovenliggende klanttenant, met inbegrip van de beschermingsschema's die daarin zijn gemaakt.

Een Microsoft 365-organisatie verwijderen

Als u een Microsoft 365-organisatie verwijdert, heeft dit geen invloed op de bestaande back-ups van de gegevens van deze organisatie. Als u deze back-ups niet meer nodig hebt, verwijdert u ze eerst en verwijdert u vervolgens de Microsoft 365-organisatie. Anders zullen de back-ups nog steeds ruimte in de cloudopslag gebruiken die mogelijk in rekening wordt gebracht.

Zie "Back-ups of back-uparchieven verwijderen" (p. 565) voor meer informatie over het verwijderen van back-ups.

Een Microsoft 365-organisatie verwijderen

1. Meld u aan bij de Cyber Protect-console als bedrijfbeheerder of eenheidbeheerder, afhankelijk van waar de organisatie is toegevoegd.
2. [Voor bedrijfbeheerders die werken op eenheidniveau] Navigeer in de beheerportal naar de gewenste eenheid.
3. Ga naar **Apparaten** > **Microsoft 365**.
4. Selecteer de organisatie en klik vervolgens op **Groep verwijderen**.

De back-upschema's voor deze groep worden dan ingetrokken.

U moet echter ook de toegangsrechten van de Backup Service-toepassing voor de gegevens van de Microsoft 365-organisatie handmatig intrekken.

Toegangsrechten intrekken

1. Meld u aan bij Office 365 als globale beheerder.
2. Ga naar **Beheercentrum** > **Azure Active Directory** > **Bedrijfstoepassingen** > **Alle toepassingen**.
3. Selecteer de **Backup Service**-toepassing en bekijk de details.
4. Ga naar het tabblad **Eigenschappen** en klik vervolgens in het actiepaneel op **Verwijderen**.
5. Bevestig de verwijdering.

De toegangsrechten van de Backup Service-toepassing voor de gegevens van de Microsoft 365-organisatie worden dan ingetrokken.

Microsoft 365-resources detecteren

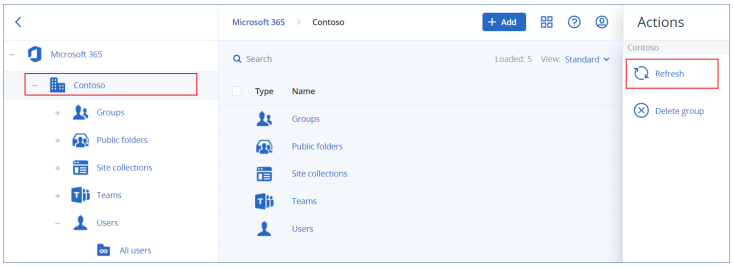
Wanneer u een Microsoft 365-organisatie toevoegt aan de Cyber Protection-service, worden de resources in deze organisatie, zoals postvakken, OneDrive-opslagplaatsen, Microsoft Teams en SharePoint-sites, gesynchroniseerd met de Cyber Protect-console. Deze bewerking wordt detectie genoemd en wordt vastgelegd in **Controle** > **Activiteiten**.

Wanneer de detectie is voltooid, kunt u de resources van de Microsoft 365-organisatie bekijken op het tabblad **Apparaten** > **Microsoft 365** in de Cyber Protect-console en kunt u hierop back-upschema's toepassen.

Eén keer per dag wordt een automatische detectiebewerking uitgevoerd om de lijst met resources in de Cyber Protect-console up-to-date te houden. U kunt deze lijst ook synchroniseren op aanvraag door een detectiebewerking handmatig opnieuw uit te voeren.

Handmatig een detectiebewerking opnieuw uitvoeren:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Microsoft 365**.
2. Selecteer uw Microsoft 365-organisatie en klik vervolgens in het deelvenster **Acties** op **Vernieuwen**.



Opmerking
U kunt maximaal 10 keer per uur een handmatige detectiebewerking uitvoeren. Wanneer dit aantal is bereikt, wordt het aantal toegestane uitvoeringen teruggezet op één per uur, en daarna komt er elk uur een extra uitvoering bij tot het totaal van 10 uitvoeringen per uur weer is bereikt.

De frequentie van Microsoft 365-back-ups instellen

Microsoft 365-back-ups worden standaard eenmaal per dag uitgevoerd en er zijn geen extra planningsopties beschikbaar.

Als het Advanced Backup-pakket is ingeschakeld in uw tenant, kunt u frequentere back-ups configureren. U kunt het aantal back-ups per dag selecteren, maar de starttijd van de back-up kunt u niet configureren. De back-ups worden automatisch gestart met een interval dat afhangt van de huidige belasting van de cloudagent, die wordt gebruikt voor meerdere klanten in een datacenter. Zo wordt de belasting gelijkmatig verdeeld gedurende de dag en krijgen alle klanten eenzelfde serviceniveau.

De volgende opties zijn beschikbaar.

Planningsopties	Interval (bij benadering) tussen elke back-up
Eén keer per dag	24 uur
Twee keer per dag (standaard)	12 uur
Drie keer per dag	8 uur
Zes keer per dag	4 uur

Opmerking
Afhankelijk van de belasting van de cloudagent en een mogelijke beperking door Microsoft 365, kan het zijn dat een back-up later wordt gestart dan gepland of langer duurt. Als een back-up langer duurt dan het gemiddelde interval tussen twee back-ups, wordt de volgende back-up opnieuw gepland, waardoor er minder back-ups per dag worden uitgevoerd dan wat was geselecteerd. Er kunnen bijvoorbeeld slechts twee back-ups per dag worden voltooid, ook al hebt u er zes per dag geselecteerd.

Back-ups van groepspostvakken kunnen slechts eenmaal per dag worden uitgevoerd.

Exchange Online-gegevens beveiligen

Van welke items kan een back-up worden gemaakt?

U kunt een back-up maken van gebruikerspostvakken, gedeelde postvakken en groepspostvakken. U kunt er ook voor kiezen een back-up te maken van de online archiefpostvakken (**In-place archief**) van de geselecteerde postvakken.

Vanaf versie 8.0 van de Cyber Protection-service kunt u een back-up maken van openbare mappen. Als uw organisatie vóór de release van versie 8.0 aan de Cyber Protection-service is toegevoegd, moet u de organisatie opnieuw toevoegen om deze functionaliteit te verkrijgen. Verwijder de organisatie niet, maar herhaal de stappen zoals beschreven in "Een Microsoft 365-organisatie toevoegen" (p. 642). Als gevolg hiervan krijgt de Cyber Protection-service toestemming om de betreffende API te gebruiken.

Welke items kunnen worden hersteld?

De volgende items kunnen worden hersteld vanuit een back-up van een postvak:

- Postvakken
- E-mailmappen
- E-mailberichten
- Agendagebeurtenissen
- Taken
- Contacten

- Logboekvermeldingen
- Notities

De volgende items kunnen worden hersteld vanuit een back-up van een openbare map:

- Submappen
- Posten
- E-mailberichten

U kunt een zoekopdracht gebruiken om de items te vinden.

Wanneer u postvakken, postvakitems, openbare mappen en items uit openbare mappen herstelt, kunt u selecteren of u de items op de doellocatie wilt overschrijven.

Postvakken selecteren

Selecteer de postvakken zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

Exchange Online-postvakken selecteren

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gebruikersgegevens waarvan u een back-up wilt maken. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u een back-up wilt maken van de postvakken van alle gebruikers en van alle gedeelde postvakken (inclusief postvakken die in de toekomst worden gemaakt), vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers** en klikt u vervolgens op **Back-up van groep**.
   - Als u een back-up wilt maken van de postvakken van afzonderlijke gebruikers of van gedeelde postvakken, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u de gebruikers met de postvakken waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.
   - Als u een back-up wilt maken van alle postvakken van een groep (inclusief postvakken van groepen die in de toekomst worden gemaakt), vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen** en klikt u vervolgens op **Back-up van groep**.
   - Als u een back-up wilt maken van afzonderlijke postvakken van een groep, vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen**, selecteert u de groepen met de postvakken waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.

Opmerking
De cloudagent voor Microsoft 365 gebruikt een account met de juiste rechten voor toegang tot een groepspostvak. Als u een back-up van een groepspostvak wilt maken, moet dus ten minste een van de groepseigenaren een gelicentieerde Microsoft 365-gebruiker met een postvak zijn. Als de groep privé is of een verborgen lidmaatschap heeft, moet de eigenaar ook lid zijn van de groep.

4. In het deelvenster voor het beschermingsschema:
   - Controleer of het item **Microsoft 365-postvakken** is geselecteerd in **Back-up maken van**.
     U kunt deze optie niet selecteren als sommige van de afzonderlijk geselecteerde gebruikers de Exchange-service niet hebben opgenomen in hun Microsoft 365-abonnement.
     U kunt deze optie wel selecteren als sommige van de geselecteerde gebruikers voor back-ups van groepen de Exchange-service niet hebben opgenomen in hun Microsoft 365-abonnement, maar het beschermingsschema wordt dan niet toegepast op die gebruikers.
   - Als u geen back-up van de archiefpostvakken wilt maken, schakelt u de schakelaar **Archiefpostvak** uit.

Openbare mappen selecteren

Selecteer de openbare mappen zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

Opmerking
Voor openbare mappen worden licenties van uw back-upquota voor Microsoft 365-seats verbruikt.

Openbare mappen van Exchange Online selecteren

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, vouwt u de organisatie uit die de gegevens bevat waarvan u een back-up wilt maken. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Openbare mappen** uit en selecteer vervolgens **Alle openbare mappen**.
4. Voer een van de volgende handelingen uit:
   - Als u een back-up wilt maken van alle openbare mappen (inclusief openbare mappen die in de toekomst worden gemaakt), klikt u op **Back-up van groep**.
   - Als u een back-up wilt maken van afzonderlijke openbare mappen, selecteert u de openbare mappen waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.
5. Controleer in het deelvenster voor het beschermingsschema of het item **Microsoft 365-postvakken** is geselecteerd in **Back-up maken van**.

Postvakken en postvakitems herstellen

Postvakken herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gegevens die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u een gebruikerspostvak wilt herstellen, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u de gebruiker van wie u het postvak wilt herstellen en klikt u vervolgens op **Herstel**.
   - Als u een gedeeld postvak wilt herstellen, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u het gedeelde postvak dat u wilt herstellen en klikt u vervolgens op **Herstel**.
   - Als u een groepspostvak wilt herstellen, vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen**, selecteert u de groep waarvan u het postvak wilt herstellen en klikt u vervolgens op **Herstel**.
   - Als de gebruiker, de groep of het gedeelde postvak is verwijderd, selecteert u het gewenste item in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-ups en klikt u vervolgens op **Back-ups weergeven**.

   U kunt gebruikers en groepen zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.

   Opmerking
   Als u alleen de herstelpunten wilt zien die postvakken bevatten, selecteert u **Postvakken** in **Filteren op inhoud**.

5. Klik op **Herstellen** > **Volledig postvak**.
6. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.
   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
7. In **Herstellen naar postvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.
   Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u het doelpostvak opgeven.
   U kunt geen nieuw doelpostvak maken tijdens het herstel. Als u een postvak wilt herstellen naar een nieuw postvak, moet u eerst het doelpostvak maken in de gewenste Microsoft 365-organisatie en vervolgens de wijziging laten synchroniseren door de cloudagent. De cloudagent synchroniseert automatisch elke 24 uur met Microsoft 365. Als u de wijziging onmiddellijk wilt

synchroniseren, gaat u naar de Cyber Protect-console en selecteert u de organisatie op de **Microsoft 365**-pagina. Vervolgens klikt u op **Vernieuwen**.

8. Klik op **Herstel starten**.
9. Selecteer een van de opties voor overschrijven:
   - **Bestaande items overschrijven**
   - **Bestaande items niet overschrijven**
10. Klik op **Doorgaan** om uw beslissing te bevestigen.

Postvakitems herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gegevens die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u items uit een gebruikerspostvak wilt herstellen, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u de gebruiker van het postvak met de oorspronkelijke items die u wilt herstellen en klikt u vervolgens op **Herstel**.
   - Als u items uit een gedeeld postvak wilt herstellen, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u het gedeelde postvak dat oorspronkelijk de items bevatte die u wilt herstellen en klikt u vervolgens op **Herstel**.
   - Als u items uit een groepspostvak wilt herstellen, vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen**, selecteert u de groep van het postvak met de oorspronkelijke items die u wilt herstellen en klikt u vervolgens op **Herstel**.
   - Als de gebruiker, de groep of het gedeelde postvak is verwijderd, selecteert u het gewenste item in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-ups en klikt u vervolgens op **Back-ups weergeven**.

   U kunt gebruikers en groepen zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.

   Opmerking
   Als u alleen de herstelpunten wilt zien die postvakken bevatten, selecteert u **Postvakken** in **Filteren op inhoud**.

5. Klik op **Herstellen** > **E-mailberichten**.
6. Blader naar de vereiste map of gebruik de zoekfunctie om de lijst met vereiste items weer te geven.

   De volgende zoekopties zijn beschikbaar. Jokers worden niet ondersteund.
   - E-mailberichten: u kunt zoeken op onderwerp, afzender, ontvanger, naam van bijlage en datum. U kunt een begindatum of een einddatum (beide inclusief) selecteren, of beide datums als u binnen een tijdbereik wilt zoeken.

- Gebeurtenissen: u kunt zoeken op titel en datum.
- Taken: u kunt zoeken op onderwerp en datum.
- Contacten: u kunt zoeken op naam, e-mailadres en telefoonnummer.

7. Selecteer de items die u wilt herstellen. Als u mappen wilt selecteren, klikt u op het pictogram 'Mappen herstellen': 

   U kunt geen nieuw doelpostvak maken tijdens het herstel. Als u een nieuw postvakitem wilt herstellen naar een nieuw postvak, moet u eerst het nieuwe doelpostvakitem maken in de Microsoft 365-organisatie en vervolgens de wijziging laten synchroniseren door de cloudagent. De cloudagent synchroniseert automatisch elke 24 uur met Microsoft 365. Als u de wijziging onmiddellijk wilt synchroniseren, gaat u naar de Cyber Protect-console en selecteert u de organisatie op de **Microsoft 365**-pagina. Vervolgens klikt u op **Vernieuwen**.

   U kunt ook een van de volgende handelingen uitvoeren:
   - Wanneer een item is geselecteerd, klikt u op **Inhoud weergeven** om de inhoud te bekijken, inclusief bijlagen. Klik op de naam van een bijgevoegd bestand om het te downloaden.
   - Wanneer een e-mailbericht of agenda-item is geselecteerd, kunt u klikken op **Versturen als e-mail** om het bericht naar een e-mailadres te verzenden. U kunt de afzender selecteren en een tekst schrijven die u wilt toevoegen aan het doorgestuurde artikel.
   - Alleen als de back-up niet is versleuteld, u de zoekfunctie hebt gebruikt en één item in de zoekresultaten hebt geselecteerd: klik op **Versies weergeven** om de itemversie te selecteren die u wilt herstellen. U kunt elke versie selecteren waarvan een back-up is gemaakt, ongeacht of deze eerder of later is dan het geselecteerde herstelpunt.
8. Klik op **Herstellen**.
9. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
10. In **Herstellen naar postvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.

    Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u het doelpostvak opgeven.
11. [Alleen bij het herstellen naar een gebruikerspostvak of gedeeld postvak] Open **Pad** en bekijk of wijzig de doelmap in het doelpostvak. Standaard wordt de map **Herstelde items** geselecteerd.

    Items van groepspostvakken worden altijd hersteld naar de map **Postvak IN**.
12. Klik op **Herstel starten**.
13. Selecteer een van de opties voor overschrijven:
    - **Bestaande items overschrijven**
    - **Bestaande items niet overschrijven**
14. Klik op **Doorgaan** om uw beslissing te bevestigen.

Volledige postvakken herstellen als PST-gegevensbestanden

Opmerking
In-place archief kan niet worden hersteld als onderdeel van herstel naar PST-bestanden. Als u het in-place archief samen met het postvak wilt herstellen, raadpleegt u "Postvakken herstellen" (p. 649).

Postvak herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gegevens die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u een gebruikerspostvak wilt herstellen als een PST-gegevensbestand, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u het postvak dat u wilt herstellen en klikt u vervolgens op **Herstel**.
   - Als u een gedeeld postvak wilt herstellen als een PST-gegevensbestand, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u het postvak dat u wilt herstellen en klikt u vervolgens op **Herstel**.
   - Als u een groepspostvak wilt herstellen als een PST-gegevensbestand, vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen**, selecteert u de groep waarvan u het postvak wilt herstellen en klikt u vervolgens op **Herstel**.

   U kunt gebruikers en groepen zoeken op naam. Jokers worden niet ondersteund.

   Als de gebruiker, de groep of het gedeelde Outlook-gegevensbestand is verwijderd, selecteert u het gewenste item in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u vervolgens op **Back-ups weergeven**.
4. Klik op **Herstellen** > **Als PST-bestanden**.
5. Stel het wachtwoord in om het archief met de PST-bestanden te versleutelen.
   Het wachtwoord moet ten minste één symbool bevatten.
6. Bevestig het wachtwoord en klik op **Gereed**.
7. De geselecteerde postvakitems worden hersteld als PST-gegevensbestanden en gearchiveerd in zipindeling. De maximale grootte van een PST-bestand is beperkt tot 2 GB, dus als de gegevens die u herstelt, groter zijn dan 2 GB, worden de gegevens opgesplitst in verschillende PST-bestanden. Het ziparchief wordt beschermd met het door u ingestelde wachtwoord.
8. U ontvangt een e-mail met een link naar een ziparchief met de nieuw gemaakte PST-bestanden.
9. De beheerder ontvangt een e-mailbericht dat u de herstelprocedure hebt uitgevoerd.

Opmerking
Postvakherstel naar PST-bestanden kan tijdrovend zijn, omdat het niet alleen gegevensoverdracht omvat, maar ook gegevenstransformatie met complexe algoritmen.

Het archief met PST-bestanden downloaden en het herstel voltooien

1. Voer een van de volgende handelingen uit:
   - Als u het archief wilt downloaden vanuit de e-mail, volgt u de link **Bestanden downloaden**. U hebt dan 24 uur om het archief te downloaden. Als de link verloopt, herhaalt u de herstelprocedure.
   - Het archief downloaden vanuit de Cyber Protect-console:
     a. Ga naar **Back-upopslag** > **PST-bestanden**.
     b. Selecteer het meest recente gemarkeerde archief.
     c. Klik op **Downloaden** in het rechterdeelvenster.

   Het archief wordt gedownload naar de standaard downloaddirectory op uw computer.
2. Pak de PST-bestanden uit het archief uit met het wachtwoord dat u hebt ingesteld om het archief te versleutelen.
3. Open de PST-bestanden met Microsoft Outlook.
   De resulterende PST-bestanden kunnen veel kleiner zijn dan het oorspronkelijke postvak. Dat is normaal.

Belangrijk
Importeer deze bestanden niet in Microsoft Outlook via de **Wizard Importeren en exporteren**. Dubbelklik of klik met de rechtermuisknop op de bestanden om ze te openen en selecteer **Openen met...** > **Microsoft Outlook** in het contextmenu.

Postvakitems herstellen als PST-bestanden

Opmerking
In-place archief kan niet worden hersteld als onderdeel van herstel naar PST-bestanden. Als u het in-place archief samen met het postvak wilt herstellen, raadpleegt u "Postvakken herstellen" (p. 649).

Postvakitems herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gegevens die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u items uit een gebruikerspostvak wilt herstellen, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u de gebruiker van het postvak met de oorspronkelijke items die u wilt herstellen en klikt u vervolgens op **Herstel**.
   - Als u items uit een gedeeld postvak wilt herstellen, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u het gedeelde postvak dat oorspronkelijk de items bevatte die u wilt herstellen en klikt u vervolgens op **Herstel**.

- Als u items uit een groepspostvak wilt herstellen, vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen**, selecteert u de groep van het postvak met de oorspronkelijke items die u wilt herstellen en klikt u vervolgens op **Herstel**.
- Als de gebruiker, de groep of het gedeelde postvak is verwijderd, selecteert u het gewenste item in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-ups en klikt u vervolgens op **Back-ups weergeven**.

U kunt gebruikers en groepen zoeken op naam. Jokers worden niet ondersteund.

4. Klik op **Herstellen** > **E-mailberichten**.
5. Blader naar de vereiste map of gebruik de zoekfunctie om de lijst met vereiste items weer te geven.

   De volgende zoekopties zijn beschikbaar. Jokers worden niet ondersteund.
   - E-mailberichten: u kunt zoeken op onderwerp, afzender, ontvanger, naam van bijlage en datum.
   - Gebeurtenissen: u kunt zoeken op titel en datum.
   - Taken: u kunt zoeken op onderwerp en datum.
   - Contacten: u kunt zoeken op naam, e-mailadres en telefoonnummer.
6. Selecteer de items die u wilt herstellen. Als u mappen wilt selecteren, klikt u op het pictogram 'Mappen herstellen': 

   U kunt ook een van de volgende handelingen uitvoeren:
   - Wanneer een item is geselecteerd, klikt u op **Inhoud weergeven** om de inhoud ervan te bekijken, inclusief bijlagen. Klik op de naam van een bijgevoegd bestand om het te downloaden.
   - Wanneer een e-mailbericht of agenda-item is geselecteerd, kunt u klikken op **Versturen als e-mail** om het bericht naar een e-mailadres te verzenden. U kunt de afzender selecteren en een tekst schrijven die u wilt toevoegen aan het doorgestuurde artikel.
   - Alleen als de back-up niet is versleuteld, u de zoekfunctie hebt gebruikt en één item in de zoekresultaten hebt geselecteerd: klik op **Versies weergeven** om de itemversie te selecteren die u wilt herstellen. U kunt elke versie selecteren waarvan een back-up is gemaakt, ongeacht of deze eerder of later is dan het geselecteerde herstelpunt.
7. Klik op **Herstellen als PST-bestanden**.
8. Stel het wachtwoord in om het archief met de PST-bestanden te versleutelen.

   Het wachtwoord moet ten minste één symbool bevatten.
9. Bevestig het wachtwoord en klik op **GEREED**.

De geselecteerde postvakitems worden hersteld als PST-gegevensbestanden en gearchiveerd in zipindeling. De maximale grootte van een PST-bestand is beperkt tot 2 GB, dus als de gegevens die u herstelt, groter zijn dan 2 GB, worden de gegevens opgesplitst in verschillende PST-bestanden. Het ziparchief wordt beschermd met het door u ingestelde wachtwoord.

U ontvangt een e-mail met een link naar een ziparchief met de nieuw gemaakte PST-bestanden.

De beheerder ontvangt een e-mailbericht dat u de herstelprocedure hebt uitgevoerd.

Het archief met PST-bestanden downloaden en het herstel voltooien

1. Voer een van de volgende handelingen uit:
   - Als u het archief wilt downloaden vanuit de e-mail, volgt u de link **Bestanden downloaden**. U hebt dan 24 uur om het archief te downloaden. Als de link verloopt, herhaalt u de herstelprocedure.
   - Het archief downloaden vanuit de Cyber Protect-console:
     a. Ga naar **Back-upopslag** > **PST-bestanden**.
     b. Selecteer het meest recente gemarkeerde archief.
     c. Klik op **Downloaden** in het rechterdeelvenster.

   Het archief wordt gedownload naar de standaard downloaddirectory op uw computer.
2. Pak de PST-bestanden uit het archief uit met het wachtwoord dat u hebt ingesteld om het archief te versleutelen.
3. Open de PST-bestanden met Microsoft Outlook.
   De resulterende PST-bestanden kunnen veel kleiner zijn dan het oorspronkelijke postvak. Dat is normaal.

Belangrijk
Importeer deze bestanden niet in Microsoft Outlook via de **Wizard Importeren en exporteren**.
Dubbelklik of klik met de rechtermuisknop op de bestanden om ze te openen en selecteer **Openen met...** > **Microsoft Outlook** in het contextmenu.

Openbare mappen en items uit openbare mappen herstellen

Als u een openbare map of items uit een openbare map wilt herstellen, moet ten minste één beheerder van de Microsoft 365-doelorganisatie de rechten van **Eigenaar** hebben voor de openbare doelmap. Als de herstelbewerking mislukt met een fout over geweigerde toegang, dan gaat u als volgt te werk: wijs deze rechten toe in de eigenschappen van de doelmap, selecteer de doelorganisatie in de Cyber Protect-console, klik op **Vernieuwen** en herhaal de herstelbewerking.

Een openbare map of items uit en openbare map herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, vouwt u de organisatie uit waarvan u de back-upgegevens wilt herstellen. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Vouw het knooppunt **Openbare mappen** uit, selecteer **Alle openbare mappen**, selecteer de openbare map die u wilt herstellen of die oorspronkelijk de items bevatte die u wilt herstellen, en klik vervolgens op **Herstel**.
   - Als de openbare map is verwijderd, selecteert u deze in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u vervolgens op **Back-ups weergeven**.

U kunt openbare mappen zoeken op naam. Jokers worden niet ondersteund.

4. Selecteer een herstelpunt.
5. Klik op **Gegevens herstellen**.
6. Blader naar de vereiste map of gebruik de zoekfunctie om de lijst met vereiste items weer te geven.

   U kunt (e-mail)berichten zoeken op onderwerp, afzender, ontvanger en datum. Jokers worden niet ondersteund.
7. Selecteer de items die u wilt herstellen. Als u mappen wilt selecteren, klikt u op het pictogram 'Mappen herstellen': 

   U kunt ook een van de volgende handelingen uitvoeren:
   - Wanneer een (e-mail)bericht is geselecteerd, klikt u op **Inhoud weergeven** om de inhoud ervan te bekijken, inclusief bijlagen. Klik op de naam van een bijgevoegd bestand om het te downloaden.
   - Wanneer een (e-mail)bericht is geselecteerd, klikt u op **Versturen als e-mail** om het item naar opgegeven e-mailadressen te verzenden. U kunt de afzender selecteren en een tekst schrijven die u wilt toevoegen aan het doorgestuurde artikel.
   - Alleen als de back-up niet is versleuteld, u de zoekfunctie hebt gebruikt en één item in de zoekresultaten hebt geselecteerd: klik op **Versies weergeven** om de itemversie te selecteren die u wilt herstellen. U kunt elke versie selecteren waarvan een back-up is gemaakt, ongeacht of deze eerder of later is dan het geselecteerde herstelpunt.
8. Klik op **Herstellen**.
9. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
10. In **Herstellen naar openbare map** kunt u de openbare doelmap bekijken, wijzigen of opgeven.

    Standaard is de oorspronkelijke map geselecteerd. Als deze map niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u de doelmap opgeven.

    U kunt geen nieuwe openbare map maken tijdens het herstel. Als u een openbare map wilt herstellen naar een nieuwe openbare map, moet u eerst de doelmap maken in de gewenste Microsoft 365-organisatie en vervolgens de wijziging laten synchroniseren door de cloudagent. De cloudagent synchroniseert automatisch elke 24 uur met Microsoft 365. Als u de wijziging onmiddellijk wilt synchroniseren, gaat u naar de Cyber Protect-console en selecteert u de organisatie op de **Microsoft 365**-pagina. Vervolgens klikt u op **Vernieuwen**.
11. Open **Pad** en bekijk of wijzig de doelsubmap in de openbare doelmap. Standaard wordt het oorspronkelijke pad opnieuw gemaakt.
12. Klik op **Herstel starten**.
13. Selecteer een van de opties voor overschrijven:

Optie	Beschrijving
Bestaande items overschrijven	Alle bestaande bestanden op de doellocatie worden overschreven.
Bestaande items niet overschrijven	Als de doellocatie een bestand met dezelfde naam bevat, wordt dat bestand niet overschreven en wordt het bronbestand niet opgeslagen op de doellocatie.

14. Klik op **Doorgaan** om uw beslissing te bevestigen.

OneDrive-bestanden beveiligen

Van welke items kan een back-up worden gemaakt?

U kunt een back-up maken van een volledige OneDrive of van afzonderlijke bestanden en mappen.

Een aparte optie in het back-upschema maakt de back-up van OneNote-notitieblokken mogelijk.

Bij het maken van een back-up van bestanden, wordt ook een back-up gemaakt van de machtigingen voor delen van die bestanden. Van geavanceerde machtigingsniveaus (**Ontwerpen**, **Volledig**, **Bijdragen**) worden geen back-ups gemaakt.

Sommige bestanden kunnen gevoelige informatie bevatten en de toegang ertoe kan worden geblokkeerd door een regel voor preventie van gegevensverlies (DLP) in Microsoft 365. Van deze bestanden wordt geen back-up gemaakt en er worden geen waarschuwingen weergegeven wanneer de back-upbewerking is voltooid.

Beperkingen

Back-ups voor OneDrive-inhoud worden niet ondersteund voor gedeelde postvakken. Als u een back-up van deze inhoud wilt maken, converteert u het gedeelde postvak naar een regulier gebruikersaccount en schakelt u OneDrive in voor dat account.

Welke items kunnen worden hersteld?

U kunt een volledige OneDrive of een bestand of map waarvan een back-up is gemaakt, herstellen.

U kunt een zoekopdracht gebruiken om de items te vinden.

U kunt kiezen of u de machtigingen voor delen wilt herstellen of dat de bestanden de machtigingen overnemen van de map waarin ze worden hersteld.

Links voor het delen van bestanden en mappen worden niet hersteld.

OneDrive-bestanden selecteren

Selecteer de bestanden zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

OneDrive-bestanden selecteren

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gebruikersgegevens waarvan u een back-up wilt maken. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u een back-up wilt maken van de bestanden van alle gebruikers (inclusief gebruikers die in de toekomst worden gemaakt), vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers** en klikt u vervolgens op **Back-up van groep**.
   - Als u een back-up wilt maken van de bestanden van afzonderlijke gebruikers, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u de gebruikers met de bestanden waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.
4. In het deelvenster voor het beschermingsschema:
   - Controleer of het item **OneDrive** is geselecteerd in **Back-up maken van**.

     U kunt deze optie niet selecteren als sommige van de afzonderlijk geselecteerde gebruikers de OneDrive-service niet hebben opgenomen in hun Microsoft 365-abonnement.

     U kunt deze optie wel selecteren als sommige van de geselecteerde gebruikers voor back-ups van groepen de OneDrive-service niet hebben opgenomen in hun Microsoft 365-abonnement, maar het beschermingsschema wordt dan niet toegepast op die gebruikers.
   - Voer in **Items waarvan een back-up moet worden gemaakt** een van de volgende handelingen uit:
     - Behoud de standaardinstelling **[All]** (alle bestanden).
     - Voeg de namen of paden toe van de bestanden en mappen waarvan u een back-up wilt maken.

       U kunt jokertekens (*, ** en ?) gebruiken. Voor meer informatie over het opgeven van paden en het gebruik van jokers gaat u naar 'Bestandsfilters'.
     - Blader door de bestanden en mappen om op te geven van welke bestanden en mappen u een back-up wilt maken.

       De link **Bladeren** is alleen beschikbaar wanneer u een beschermingsschema voor één gebruiker maakt.
   - [Optioneel] Klik in **Items waarvan een back-up moet worden gemaakt** op **Uitsluitingen weergeven** om op te geven welke bestanden en mappen u wilt overslaan tijdens het maken van de back-up.

     Met bestandsuitsluitingen wordt de bestandsselectie overschreven, dat wil zeggen als u in beide velden hetzelfde bestand opgeeft, wordt dit bestand overgeslagen tijdens een back-up.
   - [Optioneel] Schakel de schakelaar **OneNote opnemen** in om een back-up te maken van de OneNote-notitieblokken.

OneDrive- en OneDrive-bestanden herstellen

Een volledige OneDrive herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gegevens die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Gebruikers** uit, selecteer **Alle gebruikers**, selecteer de gebruiker met de OneDrive die u wilt herstellen en klik vervolgens op **Herstel**.

   Als de gebruiker is verwijderd, selecteert u de gebruiker in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u op **Back-ups weergeven**.

   U kunt gebruikers zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.

   Opmerking
   Als u alleen de herstelpunten wilt zien die OneDrive-bestanden bevatten, selecteert u **OneDrive** in **Filteren op inhoud**.
5. Klik op **Herstellen** > **Volledige OneDrive**.
6. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.

   U kunt geen nieuw OneDrive-doel maken tijdens het herstel. Als u een OneDrive wilt herstellen naar een nieuwe OneDrive, moet u eerst de doel-OneDrive maken in de Microsoft 365-organisatie en vervolgens de wijziging laten synchroniseren door de cloudagent. De cloudagent synchroniseert automatisch elke 24 uur met Microsoft 365. Als u de wijziging onmiddellijk wilt synchroniseren, gaat u naar de Cyber Protect-console en selecteert u de organisatie op de **Microsoft 365**-pagina. Vervolgens klikt u op **Vernieuwen**.
7. In **Herstellen naar station** kunt u de doelgebruiker weergeven, wijzigen of opgeven.

   Standaard is de oorspronkelijke gebruiker geselecteerd. Als deze gebruiker niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u de doelgebruiker opgeven.
8. Selecteer of u de machtigingen voor delen voor de bestanden wilt herstellen.
9. Klik op **Herstel starten**.
10. Selecteer een van de opties voor overschrijven:

Optie	Beschrijving
Een bestaand bestand	Als er een bestand met dezelfde naam op de doellocatie is en dit bestand ouder is dan het bronbestand, wordt het bronbestand opgeslagen op de

Optie	Beschrijving
overschrijven als dit ouder is	doellocatie, ter vervanging van de oudere versie.
Bestaande bestanden overschrijven	Alle bestaande bestanden op de doellocatie worden overschreven, ongeacht de datum waarop ze voor het laatst zijn gewijzigd.
Bestaande bestanden niet overschrijven	Als er een bestand met dezelfde naam op de doellocatie is, worden hierin geen wijzigingen aangebracht en wordt het bronbestand niet opgeslagen op de doellocatie.

Opmerking
Wanneer u OneNote-notitieblokken herstelt, worden de bestaande OneNote-notitieblokken overschreven, ongeacht of u **Een bestaand bestand overschrijven als dit ouder is** of **Bestaande bestanden overschrijven** kiest.

11. Klik op **Doorgaan** om uw beslissing te bevestigen.

OneDrive-bestanden herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gegevens die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Gebruikers** uit, selecteer **Alle gebruikers**, selecteer de gebruiker met de OneDrive-bestanden die u wilt herstellen en klik vervolgens op **Herstel**.
   Als de gebruiker is verwijderd, selecteert u de gebruiker in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u op **Back-ups weergeven**.
   U kunt gebruikers zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.

Opmerking
Als u alleen de herstelpunten wilt zien die OneDrive-bestanden bevatten, selecteert u **OneDrive** in **Filteren op inhoud**.

5. Klik op **Herstellen** > **Bestanden/mappen**.
6. Blader naar de vereiste map of gebruik de zoekfunctie om de lijst met vereiste bestanden en mappen weer te geven.
7. Selecteer de bestanden die u wilt herstellen.
   Als de back-up niet is versleuteld en u één bestand hebt geselecteerd, kunt u klikken op **Versies weergeven** om de bestandsversie te selecteren die u wilt herstellen. U kunt elke versie selecteren waarvan een back-up is gemaakt, ongeacht of deze eerder of later is dan het geselecteerde herstelpunt.

8. Als u een bestand wilt downloaden, selecteert u het bestand, klikt u op **Downloaden**, selecteert u de locatie waar u het bestand wilt opslaan en klikt u op **Opslaan**. Anders kunt u deze stap overslaan.
9. Klik op **Herstellen**.
10. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.
    Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
    U kunt geen nieuwe OneDrive maken tijdens het herstel. Als u een bestand wilt herstellen naar een nieuwe OneDrive, moet u eerst de doel-OneDrive maken in de gewenste Microsoft 365-organisatie en vervolgens de wijziging laten synchroniseren door de cloudagent. De cloudagent synchroniseert automatisch elke 24 uur met Microsoft 365. Als u de wijziging onmiddellijk wilt synchroniseren, gaat u naar de Cyber Protect-console en selecteert u de organisatie op de **Microsoft 365**-pagina. Vervolgens klikt u op **Vernieuwen**.
11. In **Herstellen naar station** kunt u de doelgebruiker weergeven, wijzigen of opgeven.
    Standaard is de oorspronkelijke gebruiker geselecteerd. Als deze gebruiker niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u de doelgebruiker opgeven.
12. Open **Pad** en bekijk of wijzig de doelmap in de doel-OneDrive van de gebruiker. Standaard is de oorspronkelijke locatie geselecteerd.
13. Selecteer of u de machtigingen voor delen voor de bestanden wilt herstellen.
14. Klik op **Herstel starten**.
15. Selecteer een van de opties voor het overschrijven van bestanden:

Optie	Beschrijving
Een bestaand bestand overschrijven als dit ouder is	Als er een bestand met dezelfde naam op de doellocatie is en dit bestand ouder is dan het bronbestand, wordt het bronbestand opgeslagen op de doellocatie, ter vervanging van de oudere versie.
Bestaande bestanden overschrijven	Alle bestaande bestanden op de doellocatie worden overschreven, ongeacht de datum waarop ze voor het laatst zijn gewijzigd.
Bestaande bestanden niet overschrijven	Als er een bestand met dezelfde naam op de doellocatie is, worden hierin geen wijzigingen aangebracht en wordt het bronbestand niet opgeslagen op de doellocatie.

Opmerking
Wanneer u OneNote-notitieblokken herstelt, worden de bestaande OneNote-notitieblokken overschreven, ongeacht of u **Een bestaand bestand overschrijven als dit ouder is** of **Bestaande bestanden overschrijven** kiest.

16. Klik op **Doorgaan** om uw beslissing te bevestigen.

SharePoint Online-sites beveiligen

Van welke items kan een back-up worden gemaakt?

U kunt een back-up maken van klassieke SharePoint-siteverzamelingen, groepssites (van moderne teams) en communicatiesites. U kunt ook afzonderlijke subsites, lijsten en bibliotheken selecteren voor back-up.

Een aparte optie in het back-upschema maakt de back-up van OneNote-notitieblokken mogelijk.

De volgende items worden *overgeslagen* tijdens een back-up:

- De instellingen van **Vormgeving** voor de site (behalve **Titel, beschrijving en logo**).
- Opmerkingen op de sitepagina en instellingen voor de paginaopmerkingen (opmerkingen **Aan**/**Uit**).
- De site-instellingen van **Sitefuncties**.
- Pagina's van webonderdelen en webonderdelen die zijn ingesloten in de wiki-pagina's (vanwege beperkingen van de SharePoint Online API).
- Uitgecheckte bestanden: bestanden die handmatig worden uitgecheckt voor bewerking en alle bestanden die zijn gemaakt of geüpload in bibliotheken en waarvoor de optie **Uitchecken vereisen** was ingeschakeld. Als u een back-up van deze bestanden wilt maken, checkt u ze eerst in.
- Externe gegevens en kolommen van het type Beheerde metagegevens.
- De standaardsiteverzameling 'domain-my.sharepoint.com'. Dit is een verzameling met alle OneDrive-bestanden van de gebruikers van de organisatie.
- De inhoud van de prullenbak.

Beperkingen

- Titels en beschrijvingen van sites/subsites/lijsten/kolommen worden afgekapt tijdens een back-up als de titel/beschrijving groter is dan 10.000 bytes.
- U kunt geen back-up maken van vorige versies van bestanden die zijn gemaakt in SharePoint Online. Alleen de nieuwste versies van de bestanden worden beschermd.
- U kunt geen back-up maken van de opslagbibliotheek.
- U kunt geen back-up maken van sites die zijn gemaakt in de Business Productivity Online Suite (BPOS), de voorganger van Microsoft 365.
- U kunt geen back-up maken van de instellingen voor sites die gebruikmaken van het beheerde pad `/portals` (bijvoorbeeld `https://<tenant>.sharepoint.com/portals/...`).
- De Information Rights Management (IRM)-instellingen van een lijst of een bibliotheek kunnen alleen worden hersteld als IRM is ingeschakeld in de Microsoft 365-doelorganisatie.

Welke items kunnen worden hersteld?

De volgende items kunnen worden hersteld vanuit een back-up van een site:

- Volledige site
- Subsites
- Lijsten
- Lijstitems
- Documentbibliotheken
- Documenten
- Bijlagen van lijstitems
- Sitepagina's en wiki-pagina's

U kunt een zoekopdracht gebruiken om de items te vinden.

Items kunnen worden hersteld naar de oorspronkelijke site of een andere site. Het pad naar een hersteld item is hetzelfde als voor het oorspronkelijke item. Als het pad niet bestaat, wordt het gemaakt.

U kunt kiezen of u de machtigingen voor delen wilt herstellen of dat de items de machtigingen overnemen van het bovenliggende object na het herstel.

Welke items kunnen niet worden hersteld?

- Subsites gebaseerd op de **Visio Process Repository**-sjabloon.
- Lijsten van de volgende typen: **Enquêtelijst**, **Takenlijst**, **Afbeeldingenbibliotheek**, **Links**, **Agenda**, **Discussiebord**, **Extern** en **Geïmporteerde spreadsheet**.
- Lijsten waarvoor meerdere inhoudstypen zijn ingeschakeld.

SharePoint Online-gegevens selecteren

Selecteer de gegevens zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

SharePoint Online-gegevens selecteren

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gebruikersgegevens waarvan u een back-up wilt maken. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u een back-up wilt maken van alle klassieke SharePoint-sites in de organisatie, inclusief sites die in de toekomst worden gemaakt, vouwt u het knooppunt **Siteverzamelingen** uit, selecteert u **Alle siteverzamelingen** en klikt u vervolgens op **Back-up van groep**.
   - Als u een back-up wilt maken van afzonderlijke klassieke sites, vouwt u het knooppunt **Siteverzamelingen** uit, selecteert u **Alle siteverzamelingen**, selecteert u de sites waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.

- Als u een back-up wilt maken van alle groepssites (van moderne teams), inclusief sites die in de toekomst worden gemaakt, vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen** en klikt u vervolgens op **Back-up van groep**.
- Als u een back-up wilt maken van afzonderlijke groepssites (van moderne teams), vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen**, selecteert u de groepen met de sites waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.

4. In het deelvenster voor het beschermingsschema:
   - Controleer of het item **SharePoint-sites** is geselecteerd in **Back-up maken van**.
   - Voer in **Items waarvan een back-up moet worden gemaakt** een van de volgende handelingen uit:
     - Behoud de standaardinstelling **[All]** (alle items van de geselecteerde sites).
     - Voeg de namen of paden toe van de subsites, lijsten en bibliotheken waarvan u een back-up wilt maken.

       Als u een back-up wilt maken van een sitelijst/bibliotheek op subsiteniveau of op het hoogste niveau, geeft u de weergavenaam op in de volgende indeling: `/weergavenaam/**`

       Als u een back-up wilt maken van een sitelijst/bibliotheek van een subsite, geeft u de weergavenaam op in de volgende indeling: `/weergavenaam van subsite/weergavenaam van lijst/**`

       De weergavenamen van subsites, lijsten en bibliotheken worden weergegeven op de pagina **Site-inhoud** van een SharePoint-site of -subsite.
     - Blader door de subsites om op te geven van welke subsites u een back-up wilt maken.

       De link **Bladeren** is alleen beschikbaar wanneer u een beschermingsschema voor één site maakt.
   - [Optioneel] Klik in **Items waarvan een back-up moet worden gemaakt** op **Uitsluitingen weergeven** om op te geven welke subsites, lijsten en bibliotheken u wilt overslaan tijdens het maken van de back-up.

     Met itemuitsluitingen wordt de itemselectie overschreven, dat wil zeggen als u in beide velden dezelfde subsite opgeeft, wordt deze subsite overgeslagen tijdens een back-up.
   - [Optioneel] Schakel de schakelaar **OneNote opnemen** in om een back-up te maken van de OneNote-notitieblokken.

SharePoint Online-gegevens herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gegevens die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u gegevens uit een groepssite (van moderne teams) wilt herstellen, vouwt u het knooppunt **Groepen** uit, selecteert u **Alle groepen**, selecteert u de groep van de site met de oorspronkelijke items die u wilt herstellen en klikt u vervolgens op **Herstel**.

- Als u gegevens uit een klassieke site wilt herstellen, vouwt u het knooppunt **Siteverzamelingen** uit, selecteert u **Alle siteverzamelingen**, selecteert u de site met de oorspronkelijke items die u wilt herstellen en klikt u vervolgens op **Herstel**.
- Als de site is verwijderd, selecteert u deze in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-ups en klikt u vervolgens op **Back-ups weergeven**.

U kunt groepen en sites zoeken op naam. Jokers worden niet ondersteund.

4. Selecteer een herstelpunt.

   Opmerking
   Als u alleen de herstelpunten wilt zien die SharePoint-sites bevatten, selecteert u **SharePoint-sites** in **Filteren op inhoud**.

5. Klik op **SharePoint-bestanden herstellen**.
6. Blader naar de vereiste map of gebruik de zoekfunctie om de lijst met vereiste gegevensitems weer te geven.
7. Selecteer de items die u wilt herstellen.

   Als de back-up niet is versleuteld, u de zoekfunctie hebt gebruikt en één item in de zoekresultaten hebt geselecteerd: klik op **Versies weergeven** om de itemversie te selecteren die u wilt herstellen. U kunt elke versie selecteren waarvan een back-up is gemaakt, ongeacht of deze eerder of later is dan het geselecteerde herstelpunt.
8. [Optioneel] Als u een item wilt downloaden, selecteert u het item, klikt u op **Downloaden** en selecteert u de locatie waar u het item wilt opslaan. Klik vervolgens op **Opslaan**.
9. Klik op **Herstellen**.
10. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

    Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
11. In **Herstellen naar site** kunt u de doelsite weergeven, wijzigen of opgeven.

    U kunt geen nieuwe SharePoint-site maken tijdens het herstel. Als u een SharePoint-site wilt herstellen naar een nieuwe SharePoint-site, moet u eerst de doelsite maken in de gewenste Microsoft 365 organisatie, en vervolgens de wijziging laten synchroniseren door de cloudagent. De cloudagent synchroniseert automatisch elke 24 uur met Microsoft 365. Als u de wijziging onmiddellijk wilt synchroniseren, gaat u naar de Cyber Protect-console en selecteert u de organisatie op de **Microsoft 365**-pagina. Vervolgens klikt u op **Vernieuwen**.
12. Selecteer of u de machtigingen voor delen voor de herstelde items wilt herstellen.
13. Klik op **Herstel starten**.
14. Selecteer een van de opties voor overschrijven:

Optie	Beschrijving
Een bestaand	Als er een bestand met dezelfde naam op de doellocatie is en dit bestand ouder is dan het bronbestand, wordt het bronbestand opgeslagen op de

Optie	Beschrijving
bestand overschrijven als dit ouder is	doellocatie, ter vervanging van de oudere versie.
Bestaande bestanden overschrijven	Alle bestaande bestanden op de doellocatie worden overschreven, ongeacht de datum waarop ze voor het laatst zijn gewijzigd.
Bestaande bestanden niet overschrijven	Als er een bestand met dezelfde naam op de doellocatie is, worden hierin geen wijzigingen aangebracht en wordt het bronbestand niet opgeslagen op de doellocatie.

Opmerking
Wanneer u OneNote-notitieblokken herstelt, worden de bestaande OneNote-notitieblokken overschreven, ongeacht of u **Een bestaand bestand overschrijven als dit ouder is** of **Bestaande bestanden overschrijven** kiest.

15. Klik op **Doorgaan** om uw beslissing te bevestigen.

Microsoft 365 Teams beschermen

Van welke items kan een back-up worden gemaakt?

U kunt een back-up maken van volledige teams. Dit omvat teamnaam, teamledenlijst, teamkanalen met inhoud, teampostvak en -vergaderingen en teamsite.

Een aparte optie in het back-upschema maakt de back-up van OneNote-notitieblokken mogelijk.

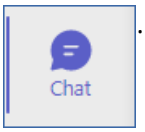
Welke items kunnen worden hersteld?

- Volledig team
- Teamkanalen
- Kanaalbestanden
- Teampostvak
- E-mailmappen in het teampostvak
- E-mailberichten in het teampostvak
- Vergaderingen
- Teamsite

U kunt gesprekken in teamkanalen niet herstellen, maar u kunt ze downloaden als een enkel html-bestand.

Beperkingen

Van de volgende items worden geen back-ups gemaakt:

- De instellingen van het algemene kanaal (beheervoorkeuren). Dit is vanwege een beperking van de Microsoft Teams bèta-API.
- De instellingen van de algemene kanalen (beheervoorkeuren). Dit is vanwege een beperking van de Microsoft Teams bèta-API.
- Vergaderingsnotities.
- Berichten in het chatgedeelte 

. Dit gedeelte bevat privé één-op-één chats en groepschats.
- Stickers en lof.

Back-up en herstel worden ondersteund voor de volgende kanaaltabs:

- Word
- Excel
- PowerPoint
- PDF
- Documentbibliotheek

Teams selecteren

Selecteer teams zoals hieronder beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

Teams selecteren

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de teams waarvan u een back-up wilt maken. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u een back-up wilt maken van alle teams in de organisatie (inclusief teams die in de toekomst worden gemaakt), vouwt u het knooppunt **Teams** uit, selecteert u **Alle teams** en klikt u vervolgens op **Back-up van groep**.
   - Als u een back-up wilt maken van afzonderlijke teams, vouwt u het knooppunt **Teams** uit, selecteert u **Alle teams**, selecteert u de teams waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.

   U kunt teams zoeken op naam. Jokers worden niet ondersteund.
4. In het deelvenster voor het beschermingsschema:

- Controleer of het item **Microsoft Teams** is geselecteerd in **Back-up maken van**.
- [Optioneel] Stel in **Bewaartijd** de opties voor opschonen in.
- [Optioneel] Als u uw back-up wilt versleutelen, schakelt u de schakelaar **Versleuteling** in. Vervolgens stelt u uw wachtwoord in en selecteert u het versleutelingsalgoritme.
- [Optioneel] Schakel de schakelaar **OneNote opnemen** in om een back-up te maken van de OneNote-notitieblokken.

Een volledig team herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de teams die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Teams** uit, selecteer **Alle teams**, selecteer het team dat u wilt herstellen en klik vervolgens op **Herstel**.
   U kunt teams zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.
5. Klik op **Herstellen** > **Volledig team**.
   Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.
   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
6. In **Herstellen naar team** kunt u het doelteam weergeven of een ander team selecteren.
   Standaard is het oorspronkelijke team geselecteerd. Als dit team niet bestaat (bijvoorbeeld als het is verwijderd) of als u een organisatie hebt geselecteerd waarin het oorspronkelijke team niet voorkomt, moet u een doelteam selecteren in de vervolgkeuzelijst.
   U kunt een team alleen herstellen in een bestaand team. Je kunt geen nieuwe teams maken tijdens herstelbewerkingen.
7. Klik op **Herstel starten**.
8. Selecteer een van de opties voor overschrijven:
   - **Bestaande inhoud overschrijven als deze ouder is**
   - **Bestaande inhoud overschrijven**
   - **Bestaande inhoud niet overschrijven**

   Opmerking
   Wanneer u OneNote-notitieblokken herstelt, worden de bestaande OneNote-notitieblokken overschreven, ongeacht of u **Bestaande inhoud overschrijven als deze ouder is** of **Bestaande inhoud overschrijven** kiest.
9. Klik op **Doorgaan** om uw beslissing te bevestigen.

Wanneer u een kanaal verwijdert in de grafische interface van Microsoft Teams, wordt het niet onmiddellijk verwijderd uit het systeem. Dus wanneer u het volledige team herstelt, kan de naam van dit kanaal niet worden gebruikt en wordt er een achtervoegsel aan toegevoegd.

Gesprekken worden hersteld als een enkel html-bestand op het tabblad **Bestanden** van het kanaal. U vindt dit bestand in een map dat een naam heeft met het volgende patroon: `<Teamnaam>_<Kanaalnaam>_back-up van gesprekken_<hersteldatum>T<hersteltijd>Z`.

Opmerking
Nadat u een team of teamkanalen hebt hersteld, gaat u naar Microsoft Teams, selecteert u de kanalen die zijn hersteld en klikt u op het tabblad **Bestanden** van elk kanaal. Anders zullen de daaropvolgende back-ups van deze kanalen niet de inhoud van dit tabblad bevatten. Dit is vanwege een beperking van de Microsoft Teams bèta-API.

Teamkanalen of bestanden in teamkanalen herstellen

Teamkanalen herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de teams die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Teams** uit, selecteer **Alle teams**, selecteer het team waarvan u de kanalen wilt herstellen en klik vervolgens op **Herstel**.
4. Selecteer een herstelpunt.
5. Klik op **Herstellen** > **Kanalen**.
6. Selecteer de kanalen die u wilt herstellen en klik vervolgens op **Herstellen**. Als u een kanaal in het hoofdvenster wilt selecteren, schakelt u het selectievakje voor de naam in.
   De volgende zoekopties zijn beschikbaar:
   - **Gesprekken**: afzender, onderwerp, inhoud, taal, naam van bijlage, datum of datumbereik.
   - Voor **Bestanden**: bestandsnaam of mapnaam, bestandstype, grootte, datum of datumbereik van de laatste wijziging.

     Opmerking
     U kunt de bestanden ook lokaal downloaden in plaats van ze te herstellen.
7. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.
   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
8. In **Herstellen naar team** kunt u het doelteam weergeven, wijzigen of opgeven.
   Standaard is het oorspronkelijke team geselecteerd. Als dit team niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u het doelteam opgeven.

9. In **Herstellen naar kanaal** kunt u het doelkanaal weergeven, wijzigen of opgeven.
10. Klik op **Herstel starten**.
11. Selecteer een van de opties voor overschrijven:
    - **Bestaande inhoud overschrijven als deze ouder is**
    - **Bestaande inhoud overschrijven**
    - **Bestaande inhoud niet overschrijven**

    Opmerking
    Wanneer u OneNote-notitieblokken herstelt, worden de bestaande OneNote-notitieblokken overschreven, ongeacht of u **Bestaande inhoud overschrijven als deze ouder is** of **Bestaande inhoud overschrijven** kiest.
12. Klik op **Doorgaan** om uw beslissing te bevestigen.

Gesprekken worden hersteld als een enkel html-bestand op het tabblad **Bestanden** van het kanaal. U vindt dit bestand in een map dat een naam heeft met het volgende patroon: `<Teamnaam>_<Kanaalnaam>_back-up van gesprekken_<hersteldatum>T<hersteltijd>Z`.

Opmerking
Nadat u een team of teamkanalen hebt hersteld, gaat u naar Microsoft Teams, selecteert u de kanalen die zijn hersteld en klikt u op het tabblad **Bestanden** van elk kanaal. Anders zullen de daaropvolgende back-ups van deze kanalen niet de inhoud van dit tabblad bevatten. Dit is vanwege een beperking van de Microsoft Teams bèta-API.

Bestanden herstellen in een teamkanaal

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de teams die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Teams** uit, selecteer **Alle teams**, selecteer het team waarvan u de kanalen wilt herstellen en klik vervolgens op **Herstel**.
4. Selecteer een herstelpunt.
5. Klik op **Herstellen** > **Kanalen**.
6. Selecteer het gewenste kanaal en open vervolgens de map **Bestanden**.
   Blader naar de vereiste items of gebruik de zoekfunctie om de lijst met de vereiste items op te halen. De volgende zoekopties zijn beschikbaar: bestandsnaam of mapnaam, bestandstype, grootte, datum of datumbereik van de laatste wijziging.
7. [Optioneel] Als u een item wilt downloaden, selecteert u het item, klikt u op **Downloaden** en selecteert u de locatie waar u het item wilt opslaan. Klik vervolgens op **Opslaan**.
8. Selecteer de items die u wilt herstellen en klik vervolgens op **Herstellen**

9. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op Microsoft 365-organisatie om de doelorganisatie te bekijken, te wijzigen of op te geven.
   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
10. In **Herstellen naar team** kunt u het doelteam weergeven, wijzigen of opgeven.
    Standaard is het oorspronkelijke team geselecteerd. Als dit team niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u het doelteam opgeven.
11. In **Herstellen naar kanaal** kunt u het doelkanaal weergeven, wijzigen of opgeven.
12. Selecteer of u de machtigingen voor delen voor de herstelde items wilt herstellen.
13. Klik op **Herstel starten**.
14. Selecteer een van de opties voor overschrijven:
    - **Bestaande inhoud overschrijven als deze ouder is**
    - **Bestaande inhoud overschrijven**
    - **Bestaande inhoud niet overschrijven**

    Opmerking
    Wanneer u OneNote-notitieblokken herstelt, worden de bestaande OneNote-notitieblokken overschreven, ongeacht of u **Bestaande inhoud overschrijven als deze ouder is** of **Bestaande inhoud overschrijven** kiest.
15. Klik op **Doorgaan** om uw beslissing te bevestigen.

Individuele gesprekken kunt u niet herstellen. In het hoofdvenster kunt u alleen bladeren in de map **Gesprekken** of de inhoud ervan downloaden als enkel html-bestand. Als u dit wilt doen, klikt u op het pictogram  voor 'mappen herstellen' selecteert u de gewenste map **Gesprekken** en klikt u vervolgens op **Downloaden**.

U kunt de berichten in de map **Gesprekken** doorzoeken op:

- Afzender
- Inhoud
- Bijlagenaam
- Datum

Een teampostvak herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de teams die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.

3. Vouw het knooppunt **Teams** uit, selecteer **Alle teams**, selecteer het team waarvan u het postvak wilt herstellen en klik vervolgens op **Herstel**.
   U kunt teams zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.
5. Klik op **Herstellen** > **E-mailberichten**.
6. Klik op het pictogram  voor 'mappen herstellen', selecteer de hoofdpostvakmap en klik vervolgens op **Herstellen**.

   Opmerking
   U kunt ook afzonderlijke mappen herstellen vanuit het geselecteerde postvak.

7. Klik op **Herstellen**.
8. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.
   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
9. In **Herstellen naar postvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.
   Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u het doelpostvak opgeven.
10. Klik op **Herstel starten**.
11. Selecteer een van de opties voor overschrijven:
    - **Bestaande items overschrijven**
    - **Bestaande items niet overschrijven**
12. Klik op **Doorgaan** om uw beslissing te bevestigen.

Teampostvakitems herstellen als PST-bestanden

Teampostvakitems herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gegevens die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. U kunt gebruikers en groepen zoeken op naam. Jokers worden niet ondersteund.
4. Vouw het knooppunt **Teams** uit, selecteer **Alle teams**, selecteer een team waarvan het postvak oorspronkelijk de items bevatte die u wilt herstellen, en klik vervolgens op **Herstel**.
5. Klik op **Herstellen** > **E-mailberichten**.
6. Blader naar de vereiste map of gebruik de zoekfunctie om de lijst met vereiste items weer te geven.
   De volgende zoekopties zijn beschikbaar. Jokers worden niet ondersteund.

- E-mailberichten: u kunt zoeken op onderwerp, afzender, ontvanger, naam van bijlage en datum.
- Gebeurtenissen: u kunt zoeken op titel en datum.
- Taken: u kunt zoeken op onderwerp en datum.
- Contacten: u kunt zoeken op naam, e-mailadres en telefoonnummer.

7. Selecteer de items die u wilt herstellen. Als u mappen wilt selecteren, klikt u op het pictogram 'Mappen herstellen': 

   U kunt ook een van de volgende handelingen uitvoeren:
   - Wanneer een item is geselecteerd, klikt u op **Inhoud weergeven** om de inhoud ervan te bekijken, inclusief bijlagen. Klik op de naam van een bijgevoegd bestand om het te downloaden.
   - Wanneer een e-mailbericht of agenda-item is geselecteerd, kunt u klikken op **Versturen als e-mail** om het bericht naar een e-mailadres te verzenden. U kunt de afzender selecteren en een tekst schrijven die u wilt toevoegen aan het doorgestuurde artikel.
   - Wanneer de back-up niet is versleuteld, u de zoekfunctie hebt gebruikt en één item in de zoekresultaten hebt geselecteerd: klik op **Versies weergeven** om de itemversie weer te geven. U kunt elke versie selecteren waarvan een back-up is gemaakt, ongeacht of deze eerder of later is dan het geselecteerde herstelpunt.
8. Klik op **Herstellen als PST-bestanden**.
9. Stel het wachtwoord in om het archief met de PST-bestanden te versleutelen.
   Het wachtwoord moet ten minste één symbool bevatten.
10. Bevestig het wachtwoord en klik op **GEREED**.

De geselecteerde postvakitems worden hersteld als PST-gegevensbestanden en gearchiveerd in zipindeling. De maximale grootte van een PST-bestand is beperkt tot 2 GB, dus als de gegevens die u herstelt, groter zijn dan 2 GB, worden de gegevens opgesplitst in verschillende PST-bestanden. Het ziparchief wordt beschermd met het door u ingestelde wachtwoord.

U ontvangt een e-mail met een link naar een ziparchief met de nieuw gemaakte PST-bestanden.

De beheerder ontvangt een e-mailbericht dat u de herstelprocedure hebt uitgevoerd.

Het archief met PST-bestanden downloaden en het herstel voltooien

1. Voer een van de volgende handelingen uit:
   - Als u het archief wilt downloaden vanuit de e-mail, volgt u de link **Bestanden downloaden**. U hebt dan 24 uur om het archief te downloaden. Als de link verloopt, herhaalt u de herstelprocedure.
   - Het archief downloaden vanuit de Cyber Protect-console:
     a. Ga naar **Back-upopslag** > **PST-bestanden**.
     b. Selecteer het meest recente gemarkeerde archief.
     c. Klik op **Downloaden** in het rechterdeelvenster.

Het archief wordt gedownload naar de standaard downloaddirectory op uw computer.

2. Pak de PST-bestanden uit het archief uit met het wachtwoord dat u hebt ingesteld om het archief te versleutelen.
3. Open of importeer de PST-bestanden in Microsoft Outlook. Raadpleeg de Microsoft-documentatie voor informatie over hoe u dit doet.

E-mailberichten en vergaderingen herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de teams die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Teams** uit, selecteer **Alle teams**, selecteer het team waarvan u de e-mailberichten of vergaderingen wilt herstellen en klik vervolgens op **Herstel**.
   U kunt teams zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.
5. Klik op **Herstellen** > **E-mailberichten**.
6. Blader naar het vereiste item of gebruik de zoekfunctie om de lijst met de vereiste items op te halen.
   De volgende zoekopties zijn beschikbaar:
   - E-mailberichten: u kunt zoeken op onderwerp, afzender, ontvanger en datum.
   - Voor vergaderingen: zoek op naam en datum van de gebeurtenis.
7. Selecteer de items die u wilt herstellen en klik vervolgens op **Herstellen**.

   Opmerking
   U kunt de vergaderingen vinden in de map **Agenda**.

   U kunt ook een van de volgende handelingen uitvoeren:
   - Wanneer een item is geselecteerd, klikt u op **Inhoud weergeven** om de inhoud ervan te bekijken, inclusief bijlagen. Klik op de naam van een bijgevoegd bestand om het te downloaden.
   - Wanneer een e-mailbericht of vergadering is geselecteerd, kunt u klikken op **Versturen als e-mail** om het item naar de opgegeven e-mailadressen te verzenden. U kunt de afzender selecteren en een tekst schrijven die u wilt toevoegen aan het doorgestuurde artikel.
8. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.
   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
9. In **Herstellen naar postvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.
   Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u het doelpostvak opgeven.

10. Klik op **Herstel starten**.
11. Selecteer een van de opties voor overschrijven:
    - **Bestaande items overschrijven**
    - **Bestaande items niet overschrijven**
12. Klik op **Doorgaan** om uw beslissing te bevestigen.

Een teamsite of specifieke items van een site herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de teams die u wilt herstellen vanuit de back-up. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Teams** uit, selecteer **Alle teams**, selecteer het team waarvan u de site wilt herstellen en klik vervolgens op **Herstel**.
   U kunt teams zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.
5. Klik op **Herstellen** > **Teamsite**.
6. Blader naar het vereiste item of gebruik de zoekfunctie om de lijst met de vereiste items op te halen.
7. [Optioneel] Als u een item wilt downloaden, selecteert u het item, klikt u op **Downloaden** en selecteert u de locatie waar u het item wilt opslaan. Klik vervolgens op **Opslaan**.
8. Selecteer de items die u wilt herstellen en klik vervolgens op **Herstellen**.
9. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Microsoft 365-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.
   Standaard zijn de oorspronkelijke organisatie en oorspronkelijke team geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u de doelorganisatie opgeven.
10. In **Herstellen naar team** kunt u het doelteam weergeven, wijzigen of opgeven.
    Standaard is het oorspronkelijke team geselecteerd. Als dit team niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u de doelsite opgeven.
11. Selecteer of u de machtigingen voor delen voor de herstelde items wilt herstellen.
12. Klik op **Herstel starten**.
13. Selecteer een van de opties voor overschrijven:
    - **Bestaande inhoud overschrijven als deze ouder is**
    - **Bestaande inhoud overschrijven**
    - **Bestaande inhoud niet overschrijven**

Opmerking
Wanneer u OneNote-notitieblokken herstelt, worden de bestaande OneNote-notitieblokken overschreven, ongeacht of u **Bestaande inhoud overschrijven als deze ouder is** of **Bestaande inhoud overschrijven** kiest.

14. Klik op **Doorgaan** om uw beslissing te bevestigen.

OneNote-notitieblokken beschermen

OneNote-notitieblokken worden standaard opgenomen in de back-ups van OneDrive-bestanden, Microsoft Teams en SharePoint-sites.

Als u de OneNote-notitieblokken wilt uitsluiten van deze back-ups, zet u de schakelaar **OneNote opnemen** in het betreffende back-upschema uit.

Back-up van OneNote-notitieblokken herstellen

Raadpleeg het betreffende onderwerp voor meer informatie over het herstellen van een back-up van een OneNote-notitieblok:

- Zie "Een volledige OneDrive herstellen" (p. 659) of "OneDrive-bestanden herstellen" (p. 660) voor back-ups van OneDrive.
- Zie "Een volledig team herstellen" (p. 668), "Teamkanalen of bestanden in teamkanalen herstellen" (p. 669) of "Een teamsite of specifieke items van een site herstellen" (p. 675) voor back-ups van Teams.
- Voor back-ups van SharePoint-sites: zie "SharePoint Online-gegevens herstellen" (p. 664).

Ondersteunde -versies

- OneNote (OneNote 2016 en later)
- OneNote voor Windows 10

Beperkingen en bekende problemen

- OneNote-notitieblokken die zijn opgeslagen in OneDrive of SharePoint, worden beperkt tot 2 GB. U kunt geen grotere OneNote-notitieblokken herstellen naar OneDrive- of SharePoint-doelen.
- OneNote-notitieblokken met sectiegroepen worden niet ondersteund.
- In back-ups van OneNote-notitieblokken die secties bevatten met niet-standaardnamen, wordt de eerste sectie met de standaardnaam weergegeven (zoals `Nieuwe sectie` of `Naamloze sectie`). Dit kan van invloed zijn op de sectievolgorde in notitieboeken met meerdere secties.
- Wanneer u OneNote-notitieblokken herstelt, worden de bestaande OneNote-notitieblokken overschreven, ongeacht of u **Bestaande inhoud overschrijven als deze ouder is** of **Bestaande inhoud overschrijven** kiest.
- Wanneer u een heel team, een teamsite of de map `Site-assets` van een teamsite herstelt en u de optie **Bestaande inhoud overschrijven als deze ouder is** of de optie **Bestaande inhoud**

overschrijven hebt geselecteerd, wordt het standaard OneNote-notitieblok van dat team niet overschreven. Het herstel is uitgevoerd met de waarschuwing *Kan de eigenschappen van bestand '/sites/<teamnaam> /SiteAssets/<naam van OneNote-notitieblok>'* niet bijwerken.

Seats voor de Microsoft 365-apps voor samenwerking beschermen

U kunt gebruikmaken van het Advanced Email Security-pakket dat realtime bescherming biedt voor uw Microsoft 365-, Google Workspace- of Open-Xchange-postvakken:

- Antimalware en antispam
- URL-scan in e-mails
- DMARC-analyse
- Antiphishing
- Bescherming tegen imitatie
- Scan van bijlagen
- Content Disarm and Reconstruction
- Vertrouwensgrafiek

U kunt ook seats voor de Microsoft 365-apps voor samenwerking inschakelen, zodat Microsoft 365-toepassingen voor samenwerking in de cloud kunnen worden beschermd tegen inhoud die een beveiligingsbedreiging kan zijn. Het gaat hierbij om toepassingen zoals OneDrive, SharePoint en Teams.

Advanced Email Security kan per workload of per gigabyte worden ingeschakeld en is van invloed op uw licentiemodel.

Toegang krijgen tot Advanced Email Security-onboarding vanuit de Cyber Protect Cloud-console:

1. Klik op **Apparaten** > **Microsoft 365**.
2. Klik op het knooppunt **Gebruikers** en klik vervolgens op de koppeling **Ga naar E-mailbeveiliging** in de rechterbovenhoek.

Meer informatie over Advanced Email Security vindt u in de datasheet Advanced Email Security.

Zie Advanced Email Security met Perception Point voor configuratie-instructies.

Google Workspace-gegevens beveiligen

Opmerking
Deze functie is niet beschikbaar voor tenants in de compliancemodus. Zie "Compliancemodus" (p. 1165) voor meer informatie.

Wat betekent Google Workspace-beveiliging?

- Cloud-to-cloud back-up en herstel van Google Workspace-gebruikersgegevens (Gmail-postvakken, agenda's, contacten, Google Drives) en gedeelde Drives in Google Workspace.
- Granulair herstel van e-mails, bestanden, contacten en andere items.
- Ondersteuning en herstel van meerdere Google Workspace-organisaties.
- Optionele notarisatie van de back-upbestanden via de Ethereum-blockchaindatabase. Wanneer deze optie is ingeschakeld, kunt u bewijzen dat een bestand authentiek en ongewijzigd is sinds de back-up is gemaakt.
- Optioneel zoeken in volledige tekst. Wanneer deze optie is ingeschakeld, kunt u e-mails doorzoeken op inhoud.
- Tot 5000 items (postvakken, Google Drives en gedeelde Drives) per bedrijf kunnen worden beschermd zonder dat de prestaties afnemen.
- Back-upgegevens worden automatisch gecomprimeerd en nemen op de back-uplocatie minder ruimte in beslag dan op de oorspronkelijke locatie. Het compressieniveau voor cloud-to-cloud back-ups kan niet worden veranderd. Het niveau komt overeen met het niveau **Normaal** voor niet-cloud-to-cloud back-ups. Zie "Compressieniveau" (p. 486) voor meer informatie over deze niveaus.

Vereiste gebruikersrechten

In Cyber Protection

In Cyber Protection moet u een bedrijfbeheerder zijn die werkt op klanttenantniveau. Bedrijfbeheerders die op eenheidniveau werken, eenheidbeheerders en gebruikers kunnen geen back-up- of herstelbewerkingen uitvoeren voor Google Workspace-gegevens.

In Google Workspace

Als u uw Google Workspace-organisatie wilt toevoegen aan de Cyber Protection-service, moet u zijn aangemeld als superbeheerder en moet API-toegang zijn ingeschakeld (**Beveiliging** > **API-referentie** > **API-toegang inschakelen** in de Google-beheerconsole).

Het wachtwoord van de superbeheerder wordt nergens opgeslagen en wordt niet gebruikt om back-ups en herstel uit te voeren. Het wijzigen van dit wachtwoord in Google Workspace heeft geen invloed op de werking van de Cyber Protection-service.

Als de superbeheerder die de Google Workspace-organisatie heeft toegevoegd, wordt verwijderd uit de Google Workspace of een rol krijgt met minder rechten, mislukken de back-ups met een foutmelding zoals 'Toegang geweigerd'. Herhaal in dit geval de procedure die is beschreven in "Een Google Workspace-organisatie toevoegen" (p. 680) en geef geldige referenties voor de superbeheerder op. Als u dit geval wilt voorkomen, raden wij u aan een speciale gebruiker met superbeheerdersrechten te maken voor back-ups en herstel.

Over het back-upschema

Aangezien de cloudagent voor meerdere klanten wordt gebruikt, wordt de starttijd voor elk beschermingsschema autonoom bepaald om een gelijkmatige belasting gedurende de dag en gelijke servicekwaliteit voor alle klanten te waarborgen.

Elk beschermingsschema wordt dagelijks op hetzelfde tijdstip uitgevoerd.

De standaardoptie is **Eén keer per dag**. Met het Advanced Backup-pakket kunt u tot zes back-ups per dag plannen. De back-ups worden gestart met een interval dat afhangt van de huidige belasting van de cloudagent, die wordt gebruikt voor meerdere klanten in een datacenter. Zo wordt de belasting gelijkmatig verdeeld gedurende de dag en krijgen alle klanten eenzelfde serviceniveau.

Beperkingen

- Alleen gebruikers met een toegewezen Google Workspace-licentie en een postvak of Google Drive worden weergegeven in de console.
- De back-ups van documenten in de native Google-indelingen worden gemaakt als generieke Office-documenten en worden in de Cyber Protect-console weergegeven met een andere extensie, bijvoorbeeld .docx of .pptx. De documenten worden tijdens het herstel terug geconverteerd naar hun oorspronkelijke indeling.
- Niet meer dan 10 handmatige back-ups in één uur.
- Niet meer dan 10 gelijktijdige herstelbewerkingen (bij dit aantal is zowel Microsoft 365- als Google Workspace-herstel inbegrepen).
- U kunt niet gelijktijdig items van verschillende herstelpunten herstellen, maar u kunt dergelijke items wel selecteren in de zoekresultaten.
- De back-ups van verwijderde Google Workspace-gebruikersaccounts worden niet automatisch verwijderd uit de cloudopslag. Deze back-ups worden gefactureerd voor de opslagruimte die ze gebruiken.
- U kunt niet meer dan één afzonderlijk back-upschema toepassen op dezelfde workload.
- Wanneer een afzonderlijk back-upschema en een groepsback-upschema op dezelfde workload worden toegepast, hebben de instellingen in het afzonderlijke schema voorrang.

Aanmelden

Acties met cloud-to-cloud resources kunnen de privacy van de gebruiker schenden, bijvoorbeeld door het bekijken van de inhoud van e-mails in de back-up, het downloaden van bijlagen of bestanden, het herstellen van e-mails naar andere postvakken dan het oorspronkelijke postvak of het versturen van de resources als e-mail. Deze acties worden vastgelegd in **Controle** > **Auditlogboek** in de beheerportal.

Een Google Workspace-organisatie toevoegen

Als u een Google Workspace-organisatie wilt toevoegen aan de Cyber Protection-service, hebt u een speciaal persoonlijk Google Cloud-project nodig. Zie "Een persoonlijk Google Cloud project maken" (p. 681) voor meer informatie over hoe u een dergelijk project kunt maken en configureren.

Een Google Workspace-organisatie toevoegen via een speciaal persoonlijk Google Cloud-project

1. Meld u als bedrijfbeheerder aan bij de Cyber Protect-console.
2. Klik op **Apparaten** > **Toevoegen** > **Google Workspace**.
3. Voer het e-mailadres van een hoofdbeheerder van uw Google Workspace-account in.
   Voor deze procedure is het niet relevant of verificatie in twee stappen is ingeschakeld voor het e-mailaccount van de superbeheerder.
4. Zoek naar het JSON-bestand dat de persoonlijke sleutel bevat van het serviceaccount dat u hebt gemaakt in uw Google Cloud-project.
   U kunt de inhoud van het bestand ook plakken als tekst.
5. Klik op **Bevestigen**.

Uw Google Workspace-organisatie wordt dan weergegeven op het tabblad **Apparaten** in de Cyber Protect-console.

Nuttige tips

- Wanneer u een Google Workspace-organisatie hebt toegevoegd, wordt er een back-up gemaakt van de gebruikersgegevens en gedeelde Drives in zowel het primaire domein als alle secundaire domeinen (indien van toepassing). De resources waarvan een back-up is gemaakt, worden in één lijst weergegeven en worden niet gegroepeerd op domein.
- De cloudagent wordt om de 24 uur gesynchroniseerd met Google Workspace, te beginnen vanaf het moment dat de organisatie wordt toegevoegd aan de Cyber Protection-service. Als u een gebruiker of gedeelde Drive toevoegt of verwijdert, ziet u deze wijziging niet onmiddellijk in de Cyber Protect-console. Als u de wijziging onmiddellijk wilt synchroniseren, selecteert u de organisatie op de pagina **Google Workspace** en klikt u op **Vernieuwen**.
  Voor meer informatie over het synchroniseren van de resources van een Google Workspace-organisatie en de Cyber Protect-console raadpleegt u "Google Workspace-resources detecteren" (p. 684).
- Als u een beschermingsschema hebt toegepast op de groep **Alle gebruikers** of **Alle gedeelde Drives**, worden de nieuw toegevoegde items pas na de synchronisatie in de back-up opgenomen.
- Volgens het beleid van Google blijft een gebruiker of gedeelde Drive die is verwijderd uit de grafische gebruikersinterface van Google Workspace, nog enkele dagen beschikbaar via een API. Tijdens deze periode is het verwijderde item inactief (grijs weergegeven) in de Cyber Protect-console en worden hiervan geen back-ups gemaakt. Wanneer het verwijderde item niet meer beschikbaar is via de API, wordt het niet meer weergegeven in de Cyber Protect-console. Eventuele back-ups vindt u in **Back-upopslag** > **Back-ups van cloudtoepassingen**.

Een persoonlijk Google Cloud project maken

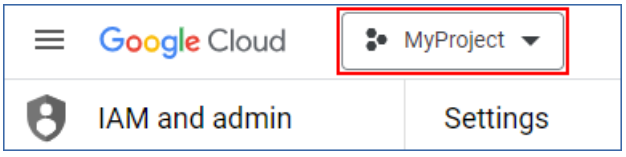
Als u uw Google Workspace-organisatie wilt toevoegen aan de Cyber Protection-service door gebruik te maken van een speciaal Google Cloud-project, moet u het volgende doen:

1. Maak een nieuw Google Cloud-project.
2. Schakel de vereiste API's voor dit project in.
3. Configureer de referenties voor dit project:
   a. Configureer het OAuth-toestemmingsscherm.
   b. Maak en configureer het serviceaccount voor de Cyber Protection-service.
4. Verleen het nieuwe project toegang tot uw Google Workspace-account.

Opmerking
Dit onderwerp bevat een beschrijving van de gebruikersinterface van derden, maar deze kan zonder voorafgaande kennisgeving worden gewijzigd.

Een nieuw Google Cloud-project maken

1. Meld u aan bij het Google Cloud Platform (console.cloud.google.com) als superbeheerder.
2. Klik in de Google Cloud Platform-console op de projectkiezer in de linkerbovenhoek.



3. Ga naar het scherm dat wordt geopend, selecteer een organisatie en klik vervolgens op **Nieuw project**.

4. Geef een naam op voor uw nieuwe project.
5. Klik op **Maken**.

Als resultaat wordt uw nieuwe Google Cloud-project gemaakt.

De vereiste API's voor dit project inschakelen

1. Selecteer uw nieuwe project in de Google Cloud Platform-console.
2. Selecteer in het navigatiemenu **API's en services** > **Ingeschakelde API's en services**.
3. Schakel één voor één alle API's uit die standaard zijn ingeschakeld in dit project:
   a. Schuif omlaag op de pagina **Ingeschakelde API's en services** en klik op de naam van een ingeschakelde API.
   De pagina **Details van API/service** van de geselecteerde API wordt geopend.
   b. Klik op **API uitschakelen** en vervolgens op **Uitschakelen** om uw keuze te bevestigen.

c. [Indien gevraagd] Bevestig uw keuze door te klikken op **Bevestigen**.

d. Ga terug naar **API's en services** > **Ingeschakelde API's en services** en schakel de volgende API uit.

4. Selecteer in het navigatiemenu de optie **API's en services** > **Bibliotheek**.
5. Schakel in de API-bibliotheek de volgende API's één voor één in:
   - Admin SDK API
   - Gmail API
   - Google Calendar API
   - Google Drive API
   - Google People API

   Gebruik de zoekbalk om de nodige API's te vinden. Als u een API wilt inschakelen, klikt u op de naam ervan en vervolgens klikt u op **Inschakelen**. Zoek de volgende API door terug te gaan naar de API-bibliotheek en selecteer **API's en services** > **Bibliotheek** in het navigatiemenu.

Het OAuth-toestemmingsscherm configureren

1. Selecteer in het navigatiemenu in het Google Cloud Platform de optie **API's en services** > **OAuth-toestemmingsscherm**.
2. In het venster dat wordt geopend, selecteert u **Intern** als gebruikerstype en klikt u vervolgens op **Maken**.
3. Geef in het veld **App-naam** een naam op voor uw toepassing.
4. Voer in het veld **E-mailadres van gebruiker** het e-mailadres van de superbeheerder in.
5. Voer in het veld **Contactgegevens van ontwikkelaar** het e-mailadres van de superbeheerder in.
6. Laat alle andere velden leeg, en klik vervolgens op **Opslaan en doorgaan**.
7. Klik op de pagina **Scopes** op **Opslaan en doorgaan** zonder iets te veranderen.
8. Controleer uw instellingen op de pagina **Overzicht** en klik vervolgens op **Terug naar dashboard**.

Het serviceaccount voor de Cyber Protection-service maken en configureren

1. Selecteer in het navigatiemenu van het Google Cloud Platform de optie **IAM en beheerder** > **Serviceaccounts**.
2. Klik op **Serviceaccount maken**.
3. Geef een naam op voor het serviceaccount.
4. [Optioneel] Geef een beschrijving op voor het serviceaccount.
5. Klik op **Maken en doorgaan**.
6. Wijzig niets in de stappen **Dit serviceaccount toegang verlenen tot het project** en **Gebruikers toegang verlenen tot dit serviceaccount**.
7. Klik op **Gereed**.

De pagina **Serviceaccounts** wordt geopend.

8. Selecteer het nieuwe serviceaccount op de pagina **Serviceaccounts** en klik vervolgens onder **Acties** op **Sleutels beheren**.
9. Klik onder **Sleutels** op **Sleutel toevoegen** > **Nieuwe sleutel maken** en selecteer vervolgens het sleuteltype **JSON**.
10. Klik op **Maken**.

    Er wordt dan automatisch een JSON-bestand met de persoonlijke sleutel van het serviceaccount gedownload naar uw machine. Bewaar dit bestand veilig want u hebt het nodig om uw Google Workspace-organisatie toe te voegen aan de Cyber Protection-service.

Het nieuwe project toegang verlenen tot uw Google Workspace-account

1. Selecteer in het navigatiemenu van het Google Cloud Platform de optie **IAM en beheerder** > **Serviceaccounts**.
2. Zoek in de lijst naar het serviceaccount dat u hebt gemaakt en kopieer de client-id die wordt weergegeven in de kolom **OAuth 2.0-client-id**.
3. Meld u aan bij de Google-beheerconsole (admin.google.com) als superbeheerder.
4. Selecteer in het navigatiemenu de optie **Beveiliging** > **Toegang en gegevensbeheer** > **API-besturingselementen**.
5. Schuif omlaag op de pagina **API-besturingselementen** en klik vervolgens onder **Domeinbrede machtiging** op **Domeinbrede machtiging beheren**.
   De pagina **Domeinbrede machtiging** wordt geopend.
6. Op de pagina **Domeinbrede machtiging** klikt u op **Nieuwe toevoegen**.
   Het venster **Een nieuwe client-id toevoegen** wordt geopend.
7. In het veld **Client-ID** voert u de client-id van uw serviceaccountclient in.
8. Kopieer en plak in het veld **OAuth-scopes** de volgende lijst met door komma's gescheiden scopes:

   ```
   https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googlea
   pis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,
   https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleap
   is.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
   ```

   Indien gewenst kunt u ook één scope per regel toevoegen:
   - https://mail.google.com
   - https://www.googleapis.com/auth/contacts
   - https://www.googleapis.com/auth/calendar
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.domain.readonly
   - https://www.googleapis.com/auth/drive
   - https://www.googleapis.com/auth/gmail.modify
9. Klik op **Autoriseren**.

Uw nieuwe Google Cloud-project kan dan toegang krijgen tot de gegevens in uw Google Workspace-account. Als u een back-up van de gegevens wilt maken, moet u dit project aan de Cyber Protection-service koppelen. Zie "Een Google Workspace-organisatie toevoegen via een speciaal persoonlijk Google Cloud-project" (p. 680) voor meer informatie over hoe u dit kunt doen.

Als u niet meer wilt dat uw Google Cloud-project toegang heeft tot uw Google Workspace-account, respectievelijk tot de Cyber Protection-service, verwijdert u de API-client die door uw project wordt gebruikt.

De toegang tot uw Google Workspace-account intrekken

1. Meld u in de Google Admin-console (admin.google.com) aan als superbeheerder.
2. Selecteer in het navigatiemenu de optie **Beveiliging** > **Toegang en gegevensbeheer** > **API-besturingselementen**.
3. Schuif omlaag op de pagina **API-besturingselementen** en klik vervolgens onder **Domeinbrede machtiging** op **Domeinbrede machtiging beheren**.
   De pagina **Domeinbrede machtiging** wordt geopend.
4. Op de pagina **Domeinbrede machtiging** selecteert u de API-client die door uw project wordt gebruikt en klikt u vervolgens op **Verwijderen**.
   Uw Google Cloud-project en de Cyber Protection-service hebben dan geen toegang meer tot uw Google Workspace-account en kunnen geen back-ups maken van de gegevens in uw account.

Google Workspace-resources detecteren

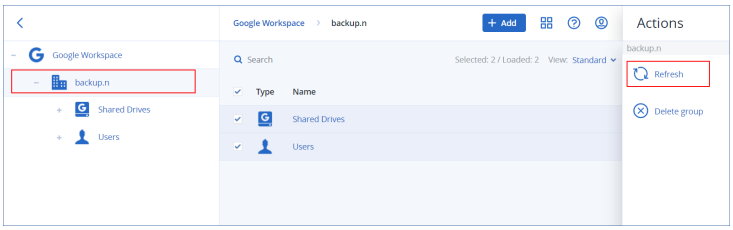
Wanneer u een Google Workspace-organisatie toevoegt aan de Cyber Protection-service, worden de resources in deze organisatie, zoals postvakken en Google Drives, gesynchroniseerd met de Cyber Protect-console. Deze bewerking wordt detectie genoemd en wordt vastgelegd in **Controle** > **Activiteiten**.

Wanneer de detectie is voltooid, kunt u de resources van de Google Workspace-organisatie bekijken op het tabblad **Apparaten** > **Google Workspace** in de Cyber Protect-console en kunt u hierop back-upschema's toepassen.

Eén keer per dag wordt een automatische detectiebewerking uitgevoerd om de lijst met resources in de Cyber Protect-console up-to-date te houden. U kunt deze lijst ook synchroniseren op aanvraag door een detectiebewerking handmatig opnieuw uit te voeren.

Handmatig een detectiebewerking opnieuw uitvoeren:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Google Workspace**.
2. Selecteer uw Google Workspace-organisatie en klik vervolgens in het deelvenster **Acties** op **Vernieuwen**.



Opmerking

U kunt maximaal 10 keer per uur een handmatige detectiebewerking uitvoeren. Wanneer dit aantal is bereikt, wordt het aantal toegestane uitvoeringen teruggezet op één per uur, en daarna komt er elk uur een extra uitvoering bij tot het totaal van 10 uitvoeringen per uur weer is bereikt.

De frequentie van Google Workspace-back-ups instellen

Google Workspace-back-ups worden standaard eenmaal per dag uitgevoerd en er zijn geen extra planningsopties beschikbaar.

Als het Advanced Backup-pakket is ingeschakeld in uw tenant, kunt u frequentere back-ups configureren. U kunt het aantal back-ups per dag selecteren, maar de starttijd van de back-up kunt u niet configureren. De back-ups worden automatisch gestart met een interval dat afhangt van de huidige belasting van de cloudagent, die wordt gebruikt voor meerdere klanten in een datacenter. Zo wordt de belasting gelijkmatig verdeeld gedurende de dag en krijgen alle klanten eenzelfde serviceniveau.

De volgende opties zijn beschikbaar.

Planningsopties	Interval (bij benadering) tussen elke back-up
Eén keer per dag	24 uur
Twee keer per dag (standaard)	12 uur
Drie keer per dag	8 uur
Zes keer per dag	4 uur

Opmerking

Afhankelijk van de belasting van de cloudagent en een mogelijke beperking door Google Workspace, kan het zijn dat een back-up later wordt gestart dan gepland of langer duurt. Als een back-up langer duurt dan het gemiddelde interval tussen twee back-ups, wordt de volgende back-up opnieuw gepland, waardoor er minder back-ups per dag worden uitgevoerd dan wat was geselecteerd. Er kunnen bijvoorbeeld slechts twee back-ups per dag worden voltooid, ook al hebt u er zes per dag geselecteerd.

Gmail-gegevens beveiligen

Van welke items kan een back-up worden gemaakt?

U kunt een back-up maken van de postvakken van Gmail-gebruikers. Een back-up van een postvak bevat ook de agenda- en contactgegevens. U kunt er ook voor kiezen een back-up te maken van de gedeelde agenda's.

De volgende items worden *overgeslagen* tijdens een back-up:

- De agenda's met **verjaardagen**, **herinneringen** en **taken**
- Mappen gekoppeld aan agendagebeurtenissen
- De map **Directory** in Contacten

De volgende agenda-items worden *overgeslagen* vanwege beperkingen van de Google Agenda-API:

- Afspraaktijden
- Het vergaderingveld van een gebeurtenis
- De agenda-instelling **Meldingen voor gebeurtenissen die de hele dag duren**
- De agenda-instelling **Uitnodigingen automatisch accepteren** (in agenda's voor ruimtes of gedeelde ruimtes)

De volgende contactitems worden *overgeslagen* vanwege beperkingen van de Google Personen-API:

- De map **Overige contacten**
- De externe profielen van een contact (**Directory-profiel**, **Google-profiel**)
- Het contactveld **Opslaan als**

Welke items kunnen worden hersteld?

De volgende items kunnen worden hersteld vanuit een back-up van een postvak:

- Postvakken
- E-mailmappen ('labels' in Google-terminologie. **Labels** worden in de back-upsoftware weergegeven als mappen, voor consistentie met andere gegevensweergaven.)
- E-mailberichten
- Agendagebeurtenissen
- Contacten

U kunt de zoekfunctie gebruiken om items te vinden in een back-up.

Wanneer u postvakken en postvakitems herstelt, kunt u selecteren of u de items op de doellocatie wilt overschrijven.

Beperkingen

- Contactfoto's kunnen niet worden hersteld
- Het agenda-item **Niet aanwezig** wordt hersteld als een gewone agendagebeurtenis vanwege beperkingen van de Google Agenda-API

Gmail-postvakken selecteren

Selecteer de postvakken zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

Gmail-postvakken selecteren

1. Klik op **Google Workspace**.
2. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gebruikersgegevens waarvan u een back-up wilt maken. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u een back-up wilt maken van de postvakken van alle gebruikers (inclusief postvakken die in de toekomst worden gemaakt), vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers** en klikt u vervolgens op **Back-up van groep**.
   - Als u een back-up wilt maken van de postvakken van afzonderlijke gebruikers, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u de gebruikers met de postvakken waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.
4. In het deelvenster voor het beschermingsschema:
   - Controleer of het item **Gmail** is geselecteerd in **Back-up maken van**.
   - Als u een back-up wilt maken van de agenda's die met de geselecteerde gebruikers worden gedeeld, schakelt u de optie **Gedeelde agenda's opnemen** in.
   - Kies of u Zoekopdracht in volledige tekst nodig hebt voor de e-mailberichten waarvan u een back-up maakt. Voor toegang tot deze optie klikt u op het tandwielpictogram en vervolgens op **Back-upopties** > **Zoekopdracht in volledige tekst**.

Postvakken en postvakitems herstellen

Postvakken herstellen

1. Klik op **Google Workspace**.
2. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie waarvan u de back-upgegevens wilt herstellen. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Gebruikers** uit, selecteer **Alle gebruikers**, selecteer de gebruiker met het postvak dat u wilt herstellen en klik vervolgens op **Herstel**.

Als de gebruiker is verwijderd, selecteert u de gebruiker in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u op **Back-ups weergeven**.

U kunt gebruikers en groepen zoeken op naam. Jokers worden niet ondersteund.

4. Selecteer een herstelpunt.

   Opmerking
   Als u alleen de herstelpunten wilt zien die bepaalde postvakken bevatten, selecteert u **Gmail** in **Filteren op inhoud**.

5. Klik op **Herstellen** > **Volledig postvak**.
6. Als meerdere Google Workspace-organisaties worden toegevoegd aan de Cyber Protection-service, klikt u op **Google Workspace-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u een nieuwe doelorganisatie opgeven door deze te kiezen uit de beschikbare geregistreerde organisaties.
7. In **Herstellen naar postvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.

   Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u het doelpostvak opgeven.

   U kunt tijdens het herstel geen nieuw doelpostvak maken. Als u een postvak wilt herstellen naar een nieuw postvak, moet u eerst het doelpostvak maken in de gewenste Google Workspace-organisatie en vervolgens de wijziging laten synchroniseren door de cloudagent. De cloudagent wordt om de 24 uur automatisch gesynchroniseerd met Google Workspace. Als u de wijziging onmiddellijk wilt synchroniseren, gaat u naar de Cyber Protect-console, selecteert u de organisatie op de pagina **Google Workspace** en klikt u op **Vernieuwen**.
8. Klik op **Herstel starten**.
9. Selecteer een van de opties voor overschrijven:
   - **Bestaande items overschrijven**
   - **Bestaande items niet overschrijven**
10. Klik op **Doorgaan** om uw beslissing te bevestigen.

Postvakitems herstellen

1. Klik op **Google Workspace**.
2. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie waarvan u de back-upgegevens wilt herstellen. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Gebruikers** uit, selecteer **Alle gebruikers**, selecteer de gebruiker van het postvak met de oorspronkelijke items die u wilt herstellen, en klik vervolgens op **Herstel**.

   Als de gebruiker is verwijderd, selecteert u de gebruiker in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u op **Back-ups weergeven**.

U kunt gebruikers en groepen zoeken op naam. Jokers worden niet ondersteund.

4. Selecteer een herstelpunt.

   Opmerking
   Als u alleen de herstelpunten wilt zien die bepaalde postvakken bevatten, selecteert u **Gmail** in **Filteren op inhoud**.

5. Klik op **Herstellen** > **E-mailberichten**.
6. Blader naar de vereiste map. Als de back-up niet is versleuteld, kunt u de zoekfunctie gebruiken om de lijst met vereiste items op te halen.

   De volgende zoekopties zijn beschikbaar. Jokers worden niet ondersteund.

   - E-mailberichten: u kunt zoeken op onderwerp, afzender, ontvanger, datum, naam van bijlage en berichtinhoud.

     Wanneer u op datum zoekt, kunt u een begindatum of een einddatum (beide inclusief) selecteren, of beide datums als u binnen een tijdbereik wilt zoeken.

     Als u zoekt op naam van een bijlage of in de berichtinhoud, krijgt u alleen resultaten als de optie **Zoeken in volledige tekst** was ingeschakeld tijdens de back-up. Als aanvullende parameter kunt u de taal opgeven van het berichtfragment dat wordt doorzocht.
   - Gebeurtenissen: u kunt zoeken op titel en datum.
   - Contacten: u kunt zoeken op naam, e-mailadres en telefoonnummer.
7. Selecteer de items die u wilt herstellen. Als u mappen wilt selecteren, klikt u op het pictogram 'Mappen herstellen': 

   U kunt ook een van de volgende handelingen uitvoeren:

   - Wanneer een item is geselecteerd, klikt u op **Inhoud weergeven** om de inhoud ervan te bekijken, inclusief bijlagen. Klik op de naam van een bijgevoegd bestand om het te downloaden.
   - Alleen als de back-up niet is versleuteld, u de zoekfunctie hebt gebruikt en één item in de zoekresultaten hebt geselecteerd: klik op **Versies weergeven** om de itemversie te selecteren die u wilt herstellen. U kunt elke versie selecteren waarvan een back-up is gemaakt, ongeacht of deze eerder of later is dan het geselecteerde herstelpunt.
8. Klik op **Herstellen**.
9. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Google Workspace-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u een nieuwe doelorganisatie opgeven door deze te kiezen uit de beschikbare geregistreerde organisaties.
10. In **Herstellen naar postvak** kunt u het doelpostvak weergeven, wijzigen of opgeven.

    Standaard is het oorspronkelijke postvak geselecteerd. Als dit postvak niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u het doelpostvak opgeven.

11. Open **Pad** en bekijk of wijzig de doelmap in het doelpostvak. Standaard is de oorspronkelijke map geselecteerd.
12. Klik op **Herstel starten**.
13. Selecteer een van de opties voor overschrijven:
    - **Bestaande items overschrijven**
    - **Bestaande items niet overschrijven**
14. Klik op **Doorgaan** om uw beslissing te bevestigen.

Google Drive-bestanden beveiligen

Van welke items kan een back-up worden gemaakt?

U kunt een back-up maken van een volledige Google Drive of van afzonderlijke bestanden en mappen. Bij het maken van een back-up van bestanden, wordt ook een back-up gemaakt van de machtigingen voor delen van die bestanden.

Belangrijk
Van de volgende items worden geen back-ups gemaakt:

- De map **Gedeeld met mij**
- De map **Computers** (gemaakt door de back-up en synchronisatieclient)

Beperkingen

Specifieke Google-bestandsindelingen: alleen Google Documenten, Google Spreadsheets en Google Presentaties worden volledig ondersteund voor het maken van back-ups en het uitvoeren van herstelbewerkingen. Andere specifieke Google-indelingen worden mogelijk niet volledig of helemaal niet ondersteund. Bestanden van Google Tekeningen worden bijvoorbeeld hersteld als `.svg`-bestanden, bestanden van Google Sites worden hersteld als `.txt`-bestanden, bestanden van Google Jamboard worden hersteld als `.pdf`-bestanden en bestanden van Google My Maps worden tijdens een back-up overgeslagen.

Opmerking
Bestandsindelingen die niet specifiek van Google zijn, zoals `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png` en `.zip`, worden volledig ondersteund voor back-up en herstel.

Welke items kunnen worden hersteld?

U kunt een volledige Google Drive herstellen, of een bestand of map herstellen waarvan een back-up is gemaakt.

U kunt kiezen of u de machtigingen voor delen wilt herstellen of dat de machtigingen voor de bestanden worden overgenomen van de map waarin de bestanden worden hersteld.

Beperkingen

- Opmerkingen in bestanden worden niet hersteld.
- Links voor het delen van bestanden en mappen worden niet hersteld.
- De alleen-lezen **Eigenaarinstellingen** voor gedeelde bestanden (**Toegangswijziging en toevoeging van nieuwe personen door bewerkers voorkomen** en **Opties voor downloaden, afdrukken en kopiëren door commentatoren en lezers uitschakelen**) kunnen niet worden gewijzigd tijdens een herstelbewerking.
- Eigendom van een gedeelde map kan niet worden gewijzigd tijdens een herstelbewerking als de optie **Toegangswijziging en toevoeging van nieuwe personen door bewerkers voorkomen** is ingeschakeld voor deze map. Met deze instelling voorkomt u dat de Google Drive-API een lijst van de mapmachtigingen kan weergeven. Eigendom van de bestanden in de map wordt correct hersteld.

Google Drive-bestanden selecteren

Selecteer de bestanden zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

Google Drive-bestanden selecteren

1. Klik op **Google Workspace**.
2. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gebruikersgegevens waarvan u een back-up wilt maken. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u een back-up wilt maken van de bestanden van alle gebruikers (inclusief gebruikers die in de toekomst worden gemaakt), vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers** en klikt u vervolgens op **Back-up van groep**.
   - Als u een back-up wilt maken van de bestanden van afzonderlijke gebruikers, vouwt u het knooppunt **Gebruikers** uit, selecteert u **Alle gebruikers**, selecteert u de gebruikers met de bestanden waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.
4. In het deelvenster voor het beschermingsschema:
   - Controleer of het item **Google Drive** is geselecteerd in **Back-up maken van**.
   - Voer in **Items waarvan een back-up moet worden gemaakt** een van de volgende handelingen uit:
     - Behoud de standaardinstelling **[All]** (alle bestanden).
     - Voeg de namen of paden toe van de bestanden en mappen waarvan u een back-up wilt maken.

       U kunt jokertekens (*, ** en ?) gebruiken. Voor meer informatie over het opgeven van paden en het gebruik van jokers gaat u naar 'Bestandsfilters'.

- Blader door de bestanden en mappen om op te geven van welke bestanden en mappen u een back-up wilt maken.

  De link **Bladeren** is alleen beschikbaar wanneer u een beschermingsschema voor één gebruiker maakt.

- [Optioneel] Klik in **Items waarvan een back-up moet worden gemaakt** op **Uitsluitingen weergeven** om op te geven welke bestanden en mappen u wilt overslaan tijdens het maken van de back-up.

  Met bestandsuitsluitingen wordt de bestandsselectie overschreven, dat wil zeggen als u in beide velden hetzelfde bestand opgeeft, wordt dit bestand overgeslagen tijdens een back-up.
- Als u notarisatie wilt inschakelen voor alle bestanden die zijn geselecteerd voor het maken van een back-up, schakelt u de optie **Notarisatie** in. Ga voor meer informatie over notarisatie naar 'Notarisatie'.

Google Drive en Google Drive-bestanden herstellen

Een volledige Google Drive herstellen

1. Klik op **Google Workspace**.
2. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie waarvan u de back-upgegevens wilt herstellen. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Gebruikers** uit, selecteer **Alle gebruikers**, selecteer de gebruiker met de Google Drive die u wilt herstellen en klik vervolgens op **Herstel**.

   Als de gebruiker is verwijderd, selecteert u de gebruiker in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u op **Back-ups weergeven**.

   U kunt gebruikers zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.

   Opmerking
   Als u alleen de herstelpunten wilt zien die Google Drive-bestanden bevatten, selecteert u **Google Drive** in **Filteren op inhoud**.

5. Klik op **Herstellen** > **Volledig station**.
6. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Google Workspace-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u een nieuwe doelorganisatie opgeven door deze te kiezen uit de beschikbare geregistreerde organisaties.
7. In **Herstellen naar station** kunt u de doelgebruiker of de doel-Drive in de gedeelde Drives bekijken, wijzigen of opgeven.

Standaard is de oorspronkelijke gebruiker geselecteerd. Als deze gebruiker niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u de doelgebruiker of de doel-Drive in de gedeelde Drives opgeven.

Als de back-up gedeelde bestanden bevat, worden de bestanden hersteld naar de hoofdmap van het doelstation.

8. Selecteer of u de machtigingen voor delen voor de bestanden wilt herstellen.
9. Klik op **Herstel starten**.
10. Selecteer een van de opties voor overschrijven:

Optie	Beschrijving
Een bestaand bestand overschrijven als dit ouder is	Als er een bestand met dezelfde naam op de doellocatie is en dit bestand ouder is dan het bronbestand, wordt het bronbestand opgeslagen op de doellocatie, ter vervanging van de oudere versie.
Bestaande bestanden overschrijven	Alle bestaande bestanden op de doellocatie worden overschreven, ongeacht de datum waarop ze voor het laatst zijn gewijzigd.
Bestaande bestanden niet overschrijven	Als er een bestand met dezelfde naam op de doellocatie is, worden hierin geen wijzigingen aangebracht en wordt het bronbestand niet opgeslagen op de doellocatie.

11. Klik op **Doorgaan** om uw beslissing te bevestigen.

Google Drive-bestanden herstellen

1. Klik op **Google Workspace**.
2. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie waarvan u de back-upgegevens wilt herstellen. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Gebruikers** uit, selecteer **Alle gebruikers**, selecteer de gebruiker met de Google Drive-bestanden die u wilt herstellen en klik vervolgens op **Herstel**.

   Als de gebruiker is verwijderd, selecteert u de gebruiker in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u op **Back-ups weergeven**.

   U kunt gebruikers zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.

   Opmerking
   Als u alleen de herstelpunten wilt zien die Google Drive-bestanden bevatten, selecteert u **Google Drive** in **Filteren op inhoud**.

5. Klik op **Herstellen** > **Bestanden/mappen**.

6. Blader naar de vereiste map of gebruik de zoekfunctie om de lijst met vereiste bestanden en mappen weer te geven.
7. Selecteer de bestanden die u wilt herstellen.

   Als de back-up niet is versleuteld en u één bestand hebt geselecteerd, kunt u klikken op **Versies weergeven** om de bestandsversie te selecteren die u wilt herstellen. U kunt elke versie selecteren waarvan een back-up is gemaakt, ongeacht of deze eerder of later is dan het geselecteerde herstelpunt.
8. Als u een bestand wilt downloaden, selecteert u het bestand, klikt u op **Downloaden**, selecteert u de locatie waar u het bestand wilt opslaan en klikt u op **Opslaan**. Anders kunt u deze stap overslaan.
9. Klik op **Herstellen**.
10. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Google Workspace-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

    Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u een nieuwe doelorganisatie opgeven door deze te kiezen uit de beschikbare geregistreerde organisaties.
11. In **Herstellen naar station** kunt u de doelgebruiker of de doel-Drive in de gedeelde Drives bekijken, wijzigen of opgeven.

    Standaard is de oorspronkelijke gebruiker geselecteerd. Als deze gebruiker niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u de doelgebruiker of de doel-Drive in de gedeelde Drives opgeven.
12. Open **Pad** en bekijk of wijzig de doelmap in de Google Drive van de doelgebruiker of in de doel-Drive in de gedeelde Drives. Standaard is de oorspronkelijke locatie geselecteerd.
13. Selecteer of u de machtigingen voor delen voor de bestanden wilt herstellen.
14. Klik op **Herstel starten**.
15. Selecteer een van de opties voor het overschrijven van bestanden:

Optie	Beschrijving
Een bestaand bestand overschrijven als dit ouder is	Als er een bestand met dezelfde naam op de doellocatie is en dit bestand ouder is dan het bronbestand, wordt het bronbestand opgeslagen op de doellocatie, ter vervanging van de oudere versie.
Bestaande bestanden overschrijven	Alle bestaande bestanden op de doellocatie worden overschreven, ongeacht de datum waarop ze voor het laatst zijn gewijzigd.
Bestaande bestanden niet overschrijven	Als er een bestand met dezelfde naam op de doellocatie is, worden hierin geen wijzigingen aangebracht en wordt het bronbestand niet opgeslagen op de doellocatie.

16. Klik op **Doorgaan** om uw beslissing te bevestigen.

Shared drive-bestanden beveiligen

Van welke items kan een back-up worden gemaakt?

U kunt een back-up maken van een volledige Shared drive, of van afzonderlijke bestanden en mappen. Bij het maken van een back-up van bestanden, wordt ook een back-up gemaakt van de machtigingen voor delen van die bestanden.

Belangrijk
Er wordt geen back-up gemaakt van de map **Gedeeld met mij**.

Beperkingen

- Er kan geen back-up worden gemaakt van een Shared drive zonder leden vanwege beperkingen van de Google Drive-API.
- Specifieke Google-bestandsindelingen: alleen Google Documenten, Google Spreadsheets en Google Presentaties worden volledig ondersteund voor het maken van back-ups en het uitvoeren van herstelbewerkingen. Andere specifieke Google-indelingen worden mogelijk niet volledig of helemaal niet ondersteund. Bestanden van Google Tekeningen worden bijvoorbeeld hersteld als `.svg`-bestanden, bestanden van Google Sites worden hersteld als `.txt`-bestanden, bestanden van Google Jamboard worden hersteld als `.pdf`-bestanden en bestanden van Google My Maps worden tijdens een back-up overgeslagen.

  Opmerking
  Bestandsindelingen die niet specifiek van Google zijn, zoals `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png` en `.zip`, worden volledig ondersteund voor back-up en herstel.

Welke items kunnen worden hersteld?

U kunt een volledige Shared drive herstellen, of een bestand of map herstellen waarvan een back-up is gemaakt.

U kunt kiezen of u de machtigingen voor delen wilt herstellen of dat de machtigingen voor de bestanden worden overgenomen van de map waarin de bestanden worden hersteld.

De volgende items worden niet hersteld:

- Machtigingen voor het delen van een bestand dat is gedeeld met een gebruiker buiten de organisatie, worden niet hersteld als het delen buiten de organisatie is uitgeschakeld in de doel-Shared drive.
- Machtigingen voor het delen van een bestand dat is gedeeld met een gebruiker die geen lid is van de doel-Shared drive, worden niet hersteld als **Delen met niet-leden** is uitgeschakeld in de doel-Shared drive.

Beperkingen

- Opmerkingen in bestanden worden niet hersteld.
- Links voor het delen van bestanden en mappen worden niet hersteld.

Gedeelde Drive-bestanden selecteren

Selecteer de bestanden zoals hier beschreven en geef vervolgens naar wens de andere instellingen van het beschermingsschema op.

Gedeelde Drive-bestanden selecteren

1. Klik op **Google Workspace**.
2. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie met de gebruikersgegevens waarvan u een back-up wilt maken. Anders kunt u deze stap overslaan.
3. Voer een van de volgende handelingen uit:
   - Als u een back-up wilt maken van de bestanden van alle gedeelde Drives (inclusief gedeelde Drives die in de toekomst worden gemaakt), vouwt u het knooppunt **Gedeelde Drives** uit, selecteert u **Alle gedeelde Drives** en klikt u vervolgens op **Back-up van groep**.
   - Als u een back-up wilt maken van de bestanden van afzonderlijke gedeelde Drives, vouwt u het knooppunt **Gedeelde Drives** uit, selecteert u **Alle gedeelde Drives**, selecteert u de gedeelde Drives waarvan u een back-up wilt maken en klikt u vervolgens op **Back-up**.
4. In het deelvenster voor het beschermingsschema:
   - Voer in **Items waarvan een back-up moet worden gemaakt** een van de volgende handelingen uit:
     - Behoud de standaardinstelling **[All]** (alle bestanden).
     - Voeg de namen of paden toe van de bestanden en mappen waarvan u een back-up wilt maken.

       U kunt jokertekens (*, ** en ?) gebruiken. Voor meer informatie over het opgeven van paden en het gebruik van jokers gaat u naar 'Bestandsfilters'.
     - Blader door de bestanden en mappen om op te geven van welke bestanden en mappen u een back-up wilt maken.

       De link **Bladeren** is alleen beschikbaar wanneer u een beschermingsschema voor één gedeelde Drive maakt.
   - [Optioneel] Klik in **Items waarvan een back-up moet worden gemaakt** op **Uitsluitingen weergeven** om op te geven welke bestanden en mappen u wilt overslaan tijdens het maken van de back-up.

     Met bestandsuitsluitingen wordt de bestandsselectie overschreven, dat wil zeggen als u in beide velden hetzelfde bestand opgeeft, wordt dit bestand overgeslagen tijdens een back-up.

- Als u notarisatie wilt inschakelen voor alle bestanden die zijn geselecteerd voor het maken van een back-up, schakelt u de optie **Notarisatie** in. Ga voor meer informatie over notarisatie naar 'Notarisatie'.

Shared drive en Shared drive-bestanden herstellen

Een volledige gedeelde Drive herstellen

1. Klik op **Google Workspace**.
2. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie waarvan u de back-upgegevens wilt herstellen. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Gedeelde Drives** uit, selecteer **Alle gedeelde Drives**, selecteer de gedeelde Drive die u wilt herstellen en klik vervolgens op **Herstel**.
   Als de gedeelde Drive is verwijderd, selecteert u deze in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u vervolgens op **Back-ups weergeven**.
   U kunt gedeelde Drives zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.
5. Klik op **Herstellen** > **Volledige gedeelde Drive**.
6. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Google Workspace-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.
   Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u een nieuwe doelorganisatie opgeven door deze te kiezen uit de beschikbare geregistreerde organisaties.
7. In **Herstellen naar station** kunt u de doel-Drive in de gedeelde Drives of de doelgebruiker bekijken, wijzigen of opgeven. Als u een gebruiker opgeeft, worden de gegevens hersteld op de Google Drive van deze gebruiker.
   Standaard wordt de oorspronkelijke gedeelde Drive geselecteerd. Als deze gedeelde Drive niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u de doel-Drive in de gedeelde Drives of de doelgebruiker opgeven.
8. Selecteer of u de machtigingen voor delen voor de bestanden wilt herstellen.
9. Klik op **Herstel starten**.

10. Selecteer een van de opties voor overschrijven:

Optie	Beschrijving
Een bestaand bestand overschrijven als dit ouder is	Als er een bestand met dezelfde naam op de doellocatie is en dit bestand ouder is dan het bronbestand, wordt het bronbestand opgeslagen op de doellocatie, ter vervanging van de oudere versie.
Bestaande bestanden overschrijven	Alle bestaande bestanden op de doellocatie worden overschreven, ongeacht de datum waarop ze voor het laatst zijn gewijzigd.
Bestaande bestanden niet overschrijven	Als er een bestand met dezelfde naam op de doellocatie is, worden hierin geen wijzigingen aangebracht en wordt het bronbestand niet opgeslagen op de doellocatie.

11. Klik op **Doorgaan** om uw beslissing te bevestigen.

Gedeelde Drive-bestanden herstellen

1. Klik op **Google Workspace**.
2. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, selecteert u de organisatie waarvan u de back-upgegevens wilt herstellen. Anders kunt u deze stap overslaan.
3. Vouw het knooppunt **Gedeelde Drives** uit, selecteer **Alle gedeelde Drives**, selecteer de gedeelde Drive met de oorspronkelijke bestanden die u wilt herstellen en klik vervolgens op **Herstel**.

   Als de gedeelde Drive is verwijderd, selecteert u deze in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u vervolgens op **Back-ups weergeven**.

   U kunt gedeelde Drives zoeken op naam. Jokers worden niet ondersteund.
4. Selecteer een herstelpunt.
5. Klik op **Herstellen** > **Bestanden/mappen**.
6. Blader naar de vereiste map of gebruik de zoekfunctie om de lijst met vereiste bestanden en mappen weer te geven.
7. Selecteer de bestanden die u wilt herstellen.

   Als de back-up niet is versleuteld en u één bestand hebt geselecteerd, kunt u klikken op **Versies weergeven** om de bestandsversie te selecteren die u wilt herstellen. U kunt elke versie selecteren waarvan een back-up is gemaakt, ongeacht of deze eerder of later is dan het geselecteerde herstelpunt.
8. Als u een bestand wilt downloaden, selecteert u het bestand, klikt u op **Downloaden**, selecteert u de locatie waar u het bestand wilt opslaan en klikt u op **Opslaan**. Anders kunt u deze stap overslaan.
9. Klik op **Herstellen**.

10. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyber Protection-service, klikt u op **Google Workspace-organisatie** om de doelorganisatie te bekijken, te wijzigen of op te geven.

    Standaard is de oorspronkelijke organisatie geselecteerd. Als deze organisatie niet meer is geregistreerd in de Cyber Protection-service, moet u een nieuwe doelorganisatie opgeven door deze te kiezen uit de beschikbare geregistreerde organisaties.
11. In **Herstellen naar station** kunt u de doel-Drive in de gedeelde Drives of de doelgebruiker bekijken, wijzigen of opgeven. Als u een gebruiker opgeeft, worden de gegevens hersteld op de Google Drive van deze gebruiker.

    Standaard wordt de oorspronkelijke gedeelde Drive geselecteerd. Als deze gedeelde Drive niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u de doel-Drive in de gedeelde Drives of de doelgebruiker opgeven.
12. Open **Pad** en bekijk of wijzig de doelmap in de doel-Drive in de gedeelde Drives of de Google Drive van de doelgebruiker. Standaard is de oorspronkelijke locatie geselecteerd.
13. Selecteer of u de machtigingen voor delen voor de bestanden wilt herstellen.
14. Klik op **Herstel starten**.
15. Selecteer een van de opties voor het overschrijven van bestanden:

Optie	Beschrijving
Een bestaand bestand overschrijven als dit ouder is	Als er een bestand met dezelfde naam op de doellocatie is en dit bestand ouder is dan het bronbestand, wordt het bronbestand opgeslagen op de doellocatie, ter vervanging van de oudere versie.
Bestaande bestanden overschrijven	Alle bestaande bestanden op de doellocatie worden overschreven, ongeacht de datum waarop ze voor het laatst zijn gewijzigd.
Bestaande bestanden niet overschrijven	Als er een bestand met dezelfde naam op de doellocatie is, worden hierin geen wijzigingen aangebracht en wordt het bronbestand niet opgeslagen op de doellocatie.

16. Klik op **Doorgaan** om uw beslissing te bevestigen.

Notarisatie

Met notarisatie kunt u bewijzen dat een bestand authentiek en ongewijzigd is sinds er een back-up van is gemaakt. Het wordt aanbevolen om notarisatie in te schakelen wanneer u back-ups maakt van bestanden met juridische documenten of andere bestanden waarvoor bewezen authenticiteit is vereist.

Notarisatie is alleen beschikbaar voor back-ups van Google Drive-bestanden en gedeelde Drive-bestanden in Google Workspace.

Notarisatie gebruiken

Als u notarisatie wilt inschakelen voor alle bestanden die zijn geselecteerd voor het maken van een back-up, schakelt u de optie **Notarisatie** in wanneer u een beschermingsschema maakt.

Wanneer u herstel configureert, worden de genotariseerde bestanden gemarkeerd met een speciaal pictogram en kunt u de authenticiteit van het bestand verifiëren.

Zo werkt het

Tijdens een back-up berekent de agent de hashcodes van de bestanden waarvan een back-up is gemaakt. Daarnaast wordt een hash-boom gemaakt (op basis van de mapstructuur), wordt de boom opgeslagen in de back-up en wordt de root van de hash-boom verzonden naar de Notary-service. De Notary-service slaat de root van de hash-boom op in de Ethereum-blockchaindatabase om te waarborgen dat deze waarde niet wordt gewijzigd.

Wanneer u de authenticiteit van een bestand verifieert, berekent de agent de hash van het bestand en vergelijkt deze met de hash die is opgeslagen in de hash-boom binnen de back-up. Als deze hashes niet overeenkomen, wordt het bestand beschouwd als niet-authentiek. In andere gevallen wordt de authenticiteit van een bestand gegarandeerd door de hash-boom.

De agent verzendt de root van de hash-boom naar de Notary-service om te verifiëren of de hash-boom niet zelf is aangetast. De Notary-service vergelijkt deze met de root die is opgeslagen in de blockchaindatabase. Als de hashes overeenkomen, is het geselecteerde bestand gegarandeerd authentiek. Zo niet, dan ziet u een bericht dat het bestand niet authentiek is.

De authenticiteit van bestanden verifiëren met de Notary-service

Als notarisatie is ingeschakeld tijdens het maken van een back-up, kunt u de authenticiteit verifiëren van een bestand waarvan een back-up is gemaakt.

De authenticiteit van bestanden verifiëren

1. Voer een van de volgende handelingen uit:
   - Als u de authenticiteit van een Google Drive-bestand wilt verifiëren, selecteert u het bestand zoals beschreven in de stappen 1-7 van het gedeelte 'Google Drive-bestanden herstellen'.
   - Als u de authenticiteit van een Google Workspace Shared drive-bestand wilt verifiëren, selecteert u het bestand zoals beschreven in de stappen 1-7 van het gedeelte 'Shared drive-bestanden herstellen'.
2. Controleer of het geselecteerde bestand is gemarkeerd met het volgende pictogram:  . Dit betekent dat het bestand is genotariseerd.
3. Voer een van de volgende handelingen uit:
   - Klik op **Verifiëren**.
     De software controleert de authenticiteit van het bestand en geeft het resultaat weer.
   - Klik op **Certificaat ophalen**.

Een certificaat dat bevestigt dat het bestand is genotariseerd, wordt geopend in een browservenster. Het venster bevat ook instructies voor het handmatig verifiëren van de authenticiteit van het bestand.

Zoeken in cloud-naar-cloud back-ups

Tijdens het herstellen van gegevens kunt u zoeken naar specifieke back-upitems, zodat u niet door het hele back-uparchief hoeft te bladeren.

In niet-versleutelde back-ups is de zoekfunctie altijd beschikbaar. Alleen uitgebreid zoeken (via index) wordt ondersteund.

Zoeken via index is sneller en biedt extra opties, zoals weergave van de versies van de back-upitems, zoeken in de namen van bijlagen en zoeken in volledige tekst in back-ups van Gmail.

Zoekopdracht in volledige tekst

Zoeken in volledige tekst is alleen beschikbaar voor back-ups van Gmail en is standaard ingeschakeld. Hiermee kunt u zoeken in de tekst van back-ups van e-mails. Als deze optie is uitgeschakeld, kunt u alleen zoeken op onderwerp, afzender, ontvanger en datum.

Een index voor zoeken in volledige tekst neemt tussen de 10 en 30 procent van de opslagruimte voor back-ups van Gmail in beslag. Een index zonder de gegevens van zoeken in volledige tekst is aanzienlijk kleiner. Als u opslagruimte wilt besparen, kunt u de functie voor zoeken in volledige tekst uitschakelen en het gedeelte met de gegevens van zoeken in volledige tekst in de index wissen.

Zoekindexen

Zoekindexen bieden uitgebreide zoekmogelijkheden in archieven van cloud-naar-cloud back-ups.

De archieven worden automatisch geïndexeerd na elke back-upbewerking. Het indexeringsproces heeft geen invloed op de back-upprestaties omdat indexering en back-ups worden uitgevoerd door verschillende softwareonderdelen.

De zoekresultaten wordt pas weergegeven nadat de indexeringsbewerking is voltooid (dit kan tot 24 uur duren). Indexering van de eerste back-up (een volledige back-up) duurt meestal langer dan indexering van de daaropvolgende incrementele back-ups.

Alle indexen bevatten metagegevens die de belangrijkste zoekfunctionaliteit ondersteunen: zoeken op onderwerp, afzender, ontvanger of datum. De indexen voor back-ups van Gmail bevatten extra gegevens als zoeken in volledige tekst is ingeschakeld.

De grootte van een zoekindex controleren

Zoekindexen worden na verloop van tijd groter. De indexen voor back-uparchieven waarin zoeken in volledige tekst is ingeschakeld, kunnen tot 30 procent van de archiefgrootte in beslag nemen.

De grootte van een zoekindex controleren:

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Open het tabblad **Back-upopslag** en klik op **Back-ups van cloudtoepassingen**.
3. Controleer de waarde in de kolom **Indexgrootte**.

Indexen bijwerken, herbouwen of verwijderen

U kunt zoekindexen bijwerken, herbouwen of verwijderen om u te helpen problemen met de zoekfunctie in cloud-naar-cloud back-ups op te lossen.

Opmerking
We raden u aan om contact op te nemen met het ondersteuningsteam voordat u een index gaat bijwerken, herbouwen of verwijderen.

Een index bijwerken, herbouwen of verwijderen:

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Open het tabblad **Back-upopslag** en klik op **Back-ups van cloudtoepassingen**.
   Selecteer het archief waarvan u de index wilt bijwerken, herbouwen of verwijderen.
   De beschikbaarheid van deze acties hangt af van het beheerdersniveau en de rol, als volgt:

Accountniveau	Rol	Kan index bijwerken	Kan index opnieuw maken	Kan index verwijderen
Partnertenant	Bedrijfbeheerder	+	+	+
	Beheerder cyberbescherming	+	-	-
	Beschermingsbeheerder	+	-	-
	Beschermingsbeheerder met alleen-lezen rechten	-	-	-
Klanttenant	Bedrijfbeheerder	+	-	-
	Beschermingsbeheerder	+	-	-
	Beschermingsbeheerder met alleen-lezen rechten	-	-	-
Eenheid	Eenheidbeheerder	+	-	-
	Beschermingsbeheerder	+	-	-
	Beschermingsbeheerder met alleen-lezen rechten	-	-	-

3. Ga naar het deelvenster **Acties** en selecteer de actie die u wilt uitvoeren:
   - **Index bijwerken**: de herstelpunten in het archief worden gecontroleerd en de ontbrekende indexen worden toegevoegd.

- **Index opnieuw maken**: de indexen voor alle herstelpunten in het archief worden verwijderd en vervolgens worden de indexen opnieuw gemaakt.
- **Index verwijderen**: de indexen voor alle herstelpunten in het archief worden verwijderd.

4. [Voor versleutelde archieven] Geef het versleutelingswachtwoord op en klik vervolgens op **OK**.
5. Selecteer het bereik van de actie en klik vervolgens op **OK**.

   Afhankelijk van het archief en de geselecteerde actie zijn een of meer van de volgende opties beschikbaar:
   - **Alleen metagegevens**
   - **Alleen inhoud**
   - **Metagegevens en inhoud zoeken**

Zoeken in volledige tekst uitschakelen voor back-ups van Gmail

Zoeken in volledige tekst is alleen beschikbaar voor back-ups van Gmail en is standaard ingeschakeld. Hiermee kunt u zoeken in de tekst van back-ups van e-mails. Als deze optie is uitgeschakeld, kunt u alleen zoeken op onderwerp, afzender, ontvanger en datum.

Als u de grootte van de zoekindex minimaal wilt houden, kunt u overwegen zoeken in volledige tekst uit te schakelen.

Zoeken in volledige tekst uitschakelen

1. Tijdens het maken of bewerken van een back-upplan klikt u op het tandwielpictogram in de rechterbovenhoek.
2. Op het tabblad **Zoeken in volledige tekst** zet u de schakelaar uit.
3. Klik op **Gereed**.
4. [Tijdens het maken van een plan] Klik op **Toepassen**.
5. [Tijdens het bewerken van een plan] Klik op **Instellingen opslaan**.

Opmerking
Als u de functie voor zoeken in volledige tekst opnieuw inschakelt, wordt er een nieuwe index gemaakt voor alle archieven die door dit back-upplan zijn gemaakt. Dit kan veel tijd in beslag nemen.

Oracle Database beschermen

Opmerking
Deze functie is alleen beschikbaar met het Advanced Backup-pakket.

De beveiliging van Oracle Database wordt beschreven in een afzonderlijk document dat beschikbaar is op: https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf

SAP HANA beveiligen

Opmerking
Deze functie is alleen beschikbaar met het Advanced Backup-pakket.

De beveiliging van SAP HANA wordt beschreven in een afzonderlijk document dat beschikbaar is op https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf

MySQL- en MariaDB-gegevens beschermen

U kunt MySQL- en MariaDB-gegevens beschermen met applicatiegerichte back-up. Hiermee worden metagegevens van toepassingen verzameld en is gedetailleerd herstel van exemplaren, databases en tabellen mogelijk.

Opmerking
Applicatiegerichte back-up van MySQL- of MariaDB-gegevens is beschikbaar met het Advanced Backup-pakket.

Voor het beschermen van een fysieke of virtuele machine waarop MySQL- of MariaDB-exemplaren worden uitgevoerd met applicatiegerichte back-up, moet u Agent voor MySQL/MariaDB op de betreffende machine installeren. Agent voor MySQL/MariaDB is gebundeld met Agent voor Linux (64-bits) en kan daarom alleen worden geïnstalleerd op 64-bits Linux-besturingssystemen. Zie "Ondersteunde besturingssystemen en omgevingen" (p. 23).

Het installatiebestand voor Agent voor Linux (64 bits) downloaden

1. Meld u aan bij de Cyber Protect-console.
2. Klik op het accountpictogram in de rechterbovenhoek en selecteer vervolgens **Downloads**.
3. Klik op **Agent voor Linux (64 bits)**.

   Het installatiebestand wordt naar uw machine gedownload. U kunt de agent installeren zoals beschreven in "Beveiligingsagents installeren in Linux" (p. 84) of "Beveiligingsagents installeren en verwijderen in Linux" (p. 106). Vergeet niet om het optionele onderdeel Agent voor MySQL/MariaDB te selecteren.

   Voor het herstel van databases en tabellen naar een live exemplaar heeft Agent voor MySQL/MariaDB een tijdelijke opslag nodig. Standaard wordt de map `/tmp` gebruikt. U kunt deze map wijzigen door de omgevingsvariabele `ACRONIS_MYSQL_RESTORE_DIR` in te stellen.

Beperkingen

- MySQL- of MariaDB-clusters worden niet ondersteund.
- MySQL- of MariaDB-exemplaren die in Docker-containers worden uitgevoerd, worden niet ondersteund.

- MySQL- of MariaDB-exemplaren uitgevoerd op besturingssystemen waarvoor het BTRFS-bestandssysteem wordt gebruikt, worden niet ondersteund.
- Systeemdatabases (`sys`, `mysql`, `information-schema` en `performance_schema`) en databases die geen tabellen bevatten, kunnen niet worden hersteld naar live exemplaren. Deze databases kunnen wel als bestanden worden hersteld wanneer het hele exemplaar wordt hersteld.
- Herstel wordt alleen ondersteund voor doelexemplaren van dezelfde versie (of later) als het exemplaar waarvan een back-up is gemaakt. Hierbij gelden de volgende beperkingen:
  - Herstel van MySQL 5.x-exemplaren naar MySQL 8.x-exemplaren wordt niet ondersteund.
  - Herstel naar een latere versie van MySQL 5.x (inclusief de secundaire versies) wordt alleen ondersteund als het hele exemplaar wordt hersteld als bestanden. Zie de officiële MySQL-upgradehandleiding voor de doelversie (bijvoorbeeld de MySQL 5.7-upgradehandleiding) voordat u het herstel probeert uit te voeren.
- Herstel van back-ups die zijn opgeslagen in Secure Zone, wordt niet ondersteund.
- Databases en tabellen kunnen niet worden hersteld als Agent voor MySQL/MariaDB wordt uitgevoerd op een machine waarop AppArmor is geïnstalleerd. U kunt een exemplaar wel herstellen als bestanden, of u kunt de hele machine herstellen.
- Herstel naar doeldatabases die zijn geconfigureerd met symbolische links, wordt niet ondersteund. U kunt de databases waarvan een back-up is gemaakt, herstellen als nieuwe databases door de naam van de betreffende databases te wijzigen.

Bekende problemen

Als u problemen ondervindt bij het herstel van gegevens uit Samba-shares die met een wachtwoord zijn beveiligd, meldt u zich af bij de Cyber Protect-console en meldt u zich daarna weer aan. Selecteer het gewenste herstelpunt en klik vervolgens op **MySQL/MariaDB-databases**. Klik niet op **Volledige machine** of **Bestanden/mappen**.

Een applicatiegerichte back-up configureren

Vereisten

- Er moet ten minste één MySQL- of MariaDB-exemplaar op de geselecteerde machine worden uitgevoerd.
- Op de machine waarop het MySQL- of MariaDB-exemplaar wordt uitgevoerd, moet de beveiligingsagent worden gestart onder de rootgebruiker.
- Applicatiegerichte back-up is alleen beschikbaar wanneer **Volledige machine** is geselecteerd als back-upbron in het beschermingsschema.
- De back-upoptie **Sector-voor-sector** moet worden uitgeschakeld in het beschermingsschema. Anders is het onmogelijk om toepassingsgegevens te herstellen.

Een applicatiegerichte back-up configureren

1. Open de Cyber Protect-console en selecteer een of meer machines waarop MySQL- of MariaDB-exemplaren worden uitgevoerd.

U kunt een of meer exemplaren hebben op elke machine.

2. Maak een beschermingsschema terwijl de back-upmodule is ingeschakeld.
3. Selecteer **Volledige machine** in **Back-up maken van**.
4. Klik op **Back-up van toepassing** en schakel vervolgens de schakelaar naast **MySQL/MariaDB Server** in.
5. Selecteer hoe u de MySQL- of MariaDB-exemplaren wilt opgeven:
   - **Voor alle workloads**

     Gebruik deze optie als u exemplaren met identieke configuraties op meerdere servers uitvoert. Voor alle exemplaren worden dezelfde verbindingsparameters en toegangsreferenties gebruikt.
   - **Voor specifieke workloads**

     Gebruik deze optie om de verbindingsparameters en toegangsreferenties voor elk exemplaar op te geven.
6. Klik op **Exemplaar toevoegen** om de verbindingsparameters en toegangsreferenties te configureren.
   a. Selecteer het verbindingstype en geef vervolgens het volgende op:
      - [Voor TCP-socket] IP-adres en poort.
      - [Voor Unix-socket] Pad van socket.

   b. Geef de referenties op van een gebruikersaccount met de volgende bevoegdheden voor het exemplaar:
      - `FLUSH_TABLES` of `RELOAD` voor alle databases en tabellen (`*.*`)
      - `SELECT` voor de `information_schema.tables`

   c. Klik op **OK**.
7. Klik op **Gereed**.

Gegevens herstellen vanaf een applicatiegerichte back-up

Vanuit een applicatiegerichte back-up kunt u MySQL- of MariaDB-exemplaren, databases en tabellen herstellen. U kunt ook de volledige server waarop de exemplaren worden uitgevoerd, of bestanden en mappen van deze server herstellen.

De onderstaande tabel bevat een overzicht van alle herstelopties.

Te herstellen	Herstellen als	Herstellen naar
MySQL Server MariaDB Server	Volledige machine	Machine* waarop Agent voor Linux is geïnstalleerd
MySQL	Bestanden of	Machine* waarop Agent voor Linux is geïnstalleerd

Te herstellen	Herstellen als	Herstellen naar
Server MariaDB Server	mappen	
Exemplaar	Bestanden	Machine* waarop Agent voor MySQL/MariaDB is geïnstalleerd
Database	Dezelfde database Nieuwe database	Machine* waarop Agent voor MySQL/MariaDB is geïnstalleerd • Oorspronkelijk exemplaar • Een ander exemplaar • Oorspronkelijke database • Nieuwe database
Tabel	Dezelfde tabel Nieuwe tabel	Machine* waarop Agent voor MySQL/MariaDB is geïnstalleerd • Oorspronkelijk exemplaar • Een ander exemplaar • Oorspronkelijke database • Oorspronkelijke tabel • Nieuwe tabel

* Back-ups voor een virtuele machine met ingebouwde agent worden op dezelfde manier gemaakt als voor een fysieke machine.

De volledige server herstellen

Zie "Een machine herstellen" (p. 529) voor meer informatie over het herstellen van de volledige server waarop MySQL- of MariaDB-exemplaren worden uitgevoerd.

Exemplaren herstellen

Vanuit een applicatiegerichte back-up kunt u MySQL- of MariaDB-exemplaren herstellen als bestanden.

Een exemplaar herstellen

1. Open de Cyber Protect-console en selecteer de machine met de oorspronkelijke gegevens die u wilt herstellen.
2. Klik op **Herstel**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de machine offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:
   - Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een online

machine met Agent voor MySQL/MariaDB en selecteert u vervolgens een herstelpunt.
- Selecteer een herstelpunt op het tabblad **Back-upopslag**.

De machine die u hebt gekozen om te bladeren via een van de genoemde acties, wordt een doelmachine voor de herstelbewerking.

4. Klik op **Herstellen** > **MySQL-/MariaDB-databases**.
5. Selecteer het exemplaar dat u wilt herstellen en klik vervolgens op **Herstellen als bestanden**.
6. Ga naar **Pad** en selecteer de map waarnaar u de bestanden wilt herstellen.
7. Klik op **Herstel starten**.

Databases herstellen

Vanuit een applicatiegerichte back-up kunt u databases herstellen naar live MySQL- of MariaDB-exemplaren.

1. Open de Cyber Protect-console en selecteer de machine met de oorspronkelijke gegevens die u wilt herstellen.
2. Klik op **Herstel**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de machine offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:
   - Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een online machine met Agent voor MySQL/MariaDB en selecteert u vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad **Back-upopslag**.

   De machine die u hebt gekozen om te bladeren via een van de genoemde acties, wordt een doelmachine voor de herstelbewerking.
4. Klik op **Herstellen** > **MySQL-/MariaDB-databases**.
5. Klik op de naam van het gewenste exemplaar om naar de databases te gaan.
6. Selecteer een of meer databases die u wilt herstellen.
7. Klik op **Herstellen**.
8. Klik op **MySQL-/MariaDB-doelexemplaar** om de verbindingsparameters en toegangsreferenties voor het doelexemplaar op te geven.
   - Controleer naar welk exemplaar u gegevens wilt herstellen. Standaard is het oorspronkelijke exemplaar geselecteerd.
   - Geef de referenties op van een gebruikersaccount dat toegang heeft tot het doelexemplaar. Aan dit gebruikersaccount moeten de volgende rechten zijn toegewezen voor alle databases en tabellen (`*.*`):
     - `INSERT`
     - `CREATE`

- DROP
- LOCK_TABLES
- ALTER
- SELECT

- Klik op **OK**.

9. Controleer de doeldatabase.

   Standaard is de oorspronkelijke database geselecteerd.

   Als u een database wilt herstellen als nieuwe database, klikt u op de naam van de doeldatabase en wijzigt u deze. Deze actie is alleen beschikbaar wanneer u een enkele database herstelt.
10. Ga naar **Bestaande databases overschrijven** en selecteer de modus voor overschrijven.

    Overschrijven is standaard ingeschakeld, dat wil zeggen dat de doeldatabase wordt vervangen door de back-updatabase met dezelfde naam.

    Als overschrijven is uitgeschakeld, wordt de back-updatabase overgeslagen tijdens de herstelbewerking en wordt de doeldatabase niet vervangen door de back-updatabase met dezelfde naam.
11. Klik op **Herstel starten**.

Tabellen herstellen

Vanuit een applicatiegerichte back-up kunt u tabellen herstellen naar live MySQL- of MariaDB-exemplaren.

1. Open de Cyber Protect-console en selecteer de machine met de oorspronkelijke gegevens die u wilt herstellen.
2. Klik op **Herstel**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

   Als de machine offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:

   - Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een online machine met Agent voor MySQL/MariaDB en selecteert u vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad **Back-upopslag**.

   De machine die u hebt gekozen om te bladeren via een van de genoemde acties, wordt een doelmachine voor de herstelbewerking.
4. Klik op **Herstellen** > **MySQL-/MariaDB-databases**.
5. Klik op de naam van het gewenste exemplaar om naar de databases te gaan.
6. Klik op de naam van de gewenste database om naar de tabellen te gaan.
7. Selecteer een of meer tabellen die u wilt herstellen.
8. Klik op **Herstellen**.

9. Klik op **MySQL-/MariaDB-doelexemplaar** om de verbindingsparameters en toegangsreferenties voor het doelexemplaar op te geven.
   - Controleer naar welk exemplaar u gegevens wilt herstellen. Standaard is het oorspronkelijke exemplaar geselecteerd.
   - Geef de referenties op van een gebruikersaccount dat toegang heeft tot het doelexemplaar. Aan dit gebruikersaccount moeten de volgende rechten zijn toegewezen voor alle databases en tabellen (`*.*`):
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Klik op **OK**.
10. Controleer de doeltabel.

    Standaard is de oorspronkelijke tabel geselecteerd.

    Als u een tabel wilt herstellen als nieuwe tabel, klikt u op de naam van de doeltabel en wijzigt u deze. Deze actie is alleen beschikbaar wanneer u een enkele tabel herstelt.
11. Ga naar **Bestaande tabellen overschrijven** en selecteer de modus voor overschrijven.

    Overschrijven is standaard ingeschakeld, dat wil zeggen dat de doeltabel wordt vervangen door de back-uptabel met dezelfde naam.

    Als overschrijven is uitgeschakeld, wordt de back-uptabel overgeslagen tijdens de herstelbewerking en wordt de doeltabel niet vervangen door de back-uptabel met dezelfde naam.
12. Klik op **Herstel starten**.

Opgeslagen routines herstellen

Wanneer u een volledig MySQL-exemplaar herstelt, worden de opgeslagen routines automatisch hersteld.

De opgeslagen routines worden niet automatisch hersteld wanneer u een afzonderlijke database herstelt naar een ander exemplaar dan het oorspronkelijke exemplaar of wanneer u de afzonderlijke database herstelt als nieuwe database. U kunt de routines handmatig herstellen door ze te exporteren in een SQL-bestand en ze vervolgens toe te voegen aan de herstelde database.

De opgeslagen routines exporteren en toevoegen aan een herstelde database:

1. Open Terminal op de machine met het oorspronkelijke MySQL-exemplaar.
2. Voer de volgende opdracht uit om de opgeslagen routines te exporteren.

3.
```
mysqldump -p [source_database_name] --routines --no-create-info --no-data >
[exported_db_routines.sql]
```
4. Open de MySQL-opdrachtregelclient op de machine waarop de database is hersteld.
5. Voer de volgende opdrachten uit om de routines toe te voegen aan de herstelde database.
```
mysql>  use [recovered_database_name];
```
```
mysql>  source [path_to_exported_db_routines.sql];
```

Websites en hostingservers beveiligen

Websites beschermen

Een website kan beschadigd raken door niet-geautoriseerde toegang of een aanval met malware. Maak een back-up van uw website als u deze gemakkelijk wilt kunnen terugdraaien naar een goede status in het geval van beschadiging.

Wat moet ik doen om een back-up te maken van een website?

De website moet toegankelijk zijn via het SFTP- of SSH-protocol. U hoeft geen agent te installeren. Het is voldoende om een website toe te voegen, zoals verderop in dit gedeelte wordt beschreven.

Van welke items kan een back-up worden gemaakt?

U kunt een back-up maken van de volgende items:

- **Bestanden met website-inhoud**

  Alle bestanden die toegankelijk zijn voor het account dat u opgeeft voor de SFTP- of SSH-verbinding.
- **Gekoppelde databases (indien van toepassing) die worden gehost op MySQL-servers.**

  Alle databases die toegankelijk zijn voor het MySQL-account dat u opgeeft.

Als uw website gebruikmaakt van databases, raden we u aan een back-up te maken van zowel de bestanden als de databases, zodat u deze kunt herstellen naar een consistente status.

Beperkingen

- Cloudopslag is de enige back-uplocatie die beschikbaar is voor een back-up van de website.
- U kunt verschillende beschermingsschema's toepassen op een website, maar slechts één ervan kan worden uitgevoerd volgens een schema. Andere schema's moeten handmatig worden gestart.
- De enige beschikbare back-upoptie is 'Naam van back-upbestand'.

- De beschermingsschema's voor websites worden niet weergegeven op het tabblad **Beheer** > **Beschermingsschema's**.

Back-up maken van een website

Een website toevoegen

1. Klik op **Apparaten** > **Toevoegen**.
2. Klik op **Website**.
3. Configureer de volgende toegangsinstellingen voor de website:
   - Ga naar **Naam van website** en typ een naam voor uw website. Deze naam wordt weergegeven in de Cyber Protect-console.
   - Geef bij **Host** de hostnaam of het IP-adres op waarmee u toegang wilt krijgen tot de website via SFTP of SSH. Bijvoorbeeld: `mijn.server.com` of `10.250.100.100`.
   - Geef bij **Poort** het poortnummer op.
   - Ga naar **Gebruikersnaam** en **Wachtwoord** en geef de referenties op van het account dat u wilt gebruiken voor toegang tot de website via SFTP of SSH.

     Belangrijk
     Er worden alleen back-ups gemaakt van de bestanden die toegankelijk zijn voor het opgegeven account.

     In plaats van een wachtwoord kunt u uw persoonlijke SSH-sleutel opgeven. Als u dit wilt doen, schakelt u het selectievakje **Persoonlijke SSH-sleutel gebruiken in plaats van wachtwoord** in en geeft u de sleutel op.
4. Klik op **Volgende**.
5. Als uw website MySQL-databases gebruikt, configureert u de toegangsinstellingen voor de databases. Anders klikt u op **Overslaan**.
   a. Selecteer bij **Type verbinding** hoe u toegang tot de databases wilt krijgen vanuit de cloud:
      - **Via SSH vanaf de host**: U hebt toegang tot de databases via de host die is opgegeven in stap 3.
      - **Directe verbinding**: U hebt rechtstreeks toegang tot de databases. Kies deze instelling alleen als de databases toegankelijk zijn via internet.

   b. Geef bij **Host** de naam of het IP-adres op van de host met MySQL-server.

   c. Geef bij **Poort** het poortnummer op voor de TCP/IP-verbinding met de server. Het standaardpoortnummer is 3306.

   d. Geef bij **Gebruikersnaam** en **Wachtwoord** de referenties op voor het MySQL-account.

      Belangrijk
      Er worden alleen back-ups gemaakt van de databases die toegankelijk zijn voor het opgegeven account.

e. Klik op **Maken**.

De website wordt weergegeven in de Cyber Protect-console onder **Apparaten** > **Websites**.

De verbindingsinstellingen wijzigen

1. Selecteer de website onder **Apparaten** > **Websites**.
2. Klik op **Details**.
3. Klik op het potloodpictogram naast de verbindingsinstellingen voor de website of de database.
4. Maak de gewenste wijzigingen en klik op **Opslaan**.

Een beschermingsschema voor websites maken

1. Selecteer een website of meerdere websites onder **Apparaten** > **Websites**.
2. Klik op **Beschermen**.
3. [Optioneel] Schakel back-up van databases in.
   Als meerdere websites worden geselecteerd, wordt de back-up van databases standaard uitgeschakeld.
4. [Optioneel] Wijzig de bewaarregels.
5. [Optioneel] Schakel de versleuteling van back-ups in.
6. [Optioneel] Klik op het tandwielpictogram om de optie **Naam van back-upbestand** te bewerken. Dit is nuttig in twee gevallen:
   - Als u eerder een back-up van deze website hebt gemaakt en de bestaande volgorde van back-ups wilt voortzetten
   - Als u de aangepaste naam wilt zien op het tabblad **Back-upopslag**
7. Klik op **Toepassen**.

U kunt beschermingsschema's voor websites op dezelfde manier bewerken, intrekken en verwijderen als voor machines. Deze bewerkingen worden beschreven in 'Bewerkingen voor beschermingsschema's'.

Een website herstellen

Een website herstellen

1. Voer een van de volgende handelingen uit:
   - Ga naar **Apparaten** > **Websites**, selecteer de website die u wilt herstellen en klik vervolgens op **Herstel**.
     U kunt websites zoeken op naam. Jokers worden niet ondersteund.
   - Als de website is verwijderd, selecteert u deze in het gedeelte **Back-ups van cloudtoepassingen** op het tabblad Back-upopslag en klikt u vervolgens op **Back-ups weergeven**.
     Als u een verwijderde website wilt herstellen, moet u de doelsite toevoegen als apparaat.
2. Selecteer het herstelpunt.

3. Klik op **Herstellen** en selecteer de items die u wilt herstellen: **Volledige website**, **Databases** (indien van toepassing) of **Bestanden/mappen**.
   Als u zeker wilt zijn dat uw website consistent is, raden we u aan om zowel bestanden als databases (in een willekeurige volgorde) te herstellen.
4. Voer een van de volgende procedures uit, afhankelijk van uw keuze.

De volledige website herstellen

1. Ga naar **Herstellen naar website** en bekijk of wijzig de doelwebsite.
   Standaard is de oorspronkelijke website geselecteerd. Als deze nog niet bestaat, moet u de doelwebsite selecteren.
2. Selecteer of u de machtigingen voor delen voor de herstelde items wilt herstellen.
3. Klik op **Herstel starten** en bevestig de actie.

De databases herstellen

1. Selecteer de databases die u wilt herstellen.
2. Als u een database wilt downloaden als bestand, klikt u op **Downloaden**, selecteert u de locatie waar u het bestand wilt opslaan en klikt u op **Opslaan**. Anders kunt u deze stap overslaan.
3. Klik op **Herstellen**.
4. Ga naar **Herstellen naar website** en bekijk of wijzig de doelwebsite.
   Standaard is de oorspronkelijke website geselecteerd. Als deze nog niet bestaat, moet u de doelwebsite selecteren.
5. Klik op **Herstel starten** en bevestig de actie.

De bestanden/mappen van de website herstellen

1. Selecteer de bestanden/mappen die u wilt herstellen.
2. Als u een bestand wilt opslaan, klikt u op **Downloaden**, selecteert u de locatie waar u het bestand wilt opslaan en klikt u op **Opslaan**. Anders kunt u deze stap overslaan.
3. Klik op **Herstellen**.
4. Ga naar **Herstellen naar website** en bekijk of wijzig de doelwebsite.
   Standaard is de oorspronkelijke website geselecteerd. Als deze nog niet bestaat, moet u de doelwebsite selecteren.
5. Selecteer of u de machtigingen voor delen voor de herstelde items wilt herstellen.
6. Klik op **Herstel starten** en bevestig de actie.

Webhostingservers beschermen

U kunt Linux-webhostingservers met de besturingspanelen Plesk, cPanel, DirectAdmin, VirtualMin of ISPManager beschermen. Servers met webhosting-besturingspanelen van andere leveranciers worden beschermd als gewone workloads.

Quota's

Servers met de besturingspanelen Plesk, cPanel, DirectAdmin, VirtualMin, of ISPManager worden beschouwd als webhostingservers. Elke back-up van een webhostingserver verbruikt de quota van de **webhostingservers**. Als deze quota wordt uitgeschakeld of de uitbreiding voor deze quota wordt overschreden, mislukt de back-up of wordt er als volgt een quota toegewezen:

- In het geval van een fysieke server wordt de quota voor **Servers** gebruikt. Als deze quota wordt uitgeschakeld of de uitbreiding voor deze quota wordt overschreden, mislukt de back-up.
- In het geval van een virtuele server wordt de quota voor **Virtuele machines** gebruikt. Als deze quota wordt uitgeschakeld of de uitbreiding voor deze quota wordt overschreden, mislukt de back-up.

Integraties voor DirectAdmin, cPanel en Plesk

Webhostingbeheerders die DirectAdmin, Plesk of cPanel gebruiken, kunnen deze besturingspanelen integreren met de Cyber Protection-service. Dit levert enkele krachtige mogelijkheden op, zoals:

- Een back-up van een volledige webhostingserver maken met back-up op schijfniveau
- De volledige server herstellen, inclusief alle websites en accounts
- Nauwkeurig herstel en downloads van accounts, websites, afzonderlijke bestanden, postvakken of databases
- Resellers en klanten kunnen zelf hun eigen gegevens herstellen (selfservice)

Als u de integratie wilt uitvoeren, moet u een Cyber Protection-service-extensie gebruiken. Raadpleeg de betreffende integratiehandleidingen voor meer informatie:

- Integratiehandleiding voor DirectAdmin
- Integratiegids voor WHM en cPanel
- Integratiehandleiding voor Plesk

Speciale bewerkingen met virtuele machines

Een virtuele machine uitvoeren vanaf een back-up (Instant Restore)

U kunt een virtuele machine uitvoeren vanaf een back-up op schijfniveau die een besturingssysteem bevat. Met deze bewerking, ook wel direct herstel genoemd, kunt in enkele seconden een nieuwe virtuele server bedrijfsklaar maken. De virtuele schijven worden direct vanuit de back-up geëmuleerd en nemen dus geen ruimte in beslag in de gegevensopslag. De opslagruimte is alleen vereist om wijzigingen van de virtuele schijven te bewaren.

We raden u aan om deze tijdelijke virtuele machine gedurende maximaal drie dagen uit te voeren. Vervolgens kunt u deze volledig verwijderen of zonder downtime converteren naar een gewone virtuele machine (voltooien).

Zolang de tijdelijke virtuele machine bestaat, kunnen er geen bewaarregels worden toegepast op de back-up die door die machine wordt gebruikt. Back-ups van de oorspronkelijke machine kunt u blijven uitvoeren.

Voorbeelden van gebruik

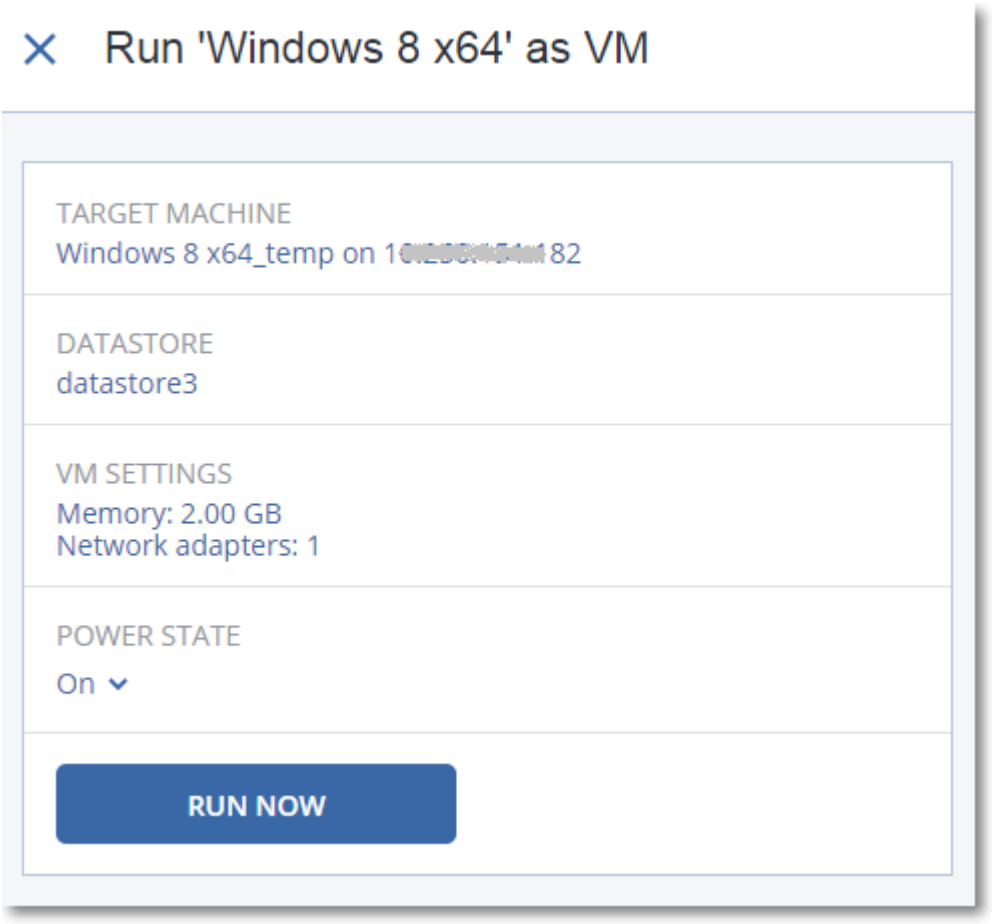
- **Noodherstel**
  Breng direct een kopie van een machine online wanneer de betreffende machine fouten heeft.
- **Back-up testen**
  Voer de machine uit vanaf de back-up en controleer of het gastbesturingssysteem en applicaties naar behoren werken.
- **Toegang tot applicatiegegevens**
  Gebruik terwijl de machine wordt uitgevoerd de eigen beheerhulpmiddelen van de applicatie om de vereiste gegevens te openen en uit te pakken.

Vereisten

- Er moet ten minste één Agent voor VMware of Agent voor Hyper-V zijn geregistreerd in de Cyber Protection-service.
- De back-up kan worden opgeslagen in een netwerkmap of in een lokale map van de machine waarop Agent voor VMware of Agent voor Hyper-V is geïnstalleerd. Als u een netwerkmap selecteert, moet deze toegankelijk zijn vanaf die machine. Een virtuele machine kan ook worden uitgevoerd vanaf een back-up in de cloudopslag, maar dit leidt tot een vertraagde werking omdat hiervoor intensieve random-acces reading vanaf de back-up is vereist.
- De back-up moet een volledige machine of alle volumes bevatten die nodig zijn om het besturingssysteem te starten.
- U kunt back-ups van zowel fysieke als virtuele machines gebruiken. Back-ups van Virtuozzo-*containers* kunnen niet worden gebruikt.
- Back-ups die Linux-logische volumes (LVM) bevatten, moeten worden gemaakt door Agent voor VMware of Agent voor Hyper-V. De virtuele machine moet van hetzelfde type zijn als de originele machine (ESXi of Hyper-V).

De machine uitvoeren

1. Voer een van de volgende handelingen uit:
   - Selecteer een machine waarvan een back-up is gemaakt, klik op **Herstel** en selecteer vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad Back-upopslag.
2. Klik op **Uitvoeren als VM**.
   De host en andere vereiste parameters worden automatisch geselecteerd.



3. [Optioneel] Klik op **Doelmachine** en wijzig het type van de virtuele machine (ESXi of Hyper-V), de host of de naam van de virtuele machine.
4. [Optioneel] Klik op **Gegevensopslag** voor ESXi of **Pad** voor Hyper-V en selecteer vervolgens de gegevensopslag voor de virtuele machine.

   De wijzigingen van de virtuele schijven worden verzameld terwijl de machine wordt uitgevoerd. Controleer of er voldoende vrije schijfruimte is in de geselecteerde gegevensopslag. Als u van plan bent om deze wijzigingen te behouden door de virtuele machine permanent te maken, selecteer dan een gegevensopslag waarmee de machine kan worden uitgevoerd in productie.
5. [Optioneel] Klik op **VM-instellingen** om de geheugengrootte en de netwerkverbindingen van de virtuele machine te wijzigen.
6. [Optioneel] Selecteer de energiestatus van de VM (**Aan**/**Uit**).
7. Klik op **Nu uitvoeren**.

De machine wordt dan in de webinterface weergegeven met een van de volgende pictogrammen:  of 

. U kunt dergelijke virtuele machines niet selecteren om back-ups te maken.

Opmerking
U kunt de bewerking Uitvoeren als virtuele machine (Instant Restore) uitvoeren met back-ups in Microsoft Azure. Deze bewerking resulteert echter in aanzienlijk uitgaand verkeer, dat wordt toegevoegd aan de factuur voor uw Microsoft Azure-abonnement. Typisch uitgaand verkeer voor een Windows-machine die wordt uitgevoerd vanaf een Microsoft Azure-back-up, bedraagt ongeveer 5 GB vanaf het opstarten van de virtuele machine tot de aanmelding.

De machine verwijderen

We raden af om een tijdelijke virtuele machine rechtstreeks te verwijderen in vSphere/Hyper-V, want dit kan leiden tot artefacten in de webinterface. Het kan ook gebeuren dat de back-up van waaruit de machine werd uitgevoerd, gedurende enige tijd vergrendeld blijft (deze kan niet worden verwijderd met bewaarregels).

Een virtuele machine verwijderen die wordt uitgevoerd vanaf een back-up

1. Ga naar het tabblad **Alle apparaten** en selecteer een machine die wordt uitgevoerd vanaf een back-up.
2. Klik op **Verwijderen**.

De machine wordt verwijderd uit de webinterface. De machine wordt ook verwijderd uit de vSphere- of Hyper-V-inventaris en -gegevensopslag. Alle wijzigingen die zijn doorgevoerd in de gegevens terwijl de machine werd uitgevoerd, gaan verloren.

De machine voltooien

Wanneer een virtuele machine wordt uitgevoerd vanaf een back-up, wordt de inhoud van de virtuele schijven rechtstreeks overgenomen uit die back-up. De machine is dan niet toegankelijk of kan zelfs beschadigd raken als de verbinding met de back-uplocatie of de beveiligingsagent wordt verbroken.

U kunt kiezen of u deze machine permanent wilt maken, dat wil zeggen dat u alle virtuele schijven, en de wijzigingen die zijn doorgevoerd terwijl de machine werd uitgevoerd, herstelt naar de gegevensopslag waar deze wijzigingen worden opgeslagen. Dit proces wordt ook wel het voltooien van de machine genoemd.

Het voltooien wordt uitgevoerd zonder downtime. De virtuele machine wordt *niet* uitgeschakeld tijdens het voltooien.

De locatie van de voltooide virtuele schijven wordt gedefinieerd in de parameters van de bewerking **Uitvoeren als VM** (**Gegevensopslag** voor ESXi of **Pad** voor Hyper-V). Voordat u het voltooien begint, controleert u of de vrije ruimte, de mogelijkheden om gegevens te delen en de prestaties van deze gegevensopslag geschikt zijn om de machine in productie uit te voeren.

Opmerking
Voltooien wordt niet ondersteund voor Hyper-V in Windows Server 2008/2008 R2 en Microsoft Hyper-V Server 2008/2008 R2 omdat de benodigde API ontbreekt in deze Hyper-V versies.

Een machine voltooien die wordt uitgevoerd vanaf een back-up

1. Ga naar het tabblad **Alle apparaten** en selecteer een machine die wordt uitgevoerd vanaf een back-up.
2. Klik op **Voltooien**.
3. [Optioneel] Geef een nieuwe naam op voor de machine.
4. [Optioneel] Wijzig de inrichtingsmethode van de schijf. De standaardinstelling is **Thin**.
5. Klik op **Voltooien**.

De naam van de machine wordt meteen gewijzigd. De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**. Wanneer de herstelbewerking is voltooid, verandert het machinepictogram in een pictogram van een gewone virtuele machine.

Voltooien

Het verschil tussen voltooien en gewoon herstel

Het voltooien kost meer tijd dan gewoon herstel om de volgende redenen:

- Tijdens het voltooien opent de agent verschillende delen van de back-up in willekeurige volgorde. Wanneer een volledige machine wordt hersteld, worden de gegevens in de back-up in sequentiële volgorde gelezen door de agent.
- Als de virtuele machine wordt uitgevoerd tijdens het voltooien, leest de agent vaker gegevens uit de back-up om beide processen tegelijkertijd te onderhouden. Tijdens gewoon herstel wordt de virtuele machine gestopt.

Voltooien van machines die worden uitgevoerd vanuit cloudback-ups

Vanwege de intensieve toegang tot de back-upgegevens hangt de snelheid van het voltooien sterk af van de bandbreedte van de verbinding tussen de back-uplocatie en de agent. Het voltooien kost meer tijd voor back-ups in de cloud dan voor lokale back-ups. Het voltooien van een machine die wordt uitgevoerd vanuit een cloudback-up, mislukt mogelijk als de internetverbinding erg traag of instabiel is. Als u kunt kiezen hoe u het voltooien wilt uitvoeren, raden we aan om virtuele machines uit te voeren vanuit lokale back-ups.

Opmerking
Hoe snel de bewerking wordt voltooid, hangt af het feit of de agent is verbonden met een VMware ESXi-host of vCenter, zoals beschreven in stap 3 van "De virtuele toepassing configureren" (p. 143). Verbinding met een VMware vCenter kan ertoe leiden dat de bewerking trager wordt voltooid vanwege de specifieke kenmerken van VMware API's. Als u de bewerking sneller wilt voltooien, gebruikt u een afzonderlijke agent voor VMware voor de bewerkingen **Uitvoeren als VM** en Voltooien. Deze agent is hierbij verbonden met een ESXi-host in plaats van met een vCenter.

Werken in VMware vSphere

In dit gedeelte worden bewerkingen beschreven die specifiek zijn voor VMware vSphere-omgevingen.

Replicatie van virtuele machines

Replicatie is alleen beschikbaar voor virtuele VMware ESXi-machines.

Replicatie betekent het maken van een exacte kopie (replica) van een virtuele machine, waarbij de replica gesynchroniseerd wordt gehouden met de oorspronkelijke machine. Door een kritieke virtuele machine te repliceren beschikt u altijd over een kopie van deze machine die direct kan worden gestart.

De replicatie kan handmatig worden gestart of volgens de planning die u opgeeft. De eerste replicatie is een volledige replicatie (de hele machine wordt gekopieerd). Alle volgende replicaties zijn incrementeel en worden uitgevoerd met Changed Block Tracking, tenzij deze optie is uitgeschakeld.

Replicatie versus back-up

In tegenstelling tot geplande back-ups wordt op een replica slechts de nieuwste status van de virtuele machine bewaard. Een replica neemt ruimte in de gegevensopslag in beslag, terwijl back-ups op een goedkopere opslagplaats kunnen worden bewaard.

Het inschakelen van een replica is echter veel sneller dan een herstelbewerking en sneller dan het uitvoeren van een virtuele machine vanaf een back-up. Wanneer een replica is ingeschakeld, werkt deze sneller dan een VM die vanaf een back-up wordt uitgevoerd en de Agent voor VMware hoeft niet te worden geladen.

Voorbeelden van gebruik

- **Virtuele machines repliceren naar een externe site.**
  Met replicatie kunt u het hoofd bieden aan gedeeltelijke of volledige storingen in het datacentrum doordat u de virtuele machines van een primaire site kunt klonen naar een secundaire site. De secundaire site bevindt zich doorgaans in een externe faciliteit die waarschijnlijk niet wordt getroffen door milieu-, infrastructuur- of andere factoren die de storing in de primaire site hebben veroorzaakt.

- **Virtuele machines repliceren binnen een site (tussen twee hosts/gegevensopslagplaatsen).**
  Onsite replicatie kan worden gebruikt voor scenario's waar hoge beschikbaarheid en noodherstel van belang zijn.

Wat u kunt doen met een replica

- **Een replica testen**
  De replica wordt ingeschakeld voor het uitvoeren van testen. Gebruik vSphere Client of andere tools om te controleren of de replica goed werkt. Replicatie wordt onderbroken tijdens het testen.
- **Failover naar een replica**
  Bij failover wordt de workload van de oorspronkelijke virtuele machine overgebracht naar de bijbehorende replica. Replicatie wordt onderbroken tijdens een failover.
- **Back-up maken van de replica**
  Zowel voor back-ups als voor replicatie is toegang tot virtuele schijven vereist, en dit is van invloed op de prestaties van de host waarop de virtuele machine wordt uitgevoerd. Als u zowel een replica als back-ups van een virtuele machine wilt, maar de productiehost niet extra wilt belasten, dan repliceert u de machine naar een andere host en stelt u back-ups van de replica in.

Beperkingen

- De volgende typen virtuele machines kunnen niet worden gerepliceerd:
  - Fouttolerante machines met ESXi 5.5 en lager.
  - Machines die worden uitgevoerd vanaf back-ups.
  - Replica's van virtuele machines.
- Bij bepaalde hardwarewijzigingen, zoals het toevoegen van een netwerkinterfacekaart (NIC) aan de ESXi-host of het verwijderen van een NIC van de host, worden de interne ID's van de host gewijzigd. Deze wijziging beïnvloedt de VM-replicatieplannen. Na een dergelijke wijziging moet u de VM-replicatieplannen waarin de ESXi-host is geselecteerd als bron of doel, opnieuw maken. Anders mislukken de VM-replicatieplannen.

Een replicatieschema maken

Voor elke machine afzonderlijk moet een replicatieschema worden gemaakt. Het is niet mogelijk een bestaand schema toe te passen op andere machines.

Een replicatieschema maken

1. Selecteer een virtuele machine die u wilt repliceren.
2. Klik op **Replicatie**.
   Er wordt een sjabloon voor een nieuw replicatieschema weergegeven.
3. [Optioneel] Klik op de standaardnaam om de naam van het replicatieschema te wijzigen.
4. Klik op **Doelmachine** en doe het volgende:

a. Kies of u een nieuwe replica wilt maken of een bestaande replica van de oorspronkelijke machine wilt gebruiken.
b. Selecteer de ESXi-host en geef de naam van de nieuwe replica op, of selecteer een bestaande replica.
   De standaardnaam van een nieuwe replica is **[Naam oorspronkelijke machine]_replica**.
c. Klik op **OK**.

5. [Alleen bij replicatie naar een nieuwe machine] Klik op **Gegevensopslag** en selecteer de gegevensopslag voor de virtuele machine.
6. [Optioneel] Klik op **Planning** om de replicatieplanning te wijzigen.
   Standaard worden replicaties dagelijks gemaakt, van maandag tot en met vrijdag. U kunt de tijd voor het uitvoeren van de replicatie kiezen.
   Als u de replicatiefrequentie wilt aanpassen, verplaatst u de schuifregelaar en geeft u de planning op.
   U kunt ook als volgt te werk gaan:
   - Stel een datumbereik in voor de periode dat de planning moet worden uitgevoerd. Schakel het selectievakje **Het schema uitvoeren binnen een datumbereik** in en geef het datumbereik op.
   - Het schema uitschakelen. In dit geval kan replicatie handmatig worden gestart.
7. [Optioneel] Klik op het tandwielpictogram om de replicatieopties te wijzigen.
8. Klik op **Toepassen**.
9. [Optioneel] Als u het schema handmatig wilt uitvoeren, klikt u op **Nu uitvoeren** in het deelvenster voor het schema.

Wanneer een replicatieschema wordt uitgevoerd, wordt de replica van de virtuele machine in de lijst **Alle apparaten** weergegeven met het volgende pictogram: 

Replica testen

Een replica voorbereiden voor een test

1. Selecteer een replica om te testen.
2. Klik op **Replica testen**.
3. Klik op **Testen starten**.
4. Kies of u de ingeschakelde replica wilt verbinden met een netwerk. De replica wordt standaard niet verbonden met een netwerk.
5. [Optioneel] Als u ervoor kiest de replica te verbinden met het netwerk, schakelt u het selectievakje **Oorspronkelijke virtuele machine stoppen** in om de oorspronkelijke machine te stoppen voordat u de replica inschakelt.
6. Klik op **Starten**.

Het testen van een replica stoppen

1. Selecteer een replica die wordt getest.
2. Klik op **Replica testen**.
3. Klik op **Testen stoppen**.
4. Bevestig uw beslissing.

Failover naar een replica uitvoeren

Failover van een machine naar een replica uitvoeren

1. Selecteer een replica voor de failover.
2. Klik op **Replica-acties**.
3. Klik op **Failover**.
4. Kies of u de ingeschakelde replica wilt verbinden met een netwerk. De replica wordt standaard verbonden met hetzelfde netwerk als de oorspronkelijke machine.
5. [Optioneel] Als u ervoor kiest de replica te verbinden met het netwerk, schakelt u het selectievakje **Oorspronkelijke virtuele machine stoppen** uit, zodat de oorspronkelijke machine online blijft.
6. Klik op **Starten**.

Terwijl de replica een failoverstatus heeft, kunt u een van de volgende acties kiezen:

- **Failover stoppen**
  Stop de failover als de oorspronkelijke machine is hersteld. De replica wordt uitgeschakeld. Replicatie wordt hervat.
- **Permanente failover naar de replica uitvoeren**
  Met deze directe bewerking wordt de replicavlag verwijderd van de virtuele machine, zodat replicatie niet meer mogelijk is. Als u replicatie wilt hervatten, opent u het replicatieschema en selecteert u deze machine als bron.
- **Failback**
  Failback is nodig als de failover is uitgevoerd naar een site die niet is bedoeld voor continue uitvoering. De replica wordt hersteld naar de oorspronkelijke of naar een nieuwe virtuele machine. Wanneer de oorspronkelijke machine weer is hersteld, wordt deze ingeschakeld en wordt replicatie hervat. Als u naar een nieuwe machine wilt herstellen, opent u het replicatieschema en selecteert u deze machine als bron.

Failover stoppen...

Een failover stoppen

1. Selecteer een replica die een failoverstatus heeft.
2. Klik op **Replica-acties**.
3. Klik op **Failover stoppen**.
4. Bevestig uw beslissing.

Permanente failover uitvoeren

Een permanente failover uitvoeren

1. Selecteer een replica die een failoverstatus heeft.
2. Klik op **Replica-acties**.
3. Klik op **Permanente failover**.
4. [Optioneel] Wijzig de naam van de virtuele machine.
5. [Optioneel] Schakel het selectievakje **Oorspronkelijke virtuele machine stoppen** in.
6. Klik op **Starten**.

Failback uitvoeren

Failback van replica uitvoeren

1. Selecteer een replica die een failoverstatus heeft.
2. Klik op **Replica-acties**.
3. Klik op **Failback van replica**.
   In de software wordt automatisch de oorspronkelijke machine geselecteerd als doelmachine.
4. [Optioneel] Klik op **Doelmachine** en doe het volgende:
   a. Selecteer of u de failback wilt uitvoeren naar een nieuwe of bestaande machine.
   b. Selecteer de ESXi-host en geef de naam van de nieuwe machine op, of selecteer een bestaande machine.
   c. Klik op **OK**.
5. [Optioneel] Wanneer u een failback uitvoert naar een nieuwe machine, kunt u ook als volgt te werk gaan:
   - Klik op **Gegevensopslag** en selecteer de gegevensopslag voor de virtuele machine.
   - Klik op **VM-instellingen** om de geheugengrootte, het aantal processors en de netwerkverbindingen van de virtuele machine te wijzigen.
6. [Optioneel] Klik op **Herstelopties** om de failbackopties te wijzigen.
7. Klik op **Herstel starten**.
8. Bevestig uw beslissing.

Replicatieopties

Als u de replicatieopties wilt wijzigen, klikt u op het tandwielpictogram naast de naam van het replicatieschema en klikt u vervolgens op **Replicatieopties**.

Changed Block Tracking (CBT, gewijzigde blokken bijhouden)

Deze optie is vergelijkbaar met de back-upoptie Changed Block Tracking (CBT).

Schijfinrichting

Met deze optie definieert u de schijfinrichtingsinstellingen voor de replica.

De vooraf ingestelde waarde is: **Thin provisioning**.

De volgende waarden zijn beschikbaar: **Thin provisioning**, **Thick provisioning**, **De oorspronkelijke instelling behouden**.

Foutafhandeling

Deze optie is vergelijkbaar met de back-upoptie Foutafhandeling.

Aangepaste opdrachten

Deze optie is vergelijkbaar met de back-upoptie Aangepaste opdrachten.

Volume Shadow Copy Service VSS voor virtuele machines

Deze optie is vergelijkbaar met de back-upoptie Volume Shadow Copy Service VSS voor virtuele machines.

Failbackopties

Als u de failbackopties wilt wijzigen, klikt u op **Herstelopties** wanneer u de failback configureert.

Foutafhandeling

Deze optie is vergelijkbaar met de hersteloptie 'Foutafhandeling'.

Prestaties

Deze optie is vergelijkbaar met de hersteloptie 'Prestaties'.

Aangepaste opdrachten

Deze optie is vergelijkbaar met de hersteloptie 'Aangepaste opdrachten'.

Energiebeheer van VM's

Deze optie is vergelijkbaar met de hersteloptie 'Energiebeheer van VM's'.

Seeding van een eerste replica

Als u replicatie naar een externe locatie wilt versnellen en netwerkbandbreedte wilt besparen, kunt u replica seeding gebruiken.

Belangrijk
Als u replica seeding wilt uitvoeren, moet Agent voor VMware (Virtual Appliance) worden uitgevoerd op de doel-ESXi.

Seeding van een eerste replica

1. Voer een van de volgende handelingen uit:
   - Als u de oorspronkelijke virtuele machine kunt uitschakelen, dan schakelt u deze uit en gaat u verder met stap 4.
   - Als u de oorspronkelijke virtuele machine niet kunt uitschakelen, gaat u verder met de volgende stap.
2. Maak een replicatieschema.

   Wanneer u het schema maakt, selecteert u bij **Doelmachine** de optie **Nieuwe replica** en de ESXi waarop de oorspronkelijke machine wordt gehost.
3. Voer het schema één keer uit.

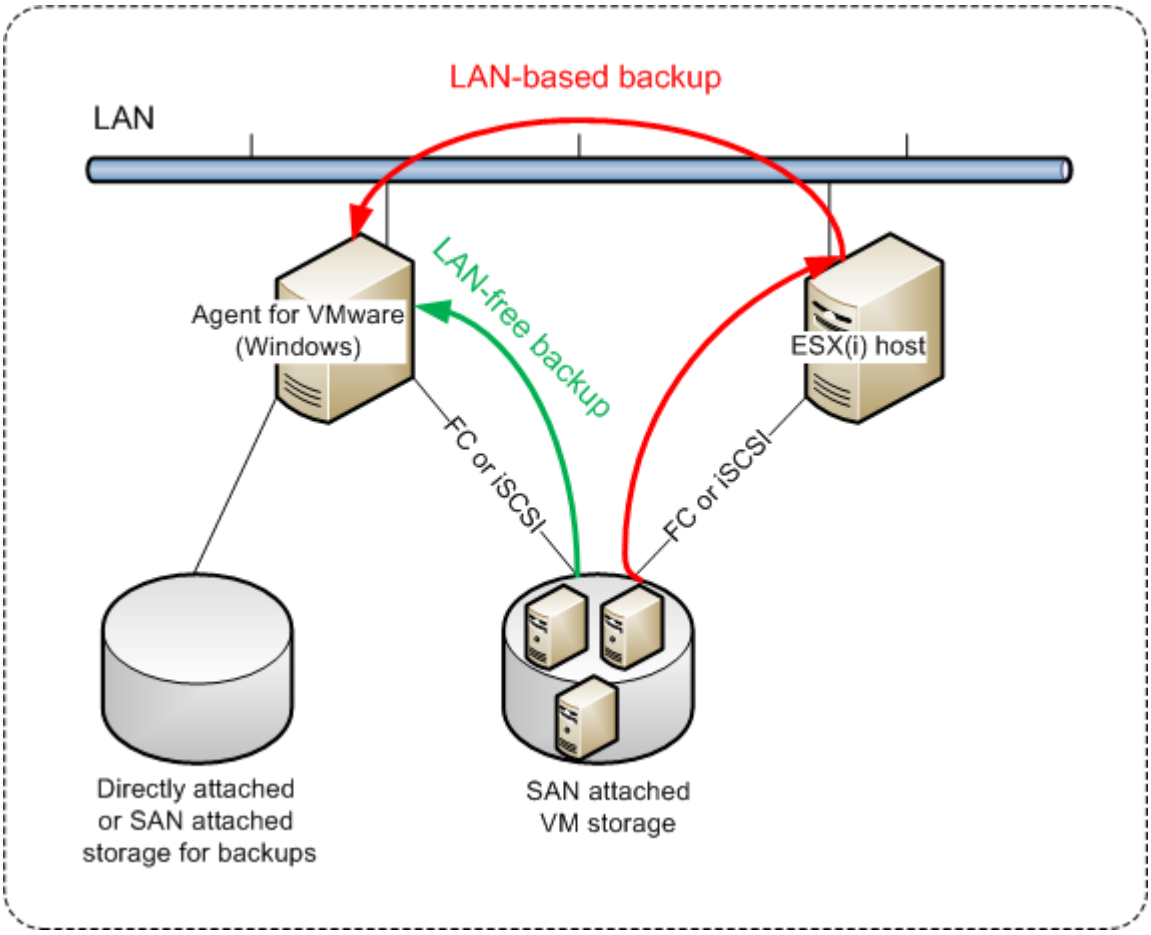
   Er wordt een replica gemaakt op de oorspronkelijke ESXi.
4. Exporteer de bestanden van de virtuele machine (of de replica) naar een externe harde schijf.
   a. Verbind de externe harde schijf met de machine waarop vSphere Client wordt uitgevoerd.
   b. Verbind vSphere Client met de oorspronkelijke vCenter\ESXi.
   c. Selecteer de nieuw gemaakte replica in de inventaris.
   d. Klik op **Bestand** > **Exporteren** > **OVF-sjabloon exporteren**.
   e. Geef bij **Directory** de map op de externe harde schijf op.
   f. Klik op **OK**.
5. Breng de harde schijf over naar de externe locatie.
6. Importeer de replica naar de doel-ESXi.
   a. Verbind de externe harde schijf met de machine waarop vSphere Client wordt uitgevoerd.
   b. Verbind vSphere Client met de doel-vCenter\ESXi.
   c. Klik op **Bestand** > **OVF-sjabloon implementeren**.
   d. Geef bij **Implementeren vanaf een bestand of URL** de sjabloon op die u hebt geëxporteerd in stap 4.
   e. Voltooi de importprocedure.
7. Bewerk het replicatieschema dat u hebt gemaakt in stap 2. Selecteer bij **Doelmachine** de optie **Bestaande replica** en selecteer vervolgens de geïmporteerde replica.

Het resultaat is dat de software de replica blijft bijwerken. Alle replicaties zijn incrementeel.

Agent voor VMware – back-up zonder LAN

Als voor uw ESXi een opslag wordt gebruikt die is gekoppeld via SAN, installeert u de agent op een machine die is aangesloten op hetzelfde SAN. De agent maakt rechtstreeks vanuit de opslag een back-up van de virtuele machines en niet via de ESXi-host en het LAN. Deze mogelijkheid wordt een back-up zonder LAN genoemd.

In het diagram ziet u een back-up met of zonder LAN. Toegang tot virtuele machines zonder gebruik te maken van LAN is beschikbaar als u een Fibre Channel (FC) of iSCSI Storage Area Network hebt. Als u helemaal geen gegevens van back-ups meer wilt overdragen via LAN, kunt u de back-ups opslaan op een lokale schijf van de machine met de agent of op een via SAN gekoppelde opslag.



Directe toegang tot gegevensopslag mogelijk maken voor een agent

1. Installeer Agent voor VMware op een Windows-machine met netwerktoegang tot de vCenter Server.
2. Verbind het LUN (Logical Unit Number) dat de gegevensopslag host, met de machine. Houd hierbij rekening met het volgende:
   - Gebruik hetzelfde protocol (d.w.z. iSCSI of FC) als voor de verbinding tussen de gegevensopslag en ESXi.
   - Het LUN *moet niet* worden geïnitialiseerd en moet worden weergegeven als 'offline' schijf in **Schijfbeheer**. Als Windows het LUN initialiseert, wordt dit mogelijk beschadigd en kan het niet meer worden gelezen door VMware vSphere.

Dit leidt ertoe dat de agent de SAN-transportmodus zal gebruiken om toegang te krijgen tot de virtuele schijven, dat wil zeggen dat raw LUN-sectoren via iSCSI/FC worden gelezen zonder dat het VMFS-bestandssysteem wordt herkend (en Windows detecteert dit niet).

Beperkingen

- In vSphere 6.0 en later kan de agent geen gebruik maken van de SAN-transportmodus als sommige VM-schijven zich wel en andere niet op een VMware Virtual Volume (VVol) bevinden. Back-ups van dergelijke virtuele machines zullen mislukken.

- Back-ups van versleutelde virtuele machines, beschikbaar vanaf VMware vSphere 6.5, worden gemaakt via LAN, zelf als u de SAN-transportmodus configureert voor de agent. De agent maakt dan gebruik van NBD-transport, want VMware biedt geen ondersteuning voor SAN-transport voor het maken van back-ups van versleutelde virtuele schijven.

Voorbeeld

Als u een iSCSI SAN gebruikt, configureert u de iSCSI-initiator op de machine met Windows waarop Agent voor VMware is geïnstalleerd.

SAN-beleid configureren

1. Meld u aan als beheerder, open de opdrachtprompt, typ `diskpart` en druk vervolgens op **Enter**.
2. Typ `san` en druk vervolgens op **Enter**. Controleer of **SAN-beleid: Offline Alles** wordt weergegeven.
3. Als er een andere waarde is ingesteld voor SAN-beleid:
   a. Typ `san policy=offlineall`.
   b. Druk op **Enter**.
   c. Voer stap 2 uit om te controleren of de instelling correct is toegepast.
   d. Start de machine opnieuw op.

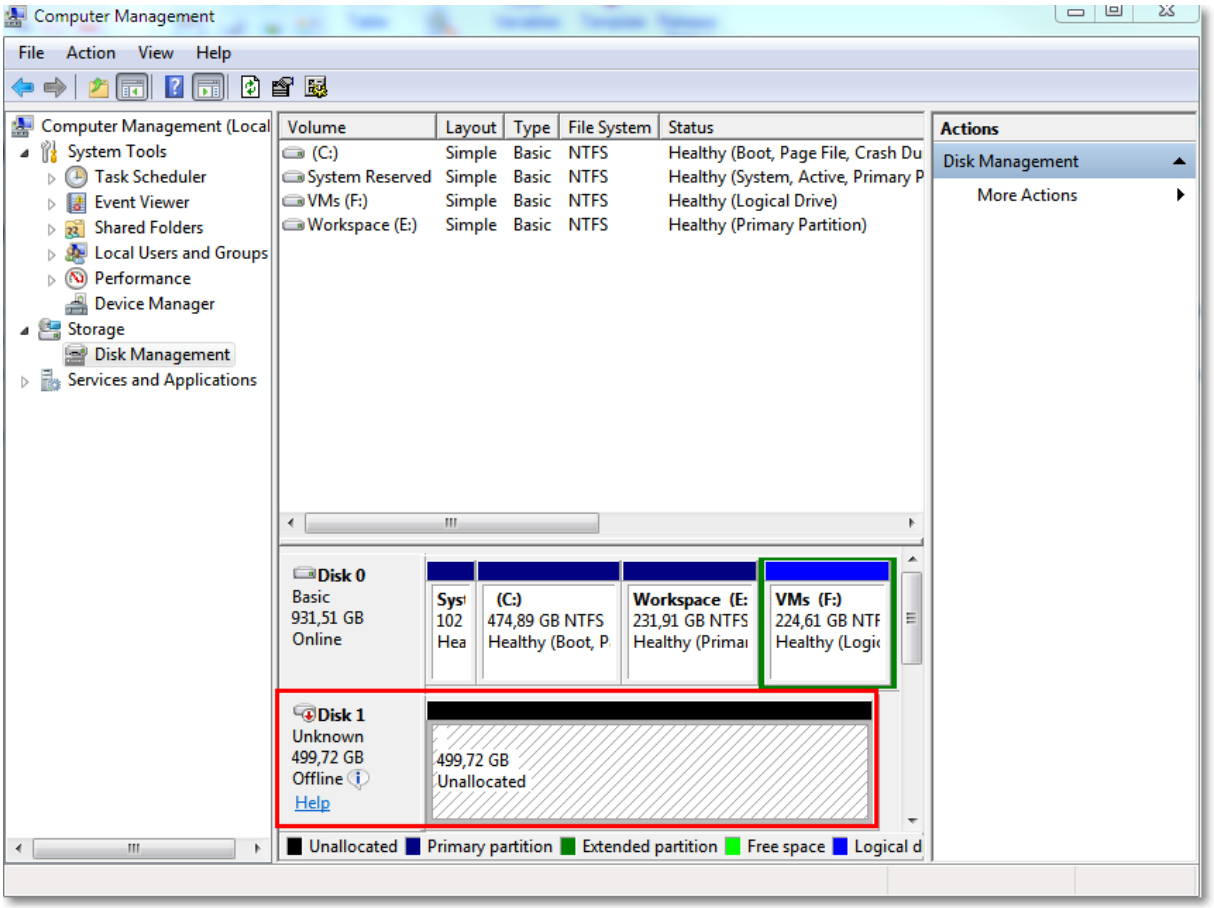
Een iSCSI-initiator configureren

1. Ga naar **Configuratiescherm** > **Systeembeheer** > **iSCSI-initiator**.

   Opmerking
   Indien nodig, kunt u de applet **Systeembeheer** vinden door de weergave van het **Configuratiescherm** in te stellen op iets anders dan **Startpagina** of **Categorie**, of u kunt de zoekfunctie gebruiken.

2. Als u Microsoft iSCSI-initiator voor het eerst opent, bevestigt u dat u de service Microsoft iSCSI-initiator wilt starten.
3. Ga naar het tabblad **Doelen**, typ de Fully Qualified Domain Name (FQDN) of het IP-adres van het SAN-doelapparaat en klik vervolgens op **Snel verbinding maken**.
4. Selecteer het LUN dat de gegevensopslag host en klik op **Verbinden**.
   Als het LUN niet wordt weergegeven, controleert u of de zonering op het iSCSI-doel toegang tot het LUN mogelijk maakt voor de machine met de agent. De machine moet worden toegevoegd aan de lijst met toegestane iSCSI-initiators op dit doel.
5. Klik op **OK**.

In **Schijfbeheer** moet dan het SAN LUN worden weergegeven dat gereed is (zie schermafbeelding).



Een lokaal gekoppelde opslag gebruiken

U kunt een aanvullende schijf koppelen aan Agent voor VMware (Virtual Appliance), zodat de agent back-ups kan maken naar deze lokaal gekoppelde opslag. Met deze aanpak is er geen netwerkverkeer tussen de agent en de back-uplocatie.

Een virtuele toepassing die wordt uitgevoerd op dezelfde host of in hetzelfde cluster als de virtuele machines waarvan een back-up is gemaakt, heeft rechtstreeks toegang tot de gegevensopslag waar de machine zich bevindt. Dit betekent dat de toepassing de schijven waarvan een back-up is gemaakt, kan koppelen via HotAdd-transport, waardoor het back-upverkeer van de ene lokale schijf naar een andere wordt geleid. Als de gegevensopslag is verbonden als **Schijf/LUN** in plaats van **NFS**, wordt voor de back-up geen gebruik gemaakt van LAN. In het geval van NFS-gegevensopslag is er dan geen netwerkverkeer tussen de gegevensopslag en de host.

Het gebruik van een lokaal gekoppelde opslag gaat ervan uit dat de agent altijd back-ups van dezelfde machines maakt. Als er meerdere agents werken in de vSphere en een of meer daarvan lokaal gekoppelde opslag gebruiken, moet u elke agent handmatig verbinden aan alle machines waarvan back-ups gemaakt moeten worden. Als de machines door de beheerserver worden herverdeeld tussen de agents, worden de back-ups van een machine mogelijk verdeeld over meerdere opslagruimten.

U kunt de opslag toevoegen aan een al werkende agent of wanneer u de agent implementeert vanaf een OVF-sjabloon.

Een opslag koppelen aan een al werkende agent

1. Klik in de inventaris van VMware vSphere met de rechtermuisknop op Agent voor VMware (Virtual Appliance).
2. U kunt de schijf toevoegen door de instellingen van de virtuele machine te bewerken. De grootte van de schijf moet ten minste 10 GB zijn.

   Waarschuwing!
   Wees voorzichtig wanneer u een reeds bestaande schijf toevoegt. Wanneer de opslag is gemaakt, gaan alle oudere gegevens op die schijf verloren.

3. Ga naar de console van de virtuele toepassing. De link **Opslag maken** is beschikbaar aan de onderzijde van het scherm. Als dit niet het geval is, klik u op **Vernieuwen**.
4. Klik op de link **Opslag maken**, selecteer de schijf en geef een naam op voor de schijf. Door beperkingen van het bestandssysteem mag de labelnaam uit maximaal 16 tekens bestaan.

Een lokaal gekoppelde opslag selecteren als back-updoel

- Wanneer u een beschermingsschema maakt, selecteert u in **Locatie van back-up** de optie **Lokale mappen** en typt u de aanduiding die overeenkomt met de lokaal gekoppelde opslag, bijvoorbeeld **D:**.

Opmerking
Locally Attached Storage (LAS) is ontworpen voor relatief kleine omgevingen met een enkele agent (virtueel apparaat). We hebben Locally Attached Storage-eenheden tot 5 TB getest. U kunt op eigen risico grotere schijven koppelen, maar dergelijke configuraties worden niet ondersteund. We raden u aan om andere typen opslag te gebruiken voor meer dan 5 TB aan back-upgegevens. U kunt bijvoorbeeld een virtuele VMware-schijf maken, deze koppelen aan een willekeurige virtuele machine, een netwerkshare maken `op de schijf en deze vervolgens gebruiken als back-upbestemming in plaats van een LAS.

Binding van virtuele machines

Dit gedeelte bevat een overzicht van de manier waarop de werking van meerdere agenten in VMware vCenter wordt georganiseerd door de Cyber Protection-service.

De onderstaande distributiealgoritme werkt zowel voor virtuele toepassingen als voor agents die zijn geïnstalleerd in Windows.

Distributiealgoritme

De virtuele machines worden automatisch gelijkmatig gedistribueerd tussen Agents voor VMware. Met gelijkmatig wordt bedoeld dat elke agent een gelijk aantal machines beheert. De hoeveelheid opslagruimte die door een virtuele machine wordt ingenomen, is niet meegerekend.

Als de software echter een agent voor een machine kiest, probeert deze de algemene systeemprestaties te optimaliseren. De software let met name op de locatie van de agent en de virtuele machine. De voorkeur gaat uit naar een agent die gehost wordt op dezelfde host. Als er geen agent op dezelfde host te vinden is, heeft een agent in hetzelfde cluster de voorkeur.

Zodra een virtuele machine aan een agent is toegewezen, worden alle back-ups van de machine aan deze agent gedelegeerd.

Herdistributie

Telkens als de bestaande balans wordt verstoord, treedt er herdistributie op, of preciezer gezegd: als de balansverstoring van de belasting onder de agents 20 procent bereikt. Dit kan gebeuren als er een machine of een agent wordt toegevoegd of verwijderd, als een machine migreert naar een andere host of een ander cluster of als u een machine handmatig aan een agent bindt. Als dit gebeurt, worden de machines met dezelfde algoritme opnieuw gedistribueerd door de Cyber Protection-service.

UU beseft bijvoorbeeld dat u meer agents nodig hebt om te helpen met de doorvoer en met het implementeren van een extra virtuele toepassing in het cluster. De meest geschikte machines worden door de Cyber Protection-service toegewezen aan de nieuwe agent. De belasting van de oude agents wordt minder.

Wanneer u een agent uit de Cyber Protection-service verwijdert, worden de machines die aan de agent zijn toegewezen, gedistribueerd onder de resterende agenten. Dit gebeurt echter niet als een agent beschadigd raakt of handmatig wordt verwijderd uit vSphere. De herdistributie begint pas als nadat u die agent uit de webinterface hebt verwijderd.

Het distributieresultaat weergeven

U kunt het resultaat van de automatische distributie bekijken:

- in de kolom **Agent** voor elke virtuele machine in het gedeelte **Alle apparaten**
- in het gedeelte **Toegewezen virtuele machines** van het deelvenster **Details** als er een agent is geselecteerd in het gedeelte **Instellingen** > **Agents**

Handmatige binding

Door de Agent voor VMware-binding kunt u een virtuele machine uitsluiten van het distributieproces; hiertoe geeft u de agent op die altijd back-ups van deze machine moet maken. De algemene balans wordt behouden, maar deze specifieke machine kan alleen aan een andere agent worden doorgegeven als de oorspronkelijke agent is verwijderd.

Een binding maken van een virtuele machine met een agent

1. Selecteer de machine.
2. Klik op **Details**.

   In het gedeelte **Toegewezen agent** geeft de software de agent weer die momenteel de geselecteerde machine beheert.

3. Klik op **Wijzigen**.
4. Selecteer **Handmatig**.
5. Selecteer de agent waarvoor u een binding met de machine wilt maken.
6. Klik op **Opslaan**.

Een binding van een machine aan een agent ongedaan maken

1. Selecteer de machine.
2. Klik op **Details**.
   In het gedeelte **Toegewezen agent** geeft de software de agent weer die momenteel de geselecteerde machine beheert.
3. Klik op **Wijzigen**.
4. Selecteer **Automatisch**.
5. Klik op **Opslaan**.

Automatische toewijzing uitschakelen voor een agent

U kunt het automatisch toewijzen uitschakelen voor Agent voor VMware en deze uitsluiten van het distributieproces door de lijst met machines op te geven waarvan de agent back-ups moet maken. De algemene balans wordt onderhouden tussen andere agents.

Automatische toewijzing kan niet worden uitgeschakeld voor een agent als er geen andere geregistreerde agents zijn of als automatische toewijzing is uitgeschakeld voor alle andere agents.

Automatische toewijzing uitschakelen voor een agent

1. Klik op **Instellingen** > **Agenten**.
2. Selecteer Agent voor VMware waarvoor u automatische toewijzing wilt uitschakelen.
3. Klik op **Details**.
4. Zet de schakelaar **Automatische toewijzing** uit.

Voorbeelden van gebruik

- Handmatige binding is handig als u back-ups van een bepaalde (erg grote) machine wilt maken met Agent voor VMware (Windows) via een Fibre Channel terwijl er back-ups van andere machines worden gemaakt door virtuele apparaten.
- Het is noodzakelijk VM's te verbinden met een agent als de agent een lokaal gekoppelde opslag heeft.
- Door de automatische toewijzing uit te schakelen zorgt u dat er back-ups van een bepaalde machine worden gemaakt volgens het schema dat u opgeeft. De agent die alleen back-ups van één VM maakt, kan zich niet bezighouden met het maken van back-ups van andere VM's als het schema dit aangeeft.
- Het uitschakelen van de automatische toewijzing is handig als u meerdere ESXi-hosts hebt die geografisch gescheiden zijn. Als u de automatische toewijzing uitschakelt en vervolgens de VM's

bindt aan alle hosts van de agent die op dezelfde host wordt uitgevoerd, kunt u zorgen dat de agent nooit back-ups maakt van machines die actief zijn op de externe ESXi-hosts, zodat het netwerkverkeer wordt verminderd.

Automatisch uitvoeren van scripts voorafgaand aan stilzetten en na afloop van reactivering

Met VMware Tools kunt u automatisch aangepaste scripts voorafgaand aan stilzetten en na afloop van reactivering uitvoeren op virtuele machines waarvan u een back-up maakt in de modus zonder agent. Zo kunt u bijvoorbeeld aangepaste scripts voor stillegging uitvoeren en applicatieconsistente back-ups maken voor virtuele machines waarop toepassingen worden uitgevoerd die niet compatibel zijn met VSS.

Vereisten

De scripts voorafgaand aan stilzetten en na afloop van reactivering moeten zijn opgeslagen in een specifieke map op de virtuele machine.

- De locatie van deze map voor virtuele Windows-machines hangt af van de ESXi-versie van de host.

  De map voor virtuele machines die worden uitgevoerd op een ESXi 6.5-host, is bijvoorbeeld: `C:\Program Files\VMware\VMware Tools\backupScripts.d\`. U moet de map `backupScritps.d` handmatig maken. Sla geen andere typen bestanden op in deze map, omdat VMware Tools hierdoor instabiel kan worden.

  Raadpleeg de VMware-documentatie voor meer informatie over de locatie van de scripts voorafgaand aan stilzetten en na afloop van reactivering voor andere ESXi-versies.
- Voor virtuele Linux-machines kopieert u uw scripts respectievelijk naar de mappen `/usr/sbin/pre-freeze-script` en `/usr/sbin/post-thaw-script`. De scripts in `/usr/sbin/pre-freeze-script` worden uitgevoerd wanneer u een momentopname maakt en de scripts in `/usr/sbin/post-thaw-script` worden uitgevoerd wanneer de momentopname is voltooid. De scripts moeten kunnen worden uitgevoerd door de VMware Tools-gebruiker.

Scripts voorafgaand aan stilzetten en na afloop van reactivering automatisch uitvoeren

1. Controleer of VMware Tools is geïnstalleerd op de virtuele machine.
2. Plaats uw aangepaste scripts in de vereiste map op de virtuele machine.
3. Schakel in het beschermingsschema voor deze machine de optie **Volume Shadow Copy Service (VSS) voor virtuele machines** in.

   Hierdoor wordt er een VMware-momentopname gemaakt terwijl de optie **Gastbestandssysteem stilleggen** is ingeschakeld, waardoor de scripts voorafgaand aan stilzetten en na afloop van reactivering worden geactiveerd op de virtuele machine.

U hoeft geen aangepaste scripts voor stillegging uit te voeren op virtuele machines met toepassingen die compatibel zijn met VSS, zoals Microsoft SQL Server of Microsoft Exchange. Als u

een applicatieconsistente back-up voor dergelijke machines wilt maken, schakelt u de optie **Volume Shadow Copy Service (VSS) voor virtuele machines** in het beschermingsschema in.

Ondersteuning voor de migratie van virtuele machines

Deze sectie bevat informatie over de migratie van virtuele machines binnen een vSphere-omgeving, inclusief migratie tussen ESXi-hosts die deel uitmaken van een vSphere-cluster.

Met vMotion kunnen de status en configuratie van een virtuele machine worden verplaatst naar een andere host terwijl de schijven van de machine op dezelfde locatie in een gedeelde opslag blijven. Met Storage vMotion kunnen schijven van virtuele machines worden verplaatst naar een andere gegevensopslag.

- Migratie met vMotion, inclusief Storage vMotion, wordt niet ondersteund voor een virtuele machine waarop Agent voor VMware (Virtual Appliance) wordt uitgevoerd, en wordt automatisch uitgeschakeld. Deze virtuele machine wordt toegevoegd aan de lijst **VM-overschrijvingen** in de vSphere-clusterconfiguratie.
- Wanneer een back-up van een virtuele machine start, wordt migratie met vMotion, inclusief Storage vMotion, automatisch uitgeschakeld. Deze virtuele machine wordt tijdelijk toegevoegd aan de lijst **VM-overschrijvingen** in de vSphere-clusterconfiguratie. Wanneer de back-up is voltooid, worden de instellingen voor **VM-overschrijvingen** automatisch teruggezet naar hun vorige status.
- Er kan geen back-up worden gestart voor een virtuele machine zolang de migratie met vMotion, inclusief Storage vMotion, nog wordt uitgevoerd. De back-up voor deze machine wordt gestart wanneer de migratie is voltooid.

Bescherming van virtualisatieomgevingen

In de Cyber Protect-console kunt u de vSphere-, Hyper-V- en Virtuozzo-omgeving bekijken in de oorspronkelijke presentatie. Wanneer u de betreffende agent hebt geïnstalleerd en geregistreerd, wordt het tabblad **VMware**, **Hyper-V** of **Virtuozzo** weergegeven onder **Apparaten**.

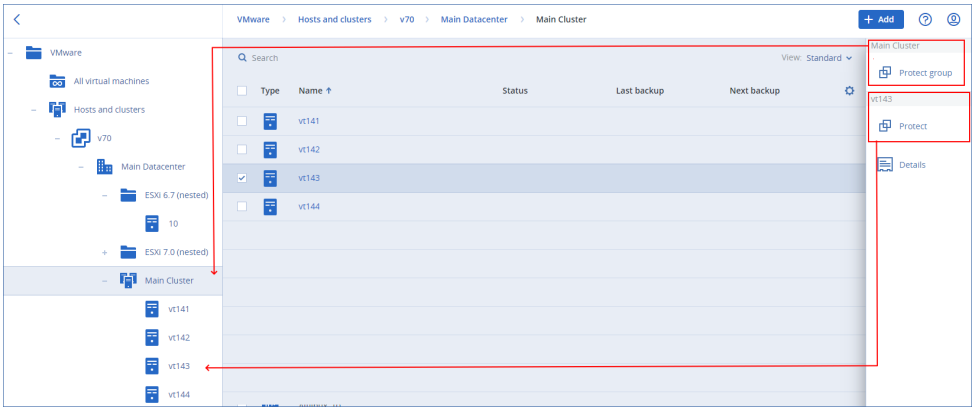
Op het tabblad **VMware** kunt u bijvoorbeeld een back-up maken van de volgende vSphere-infrastructuur objecten:

- vCenter
- Datacenter
- Map
- Cluster
- ESXi-host
- Resourcegroep
- Virtuele machine

Als u een plan wilt toepassen op een geselecteerd infrastructuurobject, klikt u op **Beschermen**. Er wordt een back-up gemaakt van alle onderliggende objecten.

Als u een plan wilt toepassen op het bovenliggende object van het geselecteerde infrastructuurobject, klikt u op **Groep beschermen**. Er wordt een back-up gemaakt van alle onderliggende objecten van het bovenliggende object.

Als u een plan bijvoorbeeld toepast op een ESXi-host, wordt er een back-up gemaakt van alle virtuele machines op de host. Als u een plan toepast op het bovenliggende cluster, wordt er een back-up gemaakt van alle virtuele machines op alle hosts in dit cluster.



Back-upstatus bekijken in vSphere Client

U kunt de back-upstatus en de laatste back-uptijd van een virtuele machine bekijken in vSphere Client.

Deze informatie vindt u in de samenvatting van de virtuele machine (**Overzicht** > **Aangepaste kenmerken**/**Aantekeningen**/**Opmerkingen**, afhankelijk van het type client en de vSphere-versie). U kunt ook de kolommen **Laatste back-up** en **Back-upstatus** op het tabblad **Virtuele machines** inschakelen voor een host, datacenter, map, resourcegroep of voor de hele vCenter-server.

Agent voor VMware moet, naast de rechten die zijn beschreven in 'Agent voor VMware - vereiste rechten', over de volgende rechten beschikken om deze kenmerken te leveren:

- **Algemeen** > **Aangepaste kenmerken beheren**
- **Algemeen** > **Aangepast kenmerk instellen**

Vereiste bevoegdheden voor Agent voor VMware

Opmerking
Als u back-ups van virtuele machines wilt maken, installeert u vStorage API's op de ESXi-host. Voor meer informatie: zie dit Knowledge Base-artikel.

Agent voor VMware voert de verificatie uit bij vCenter of de ESXi-host via een gebruikersaccount dat is opgegeven tijdens de implementatie van de agent. Het gebruikersaccount moet een rol hebben die de bevoegdheden bevat die in de onderstaande tabel worden vermeld. We raden aan om een

speciaal account en speciale rol te gebruiken in plaats van een bestaand account met de beheerdersrol.

Het gebruikersaccount moet machtigingen hebben voor toegang tot alle niveaus van de vSphere-infrastructuur, zoals vCenter, datacenters, clusters, ESXi-hosts, resourcegroepen en virtuele machines. Voor informatie over hoe u een machtiging toevoegt op vCenter-niveau en deze naar de andere niveaus doorgeeft: zie "Toegangsmachtiging verlenen aan het gebruikersaccount" (p. 740).

U kunt het gebruikersaccount dat wordt gebruikt door Agent voor VMware, wijzigen zonder de agent opnieuw te implementeren. Voor informatie over hoe u het account kunt wijzigen: zie "Het gebruikersaccount voor Agent voor VMware wijzigen" (p. 741).

Object	Recht	Bewerking			
		Back-up maken van een VM	**Herstellen naar een nieuwe VM**	**Herstellen naar een bestaande VM**	**VM uitvoeren vanaf een back-up**
Cryptografische bewerkingen (vanaf vSphere 6.5)					
	Schijf toevoegen	+*			
	Directe toegang	+*			
Gegevensopslag					
	Ruimte toewijzen		+	+	+
	Bladeren in gegevensopslag				+
	Gegevensopslag configureren	+	+	+	+
	Bestandsbewerkingen op laag niveau				+
Algemeen					
	Methoden uitschakelen	+	+	+	
	Methoden inschakelen	+	+	+	
	Licenties	+	+	+	+

Object	Recht	Bewerking			
		Back-up maken van een VM	Herstellen naar een nieuwe VM	Herstellen naar een bestaande VM	VM uitvoeren vanaf een back-up
	Aangepaste kenmerken beheren	+	+	+	
	Aangepast kenmerk instellen	+	+	+	
Host > **Configuratie**					
	Opslagpartitie configureren				+
	Cluster wijzigen				
Host > **Lokale bewerkingen**					
	Virtuele machine maken				+
	Virtuele machine verwijderen				+
	Virtuele machine opnieuw configureren				+
Netwerk					
	Netwerk toewijzen		+	+	+
Resource					
	Virtuele machine toewijzen aan resourcegroep		+	+	+
Virtuele machine > **Configuratie wijzigen**					
	Schijflease ophalen	+		+	

Object	Recht	Bewerking			
		Back-up maken van een VM	Herstellen naar een nieuwe VM	Herstellen naar een bestaande VM	VM uitvoeren vanaf een back-up
	Bestaande schijf toevoegen	+	+		+
	Nieuwe schijf toevoegen		+	+	+
	Apparaat toevoegen of verwijderen		+		+
	Geavanceerde configuratie	+	+	+	
	Aantal CPU's wijzigen		+		
	Geheugen wijzigen		+		
	Instellingen wijzigen		+	+	+
	Resource wijzigen	+	+		
	Apparaatinstellingen wijzigen	+	+		
	Schijf verwijderen	+	+	+	+
	Naam wijzigen		+		
	Aantekening instellen				+
	Bijhouden van schijfwijzigingen in- of uitschakelen	+		+	
Virtuele machine > Gastbewerkingen					
	Wijzigingen van gastbewerking	+**			
	Uitvoering van programma voor	+**			

Object	Recht	Bewerking			
		Back-up maken van een VM	**Herstellen naar een nieuwe VM**	**Herstellen naar een bestaande VM**	**VM uitvoeren vanaf een back-up**
	gastbewerkingen				
	Zoekopdrachten voor gastbewerking	+**			
Virtuele machine > **Interactie**					
	Ticket voor gastbesturing ophalen (in vSphere 4.1 en 5.0)				+
	Cd-media configureren		+	+	
	Gastbesturingssysteem beheren met VIX API (in vSphere 5.1 en later)				+
	Uitschakelen			+	+
	Inschakelen		+	+	+
Virtuele machine > **Inventaris**					
	Maken vanaf bestaande		+	+	+
	Nieuwe maken		+	+	+
	Registreren				+
	Verwijderen		+	+	+
	Registratie ongedaan maken				+
Virtuele machine >					

Object	Recht	Bewerking			
		Back-up maken van een VM	**Herstellen naar een nieuwe VM**	**Herstellen naar een bestaande VM**	**VM uitvoeren vanaf een back-up**
Provisioning					
	Schijftoegang toestaan		+	+	+
	Schijftoegang met alleen-lezen toestaan	+		+	
	Download van virtuele machine toestaan	+	+	+	+
Virtuele machine > **Status** **Virtuele machine** > **Beheer van momentopnamen** (vSphere 6.5 en later)					
	Momentopname maken	+		+	+
	Momentopname verwijderen	+		+	+
vApp					
	Virtuele machine toevoegen				+

* Deze bevoegdheid is alleen vereist voor het maken van back-ups van versleutelde machines.

** Deze bevoegdheid is alleen vereist voor applicatiegerichte back-ups.

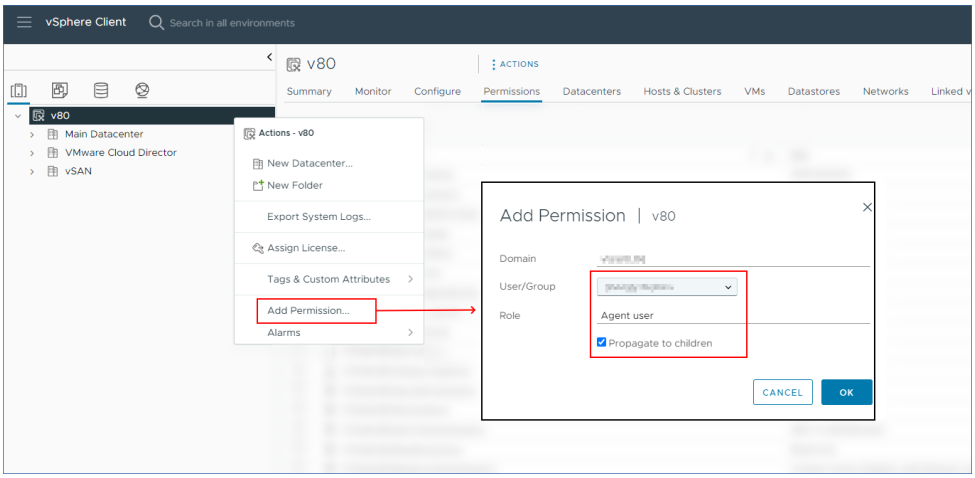
Toegangsmachtiging verlenen aan het gebruikersaccount

Het gebruikersaccount dat wordt gebruikt door Agent voor VMware, moet toegang hebben tot alle niveaus van de vSphere-infrastructuur, zoals vCenter, datacenters, clusters, ESXi-hosts, resourcegroepen en virtuele machines.

Toegangsrechten verlenen aan het gebruikersaccount:

1. Ga in vSphere Client naar **Inventaris**.
2. Klik met de rechtermuisknop op het **vCenter**-object waarvoor u een machtiging wilt verlenen en klik vervolgens op **Machtiging toevoegen**.
3. Ga naar het dialoogvenster **Machtiging toevoegen** en selecteer een gebruikersaccount en een rol.

   De rol moet de bevoegdheden bevatten die zijn vermeld in "Vereiste bevoegdheden voor Agent voor VMware" (p. 735).
4. Schakel het vakje **Doorgeven aan onderliggende items** in.
5. Klik op **OK**.



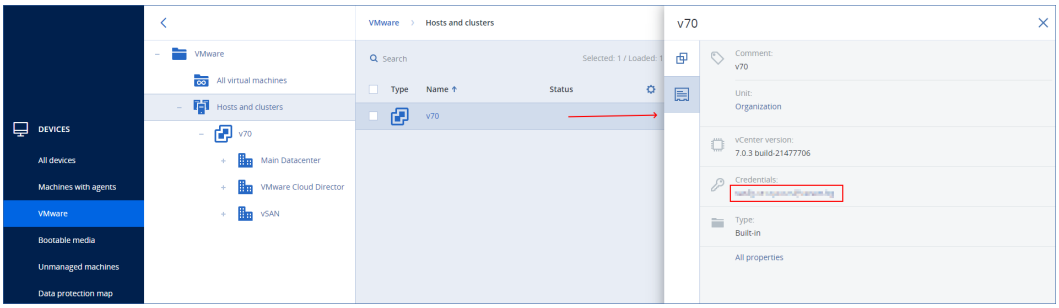
Het gebruikersaccount voor Agent voor VMware wijzigen

In de Cyber Protect-console kunt u het gebruikersaccount voor een afzonderlijke agent, of voor alle agenten, wijzigen op vCenter of een ESXi-host.

Het gebruikersaccount voor Agent voor VMware wijzigen:

Voor alle agents

1. Ga in de Cyber Protect-console naar **Apparaten** > **VMware**.
2. Klik op **Hosts en clusters**.
3. Klik in het hoofdpaneel op de lege ruimte naast de naam van vCenter of de stand-alone ESXi-host.
4. Klik in het rechterpaneel op **Details**.
5. Klik onder **Referenties** op het gebruikersaccount.

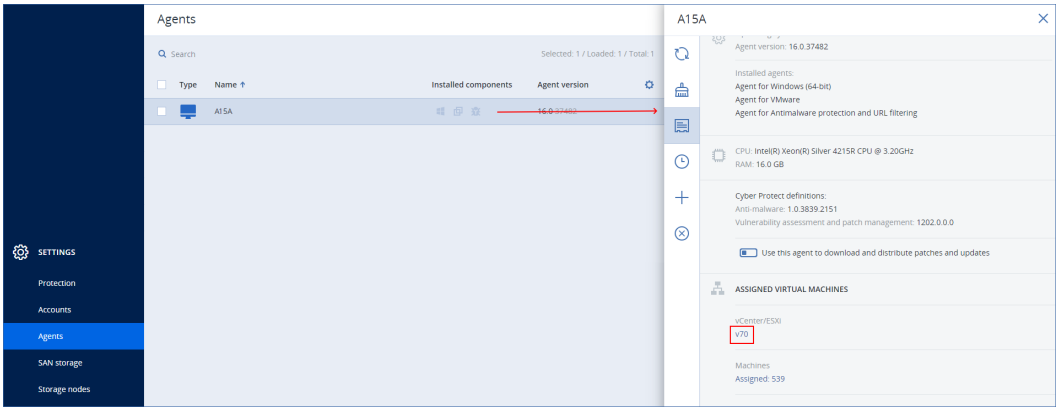


6. Geef het nieuwe gebruikersaccount en het wachtwoord voor dat account op.
7. Klik op **OK**.

Hierdoor zullen alle agents op deze vCenter of ESXi-host het nieuwe gebruikersaccount gebruiken.

Voor een afzonderlijke agent

1. Ga in de Cyber Protect-console naar **Instellingen** > **Agents**.
2. Selecteer de agent.
3. Klik in het rechterpaneel op **Details**.
4. Klik onder **Toegewezen virtuele machines**op de vCenter/ESXi-naam.



5. Geef op het scherm **VMware vCenter of ESXi-host toevoegen** het nieuwe gebruikersaccount en het wachtwoord voor dat account op.
6. Klik op **Configureren**.

Back-up maken van geclusterde Hyper-V machines

In een Hyper-V-cluster kunnen virtuele machines migreren tussen clusterknooppunten. Volg deze aanbevelingen om een juiste back-up van geclusterde Hyper-V-machines in te stellen:

1. Een machine moet beschikbaar zijn voor back-up, ongeacht naar welk knooppunt deze migreert. Als u wilt dat Agent voor Hyper-V toegang heeft tot een machine op elk knooppunt, moet de agentservice worden uitgevoerd via een domeingebruikersaccount met administratieve rechten voor elk van de clusterknooppunten.

   Wij raden u aan een dergelijk account op te geven voor de agentservice tijdens de installatie van Agent voor Hyper-V.

2. Installeer Agent voor Hyper-V op elk knooppunt van het cluster.
3. Registreer alle agenten in de Cyber Protection-service.

Hoge beschikbaarheid van een herstelde machine

Wanneer u schijven waarvan een back-up is gemaakt, herstelt op een *bestaande* virtuele Hyper-V-machine, blijft de eigenschap Hoge beschikbaarheid van de machine ongewijzigd.

Wanneer u schijven waarvan een back-up is gemaakt, herstelt op een *nieuwe* virtuele Hyper-V-machine, dan heeft de resulterende machine geen hoge beschikbaarheid. Deze wordt beschouwd als reservemachine en is standaard uitgeschakeld. Als u de machine in de productieomgeving moet gebruiken, kunt u deze configureren voor Hoge beschikbaarheid via de invoegtoepassing **Failover Cluster Management**.

Beperkingen instellen voor het totale aantal virtuele machines waarvan gelijktijdig een back-up kan worden gemaakt

In de back-upoptie **Plannen** kunt u per beschermingsschema een beperking instellen voor het aantal virtuele machines waarvan gelijktijdig een back-up kan worden gemaakt.

Wanneer een agent meerdere schema's tegelijkertijd uitvoert, kan het voorkomen dat er gelijktijdig back-ups worden gemaakt van een groot aantal machines. Dit kan de back-upprestaties beïnvloeden en leiden tot overbelasting van de host en de opslag van de virtuele machine. U kunt dergelijke problemen voorkomen door een beperking op agentniveau in te stellen.

Het aantal gelijktijdige back-ups op agentniveau beperken:

Agent voor VMware (Windows)

1. Maak op de machine met de agent een nieuw tekstdocument en open dit vervolgens in een teksteditor.
2. Kopieer en plak de volgende regels in het bestand.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Vervang `00000001` door de hexadecimale waarde van de limiet die u wilt instellen.
   Bijvoorbeeld: `00000001` is 1 en `0000000A` is 10.
4. Sla het document op als **limit.reg**.
5. Voer het bestand uit als beheerder.
6. Bevestig dat u het Windows-register wilt bewerken.
7. Start de agent opnieuw op.

a. Klik in het menu **Start** op **Uitvoeren**.

b. Typ **cmd** en klik vervolgens op **OK**.

c. Voer op de opdrachtregel de volgende opdrachten uit:

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

Agent voor Hyper-V

1. Maak op de machine met de agent een nieuw tekstdocument en open dit vervolgens in een teksteditor.
2. Kopieer en plak de volgende regels in het bestand.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Vervang `00000001` door de hexadecimale waarde van de limiet die u wilt instellen.
   Bijvoorbeeld: `00000001` is 1 en `0000000A` is 10.
4. Sla het document op als **limit.reg**.
5. Voer het bestand uit als beheerder.
6. Bevestig dat u het Windows-register wilt bewerken.
7. Start de agent opnieuw op.

   a. Klik in het menu **Start** op **Uitvoeren**.

   b. Typ **cmd** en klik vervolgens op **OK**.

   c. Voer op de opdrachtregel de volgende opdrachten uit:

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

Virtuele toepassingen

Deze procedure is van toepassing op Agent voor VMware (Virtual Appliance), Agent voor Scale Computing, Agent voor Virtuozzo Hybrid Infrastructure en Agent voor oVirt.

1. Druk in de console van de virtuele toepassing op CTRL+SHIFT+F2 om de opdrachtregelinterface te openen.
2. Open het bestand `/etc/Acronis/MMS.config` in een teksteditor.
3. Zoek het volgende gedeelte:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Vervang `10` door het maximale aantal gelijktijdige back-ups dat u wilt instellen.
5. Sla het bestand op.
6. Start de agent opnieuw door de opdracht `reboot` uit te voeren.

Machinemigratie

U kunt machinemigratie uitvoeren door de back-up te herstellen naar een andere dan de originele machine.

De volgende tabel bevat een overzicht van de beschikbare migratieopties.

Type machine waarvan een back-up wordt gemaakt	**Beschikbare herstelbestemmingen**							
	Fysieke machine	**Virtuele ESXi-machine**	**Virtuele Hyper-V-machine**	**Virtuozzo**		**Virtuele Virtuozzo Hybrid Infrastructure-machine**	**Virtuele Scale Computing HC3-machine**	**Virtuele RHV/oVirt-machine**
				Virtuele machine	**Container**			
Fysieke machine	+	+	+	-	-	+	+*	+
Virtuele VMware ESXi-machine	+	+	+	-	-	+	+*	+
Virtuele Hyper-V-machine	+	+	+	-	-	+	+*	+
Virtuele Virtuozzo-machine	+	+	+	+	-	+	+*	+
Virtuozzo-container	-	-	-	-	+	-	-	-
Virtuele Virtuozzo Hybrid Infrastructure-machine	+	+	+	-	-	+	+*	+
Virtuele Scale Computing	+	+	+	-	-	+	+	+

HC3-machine								
Virtuele Red Hat Virtualization/oVirt-machine	+	+	+	-	-	+	+*	+

*Als Secure Boot is ingeschakeld op de bronmachine, kan de herstelde VM niet opstarten, tenzij u Secure Boot na het herstel uitschakelt in de VM-console.

Opmerking
U kunt geen virtuele macOS-machines herstellen naar Hyper-V-hosts, omdat Hyper-V geen ondersteuning biedt voor macOS. U kunt virtuele macOS-machines herstellen naar een VMware-host die op Mac-hardware is geïnstalleerd.

Zie de volgende onderwerpen voor meer informatie over het uitvoeren van de migratiebewerkingen:

- Zie "Fysieke machine naar virtueel" (p. 531) voor migratie van fysiek naar virtueel (P2V).
- Zie "Een virtuele machine herstellenU kunt virtuele machines herstellen vanuit de betreffende back-ups.In de Cyber Protect-console kunt u geen back-ups herstellen voor tenants in de compliancemodus. Zie "Back-ups herstellen voor tenants in de compliancemodus" (p. 1) voor meer informatie over het herstellen van dergelijke back-ups.VereistenEen virtuele machine moet worden gestopt tijdens de herstelbewerking naar deze machine. Standaard wordt de machine gestopt zonder dat u hoeft te bevestigen. Wanneer de herstelbewerking is voltooid, moet u de machine handmatig starten. U kunt dit standaardgedrag wijzigen via de hersteloptie van het energiebeheer van de VM (klik op Herstelopties > Energiebeheer VM).ProcedureVoer een van de volgende handelingen uit:Selecteer een machine waarvan een back-up is gemaakt, klik op Herstel en selecteer vervolgens een herstelpunt.Selecteer een herstelpunt op het tabblad Back-upopslag.Klik op Herstellen > Volledige machine.Als u wilt herstellen naar een fysieke machine, selecteert u Fysieke machine in Herstellen naar. Anders kunt u deze stap overslaan.Herstel naar een fysieke machine is alleen mogelijk als de schijfconfiguratie van de doelmachine precies overeenstemt met de schijfconfiguratie in de back-up.Als dit het geval is, gaat u verder naar stap 4 in 'Fysieke machine'. Zo niet, dan raden we u aan om de V2P-migratie uit te voeren met opstartmedia.[Optioneel] Standaard wordt de oorspronkelijke machine automatisch geselecteerd als doelmachine. Als u wilt herstellen naar een andere virtuele machine, klit u op Doelmachine en doet u het volgende:Selecteer de hypervisor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 of oVirt).Alleen virtuele Virtuozzo-machines kunnen worden hersteld naar Virtuozzo. Ga voor meer informatie over V2V-migratie naar 'Machinemigratie'.Selecteer of u een naar een nieuwe of bestaande machine wilt herstellen.Selecteer de host en geef de naam van de nieuwe machine op, of selecteer en bestaande doelmachine.Klik op OK.Stel de extra herstelopties in die u nodig hebt.[Niet beschikbaar voor Virtuozzo Hybrid Infrastructure en Scale Computing HC3] Als u de

gegevensopslag voor de virtuele machine wilt selecteren: klik op Gegevensopslag voor ESXi, of Pad voor Hyper-V en Virtuozzo, of Opslagdomein voor Red Hat Virtualization (oVirt) en selecteer vervolgens de (gegevens)opslag voor de virtuele machine.Als u de (gegevens)opslag, interface en de inrichtingsmethode voor elke virtuele schijf wilt bekijken, klikt u op Schijftoewijzing. U kunt deze instellingen wijzigen, tenzij u een Virtuozzo-container of een virtuele Virtuozzo Hybrid Infrastructure-machine herstelt.Voor Virtuozzo Hybrid Infrastructure kunt u alleen het opslagbeleid voor de doelschijven selecteren. Selecteer hiervoor de gewenste doelschijf en klik vervolgens op Wijzigen. Klik in de geopende blade op het tandwielpictogram, selecteer het opslagbeleid en klik vervolgens op Gereed.In het toewijzingsgedeelte kunt u ook afzonderlijke schijven kiezen die moeten worden hersteld.[Beschikbaar voor VMware ESXi, Hyper-V en Virtuozzo] Klik op VM-instellingen om de geheugengrootte, het aantal processors en de netwerkverbindingen van de virtuele machine te wijzigen.[Voor Virtuozzo Hybrid Infrastructure] Selecteer Variant om de geheugengrootte en het aantal processors van de virtuele machine te wijzigen.[Alleen beschikbaar voor Windows-machines waarop een beveiligingsagent is geïnstalleerd] Gebruik de schakelaar om Veilig herstel in te schakelen zodat u zeker weet dat de herstelde gegevens geen malware bevatten. Zie "Veilig herstel" (p. 1) voor meer informatie over hoe veilig herstel werkt.Klik op Herstel starten.Wanneer u herstelt naar een bestaande virtuele machine, bevestigt u dat u de schijven wilt overschrijven.De voortgang van de herstelbewerking wordt weergegeven op het tabblad Activiteiten." (p. 1) voor migratie van virtueel naar virtueel (V2V).

- Zie "Een virtuele machine herstellenU kunt virtuele machines herstellen vanuit de betreffende back-ups.In de Cyber Protect-console kunt u geen back-ups herstellen voor tenants in de compliancemodus. Zie "Back-ups herstellen voor tenants in de compliancemodus" (p. 1) voor meer informatie over het herstellen van dergelijke back-ups.VereistenEen virtuele machine moet worden gestopt tijdens de herstelbewerking naar deze machine. Standaard wordt de machine gestopt zonder dat u hoeft te bevestigen. Wanneer de herstelbewerking is voltooid, moet u de machine handmatig starten. U kunt dit standaardgedrag wijzigen via de hersteloptie van het energiebeheer van de VM (klik op Herstelopties > Energiebeheer VM).ProcedureVoer een van de volgende handelingen uit:Selecteer een machine waarvan een back-up is gemaakt, klik op Herstel en selecteer vervolgens een herstelpunt.Selecteer een herstelpunt op het tabblad Back-upopslag.Klik op Herstellen > Volledige machine.Als u wilt herstellen naar een fysieke machine, selecteert u Fysieke machine in Herstellen naar. Anders kunt u deze stap overslaan.Herstel naar een fysieke machine is alleen mogelijk als de schijfconfiguratie van de doelmachine precies overeenstemt met de schijfconfiguratie in de back-up.Als dit het geval is, gaat u verder naar stap 4 in 'Fysieke machine'. Zo niet, dan raden we u aan om de V2P-migratie uit te voeren met opstartmedia.[Optioneel] Standaard wordt de oorspronkelijke machine automatisch geselecteerd als doelmachine. Als u wilt herstellen naar een andere virtuele machine, klit u op Doelmachine en doet u het volgende:Selecteer de hypervisor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 of oVirt).Alleen virtuele Virtuozzo-machines kunnen worden hersteld naar Virtuozzo. Ga voor meer informatie over V2V-migratie naar 'Machinemigratie'.Selecteer of u een naar een nieuwe of bestaande machine wilt herstellen.Selecteer de host en geef de naam van de nieuwe machine op, of selecteer en bestaande doelmachine.Klik op OK.Stel de extra herstelopties in die u nodig hebt.[Niet

beschikbaar voor Virtuozzo Hybrid Infrastructure en Scale Computing HC3] Als u de gegevensopslag voor de virtuele machine wilt selecteren: klik op Gegevensopslag voor ESXi, of Pad voor Hyper-V en Virtuozzo, of Opslagdomein voor Red Hat Virtualization (oVirt) en selecteer vervolgens de (gegevens)opslag voor de virtuele machine.Als u de (gegevens)opslag, interface en de inrichtingsmethode voor elke virtuele schijf wilt bekijken, klikt u op Schijftoewijzing. U kunt deze instellingen wijzigen, tenzij u een Virtuozzo-container of een virtuele Virtuozzo Hybrid Infrastructure-machine herstelt.Voor Virtuozzo Hybrid Infrastructure kunt u alleen het opslagbeleid voor de doelschijven selecteren. Selecteer hiervoor de gewenste doelschijf en klik vervolgens op Wijzigen. Klik in de geopende blade op het tandwielpictogram, selecteer het opslagbeleid en klik vervolgens op Gereed.In het toewijzingsgedeelte kunt u ook afzonderlijke schijven kiezen die moeten worden hersteld.[Beschikbaar voor VMware ESXi, Hyper-V en Virtuozzo] Klik op VM-instellingen om de geheugengrootte, het aantal processors en de netwerkverbindingen van de virtuele machine te wijzigen.[Voor Virtuozzo Hybrid Infrastructure] Selecteer Variant om de geheugengrootte en het aantal processors van de virtuele machine te wijzigen.[Alleen beschikbaar voor Windows-machines waarop een beveiligingsagent is geïnstalleerd] Gebruik de schakelaar om Veilig herstel in te schakelen zodat u zeker weet dat de herstelde gegevens geen malware bevatten. Zie "Veilig herstel" (p. 1) voor meer informatie over hoe veilig herstel werkt.Klik op Herstel starten.Wanneer u herstelt naar een bestaande virtuele machine, bevestigt u dat u de schijven wilt overschrijven.De voortgang van de herstelbewerking wordt weergegeven op het tabblad Activiteiten." (p. 1) en "Schijven herstellen met opstartmedia" (p. 537) voor migratie van virtueel naar fysiek (V2P).

Migratie via opstartmedia

In plaats van de machinemigratie in de Cyber Protect-console te gebruiken kunt u een machine ook herstellen via opstartmedia.

We raden aan om opstartmedia te gebruiken in de volgende gevallen:

- Een migratie uitvoeren die niet standaard wordt ondersteund.
  Gebruik bijvoorbeeld opstartmedia om een fysieke machine of een virtuele niet-Virtuozzo-machine te herstellen als een virtuele Virtuozzo-machine op een Virtuozzo-host.
- Een migratie van een Linux-machine met logische volumes (LVM) uitvoeren.
  Gebruik Agent voor Linux of opstartmedia om de back-up te maken en gebruik vervolgens opstartmedia om de back-up te herstellen.
- Stuurprogramma's leveren voor specifieke hardware die essentieel is voor de opstartbaarheid van het systeem.
  Bouw een opstartmedium dat de vereiste stuurprogramma's kan gebruiken. Zie "Bootable Media Builder" (p. 751) voor meer informatie.

Virtuele Microsoft Azure- en Amazon EC2-machines

Als u een back-up wilt maken van een virtuele Microsoft Azure- of Amazon EC2-machine, installeert u een beveiligingsagent op de machine. Back-ups en herstel worden op dezelfde manier uitgevoerd

als voor een fysieke machine. De machine wordt wel als virtuele machine geteld wanneer u quota's instelt voor het aantal machines.

Het verschil met een fysieke machine is dat virtuele Microsoft Azure- en Amazon EC2-machines niet kunnen worden opgestart vanaf opstartmedia. Als u wilt herstellen naar een nieuwe virtuele Microsoft Azure- of Amazon EC2-machine, volgt u de volgende procedure.

Opmerking
De volgende herstelprocedure is alleen van toepassing voor back-ups van machines die alle nodige stuurprogramma's bevatten om native in Microsoft Azure te worden uitgevoerd (back-ups gemaakt van een Azure VM, een lokale Hyper-V-machine of de bronmachine is een Windows Server 2016 en hoger). Zie dit Knowledge Base-artikel voor platformonafhankelijk herstel.

Een machine herstellen als virtuele Microsoft Azure- of Amazon EC2-machine

1. Maak een nieuwe virtuele machine vanaf een image/sjabloon in Microsoft Azure of Amazon EC2. De nieuwe machine moet dezelfde schijfconfiguratie hebben als de machine die u wit herstellen.
2. Installeer Agent voor Windows of Agent voor Linux op de nieuwe machine.
3. Herstel de machine waarvan een back-up is gemaakt, zoals beschreven in 'Fysieke machine'. Wanneer u de herstelbewerking configureert, selecteert u de nieuwe machine als doelmachine.

Opstartmedia maken om besturingssystemen te herstellen

Een opstartmedium is een cd, dvd, USB-flashstation of een ander verwisselbaar medium waarmee u de beveiligingsagent kunt uitvoeren in een Linux-omgeving of een Windows Preinstallation Environment/Windows Recovery Environment (WinPE/WinRE), zonder gebruik te maken van een besturingssysteem. Het belangrijkste doel van opstartmedia is om een besturingssysteem te herstellen dat niet kan worden gestart.

Opmerking
Opstartmedia bieden geen ondersteuning voor hybride schijven.

Aangepaste of kant-en-klare opstartmedia?

Door gebruik te maken van Bootable Media Builder kunt u aangepaste opstartmedia (op Linux gebaseerd of op WinPE gebaseerd) maken voor Windows-, Linux- of macOS-computers. Op de aangepaste opstartmedia (zowel op Linux gebaseerd als op WinPE/WinRE gebaseerd) kunt u aanvullende instellingen configureren, zoals automatische registratie, netwerkinstellingen, of proxyserverinstellingen. Op de op WinPE/WinRE gebaseerde aangepaste opstartmedia kunt u ook aanvullende stuurprogramma's toevoegen.

U kunt ook een kant-en-klaar opstartmedium downloaden (alleen op Linux gebaseerd). U kunt de gedownloade opstartmedia alleen gebruiken voor herstelbewerkingen en toegang tot de functie Universal Restore.

Op Linux of op WinPE/WinRE gebaseerde opstartmedia?

Op Linux gebaseerd

Op Linux gebaseerde opstartmedia bevatten een beveiligingsagent gebaseerd op een Linux-kernel. De agent kan opstarten en bewerkingen uitvoeren op elke hardware die compatibel is met de pc, inclusief bare metal en machines met beschadigde of niet-ondersteunde bestandssystemen.

Op WinPE/WinRE gebaseerd

Op WinPE gebaseerde opstartmedia bevatten een minimaal Windows-systeem, de zogenaamde Windows Preinstallation Environment (WinPE), en een Cyber Protection-plug-in voor WinPE, dat wil zeggen een aangepaste beveiligingsagent die kan worden uitgevoerd in de Preinstallation-omgeving. Op de op WinRE gebaseerde opstartbare media wordt Windows Recovery Environment gebruikt en is geen installatie van aanvullende Windows-pakketten vereist.

In de praktijk is WinPE de handigste opstartbare oplossing voor grote omgevingen met heterogene hardware.

Voordelen:

- Bij het gebruik van Cyber Protection met Windows Preinstallation Environment beschikt u over meer functionaliteit dan bij op Linux gebaseerde opstartmedia. Na het opstarten van compatibele hardware in WinPE, kunt u niet alleen de beveiligingsagent gebruiken, maar ook PE-opdrachten en -scripts, en andere plug-ins die u hebt toegevoegd aan PE.
- Met op PE gebaseerde opstartmedia vermijdt u enkele problemen van de Linux-opstartmedia, zoals alleen ondersteuning voor bepaalde RAID-controllers of bepaalde niveaus van RAID-arrays. Met media gebaseerd op WinPE 2.x en later kunt u de nodige apparaatstuurprogramma's dynamisch laden.

Beperkingen:

- Opstartmedia gebaseerd op WinPE-versies ouder dan 4.0 kunnen niet opstarten op machines die gebruikmaken van Unified Extensible Firmware Interface (UEFI).

Fysieke opstartmedia maken

Het wordt ten zeerste aangeraden de opstartmedia te maken en testen wanneer u back-ups op schijfniveau gaat gebruiken. Daarnaast is het verstandig om de media opnieuw te maken na elke belangrijke update van de beveiligingsagent.

U kunt Windows of Linux herstellen met hetzelfde medium. Voor het herstellen van macOS moet u een afzonderlijk medium op een machine met macOS maken.

Fysieke opstartmedia maken in Windows of Linux

1. Maak een aangepast ISO-bestand voor het opstartmedium of download het kant-en-klare ISO-bestand.

   Gebruik "Bootable Media Builder" (p. 751) om een aangepast ISO-bestand te maken.

   Als u het kant-en-klare ISO-bestand wilt downloaden, selecteert u een machine in de Cyber Protect-console en klikt u vervolgens op **Herstellen** > **Meer herstelbewerkingen...** > **ISO-image downloaden**.
2. [Optioneel] Genereer een registratietoken in de Cyber Protect-console. Het registratietoken wordt automatisch weergegeven wanneer u een kant-en-klaar ISO-bestand downloadt.

   Dit token geeft toegang tot de cloudopslag vanaf de opstartmedia zonder dat u een gebruikersnaam en wachtwoord hoeft in te voeren.
3. Gebruik een van de volgende manieren om fysieke opstartmedia te maken:
   - Brand het ISO-bestand op een cd/dvd.
   - Gebruik een van de gratis tools die online beschikbaar zijn om een opstartbaar USB-flashstation met het ISO-bestand te maken.

     Gebruik `ISO to USB` of `RUFUS` als u een UEFI-machine wilt opstarten. Gebruik `Win32DiskImager` voor een BIOS-machine. In Linux kunt u bijvoorbeeld het hulpprogramma `dd` gebruiken.

   Voor virtuele machine kunt u het ISO-bestand als een cd-/dvd-station koppelen aan de machine die u wilt herstellen.

Fysieke opstartmedia maken in macOS

1. Klik op een machine met Agent voor Mac op **Applicaties** > **Rescue Media Builder**.
2. Het aangesloten verwisselbare medium wordt weergegeven. Selecteer het medium dat u opstartbaar wilt maken.

   Waarschuwing!
   Alle gegevens op de schijf worden gewist.
3. Klik op **Maken**.
4. Wacht totdat het opstartmedium is gemaakt.

Bootable Media Builder

Bootable Media Builder is een tool die specifiek is bedoeld voor het maken van opstartmedia. De tool wordt geïnstalleerd als optioneel onderdeel op de machine waarop de beveiligingsagent is geïnstalleerd.

Waarom Bootable Media Builder gebruiken?

De kant-en-klare opstartmedia die beschikbaar zijn om te downloaden in de Cyber Protect-console, zijn gebaseerd op een Linux-kernel. In tegenstelling tot Windows PE kunnen aangepaste stuurprogramma's niet direct worden geplaatst.

Met Bootable Media Builder kunt u aangepaste op Linux gebaseerde of op WinPE gebaseerde opstartbare media-images maken.

32 bits of 64 bits?

Met Bootable Media Builder kunt u opstartmedia met zowel 32-bits als 64-bits onderdelen maken. In de meeste gevallen hebt u 64-bits media nodig om een machine met Unified Extensible Firmware Interface (UEFI) op te starten.

Linux-opstartmedia

Linux-opstartmedia maken

1. Start **Bootable Media Builder**.
2. Selecteer bij **Type opstartmedia** de optie **Standaard (Linux-media)**.
3. Selecteer hoe volumes en netwerkbronnen worden weergegeven:
   - Op opstartmedia met een volumeweergave zoals in Linux worden de volumes bijvoorbeeld weergegeven als hda1 of sdb2. Voordat een herstelbewerking wordt uitgevoerd, wordt geprobeerd om MD-apparaten en logische volumes (LVM) te herstellen.
   - Op opstartmedia met volumeweergave zoals in Windows worden de volumes bijvoorbeeld weergegeven als C: en D:. Hiermee hebt u toegang tot dynamische volumes (LDM).
4. [Optioneel] Geef de parameters van de Linux-kernel op. Gebruik spaties als scheidingsteken tussen meerdere parameters.

   Als u bijvoorbeeld een weergavemodus voor de opstartbare agent wilt selecteren telkens wanneer de media worden gestart, typt u: **vga=ask**. Zie "Kernelparameters" (p. 753) voor meer informatie over de beschikbare parameters.
5. [Optioneel] Selecteer de taal van het opstartmedium.
6. [Optioneel] Selecteer de opstartmodus (BIOS of UEFI) die u voor Windows wilt gebruiken na het herstel.
7. Selecteer het onderdeel dat u op de media wilt plaatsen: de opstartbare Cyber Protection-agent.
8. [Optioneel] Geef het time-outinterval voor het opstartmenu op. Als u deze instelling niet configureert, wacht het laadprogramma tot u aangeeft of het besturingssysteem (indien aanwezig) of het onderdeel moet worden opgestart.
9. [Optioneel] Als u de bewerkingen voor de opstartbare agent wilt automatiseren, schakelt u het selectievakje **Gebruik het volgende script** in. Selecteer vervolgens een van de scripts en geef de scriptparameters op. Zie "Scripts in opstartmedia" (p. 755) voor meer informatie over de scripts.
10. [Optioneel] Selecteer hoe de opstartmedia worden geregistreerd in de Cyber Protection-service bij het opstarten. Zie "De opstartmedia registreren" (p. 764) voor meer informatie over de registratie-instellingen.
11. Geef de netwerkinstellingen voor de netwerkadapters van de opgestarte machine op of behoud de automatische DHCP-configuratie.

12. [Optioneel] Als er een proxyserver is ingeschakeld in uw netwerk, geeft u de hostnaam of het IP-adres en de poort op.
13. Selecteer het bestandstype van het gemaakte opstartmedium:
    - ISO-image
    - ZIP-bestand
14. Geef een bestandsnaam op voor het opstartmediabestand.
15. Controleer uw instellingen in het samenvattingsscherm en klik op **Doorgaan**.

Kernelparameters

U kunt een of meer parameters van de Linux-kernel opgeven die automatisch worden toegepast wanneer het opstartmedium start. Deze parameters worden doorgaans gebruikt wanneer er problemen optreden bij het werken met de opstartmedia. Gewoonlijk kunt u dit veld leeg laten.

U kunt deze parameters ook opgeven door op F11 te drukken vanuit het opstartmenu.

Parameters

Wanneer u meerdere parameters opgeeft, moet u deze scheiden met een spatie.

- **acpi=off**
  Hiermee schakelt u ACPI (Advanced Configuration and Power Interface) uit. Deze parameter kan handig zijn wanneer u problemen ondervindt met een bepaalde hardwareconfiguratie.
- **noapic**
  Hiermee schakelt u de Advanced Programmable Interrupt Controller (APIC) uit. Deze parameter kan handig zijn wanneer u problemen ondervindt met een bepaalde hardwareconfiguratie.
- **vga=ask**
  Hiermee wordt gevraagd welke videomodus moet worden gebruikt door de grafische gebruikersinterface van de opstartmedia. Zonder de parameter **vga** wordt de videomodus automatisch gedetecteerd.
- **vga=** *mode_number*
  Hiermee wordt de videomodus opgegeven die moet worden gebruikt door de grafische gebruikersinterface van de opstartmedia. *mode_number* geeft het nummer van de modus aan in hexadecimale notatie, bijvoorbeeld: **vga=0x318**
  De schermresolutie en het aantal kleuren zoals bepaald door een modusnummer kunnen per machine verschillen. We raden aan om eerst de parameter **vga=ask** te gebruiken, zodat u een waarde kunt kiezen voor *mode_number*.
- **quiet**
  Hiermee wordt de weergave van opstartberichten uitgeschakeld tijdens het laden van de Linux-kernel, en wordt de beheerconsole gestart wanneer het laden van de kernel is voltooid.
  Deze parameter is impliciet opgegeven wanneer u de opstartmedia maakt, maar u kunt deze parameter verwijderen vanuit het opstartmenu.

Als deze parameter wordt verwijderd, worden alle opstartberichten weergegeven, gevolgd door een opdrachtprompt. Als u de beheerconsole wilt starten vanaf de opdrachtprompt, gebruikt u de volgende opdracht: **/bin/product**

- **nousb**

  Hiermee wordt het laden van het USB-subsysteem (Universal Serial Bus) uitgeschakeld.
- **nousb2**

  Hiermee wordt de ondersteuning voor USB 2.0 uitgeschakeld. USB 1.1-apparaten werken wel als deze parameter is opgegeven. Met deze parameter kunt u bepaalde USB-stations in de USB 1.1-modus gebruiken als ze niet werken in de USB 2.0-modus.
- **nodma**

  Hiermee wordt DMA (Direct Memory Access) uitgeschakeld voor alle IDE-schijfstations. Dit voorkomt dat de kernel vastloopt op sommige hardware.
- **nofw**

  Hiermee wordt ondersteuning voor de FireWire (IEEE1394)-interface uitgeschakeld.
- **nopcmcia**

  Hiermee wordt de detectie van PCMCIA-hardware uitgeschakeld.
- **nomouse**

  Hiermee wordt ondersteuning voor de muis uitgeschakeld.
- *module_name* **=off**

  Hiermee wordt de module uitgeschakeld die is genoemd in *module_name*. Als u bijvoorbeeld het gebruik van de SATA-module wilt uitschakelen, geeft u het volgende op: **sata_sis=off**
- **pci=bios**

  Hiermee forceert u dat PCI BIOS wordt gebruikt in plaats van directe toegang tot het hardwareapparaat. Deze parameter kan handig zijn als de machine een niet-standaard PCI host-brug heeft.
- **pci=nobios**

  Hiermee wordt het gebruik van PCI BIOS uitgeschakeld. Alleen methoden voor directe toegang tot de hardware zijn toegestaan. Deze parameter kan handig zijn wanneer de opstartmedia niet starten vanwege een mogelijke fout met het BIOS.
- **pci=bios**

  Hiermee worden PCI BIOS-aanroepen gebruikt om de interrupt routing-tabel op te halen. Deze parameter kan handig zijn als de kernel de interrupt requests (IRQ's) niet kan toewijzen of de secundaire PCI-bussen op het moederbord niet kan ontdekken.

  Deze aanroepen werken mogelijk niet correct op sommige machines. Dit is echter mogelijk de enige manier om de interrupt routing-tabel op te halen.
- **INDELINGEN=en-US, de-DE, fr-FR, enzovoort**

  Hiermee worden de toetsenbordindelingen opgegeven die u wilt gebruiken in de grafische gebruikersinterface van de opstartmedia.

  Zonder deze parameter kunnen slechts twee indelingen worden gebruikt: Engels (VS) en de indeling die overeenkomt met de taal die is geselecteerd in het opstartmenu van de media.

  U kunt een van de volgende indelingen opgeven:

Belgisch: **be-BE**
Tsjechisch: **cz-CZ**
Engels: **en-GB**
Engels (VS): **en-US**
Frans: **fr-FR**
Frans (Zwitserland): **fr-CH**
Duits: **de-DE**
Duits (Zwitserland): **de-CH**
Italiaans: **it-IT**
Pools: **pl-PL**
Portugees: **pt-PT**
Portugees (Braziliaans): **pt-BR**
Russisch: **ru-RU**
Servisch (Cyrillisch): **sr-CR**
Servisch (Latijns): **sr-LT**
Spaans: **es-ES**
Wanneer u met opstartmedia werkt, gebruikt u CTRL + SHIFT om door de beschikbare indelingen te bladeren.

Scripts in opstartmedia

Als u wilt dat het opstartmedium een vooraf gedefinieerde reeks bewerkingen uitvoert, kunt u een script opgeven wanneer u het medium maakt met Bootable Media Builder. Telkens als een machine wordt opgestart vanaf het medium, wordt het opgegeven script uitgevoerd en de gebruikersinterface wordt niet weergegeven.

U kunt een van de vooraf gedefinieerde scripts kiezen of een aangepast script maken door de scriptconventies te volgen.

Vooraf gedefinieerde scripts

Bootable Media Builder biedt de volgende vooraf gedefinieerde scripts:

- Herstel vanuit de cloudopslag (**entire_pc_cloud**)
- Herstel vanuit een netwerkshare (**entire_pc_share**)

De scripts bevinden zich in de volgende mappen op de machine waarop Bootable Media Builder is geïnstalleerd:

- In Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- In Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Herstel vanuit de cloudopslag

Geef in Bootable Media Builder de volgende scriptparameters op:

1. De naam van het back-upbestand.
2. [Optioneel] Een wachtwoord dat door het script wordt gebruikt voor toegang tot de versleutelde back-ups.

Herstel vanuit een netwerkshare

Geef in Bootable Media Builder de volgende scriptparameters op:

- Het pad naar de netwerkshare.
- De gebruikersnaam en het wachtwoord voor de netwerkshare.
- De naam van het back-upbestand. De naam van het back-upbestand vinden:
  a. Ga in de Cyber Protect-console naar **Back-upopslag** > **Locaties**.
  b. Selecteer de netwerkshare (klik op **Locatie toevoegen** als de share niet wordt vermeld).
  c. Selecteer de back-up.
  d. Klik op **Details**. De bestandsnaam wordt weergegeven onder **Naam van back-upbestand**.
- [Optioneel] Een wachtwoord dat door het script wordt gebruikt voor toegang tot de versleutelde back-ups.

Aangepaste scripts

Belangrijk
Voor het maken van aangepaste scripts is kennis van de opdrachttaal Bash en van JavaScript Object Notation (JSON) vereist. Als u niet vertrouwd bent met Bash, kunt u informatie hierover vinden op http://www.tldp.org/LDP/abs/html. De JSON-specificatie is beschikbaar op http://www.json.org.

Bestanden van een script

Uw script moet zich in de volgende directory's bevinden op de machine waarop Bootable Media Builder is geïnstalleerd:

- In Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- In Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Het script moet uit ten minste drie bestanden bestaan:

- **<scriptbestand>.sh** - een bestand met uw Bash-script. Gebruik bij het maken van het script uitsluitend een beperkte set van shell-opdrachten. U kunt deze vinden in https://busybox.net/downloads/BusyBox.html. Ook kunnen de volgende opdrachten worden gebruikt:
  - `acrocmd`: het opdrachtregelprogramma voor back-up en herstel
  - `product`: de opdracht waarmee de gebruikersinterface voor opstartmedia wordt gestart

Dit bestand en eventuele andere bestanden die in het script voorkomen (bijvoorbeeld via de opdracht dot), moeten zich in de submap **bin** bevinden. Geef in het script de aanvullende bestandspaden op als: **/ConfigurationFiles/bin/<willekeurig_bestand>**.

- **autostart** - een bestand voor het starten van **<scriptbestand>.sh**. Het bestand moet de volgende inhoud hebben:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<scriptbestand>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - een JSON-bestand met de volgende inhoud:
  - De naam en de beschrijving van het script die moeten worden weergegeven in Bootable Media Builder.
  - De namen van de scriptvariabelen die u wilt configureren via Bootable Media Builder.
  - De parameters van besturingselementen die worden weergegeven in Bootable Media Builder voor elke variabele.

Structuur van autostart.json

Object van het hoogste niveau

Paar		Vereist	Beschrijving
Naam	**Type waarde**		
`displayName`	string	Ja	De scriptnaam die moet worden weergegeven in Bootable Media Builder.
`description`	string	Nee	De beschrijving van het script die moet worden weergegeven in Bootable Media Builder.
`timeout`	number	Nee	Een time-out (in seconden) voor het opstartmenu voordat het script wordt gestart. Als het paar niet wordt opgegeven, bedraagt de time-out tien seconden.
`variables`	object	Nee	Eventuele variabelen voor **<scriptbestand>.sh** die u wilt configureren via Bootable Media Builder. De waarde moet een set van de volgende paren zijn: de tekenreeks-id van een variabele en het object van de variabele (zie de onderstaande tabel).

Object van variabele

Paar		Vereist	Beschrijving
Naam	**Type waarde**		
`displayName`	string	Ja	De naam van de variabele die wordt gebruikt in **<scriptbestand>.sh**.
`type`	string	Ja	Het type van een besturingselement dat wordt weergegeven in Bootable Media Builder. Dit besturingselement wordt gebruikt voor het configureren van de waarde van de variabele. Zie de onderstaande tabel voor alle ondersteunde typen.
`description`	string	Ja	Het label van een besturingselement dat wordt weergegeven boven het besturingselement in Bootable Media Builder.
`default`	string voor het `type string`, `multiString`, `password` of `enum` number voor het `type number`, `spinner` of `checkbox`	Nee	De standaardwaarde voor het besturingselement. Als het paar niet wordt opgegeven, is de standaardwaarde een lege tekenreeks of een nul, afhankelijk van het type besturingselement. De standaardwaarde voor een selectievakje kan `0` (leeg) of `1` (ingeschakeld) zijn.
`order`	number (niet-negatief)	Ja	De volgorde van besturingselementen in Bootable Media Builder. Hoe hoger de waarde, des te lager de positie van het besturingselement ten opzichte van andere besturingselementen die zijn gedefinieerd in **autostart.json**. De beginwaarde moet `0` zijn.
`min` (alleen voor `spinner`)	number	Nee	De minimale waarde van het kringveld in een draaivak. Als het paar niet wordt opgegeven, is de waarde `0`.
`max` (alleen voor `spinner`)	number	Nee	De maximale waarde van het kringveld in een draaivak. Als het paar niet wordt opgegeven, is de waarde `100`.
`step` (alleen voor	number	Nee	De stapwaarde van het kringveld in een draaivak. Als het paar niet wordt opgegeven, is de waarde `1`.

spinner)			
items (alleen voor enum)	reeks van tekenreeksen	Ja	De waarden voor een vervolgkeuzelijst.
required (voor string, multiString, wachtwoord en enum)	number	Nee	Hiermee wordt opgegeven of de waarde van een besturingselement leeg (0) kan zijn of niet (1). Als het paar niet wordt opgegeven, kan de waarde van het besturingselement leeg zijn.

Type besturingselement

Naam	Beschrijving
string	Een tekstvak van één regel, zonder beperkingen, dat wordt gebruikt voor het invoeren of bewerken van korte tekenreeksen.
multiString	Een tekstvak van meerdere regels, zonder beperkingen, dat wordt gebruikt voor het invoeren of bewerken van lange tekenreeksen.
password	Een tekstvak van één regel, zonder beperkingen, dat wordt gebruikt voor het veilig invoeren van wachtwoorden.
number	Een tekstvak van één regel, voor alleen numerieke gegevens, dat wordt gebruikt voor het invoeren of bewerken van getallen.
spinner	Een tekstvak van één regel, voor alleen numerieke gegevens, dat wordt gebruikt voor het invoeren of bewerken van getallen, met een kringveld. Ook wel een draaivak genoemd.
enum	Een standaard vervolgkeuzelijst, met een vaste reeks van vooraf vastgestelde waarden.
checkbox	Een selectievakje met twee statussen: leeg en ingeschakeld.

Het onderstaande voorbeeld **autostart.json** bevat alle mogelijk typen besturingselementen die kunnen worden gebruikt voor het configureren van variabelen voor **<scriptbestand>.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
        }
    }
}
```

WinPE- en WinRE-opstartmedia

U kunt op WinRE gebaseerde images maken zonder extra voorbereiding, of WinPE-images maken na de installatie van Windows Automated Installation Kit (AIK) of Windows Assessment and Deployment Kit (ADK).

WinRE-images

Het maken van WinRE-images wordt ondersteund voor de volgende besturingssystemen:

- Windows 7 (64 bits)
- Windows 8 (32-bits en 64-bits)
- Windows 8.1 (32-bits en 64-bits)
- Windows 10 (32-bits en 64-bits)
- Windows 11 (64-bits)
- Windows Server 2012 (64-bits)
- Windows Server 2016 (64-bits)
- Windows Server 2019 (64-bits)
- Windows Server 2022 (64-bits)

WinPE-images

Na de installatie van Windows Automated Installation Kit (AIK) of Windows Assessment and Deployment Kit (ADK) ondersteunt Bootable Media Builder WinPE-distributies die zijn gebaseerd op de volgende kernels:

- Windows Vista (PE 2.0)
- Windows Vista SP1 en Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) met of zonder de aanvulling voor Windows 7 SP1 (PE 3.1)
- Windows 8 (PE 4.0)

- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

Bootable Media Builder ondersteunt zowel 32-bits als 64-bits WinPE-distributies. De 32-bits WinPE-distributies werken ook op 64-bits hardware. U hebt echter wel 64-bits distributie nodig om een machine met Unified Extensible Firmware Interface (UEFI) op te starten.

Opmerking
Voor een goede werking van PE-installatiekopieën gebaseerd op WinPE 4 en later is ongeveer 1 GB RAM vereist.

WinPE- of WinRE-opstartmedia maken

Bootable Media Builder biedt twee methoden voor de integratie van Cyber Protection met WinPE en WinRE:

- Een geheel nieuw ISO-bestand maken met de Cyber Protection-plug-in.
- De Cyber Protection-plug-in toevoegen aan een WIM-bestand voor later gebruik (handmatig bouwen van ISO, andere tools toevoegen aan de image, enzovoort).

WinPE- of WinRE-opstartmedia maken

1. Voer Bootable Media Builder uit op de machine waarop de beveiligingsagent is geïnstalleerd.
2. Selecteer bij **Type opstartmedia** de optie **Windows PE** of **Windows PE (64 bits)**. Een 64-bits medium is vereist om een machine met Unified Extensible Firmware Interface (UEFI) op te starten.
3. Selecteer het subtype van het opstartmedium: **WinRE** of **WinPE**.
   U kunt WinRE-opstartmedia maken zonder installatie van aanvullende pakketten.
   Als u 64-bits WinPE-media wilt maken, moet u Windows Automated Installation Kit (AIK) of Windows Assessment and Deployment Kit (ADK) downloaden. Als u 32-bits WinPE-media wilt maken, moet u de AIK of ADK downloaden en het volgende doen:
   a. Klik op **Download de plug-in voor WinPE (32 bits)**.
   b. Sla de plug-in op in **%PROGRAM_FILES%\BackupClient\BootableComponents\WinPE32**.
4. [Optioneel] Selecteer de taal van het opstartmedium.
5. [Optioneel] Selecteer de opstartmodus (BIOS of UEFI) die u voor Windows wilt gebruiken na het herstel.
6. Geef de netwerkinstellingen voor de netwerkadapters van de opgestarte machine op of behoud de automatische DHCP-configuratie.
7. [Optioneel] Selecteer hoe de opstartmedia worden geregistreerd in de Cyber Protection-service bij het opstarten. Zie "De opstartmedia registreren" (p. 764) voor meer informatie over de registratie-instellingen.
8. [Optioneel] Geef de Windows-stuurprogramma's op die u wilt toevoegen aan de opstartmedia.

Wanneer u een machine opstart met Windows PE of Windows RE, kunt u de stuurprogramma's gebruiken om toegang krijgen tot het apparaat met de back-up. Voeg 32-bits stuurprogramma's toe als u een 32-bits WinPE- of WinRE-distributie gebruikt en 64-bits stuurprogramma's als u een 64-bits WinPE- of WinRE-distributie gebruikt.

Ga als volgt te werk om de stuurprogramma's toe te voegen:

- Klik op **Toevoegen** en geef vervolgens het pad op naar het vereiste .inf-bestand voor een overeenkomstige SCSI-, RAID- of SATA-controller, netwerkadapter, tapestation of ander apparaat.
- Herhaal deze procedure voor elk stuurprogramma dat u wilt opnemen in de resulterende WinPE- of WinRE-media.

9. Selecteer het bestandstype van het gemaakte opstartmedium:
   - ISO-image
   - WIM-image
10. Geef het volledige pad naar het resulterende imagebestand op, met inbegrip van de bestandsnaam.
11. Controleer uw instellingen in het samenvattingsscherm en klik op **Doorgaan**.

Een PE-installatiekopie (ISO-bestand) maken van het resulterende WIM-bestand

- Vervang het standaardbestand boot.wim in uw Windows PE-map door het zojuist gemaakte WIM-bestand. Typ het volgende voor het eerder vermelde voorbeeld:

```
copy c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Gebruik de tool **Oscdimg**. Typ het volgende voor het eerder vermelde voorbeeld:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

Waarschuwing!
U moet dit voorbeeld niet kopiëren en plakken. Typ de opdracht, want anders werkt deze niet.

Voorbereiding: WinPE 2.x en 3.x

Als u images van PE 2.x of 3.x wilt maken of wijzigen, installeert u Bootable Media Builder en de Windows Automated Installation Kit (AIK) op dezelfde machine.

Een machine voorbereiden:

1. Download het AIK-imagebestand vanaf de Microsoft-website, als volgt:
   - Voor Windows Vista (PE 2.0): https://www.microsoft.com/en-us/download/details.aspx?id=10333
   - Voor Windows Vista SP1 en Windows Server 2008 (PE 2.1): https://www.microsoft.com/en-us/download/details.aspx?id=9085
   - Voor Windows 7 (PE 3.0): https://www.microsoft.com/en-gb/download/details.aspx?id=5753

Voor Windows 7 SP1 (PE 3.1) hebt u ook het AIK-supplement nodig dat beschikbaar is op https://www.microsoft.com/en-us/download/details.aspx?id=5188

2. Brand de image op een dvd-schijf of een USB-flashstation.
3. Vanuit de image installeert u het volgende:
   - Microsoft .NET Framework (NETFXx86 of NETFXx64, afhankelijk van uw hardware)
   - MSXML (Microsoft XML-parser)
   - Windows AIK
4. Installeer Bootable Media Builder op dezelfde machine.

Voorbereiding: WinPE 4.0 en later

Als u images van PE 4 of later wilt maken of wijzigen, installeert u Bootable Media Builder en Windows Assessment and Deployment Kit (ADK) op dezelfde machine.

Een machine voorbereiden:

1. Download het ADK-installatieprogramma vanaf de Microsoft-website.
   De volgende Windows versies worden ondersteund:
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)
   - Windows 8.1 (PE 5.0)
   - Windows 8 (PE 4.0)
2. Installeer Assessment en Deployment Kit.
3. Installeer Bootable Media Builder.

De opstartmedia registreren

Door de opstartmedia te registreren in de Cyber Protection-service krijgt u toegang tot de cloudopslag voor uw back-ups. U kunt de registratie vooraf configureren tijdens het maken van de opstartmedia. Als de registratie niet vooraf is geconfigureerd, kunt u de media registreren nadat u hiermee een machine hebt opgestart.

De registratie vooraf configureren in de Cyber Protection-service

1. Ga in Bootable Media Builder naar **Registratie van opstartmedia**.
2. Geef in **Service-URL** het serviceadres van Cyber Protection op.
3. [Optioneel] Geef bij **Weergavenaam** een naam op voor de opgestarte machine.
4. Als u de automatische registratie in de Cyber Protection-service wilt instellen, schakelt u het selectievakje **De opstartbare media automatisch registreren** in en selecteert u het niveau van automatische registratie:

- **Registratietoken opvragen bij opstarten**
  Het token moet opnieuw worden opgegeven telkens wanneer een machine wordt opgestart vanaf dit opstartmedium.
- **Het volgende token gebruiken**
  De machine wordt automatisch geregistreerd telkens wanneer deze wordt opgestart via dit opstartmedium.

Het opstartmedium registreren nadat hiermee een machine is opgestart

1. Start de machine op vanaf de opstartmedia.
2. Klik in het opstartvenster op **Media registreren**.
3. Geef bij **Server** het serviceadres van Cyber Protection op.
4. Voer bij **Registratietoken** het registratietoken in.
5. Klik op **Registreren**.

Netwerkinstellingen

Bij het maken van opstartmedia kunt u vooraf configureren welke netwerkverbindingen moeten worden gebruikt door de opstartagent. De volgende parameters kunnen vooraf worden geconfigureerd:

- IP-adres
- Subnetmasker
- Gateway
- DNS-server
- WINS-server

Wanneer de opstartbare agent wordt gestart op een machine, wordt de configuratie toegepast op de netwerkinterfacekaart (NIC) van de machine. Als de instellingen niet vooraf zijn geconfigureerd, gebruikt de agent de automatische DHCP-configuratie.

U kunt de netwerkinstellingen ook handmatig configureren wanneer de opstartbare agent wordt uitgevoerd op de machine.

Meerdere netwerkverbindingen van te voren configureren

U kunt de TCP/IP-instellingen van te voren configureren voor maximaal tien netwerkinterfacekaarten (NIC's). U kunt waarborgen dat de juiste instellingen aan elke NIC worden toegewezen door de media te maken op de server waarvoor de media is voorbereid. Wanneer u een bestaande NIC selecteert in het wizardvenster, worden de instellingen van die NIC geselecteerd en opgeslagen op de media. Het MAC-adres van elke bestaande NIC wordt ook opgeslagen op de media.

U kunt alle instellingen behalve het MAC-adres wijzigen of de instellingen configureren voor een niet-bestaande NIC.

Wanneer de opstartbare agent wordt gestart op de server, wordt de lijst met beschikbare NIC's opgehaald. Deze lijst wordt gesorteerd op de sleuven waarin de NIC's zich bevinden, met als eerste de sleuf die het dichtste bij de processor is.

Elke bekende NIC krijgt de juiste instellingen toegewezen door de opstartbare agent en de NIC's worden geïdentificeerd aan de hand van hun MAC-adressen. Wanneer de NIC's met bekende MAC-adressen zijn geconfigureerd, worden aan de overige NIC's de instellingen toegewezen die u hebt gemaakt voor niet-bestaande NIC's, te beginnen vanaf de eerste niet-toegewezen NIC.

U kunt de opstartmedia aanpassen voor elke machine, niet alleen voor de machine waarop de media zijn gemaakt. Dit kunt u doen door de NIC's te configureren in de volgorde van de sleuven op die machine: NIC1 bevindt zich in de sleuf het dichtste bij de processor, NIC2 in de volgende sleuf, enzovoort. Wanneer de opstartbare agent op die machine wordt gestart, worden er geen NIC's met bekende MAC-adressen gevonden en worden de NIC's geconfigureerd in dezelfde volgorde als die u hebt gehanteerd.

Voorbeeld

De opstartbare agent kan een van de netwerkadapters gebruiken voor communicatie met de beheerconsole via het productienetwerk. Voor deze verbinding kan een automatische configuratie worden uitgevoerd. Grote hoeveelheden gegevens voor herstel kunnen worden overgedragen via de tweede NIC, die is opgenomen in het toegewezen back-upnetwerk via statische TCP/IP-instellingen.

Een machine registreren die is opgestart vanaf opstartmedia

Lokale verbinding

Als u direct wilt werken op de machine die is opgestart vanaf opstartmedia, klikt u op **Deze machine lokaal beheren** in het opstartvenster.

Wanneer een machine is opgestart vanaf opstartmedia, wordt op de terminal van de machine een opstartvenster weergegeven met een of meer IP-adressen die zijn verkregen van DHCP of die zijn ingesteld volgens de vooraf geconfigureerde waarden.

Netwerkinstellingen configureren

U kunt de netwerkinstelling voor de huidige sessie wijzigen door in het opstartvenster te klikken op **Netwerk configureren**. In het venster **Netwerkinstellingen** dat wordt weergegeven, kunt u netwerkinstellingen configureren voor elke NIC-kaart (netwerkinterfacekaart) van de machine.

Wijzigingen die tijdens een sessie zijn doorgevoerd, gaan verloren wanneer de machine opnieuw wordt opgestart.

VLAN's toevoegen

In het venster **Netwerkinstellingen** kunt u virtuele lokale netwerken (VLAN's) toevoegen. Gebruik deze functionaliteit als u toegang nodig hebt tot een back-uplocatie die zich op een specifiek VLAN

bevindt.

VLAN's worden hoofdzakelijk gebruikt om een lokaal netwerk op te splitsen in segmenten. Een NIC dat is verbonden met een *toegangspoort* van de switch heeft altijd toegang tot het VLAN dat is opgegeven in de poortconfiguratie. Een NIC dat is verbonden met een *trunkpoort* van de switch kan uitsluitend toegang krijgen tot de VLAN's die zijn toegestaan in de poortconfiguratie als u de VLAN's opgeeft in de netwerkinstellingen.

Toegang tot een VLAN inschakelen via een trunkpoort

1. Klik op **VLAN toevoegen**.
2. Selecteer het NIC dat toegang tot het lokale netwerk biedt dat het vereiste VLAN bevat.
3. Geef de VLAN-id op.

Nadat u op **OK** hebt geklikt, wordt de lijst met netwerkadapters opgehaald.

Als u een VLAN moet verwijderen, klikt u op de vereiste VLAN-vermelding en klikt u vervolgens op **VLAN verwijderen**.

Lokale bewerkingen met opstartmedia

Bewerkingen met opstartmedia zijn vergelijkbaar met de herstelbewerkingen die worden uitgevoerd onder een actief besturingssysteem. Dit zijn de verschillen:

1. Als volumes op opstartmedia worden weergegeven zoals in Windows, dan heeft het volume dezelfde stationsletter als in Windows. Volumes zonder stationsletter in Windows (zoals het volume Gereserveerd voor het systeem) krijgen vrije letters toegewezen in de volgorde zoals op de schijf.

   Als het opstartmedium Windows niet kan detecteren op de machine of meer dan één Windows-systeem detecteert, dan worden alle volumes, ook die zonder stationsletters, toegewezen in de volgorde zoals op de schijf. De volumeletters kunnen dus afwijken van die in Windows. Station D: op het opstartmedium kan bijvoorbeeld overeenkomen met station E: in Windows.

   Opmerking
   Het is raadzaam om unieke namen toe te kennen aan de volumes.

2. Als volumes op een opstartmedium worden weergegeven zoals in Linux, dan worden lokale schijven en volumes weergegeven als niet-gekoppeld (sda1, sda2, enzovoort).
3. Taken kunnen niet worden gepland. Als u een bewerking moet herhalen, moet u deze helemaal opnieuw configureren.
4. De levensduur van het logboek is beperkt tot de huidige sessie. U kunt het hele logboek of de gefilterde logboekvermeldingen opslaan in een bestand.

Een weergavemodus instellen

Wanneer u een machine opstart via Linux-opstartmedia, wordt er automatisch een videoweergavemodus gedetecteerd op basis van de hardwareconfiguratie (specificaties van de

monitor en grafische kaart). Als de videomodus onjuist is gedetecteerd, doet u het volgende:

1. Druk op F11 in het opstartmenu.
2. Voer op de opdrachtregel **vga=ask** in en ga dan verder met opstarten.
3. Kies de juiste modus in de lijst met ondersteunde videomodi door het nummer ervan in te voeren (bijvoorbeeld **318**) en druk vervolgens op **Enter**.

Als u deze procedure niet elke keer wilt volgen wanneer u een bepaalde hardwareconfiguratie opstart, maak dan de opstartmedia opnieuw aan door het juiste modusnummer (in het voorbeeld hierboven: **vga=0x318**) op te geven in het venster **Kernelparameters**.

Herstel met lokale opstartmedia

1. Start de machine op vanaf de opstartmedia.
2. Klik op **Deze machine lokaal beheren**.
3. Klik op **Herstellen**.
4. Klik in **Wat moet worden hersteld** op **Gegevens selecteren**.
5. Selecteer het back-upbestand waaruit u wilt herstellen.
6. Selecteer in het deelvenster linksonder de stations/volumes (of bestanden/mappen) die u wilt herstellen en klik vervolgens op **OK**.
7. Configureer de regels voor overschrijven.
8. Configureer de hersteluitsluitingen.
9. Configureer de herstelopties.
10. Controleer of uw instellingen juist zijn en klik vervolgens op **OK**.

Bewerkingen op afstand met opstartmedia

Opmerking
Deze functie is alleen beschikbaar met het Advanced Backup-pakket.

Als u de opstartmedia in de Cyber Protect-console wilt zien, moet u deze eerst registreren, zoals beschreven in "De opstartmedia registreren" (p. 764).

Wanneer u de media in de Cyber Protect-console hebt geregistreerd, worden deze weergegeven op het tabblad **Apparaten** > **Opstartmedia**. Opstartmedia die langer dan 30 dagen offline zijn geweest, worden niet meer weergegeven op dit tabblad.

U kunt de opstartmedia op afstand beheren via de Cyber Protect-console. U kunt bijvoorbeeld gegevens herstellen, de met de media opgestarte machine opnieuw opstarten of afsluiten, of informatie, activiteiten en waarschuwingen over de media bekijken.

Belangrijk
U kunt de opstartmedia niet op afstand bijwerken via het tabblad **Instellingen** > **Agents** in de Cyber Protect-console.

Als u de opstartmedia wilt bijwerken, maakt u nieuwe aan, zoals beschreven in het gedeelte "Bootable Media Builder" (p. 751). U kunt er ook voor kiezen om de kant-en-klare media te downloaden door te klikken op uw accountpictogram > **Downloads** > **Opstartmedia** in de Cyber Protect-console.

Bestanden of mappen op afstand herstellen met opstartmedia:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Opstartmedia**.
1. Selecteer de media die u wilt gebruiken voor gegevensherstel.
2. Klik op **Herstel**.
3. Selecteer de locatie en vervolgens de gewenste back-up. Let op: back-ups worden gefilterd op locatie.
4. Selecteer het herstelpunt en klik vervolgens op **Bestanden/mappen herstellen**.
5. Blader naar de vereiste map of gebruik de zoekbalk om de lijst met de vereiste bestanden en mappen op te halen.
   Zoekopdrachten zijn taalonafhankelijk.
   U kunt een of meer jokertekens (* en ?) gebruiken. Zie "Bestandsfilters (uitsluiten/opnemen)" (p. 488) voor meer informatie over jokers.
6. Klik om de items te selecteren die u wilt herstellen en klik vervolgens op **Herstellen**.
7. Ga naar **Pad** en selecteer de herstelbestemming.
8. [Optioneel] Klik voor geavanceerde herstelconfiguratie op **Herstelopties**. Zie "Herstelopties" (p. 550) voor meer informatie.
9. Klik op **Herstel starten**.
10. Selecteer een van de opties voor het overschrijven van bestanden:
    - **Bestaande bestanden overschrijven**
    - **Een bestaand bestand overschrijven als dit ouder is**
    - **Bestaande bestanden niet overschrijven**

    Kies of u de machine automatisch opnieuw wilt opstarten.
11. Klik op **Doorgaan** om de herstelbewerking te starten. De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**.

Schijven, volumes of volledige machines op afstand herstellen met opstartmedia:

1. Ga op het tabblad **Apparaten** naar de groep **Opstartmedia** en selecteer vervolgens de media die u wilt gebruiken voor gegevensherstel.
2. Klik op **Herstel**.

3. Selecteer de locatie en vervolgens de gewenste back-up. Let op: back-ups worden gefilterd op locatie.
4. Selecteer het herstelpunt en klik vervolgens op **Herstellen** > **Volledige machine**.

   Configureer indien nodig de doelmachine en volumetoewijzing, zoals beschreven in "Fysieke machines herstellenIn dit gedeelte wordt beschreven hoe u fysieke machines herstelt met behulp van de webinterface.Gebruik in de volgende gevallen in plaats van de webinterface een opstartmedium:Een machine met macOSEen machine van een tenant in de compliancemodusElk besturingssysteem naar bare metal of naar een offline machineDe structuur van logische volumes (volumes die zijn gemaakt door Logical Volume Manager in Linux). Met de media kunt u de structuur van het logisch volume automatisch opnieuw maken.Back-ups op schijfniveau van Macs met Intel naar Macs met een Apple Silicon-processor (en omgekeerd) kunnen niet worden hersteld. U kunt bestanden en mappen herstellen.Een fysieke machine herstellenSelecteer de machine waarvan een back-up is gemaakt.Klik op Herstel.Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.Als de machine offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:Als de back-uplocatie cloudopslag of een gedeelde opslag is (dat wil zeggen dat andere agenten hier toegang toe hebben), klikt u op Machine selecteren, selecteert u een doelmachine die online is en selecteert u vervolgens een herstelpunt.Selecteer een herstelpunt op het tabblad Back-upopslag.Herstel de machine zoals wordt beschreven in 'Schijven herstellen met opstartmedia'.Klik op Herstellen > Volledige machine.De schijven uit de back-up worden automatisch toegewezen aan de schijven van de doelmachine.Als u wilt herstellen naar een andere fysieke machine, klikt u op Doelmachine en selecteert u vervolgens een doelmachine die online is.Als u niet tevreden bent over het toewijzingsresultaat of als de schijftoewijzing mislukt, klikt u op Volumetoewijzing om de schijven handmatig opnieuw toe te wijzen.In het toewijzingsgedeelte kunt u ook afzonderlijke schijven of volumes kiezen die moeten worden hersteld. U kunt schakelen tussen het herstel van schijven en volumes met de koppeling Overschakelen naar... in de rechterbovenhoek.[Alleen beschikbaar voor Windows-machines waarop een beveiligingsagent is geïnstalleerd] Gebruik de schakelaar om Veilig herstel in te schakelen zodat u zeker weet dat de herstelde gegevens geen malware bevatten. Zie "Veilig herstel" (p. 1) voor meer informatie over hoe veilig herstel werkt.Klik op Herstel starten.Bevestig dat u de schijven wilt overschrijven met de back-ups. Kies of u de machine automatisch opnieuw wilt opstarten.De voortgang van de herstelbewerking wordt weergegeven op het tabblad Activiteiten." (p. 1).
5. Klik voor geavanceerde herstelconfiguratie op **Herstelopties**. Zie "Herstelopties" (p. 550) voor meer informatie.
6. Klik op **Herstel starten**.
7. Bevestig dat u de schijven wilt overschrijven met de back-ups. Kies of u de machine automatisch opnieuw wilt opstarten.
8. De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**.

De opgestarte machine op afstand opnieuw opstarten:

1. Ga op het tabblad **Apparaten** naar de groep **Opstartmedia** en selecteer vervolgens de media die u wilt gebruiken voor gegevensherstel.
2. Klik op **Opnieuw opstarten**.
3. Bevestig dat u de met de media opgestarte machine opnieuw wilt opstarten.

De opgestarte machine op afstand afsluiten:

1. Ga op het tabblad **Apparaten** naar de groep **Opstartmedia** en selecteer vervolgens de media die u wilt gebruiken voor gegevensherstel.
2. Klik op **Afsluiten**.
3. Bevestig dat u de met de media opgestarte machine wilt afsluiten.

Informatie over de opstartmedia bekijken:

1. Ga op het tabblad **Apparaten** naar de groep **Opstartmedia** en selecteer vervolgens de media die u wilt gebruiken voor gegevensherstel.
2. Klik op **Details**, **Activiteiten** of **Waarschuwingen** om de bijbehorende informatie te zien.

Opstartmedia op afstand verwijderen:

1. Ga op het tabblad **Apparaten** naar de groep **Opstartmedia** en selecteer vervolgens de media die u wilt gebruiken voor gegevensherstel.
2. Klik op **Verwijderen** om de opstartmedia te verwijderen uit de Cyber Protect-console.
3. Bevestig dat u de opstartmedia wilt verwijderen.

Startup Recovery Manager

Startup Recovery Manager is een opstartbaar onderdeel dat zich op de harde schijf bevindt. Met Startup Recovery Manager kunt u het opstartbare hulpprogramma voor herstel starten zonder een afzonderlijk opstartmedium te gebruiken.

In het geval van een storing wordt de machine opnieuw opgestart. Wacht tot de prompt **Druk op F11 voor Acronis Startup Recovery Manager** wordt weergegeven en druk vervolgens op F11 of selecteer Startup Recovery Manager in het opstartmenu (als u de GRUB-opstartlader gebruikt). Startup Recovery Manager wordt opgestart en u kunt dan een herstelbewerking uitvoeren.

Startup Recovery Manager wordt ondersteund voor Windows- en Linux-machines.

Belangrijk
Als u Startup Recovery Manager activeert op een machine met een versleuteld systeemvolume, moet er ten minste één niet-versleuteld volume op dezelfde machine bestaan.

Schijfruimtevereisten

Startup Recovery Manager vereist schijfruimte voor tijdelijke bestanden. De vereisten variëren afhankelijk van de machine waarop Startup Recovery Manager is geactiveerd.

De onderstaande tabel bevat een overzicht van de beschikbare opties.

Opstartmodus	Machine zonder Secure Zone		Machine met Secure Zone
	Met niet-versleuteld systeemvolume	Met versleuteld systeemvolume	Met versleuteld of niet-versleuteld systeemvolume
BIOS	200 MB op het systeemvolume	400 MB op een niet-versleuteld volume	400 MB op Secure Zone
UEFI	200 MB op de EFI-systeempartitie (ESP)	Eén van het volgende: • 400 MB op de EFI-systeempartitie (ESP) • 200 MB op de EFI-systeempartitie (ESP) en 200 MB op een onversleutelde partitie die toegankelijk is tijdens het opstartproces	400 MB op Secure Zone

Opmerking
Voor herstel met opnieuw opstarten is extra schijfruimte vereist. Als u wilt controleren hoeveel extra ruimte nodig is: zie "Vereisten voor schijfruimte" (p. 536).

Beperkingen

- [Niet van toepassing op GRUB op de Master Boot Record] Door activering van Startup Recovery Manager wordt de Master Boot Record (MBR) overschreven met de eigen opstartcode. Mogelijk moet u dan alle externe opstartladers opnieuw activeren na de activering.
- [Niet van toepassing op GRUB] Voordat u Startup Recovery Manager activeert in Linux, raden we aan dat u de opstartlader installeert in de opstartrecord van de hoofdpartitie of in de opstartrecord van de /opstartpartities en niet in de Master Boot Record. Zo niet, dan configureert u de opstartlader handmatig opnieuw na de activering.

Startup Recovery Manager activeren ...

Voor activering van de opstartprompt **Druk op F11 voor Acronis Startup Recovery Manager** (of voeg het item **Startup Recovery Manager** toe aan het GRUB-menu) moet u Startup Recovery Manager activeren.

Opmerking
Back-upbewerkingen waarbij back-ups worden gemaakt met Herstel met één klik, mislukken als Startup Recovery Manager niet is geactiveerd.

Startup Recovery Manager activeren

Op een machine met agent

1. In de Cyber Protect-console: selecteer de machine waarop u Startup Recovery Manager wilt activeren.
2. Klik op **Details**.
3. Zet de schakelaar **Startup Recovery Manager** aan.

Op een machine zonder agent

1. Start de machine via een opstartmedium.
2. Open de grafische interface van het opstartmedium en klik op **Gereedschap** > **Activeren Startup Recovery Manager**.
3. Selecteer **Activeren**.
4. Klik op **OK**.
5. Open het tabblad **Details** en bekijk de rij **Resultaat** om te verifiëren of de activering is uitgevoerd.
6. Klik op **Sluiten**.

Startup Recovery Manager deactiveren ...

Met deactivering wordt de opstartprompt **Druk op F11 voor Acronis Startup Recovery Manager** uitgeschakeld (of wordt het item **Startup Recovery Manager** verwijderd uit het GRUB-menu).

Als Startup Recovery Manager niet is geactiveerd, kunt u een machine die niet kan worden opgestart, toch nog herstellen via een apart opstartmedium.

Opmerking
Back-upbewerkingen waarbij back-ups worden gemaakt met Herstel met één klik, mislukken als Startup Recovery Manager niet is geactiveerd.

Startup Recovery Manager deactiveren

Op een machine met agent

1. In de Cyber Protect-console: selecteer de machine waarop u Startup Recovery Manager wilt deactiveren.
2. Klik op **Details**.
3. Zet de schakelaar **Startup Recovery Manager** uit.

Op een machine zonder agent

1. Start de machine via een opstartmedium.
2. Open de grafische interface van het opstartmedium en klik op **Gereedschap** > **Deactiveren Startup Recovery Manager**.

3. Selecteer **Deactiveren**.
4. Klik op **OK**.
5. Open het tabblad **Details** en bekijk de rij **Resultaat** om te verifiëren of de deactivering is uitgevoerd.
6. Klik op **Sluiten**.

Noodherstel implementeren

Opmerking
Deze functionaliteit biedt geen ondersteuning voor back-uplocaties van Microsoft Azure.

Over Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) – een deel van Cyber Protection dat Disaster Recovery as a Service (DRaaS) biedt. Cyber Disaster Recovery Cloud biedt u een snelle en stabiele oplossing om de exacte kopieën van uw machines op de cloudsite te starten en de workload van de beschadigde oorspronkelijke machines te verplaatsen naar de herstelservers in de cloud in het geval van een door de natuur of de mens veroorzaakte ramp.

U kunt noodherstel op de volgende manieren instellen en configureren:

- Maak een beschermingsschema dat de module Noodherstel bevat en pas het toe op uw apparaten. Hierdoor wordt automatisch een standaardinfrastructuur voor noodherstel ingesteld. Zie Een beschermingsschema voor noodherstel maken.
- Stel de cloudinfrastructuur voor de noodherstelfunctie handmatig in en beheer elke stap. Zie "Herstelservers instellen" (p. 823).

Belangrijkste functionaliteit

Opmerking
Voor sommige functies zijn mogelijk extra licenties vereist, afhankelijk van het toegepaste licentiemodel.

- De Cyber Disaster Recovery Cloud-service beheren vanuit een enkele console
- Tot 23 lokale netwerken uitbreiden naar de cloud via een veilige VPN-tunnel
- Verbinding met de cloudsite maken zonder implementatie van een VPN-toepassing[1] (de modus Alleen cloud)
- Point-to-site-verbinding tot stand brengen met uw lokale en cloudsites
- Uw machines beveiligen door gebruik te maken van herstelservers in de cloud
- Toepassingen en apparaten beveiligen door gebruik te maken van primaire servers in de cloud
- Automatische noodherstelbewerkingen uitvoeren voor versleutelde back-ups
- Een testfailover uitvoeren in het geïsoleerde netwerk
- Runbooks gebruiken om de productieomgeving in de cloud bedrijfsklaar te maken

[1] [Noodherstel] Een speciale virtuele machine die een verbinding via een beveiligde VPN-tunnel tot stand brengt tussen het lokale netwerk en de cloudsite. De VPN-toepassing wordt geïmplementeerd op de lokale site.

Softwarevereisten

Ondersteunde besturingssystemen

Beveiliging met een herstelserver is getest voor de volgende besturingssystemen:

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.x, 21.x
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – alle installatieopties, met uitzondering van Nano Server
- Windows Server 2019 – alle installatieopties, met uitzondering van Nano Server
- Windows Server 2022 – alle installatieopties, met uitzondering van Nano Server

De software werkt mogelijk met andere Windows-besturingssystemen en Linux-distributies, maar dit is niet gegarandeerd.

Opmerking
Bescherming met een herstelserver is getest voor Microsoft Azure VM met de volgende besturingssystemen.

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – alle installatieopties, met uitzondering van Nano Server
- Windows Server 2019 – alle installatieopties, met uitzondering van Nano Server
- Windows Server 2022 – alle installatieopties, met uitzondering van Nano Server
- Ubuntu Server 20.04 LTS - Gen2 (Canonical). Ga naar https://kb.acronis.com/content/71616 voor meer informatie over toegang tot de herstelserverconsole.

Ondersteunde virtualisatieplatforms

Beveiliging van virtuele machines met een herstelserver is getest voor de volgende virtualisatieplatforms:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 met Hyper-V
- Windows Server 2012/2012 R2 met Hyper-V

- Windows Server 2016 met Hyper-V – alle installatieopties, met uitzondering van Nano Server
- Windows Server 2019 met Hyper-V – alle installatieopties, met uitzondering van Nano Server
- Windows Server 2022 met Hyper-V – alle installatieopties, met uitzondering van Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Kernel-based Virtual Machines (KVM): alleen volledig gevirtualiseerde gasten (HVM). Paravirtual gasten (PV) worden niet ondersteund.
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

De VPN-toepassing is getest voor de volgende virtualisatieplatforms:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 met Hyper-V
- Windows Server 2012/2012 R2 met Hyper-V
- Windows Server 2016 met Hyper-V – alle installatieopties, met uitzondering van Nano Server
- Windows Server 2019 met Hyper-V – alle installatieopties, met uitzondering van Nano Server
- Windows Server 2022 met Hyper-V – alle installatieopties, met uitzondering van Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

De software werkt mogelijk met andere virtualisatieplatforms en versies, maar dit is niet gegarandeerd.

Beperkingen

De volgende platforms en configuraties worden niet ondersteund in Cyber Disaster Recovery Cloud:

1. Niet-ondersteunde platforms:
   - Agent voor Virtuozzo
   - macOS
   - Besturingssystemen voor Windows-desktop worden niet ondersteund vanwege Microsoft-productvoorwaarden.
   - Windows Server Azure Edition

     Azure Edition is een speciale versie van Windows Server die specifiek is gebouwd om te worden uitgevoerd als een Azure IaaS virtuele machine (VM) in Azure of als een VM op een Azure Stack HCI-cluster. In tegenstelling tot de Standard- en Datacenter-edities heeft Azure Edition geen licentie om te worden uitgevoerd op bare metal hardware, Windows client Hyper-V, Windows Server Hyper-V, hypervisors van derden, of in clouds van derden.

2. Niet-ondersteunde configuraties:

   Microsoft Windows

   - Dynamische schijven worden niet ondersteund
   - Besturingssystemen voor Windows-desktop worden niet ondersteund (vanwege Microsoft-productvoorwaarden)
   - Active Directory-service met FRS-replicatie wordt niet ondersteund
   - Verwisselbare media zonder GPT- of MBR-indeling (zogenaamde 'superfloppy') worden niet ondersteund

   Linux

   - Bestandssystemen zonder partitietabel
   - Linux-workload s waarvan een back-up wordt gemaakt met een agent vanuit een gastbesturingssysteem en die volumes hebben met de volgende geavanceerde LVM-configuraties (Logical Volume Manager): Striped volumes, gespiegelde volumes, RAID 0-, RAID 4-, RAID 5-, RAID 6- of RAID 10-volumes.

   Opmerking
   Workloads waarvoor meerdere besturingssystemen zijn geïnstalleerd, worden niet ondersteund.

3. Niet-ondersteunde back-uptypen:
   - CDP-herstelpunten (Continuous Data Protection) zijn niet compatibel.

     Belangrijk
     Als u een herstelserver maakt van een back-up met een CDP-herstelpunt, dan gaan de gegevens in het CDP-herstelpunt verloren tijdens de failback of het maken van een back-up van een herstelserver.

   - Forensische back-ups kunnen niet worden gebruikt voor het maken van herstelservers.

Een herstelserver heeft één netwerkinterface. Als de oorspronkelijke machine meerdere netwerkinterfaces heeft, wordt er slechts één geëmuleerd.

Cloudservers worden niet versleuteld.

Cyber Disaster Recovery Cloud-proefversie

U kunt een proefversie van Acronis Cyber Disaster Recovery Cloud gebruiken gedurende 30 dagen. In dit geval heeft Noodherstel de volgende beperkingen voor partnertenants:

- Geen toegang tot openbaar internet voor herstel- en primaire servers. U kunt geen openbare IP-adressen toewijzen aan de servers.
- IPsec Multi-site VPN is niet beschikbaar.

Beperkingen bij het gebruik van Geo-redundant Cloud Storage

Geo-redundant Cloud Storage biedt een secundaire locatie voor uw back-upgegevens. De secundaire locatie bevindt zich in een regio die geografisch verschilt van de primaire opslaglocatie. Door de geografische scheiding van regio's kunnen de activiteiten doorgaan zelfs als er een ramp plaatsvindt in een van de regio's en de back-upgegevens niet meer kunnen worden hersteld, omdat de andere regio niet wordt getroffen.

Belangrijk
De Disaster Recovery-service wordt niet ondersteund als de back-upopslaglocatie wordt overgeschakeld van de primaire locatie naar de geo-redundante secundaire locatie.

Compatibiliteit van noodherstel met versleutelingssoftware

Noodherstel is compatibel met de volgende versleutelingssoftware op schijfniveau:

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

Opmerking
- Voor workloads met versleuteling op schijfniveau raden we aan dat u de beschermingsagent installeert in het gastbesturingssysteem van de workload en back-ups met agent uitvoert.
- Failover en failback worden niet ondersteund voor back-ups van versleutelde workloads zonder agent.

Voor meer informatie over de compatibiliteit van Cyber Protection met versleutelingssoftware: zie "Compatibiliteit met versleutelingssoftware" (p. 42).

Compute-punten

In Diasaster Recovery worden compute-punten gebruikt voor primaire servers en herstelservers tijdens testfailover en productiefailover. Compute-punten komen overeen met de compute-resources die worden gebruikt voor het uitvoeren van de servers (virtuele machines) in de cloud.

Het verbruik van compute-punten tijdens het noodherstel hangt af van de parameters van de server en van hoe lang de server zich in de failoverstatus bevindt. Hoe krachtiger de server en hoe langer de periode, des te meer compute-punten worden verbruikt. En hoe meer compute-punten worden verbruikt, hoe hoger de prijs die u wordt aangerekend.

Voor alle servers die worden uitgevoerd in de Acronis Cloud, worden compute-punten in rekening gebracht, afhankelijk van de geconfigureerde variant, en ongeacht de status (ingeschakeld of uitgeschakeld).

Herstelservers in standby-status verbruiken geen compute-punten en er worden geen compute-punten in rekening gebracht.

In de onderstaande tabel ziet u een voorbeeld van acht servers in de cloud met verschillende varianten, en de bijbehorende compute-punten die ze zullen verbruiken per uur. U kunt de varianten van de servers wijzigen op het tabblad **Details**.

Type	CPU	RAM	Compute-punten
F1	1 vCPU	2 GB	1
F2	1 vCPU	4 GB	2
F3	2 vCPU's	8 GB	4
F4	4 vCPU's	16 GB	8
F5	8 vCPU's	32 GB	16
F6	16 vCPU's	64 GB	32
F7	16 vCPU's	128 GB	64
F8	16 vCPU's	256 GB	128

Met behulp van de informatie in de tabel kunt u gemakkelijk schatten hoeveel compute-punten een server (virtuele machine) zal verbruiken.

Als u met Noodherstel bijvoorbeeld één virtuele machine met 4 vCPU's* van 16 GB RAM wilt beschermen, en één virtuele machine met 2 vCPU's met 8 GB RAM, zal de eerste virtuele machine 8 compute-punten per uur verbruiken, en de tweede virtuele machine 4 compute-punten per uur. Als beide virtuele machines in failover zijn, is het totale verbruik 12 compute-punten per uur, ofwel 288 compute-punten voor de hele dag (12 compute-punten x 24 uur = 288 compute-punten).

* vCPU is een fysieke centrale verwerkingseenheid (CPU) die is toegewezen aan een virtuele machine. De vCPU is een tijdsafhankelijke entiteit.

Opmerking
Als de quotumuitbreiding van de **Compute-punten** is bereikt, worden alle primaire en herstelservers afgesloten. U kunt deze servers dan niet meer gebruiken tot het begin van de volgende factureringsperiode, of totdat u het quotum verhoogt. De standaard factureringsperiode is een volledige kalendermaand.

De noodherstelfunctie instellen

Opmerking
Voor sommige functies zijn mogelijk extra licenties vereist, afhankelijk van het toegepaste licentiemodel.

De noodherstelfunctie instellen

1. Het type connectiviteit met de cloudsite configureren:
   - Point-to-site-verbinding
   - Site-to-site OpenVPN-verbinding
   - Multi-site IPsec VPN-verbinding
   - Modus Alleen cloud
2. Maak een beschermingsschema terwijl de back-upmodule is ingeschakeld en selecteer de hele machine of het systeem plus opstartvolumes voor het maken van back-ups. Er is ten minste één beschermingsschema vereist voor het maken van een herstelserver.
3. Pas het beschermingsschema toe op de lokale servers die u wilt beschermen.
4. Maak de herstelservers voor elke lokale server die u wilt beveiligen.
5. Voer een testfailover uit om te controleren hoe het werkt.
6. [Optioneel] Maak de primaire servers voor toepassingsreplicatie.

U hebt nu de functionaliteit voor noodherstel ingesteld om uw lokale servers te beschermen tegen een ramp.

Als er zich een ramp voordoet, kunt u een failover van de workload uitvoeren naar de herstelservers in de cloud. Er moet ten minste één herstelpunt worden gemaakt voordat er wordt overgeschakeld naar herstelservers. Wanneer uw lokale site is hersteld van een ramp, kunt u de workload terugverplaatsen naar uw lokale site door een failback uit te voeren. Zie "Vereisten" (p. 837) en "Vereisten" (p. 842) voor meer informatie over het failbackproces.

Een beschermingsschema voor noodherstel maken

Maak een beschermingsschema dat de module Noodherstel bevat en pas het toe op uw apparaten.

Standaard is de module Noodherstel uitgeschakeld wanneer u een nieuw beschermingsschema maakt. Wanneer u de functionaliteit voor noodherstel hebt ingeschakeld en het schema hebt toegepast op uw apparaten, wordt voor elk beschermd apparaat de cloudnetwerkinfrastructuur gemaakt, met inbegrip van een *herstelserver*. De *herstelserver:* is een virtuele machine in de cloud die een kopie is van het geselecteerde apparaat. Voor elk van de geselecteerde apparaten wordt een herstelserver met standaardinstellingen gemaakt in stand-bystatus (virtuele machine niet actief). De grootte van de herstelserver wordt automatisch afgestemd op de CPU en het RAM van het

beschermde apparaat. De standaardcloudinfrastructuur wordt ook automatisch gemaakt: De VPN-gateway en netwerken op de cloudsite waarmee de herstelservers worden verbonden.

Als u de module Noodherstel van een beschermingsschema intrekt, verwijdert of uitschakelt, worden de herstelservers en cloudnetwerken niet automatisch verwijderd. Indien nodig, kunt u de infrastructuur voor noodherstel handmatig verwijderen.

Opmerking

- Wanneer u noodherstel hebt geconfigureerd, kunt u een test- of productiefailover uitvoeren vanaf een van de herstelpunten die zijn gegenereerd nadat de herstelserver is gemaakt voor het apparaat. Herstelpunten die zijn gegenereerd voordat het apparaat was beschermd met noodherstel (bijvoorbeeld voordat de herstelserver was gemaakt), kunnen niet worden gebruikt voor failover.
- Een beschermingsschema voor noodherstel kan niet worden ingeschakeld als het IP-adres van een apparaat niet kan worden gedetecteerd. Bijvoorbeeld wanneer back-ups van virtuele machines worden gemaakt zonder agents en hieraan geen IP-adres is toegewezen.
- Wanneer u een beschermingsschema toepast, worden dezelfde netwerken en IP-adressen toegewezen op de cloudsite. De IPsec VPN-connectiviteit vereist dat de netwerksegmenten van de cloud en de lokale sites elkaar niet overlappen. Als een multi-site IPsec VPN-verbinding is geconfigureerd en u later een beschermingsschema toepast op een of meer apparaten, moet u ook de cloudnetwerken bijwerken en de IP-adressen van de cloudservers opnieuw toewijzen. Zie "IP-adressen opnieuw toewijzen" (p. 813) voor meer informatie.

Een beschermingsschema voor noodherstel maken

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de machines die u wilt beschermen.
3. Klik op **Beschermen** en vervolgens op **Schema maken**.
   Het beschermingsschema met de standaardinstellingen wordt dan geopend.
4. Configureer de back-upopties.
   Als u de noodherstelfunctie wilt gebruiken, moet dit schema een back-up maken van de volledige machine of alleen van de schijven die zijn vereist om de nodige services op te starten en te leveren naar een cloudopslag.
5. Schakel de module Noodherstel in door op de schakelaar naast de naam van de module te klikken.
6. Klik op **Maken**.
   Het schema wordt gemaakt en toegepast op de geselecteerde machines.

Volgende stappen

- U kunt de standaardconfiguratie van de herstelserver bewerken. Zie "Herstelservers instellen" (p. 823) voor meer informatie.
- U kunt de standaardnetwerkconfiguratie bewerken. Zie "Connectiviteit instellen" (p. 785) voor meer informatie.

- U kunt meer te weten komen over de standaardparameters van de herstelserver en de cloudnetwerkinfrastructuur. Zie "De standaardparameters voor de herstelserver bewerken" (p. 783) en "Cloudinfrastructuur" (p. 784) voor meer informatie.

De standaardparameters voor de herstelserver bewerken

Wanneer u een beschermingsschema voor noodherstel maakt en toepast, wordt een herstelserver met standaardparameters gemaakt. U kunt deze standaardparameters later bewerken.

Opmerking
Een herstelserver wordt alleen gemaakt als deze niet bestaat. Bestaande herstelservers worden niet gewijzigd of opnieuw gemaakt.

De standaardparameters voor de herstelserver bewerken

1. Ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer een apparaat en klik op **Noodherstel**.
3. Bewerk de standaardparameters van de herstelserver.
   De parameters van de herstelserver worden beschreven in de volgende tabel.

Herstelserver parameter	Standaard waarde	Beschrijving
CPU en RAM	automatisch	Het aantal virtuele CPU's en de hoeveelheid RAM voor de herstelserver. De standaardinstellingen worden automatisch bepaald op basis van de oorspronkelijke CPU- en RAM-configuratie van het apparaat.
Cloudnetwerk	automatisch	Het cloudnetwerk waarmee de server wordt verbonden. Zie Cloudnetwerkinfrastructuur voor details over de configuratie van cloudnetwerken.
IP-adres in productienetwerk	automatisch	Het IP-adres voor de server in het productienetwerk. Standaard wordt het IP-adres van de oorspronkelijke machine ingesteld.
IP-adres testen	uitgeschakeld	Met Test-IP-adres kunt u een failover testen in het geïsoleerde testnetwerk en verbinding maken met de herstelserver via RDP of SSH tijdens een testfailover. In de testfailovermodus vervangt de VPN-gateway het test-IP-adres door het productie-IP-adres via het NAT-protocol. Als u geen test-IP-adres opgeeft, is de console de enige manier om toegang te krijgen tot de server tijdens een testfailover.

Internettoegang	ingeschakeld	Geef de herstelserver toegang tot internet tijdens een echte of testfailover. Standaard wordt TCP-poort 25 geweigerd voor uitgaande verbindingen.
Openbaar adres gebruiken	uitgeschakeld	Als u een openbaar IP-adres hebt, is de herstelserver beschikbaar via internet tijdens een failover of test-failover. Als u geen openbaar IP-adres gebruikt, is de server alleen beschikbaar in uw productienetwerk. Als u een openbaar IP-adres wilt gebruiken, moet u internettoegang inschakelen. Het openbare IP-adres wordt weergegeven wanneer u de configuratie hebt voltooid. Standaard staat TCP-poort 443 open voor inkomende verbindingen.
RPO-drempel instellen	uitgeschakeld	De RPO-drempel bepaalt het maximaal toegestane tijdsinterval tussen het laatste herstelpunt en de huidige tijd. De waarde kan worden ingesteld op 15 - 60 minuten, 1 - 24 uur, 1 - 14 dagen.

Cloudinfrastructuur

De cloudnetwerkinfrastructuur bestaat uit de VPN-gateway op de cloudsite en cloudnetwerken waarmee de herstelservers worden verbonden.

Opmerking
Als u een beschermingsschema voor noodherstel toepast, wordt alleen een cloudnetwerkinfrastructuur gemaakt als dit niet bestaat. Bestaande cloudnetwerken worden niet gewijzigd of opnieuw gemaakt.

De IP-adressen van apparaten worden gecontroleerd en worden automatisch geschikte cloudnetwerken gemaakt als er geen bestaande cloudnetwerken zijn die passen bij een IP-adres. Als u al bestaande cloudnetwerken hebt die passen bij de IP-adressen van de herstelservers, dan worden de bestaande cloudnetwerken niet gewijzigd of opnieuw gemaakt.

- Als u geen bestaande cloudnetwerken hebt of als u voor het eerst een configuratie voor noodherstel instelt, worden de cloudnetwerken gemaakt met maximale bereiken, zoals door IANA aanbevolen voor privégebruik (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), op basis van het IP-adresbereik van uw apparaten. U kunt uw netwerk verfijnen door het netwerkmasker te bewerken.
- Als u apparaten in meerdere lokale netwerken hebt, kan het netwerk op de cloudsite een superset van de lokale netwerken worden. U kunt netwerken opnieuw configureren in het gedeelte **Connectiviteit**. Zie "Netwerken beheren" (p. 806).

- Als u site-to-site OpenVPN-connectiviteit wilt instellen, downloadt u de VPN-toepassing en stelt u deze in. Zie "Site-to-site Open VPN configureren" (p. 796). Controleer of het bereik van uw cloudnetwerken overeenkomt met het bereik van uw lokale netwerk dat is aangesloten op de VPN-toepassing.
- Als u de standaardconfiguratie van het netwerk wilt wijzigen, klikt u op de link **Ga naar connectiviteit** in de module Noodherstel van het beschermingsschema of gaat u naar **Noodherstel** > **Connectiviteit**.

Connectiviteit instellen

In deze sectie worden de netwerkconcepten uitgelegd die nodig zijn om alle functionaliteit van Cyber Disaster Recovery Cloud te begrijpen. U leert hoe u verschillende typen connectiviteit met de cloudsite kunt configureren, al naargelang uw behoeften. Tot slot leert u hoe u uw netwerken in de cloud en de instellingen van de VPN-toepassing en de VPN-gateway kunt beheren.

Netwerkconcepten

Opmerking
Voor sommige functies zijn mogelijk extra licenties vereist, afhankelijk van het toegepaste licentiemodel.

Met Cyber Disaster Recovery Cloud kunt u de volgende typen connectiviteit voor de cloudsite definiëren:

- **Modus Alleen cloud**

  Voor dit type verbinding hoeft u geen VPN-toepassing te implementeren op de lokale site.

  Het lokale netwerk en het cloudnetwerk zijn twee onafhankelijke netwerken. Dit type verbinding impliceert ofwel de failover van alle beveiligde servers van de lokale site ofwel een gedeeltelijke failover van onafhankelijke servers die niet met de lokale site hoeven te communiceren.

  Cloudservers op de cloudsite zijn toegankelijk via het point-to-site-VPN en openbare IP-adressen (indien toegewezen).
- **Site-to-site OpenVPN-verbinding**

  Voor dit type verbinding moet u een VPN-toepassing implementeren op de lokale site.

  Met de site-to-site OpenVPN-verbinding kunt u uw netwerken uitbreiden naar de cloud en de IP-adressen behouden.

  Uw lokale site is nu uitgebreid naar de cloudsite via een veilige VPN-tunnel. Dit type verbinding is geschikt als u sterk afhankelijke servers op de lokale site hebt, zoals een webserver en een databaseserver. Wanneer een van deze servers opnieuw wordt gemaakt op de cloudsite terwijl de andere op de lokale site blijft, kunnen deze servers in het geval van een gedeeltelijke failover toch nog met elkaar communiceren via een VPN-tunnel.

  Cloudservers op de cloudsite zijn toegankelijk via het lokale netwerk, het point-to-site-VPN en openbare IP-adressen (indien toegewezen).
- **Multi-site IPsec VPN-verbinding**

Voor dit type verbinding is een lokaal VPN-apparaat nodig dat IPsec IKE v2 ondersteunt.

Wanneer u de multi-site IPsec VPN-verbinding begint te configureren, wordt er door Cyber Disaster Recovery Cloud automatisch een Cloud VPN-gateway met een openbaar IP-adres gemaakt.

Met multi-site IPsec VPN worden uw lokale sites verbonden met de cloudsite via een beveiligde IPsec VPN-tunnel.

Dit type verbinding is geschikt voor noodherstelscenario's wanneer één of meerdere lokale sites kritieke workloads of onderling sterk afhankelijke services hosten.

In het geval van een gedeeltelijke failover van een van de servers wordt de server opnieuw gemaakt op de cloudsite terwijl de andere op de lokale site blijven. Deze servers kunnen dan toch nog met elkaar communiceren via een IPsec VPN-tunnel.

In het geval van een gedeeltelijke failover van een van de lokale sites blijft de rest van de lokale sites gewoon werken en ze kunnen toch nog met elkaar communiceren via een IPsec VPN-tunnel.

- **Externe point-to-site-VPN-toegang**

  Een veilige externe point-to-site-VPN-toegang tot de workloads op uw cloudsite en lokale site via uw eindpuntapparaat.

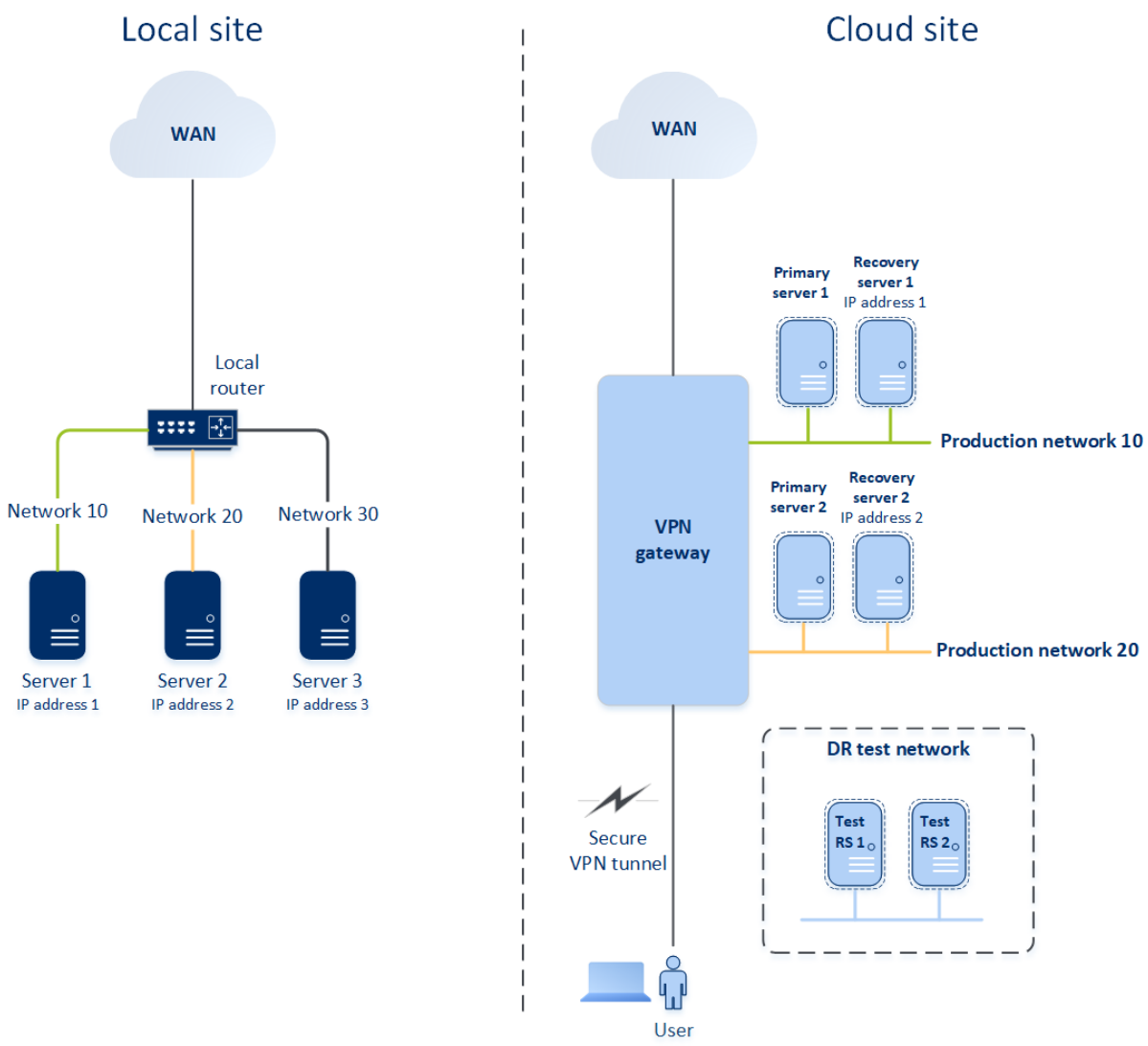
  Voor toegang tot een lokale site met dit type verbinding moet u een VPN-toepassing implementeren op de lokale site.

Modus Alleen cloud

Voor de modus Alleen cloud hoeft u geen VPN-toepassing te implementeren op de lokale site. Dit betekent dat u twee onafhankelijke netwerken hebt: een op de lokale site en een op de cloudsite. De routering wordt uitgevoerd met de router op de cloudsite.

Hoe routering werkt

In het geval dat de modus 'alleen-cloud' is ingesteld, wordt de routering uitgevoerd met de router op de cloudsite, zodat servers van verschillende cloudnetwerken met elkaar kunnen communiceren.



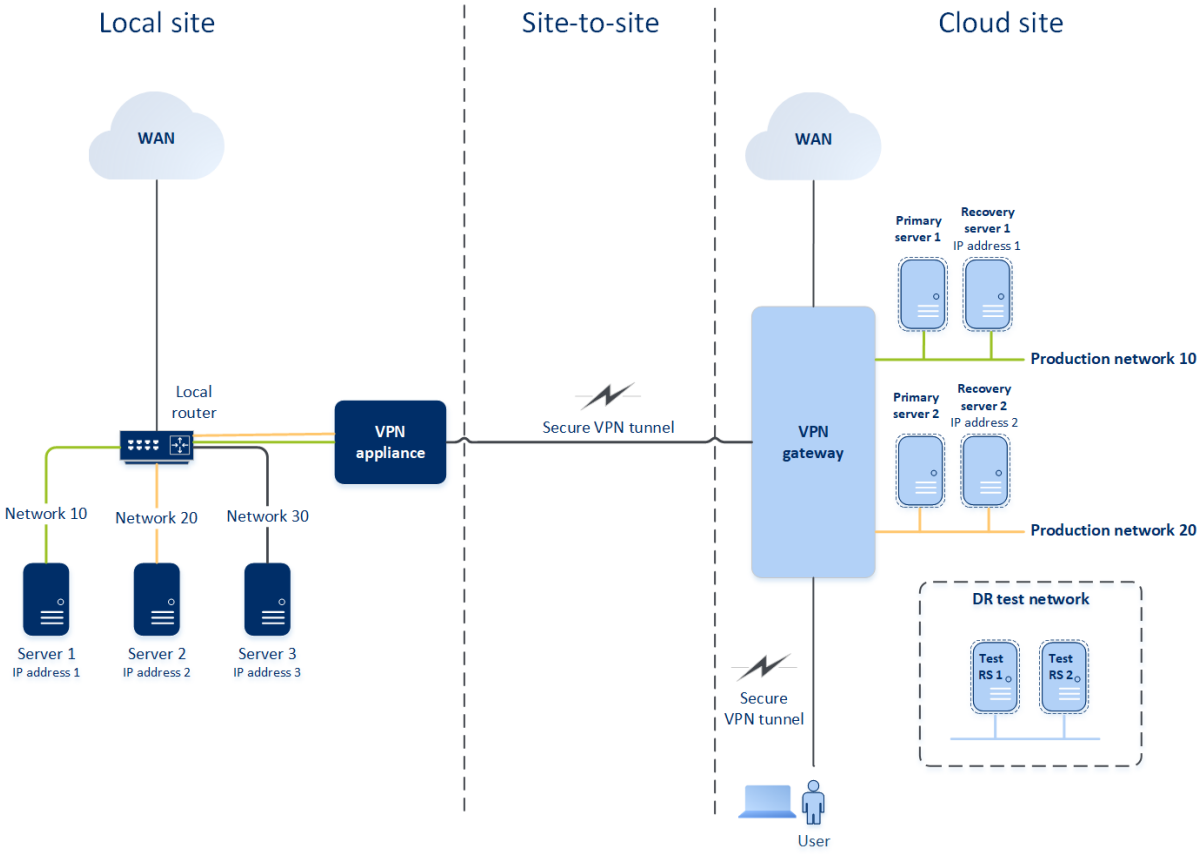
Site-to-site OpenVPN-verbinding

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

We laten zien hoe netwerken functioneren in Cyber Disaster Recovery Cloud aan de hand van een geval waar u drie netwerken hebt met elk één machine op de lokale site. U gaat de beveiliging tegen een ramp configureren voor de twee netwerken Netwerk 10 en Network 20.

In de onderstaande afbeelding ziet u de lokale site waar uw machines worden gehost en de cloudsite waar de cloudservers worden gestart in geval van een ramp.

Met de Cyber Disaster Recovery Cloud-oplossing kunt u een failover van de hele workload van de beschadigde machines op de lokale site uitvoeren naar de cloudservers in de cloud. U kunt tot 23 netwerken beschermen met Cyber Disaster Recovery Cloud.



Voor eventuele site-to-site OpenVPN-communicatie tussen de lokale site en de cloudsite wordt gebruikgemaakt van een **VPN-toepassing** en een **VPN-gateway**. Wanneer u begint met het configureren van de site-to-site OpenVPN-verbinding in de Cyber Protect-console, wordt de VPN-gateway automatisch geïmplementeerd op de cloudsite. Vervolgens moet u de VPN-toepassing implementeren op uw lokale site, de netwerken toevoegen die u wilt beveiligen en de toepassing in de cloud registreren. Cyber Disaster Recovery Cloud maakt een replica van uw lokale netwerk in de cloud. Er wordt een veilige VPN-tunnel tot stand gebracht tussen de VPN-toepassing en de VPN-gateway. Hiermee wordt uw lokale netwerk uitgebreid naar de cloud. Er wordt een brug gemaakt tussen de productienetwerken in de cloud en uw lokale netwerken. De lokale en cloudservers kunnen communiceren via deze VPN-tunnel alsof ze zich allemaal in hetzelfde ethernetsegment bevinden. De routering wordt uitgevoerd met uw lokale router.

Voor elke bronmachine die u wilt beveiligen, moet u een herstelserver maken op de cloudsite. Deze blijft de status **Stand-by** behouden totdat er een failovergebeurtenis plaatsvindt. Als er zich een ramp voordoet en u een failoverproces start (in de **productiemodus**), wordt de herstelserver die een exacte kopie van uw beschermde machine is, gestart in de cloud. Deze kan hetzelfde IP-adres krijgen als de bronmachine en in hetzelfde ethernetsegment worden gestart. Uw klanten kunnen blijven werken met de server, zonder de veranderingen op de achtergrond op te merken.

U kunt een failoverproces ook starten in de **testmodus**. Dit betekent dat de bronmachine nog werkt en dat tegelijkertijd de betreffende herstelserver met hetzelfde IP-adres in de cloud wordt gestart. In de cloud wordt een speciaal virtueel netwerk gemaakt (**testnetwerk**) om IP-adresconflicten te voorkomen. Het testnetwerk is geïsoleerd om duplicatie van het IP-adres van de bronmachine in

één ethernetsegment te voorkomen. Als u toegang wilt krijgen tot de herstelserver in de failovertestmodus, moet u het **test-IP-adres** toewijzen aan een herstelserver wanneer u deze maakt. Er zijn andere parameters voor de herstelserver die u kunt opgeven. Deze worden in de volgende gedeelten behandeld.

Hoe routering werkt

Wanneer een site-to-site-verbinding tot stand wordt gebracht, wordt de routering tussen cloudnetwerken uitgevoerd met uw lokale router. De VPN-server voert geen routering uit tussen cloudservers in verschillende cloudnetwerken. Als een cloudserver van een netwerk gaat communiceren met een server van een ander cloudnetwerk, wordt het verkeer door de VPN-tunnel naar de lokale router op de lokale site geleid en dan door de lokale router naar een ander netwerk gerouteerd. Vervolgens gaat het verkeer terug door de tunnel naar de bestemmingsserver op de cloudsite.

VPN-gateway

Het belangrijkste onderdeel dat de communicatie tussen de lokale site en cloudsite mogelijk maakt, is de **VPN-gateway**. Het is een virtuele machine in de cloud waarop de speciale software is geïnstalleerd en het netwerk specifiek is geconfigureerd. De VPN-gateway heeft de volgende functies:

- Verbindt de ethernetsegmenten van uw lokale netwerk en het productienetwerk in de cloud in de L2-modus.
- Maakt regels beschikbaar voor iptabellen en ebtabellen.
- Werkt als standaardrouter en NAT voor de machines in de test- en productienetwerken.
- Werkt als DHCP-server. Alle machines in de productie- en testnetwerken krijgen de netwerkconfiguratie (IP-adressen, DNS-instellingen) via DHCP. Een cloudserver krijgt telkens hetzelfde IP-adres van de DHCP-server. Als u een aangepaste DNS-configuratie wilt instellen, neemt u contact op met het ondersteuningsteam.
- Werkt als caching-DNS.

Netwerkconfiguratie van de VPN-gateway

De VPN-gateway heeft meerdere netwerkinterfaces:

- Externe interface, verbonden met internet
- Productie-interfaces, verbonden met de productienetwerken
- Testinterface, verbonden met het testnetwerk

Daarnaast worden er twee virtuele interfaces toegevoegd voor point-to-site- en site-to-site-verbindingen.

Wanneer de VPN-gateway wordt geïmplementeerd en geïnitialiseerd, worden de bruggen gemaakt: één voor de externe interface, één voor de clientinterface en één voor de productie-interface. De

clientproductiebrug en de testinterface gebruiken dezelfde IP-adressen, maar de VPN-gateway kan pakketten toch juist routeren dankzij een specifieke techniek.

VPN-toepassing

De **VPN-toepassing** is een virtuele machine op de lokale site waarop Linux en een speciale software zijn geïnstalleerd en een speciale netwerkconfiguratie is gemaakt. Zo wordt de communicatie tussen de lokale site en cloudsite mogelijk gemaakt.

Herstelservers

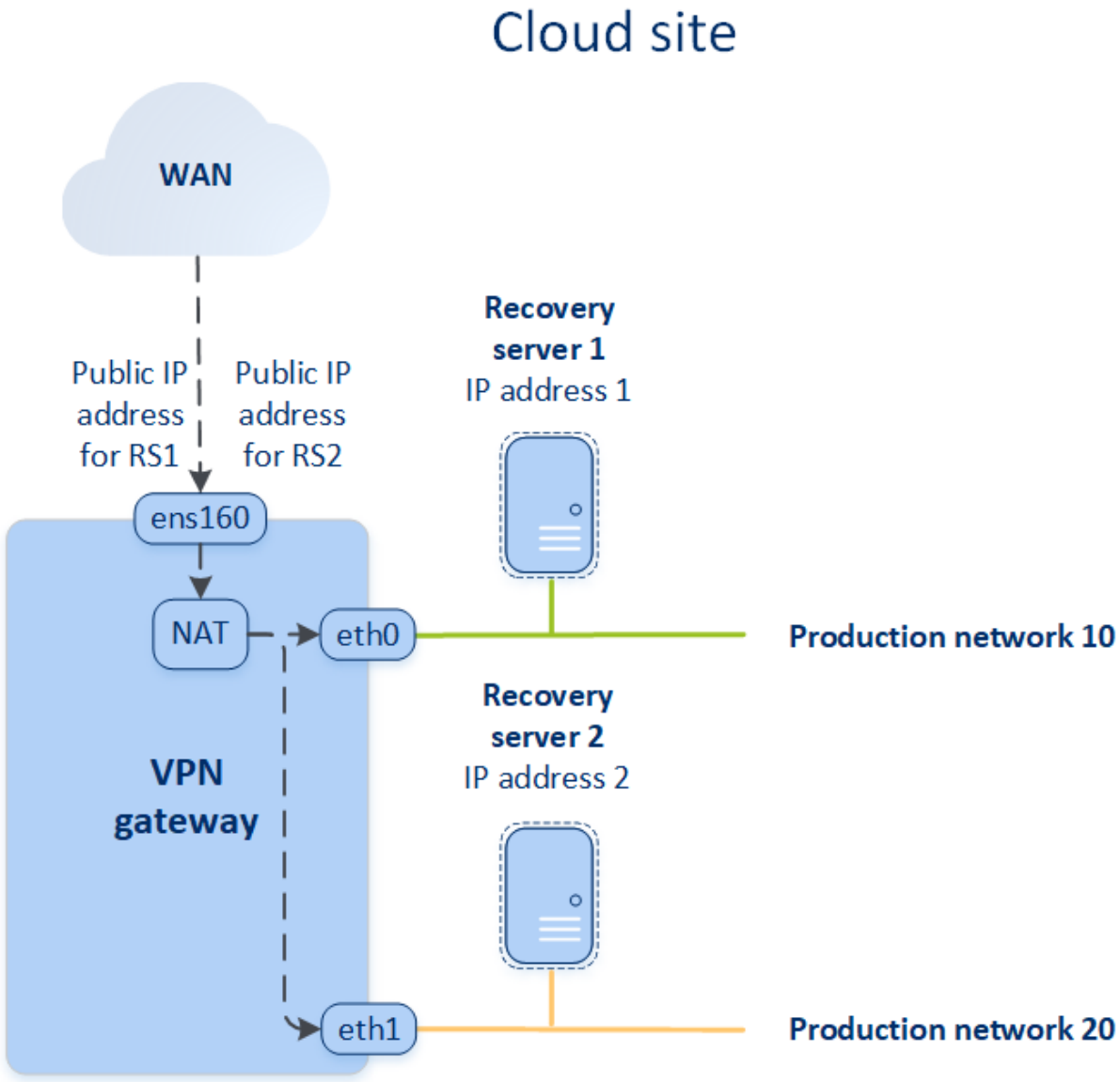
Een **herstelserver**: een replica van de oorspronkelijke machine op basis van de beveiligde serverback-ups die in de cloud zijn opgeslagen. Herstelservers worden gebruikt om workloads vanaf de oorspronkelijke servers te verplaatsen in het geval van een ramp.

Bij het maken van een herstelserver moet u de volgende netwerkparameters opgeven:

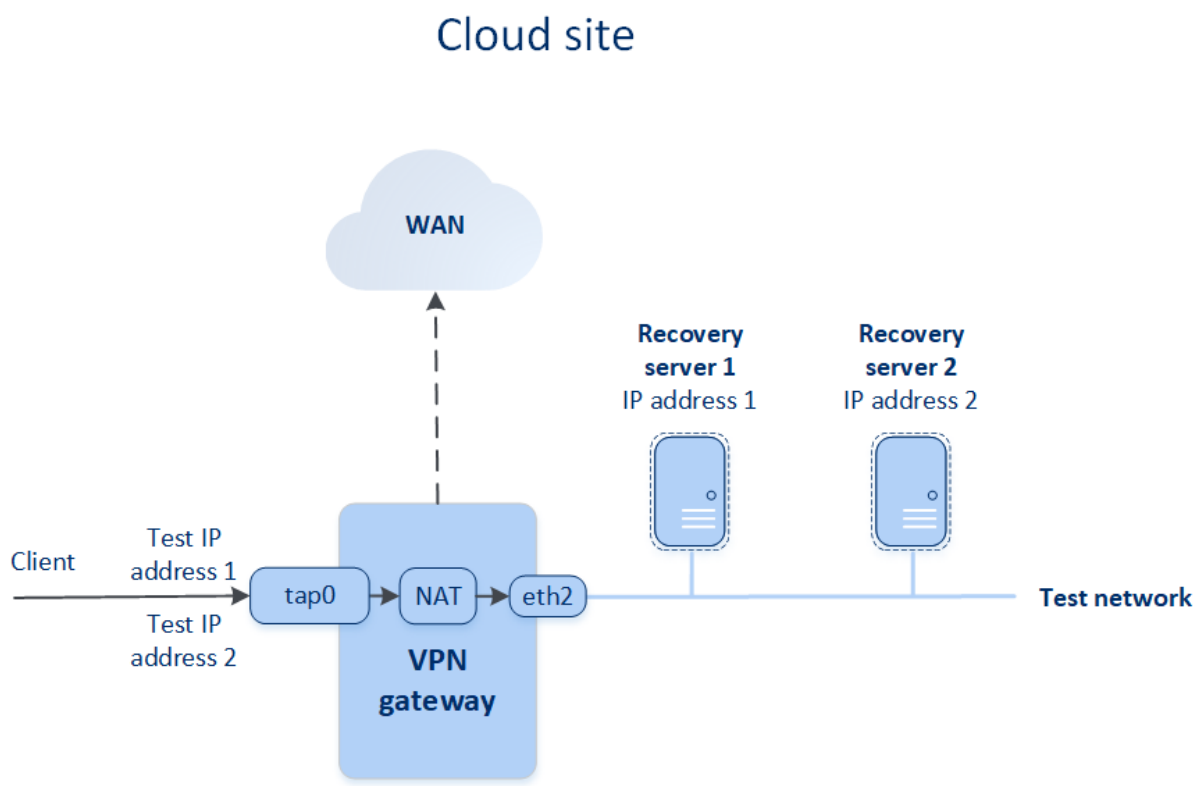
- **Cloudnetwerk** (verplicht): een cloudnetwerk gebruikt voor verbinding met een herstelserver.
- **IP-adres in productienetwerk** (verplicht): een IP-adres waarmee een virtuele machine voor een herstelserver wordt gestart. Dit adres wordt zowel in productie- als in testnetwerken gebruikt. Voor de start wordt de virtuele machine geconfigureerd om het IP-adres op te halen via DHCP.
- **Test-IP-adres** (optioneel): Een IP-adres om toegang te krijgen tot een herstelserver vanaf het klant-productienetwerk tijdens de testfailover, om te voorkomen dat het productie-IP-adres wordt gedupliceerd in hetzelfde netwerk. Dit IP-adres verschilt van het IP-adres in het productienetwerk. Servers op de lokale site kunnen de herstelserver tijdens de testfailover bereiken via het test-IP-adres, terwijl toegang in de omgekeerde richting niet beschikbaar is. Internettoegang vanaf de herstelserver in het testnetwerk is beschikbaar als de optie **Internettoegang** is geselecteerd tijdens het maken van de herstelserver.
- **Openbaar IP-adres** (optioneel): Een IP-adres om toegang te krijgen tot een herstelserver vanaf internet. Als een server geen openbaar IP-adres heeft, kan deze alleen worden bereikt via het lokale netwerk.
- **Internettoegang** (optioneel): hiermee krijgt een herstelserver toegang tot internet (zowel bij productie- als testfailover).

Openbaar IP-adres en test-IP-adres

Als u het openbare IP-adres toewijst bij het maken van een herstelserver, dan wordt deze beschikbaar vanaf internet via dit IP-adres. Wanneer een pakket van internet aankomt met het openbare IP-adres van de bestemming, wordt het door de VPN-gateway via NAT omgeleid naar het betreffende productie-IP-adres en vervolgens naar de overeenkomstige herstelserver verstuurd.



Als u het test-IP-adres toewijst bij het maken van een herstelserver, dan wordt deze beschikbaar in het testnetwerk via dit IP-adres. Wanneer u de testfailover uitvoert, wordt de oorspronkelijke machine nog steeds uitgevoerd terwijl de herstelserver met hetzelfde IP-adres wordt gestart in het testnetwerk in de cloud. Er is geen IP-adresconflict omdat het testnetwerk geïsoleerd is. De herstelservers in het testnetwerk zijn bereikbaar via hun test-IP-adressen, die via NAT naar de productie-IP-adressen worden omgeleid.



Zie "Site-to-site Open VPN - Aanvullende informatie" (p. 194) voor meer informatie over site-to-site Open VPN.

Primaire servers

Een **primaire server**: Een virtuele machine die geen gekoppelde machine op de lokale site heeft (in vergelijking met een herstelserver). Primaire servers worden gebruikt om een toepassing te beschermen of om diverse ondersteunende diensten (zoals een webserver) uit te voeren.

Doorgaans wordt een primaire server gebruikt voor realtime gegevensreplicatie op servers die cruciale toepassingen uitvoeren. U stelt de replicatie zelf in met behulp van de eigen hulpmiddelen van de toepassing. Een Active Directory-replicatie of SQL-replicatie kan bijvoorbeeld worden geconfigureerd op de lokale servers en de primaire server.

U kunt een primaire server desgewenst ook opnemen in een AlwaysOn-beschikbaarheidsgroep (AAG) of Databasebeschikbaarheidsgroep (DAG).

Voor beide methoden is een grondige kennis van de toepassing en de beheerdersrechten vereist. Een primaire server verbruikt voortdurend computerresources en ruimte in de opslag voor snel noodherstel. U moet de server onderhouden: bewaking van de replicatie, installatie van software-updates, en back-up. De voordelen zijn de minimale RPO en RTO met een minimale belasting van de productieomgeving (in vergelijking met het maken van back-ups van hele servers naar de cloud).

Primaire servers worden altijd alleen in het productienetwerk gestart en hebben de volgende netwerkparameters:

- **Cloudnetwerk** (verplicht): een cloudnetwerk waarmee een primaire server wordt verbonden.
- **IP-adres in productienetwerk** (verplicht): het IP-adres van de primaire server in het productienetwerk. Standaard wordt het eerste gratis IP-adres van uw productienetwerk ingesteld.
- **Openbaar IP-adres** (optioneel): Een IP-adres dat wordt gebruikt om toegang te krijgen tot een primaire server vanaf internet. Als een server geen openbaar IP-adres heeft, kan deze alleen worden bereikt via het lokale netwerk, niet via internet.
- **Internettoegang** (optioneel): hiermee krijgt een primaire server toegang tot internet.

Multi-site IPsec VPN-verbinding

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

U kunt de multi-site IPsec VPN-connectiviteit gebruiken om een enkele lokale site, of meerdere lokale sites te verbinden met Cyber Disaster Recovery Cloud via een beveiligde L3 IPsec VPN-verbinding.

Dit connectiviteitstype is nuttig voor noodherstelscenario's in de volgende gevallen:

- U hebt een lokale site die kritieke workloads host.
- U hebt meerdere lokale sites die kritieke workloads hosten, bijvoorbeeld kantoren op verschillende locaties.
- U maakt gebruik van softwaresites van derden, of sites van managed service providers en bent daarmee verbonden via een IPsec VPN-tunnel.

Voor de multi-site IPsec VPN-communicatie tussen de lokale sites en de cloudsites wordt gebruikgemaakt van een **VPN-gateway**. Wanneer u begint met het configureren van de multi-site IPsec VPN-verbinding in de Cyber Protect-console, wordt de VPN-gateway automatisch geïmplementeerd op de cloudsite. U moet de cloudnetwerksegmenten configureren en controleren of deze niet overlappen met de lokale netwerksegmenten. Er wordt een veilige tunnel tot stand gebracht tussen lokale sites en de cloudsite. De lokale en cloudservers kunnen communiceren via deze VPN-tunnel alsof ze zich allemaal in hetzelfde ethernetsegment bevinden.

Voor elke bronmachine die u wilt beveiligen, moet u een herstelserver maken op de cloudsite. Deze blijft de status **Stand-by** behouden totdat er een failovergebeurtenis plaatsvindt. Als er zich een ramp voordoet en u een failoverproces start (in de **productiemodus**), wordt de herstelserver die een exacte kopie van uw beschermde machine is, gestart in de cloud. Uw klanten kunnen blijven werken met de server, zonder de veranderingen op de achtergrond op te merken.

U kunt een failoverproces ook starten in de **testmodus**. Dit betekent dat de bronmachine nog werkt en dat tegelijkertijd de betreffende herstelserver in de cloud wordt gestart in een speciaal virtueel netwerk (**testnetwerk**). Het testnetwerk is geïsoleerd om duplicatie van IP-adressen in de andere cloudnetwerksegmenten te voorkomen.

VPN-gateway

Het belangrijkste onderdeel dat de communicatie tussen de lokale sites en de cloudsite mogelijk maakt, is de **VPN-gateway**. Het is een virtuele machine in de cloud waarop de speciale software is geïnstalleerd en het netwerk specifiek is geconfigureerd. De VPN-gateway heeft de volgende functies:

- Verbindt de ethernetsegmenten van uw lokale netwerk en het productienetwerk in de cloud in de L3 IPsec-modus.
- Werkt als standaardrouter en NAT voor de machines in de test- en productienetwerken.
- Werkt als DHCP-server. Alle machines in de productie- en testnetwerken krijgen de netwerkconfiguratie (IP-adressen, DNS-instellingen) via DHCP. Een cloudserver krijgt telkens hetzelfde IP-adres van de DHCP-server.

  Indien gewenst, kunt u een aangepaste DNS-configuratie instellen. Zie "Aangepaste DNS-servers configureren" (p. 814) voor meer informatie.
- Werkt als caching-DNS.

Hoe routering werkt

Routering tussen de cloudnetwerken wordt uitgevoerd met de router op de cloudsite, zodat servers van verschillende cloudnetwerken met elkaar kunnen communiceren.

Externe point-to-site-VPN-toegang

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

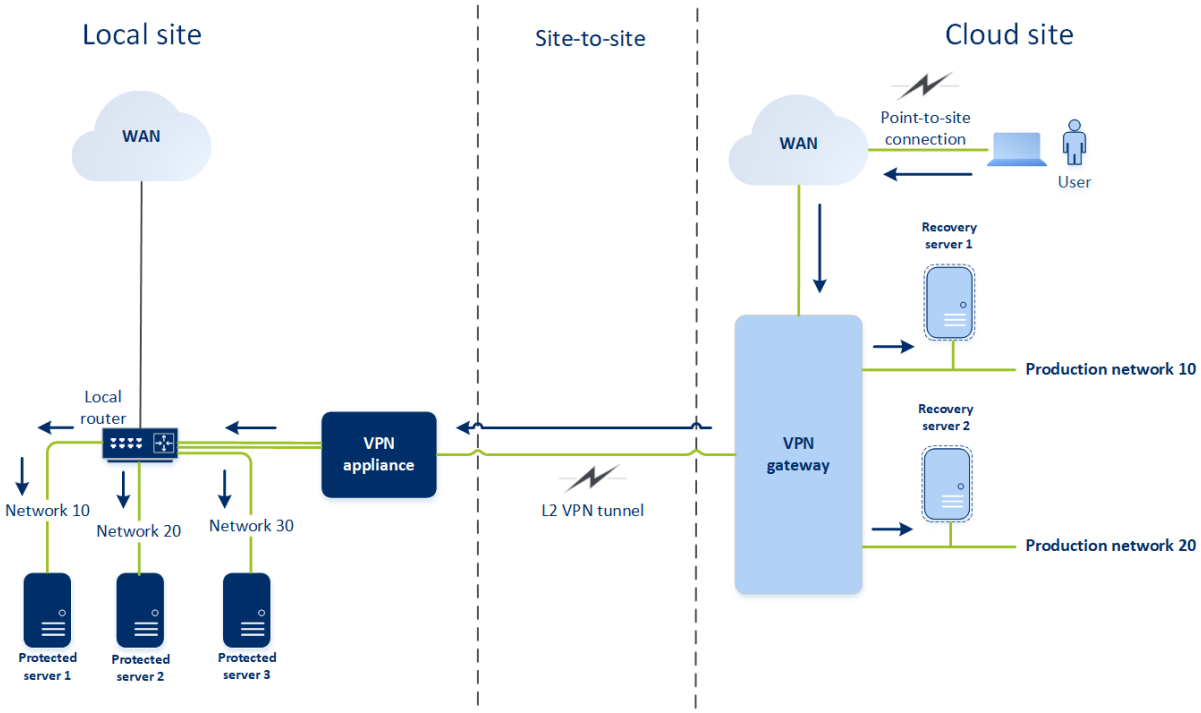
De point-to-site-verbinding is een veilige externe VPN-verbinding naar uw cloudsite en lokale site via uw eindpuntapparaten (zoals computer of laptop). Deze is beschikbaar nadat u een site-to-site OpenVPN-verbinding met de Cyber Disaster Recovery Cloud-site tot stand hebt gebracht. Dit type verbinding is nuttig in de volgende gevallen:

- In veel bedrijven zijn de zakelijke services en webresources alleen beschikbaar via het bedrijfsnetwerk. Via de point-to-site-verbinding kunt u veilig verbinding maken met de lokale site.
- In het geval van een ramp, wanneer een workload wordt verplaatst naar de cloudsite en uw lokale netwerk niet beschikbaar is, hebt u mogelijk directe toegang tot uw cloudservers nodig. Dit is mogelijk via de point-to-site-verbinding met de cloudsite.

Voor de point-to-site-verbinding met de lokale site moet u de VPN-toepassing op de lokale site installeren en vervolgens de site-to-site-verbinding en de point-to-site-verbinding met de lokale site configureren. Zo krijgen uw externe medewerkers toegang tot het bedrijfsnetwerk via L2 VPN.

In het onderstaande schema ziet u de lokale site, de cloudsite en de communicatie tussen servers (groen gemarkeerd). De L2 VPN-tunnel verbindt uw lokale site en de cloudsite. Wanneer een

gebruiker een point-to-site-verbinding tot stand brengt, wordt de communicatie naar de lokale site uitgevoerd via de cloudsite.



De point-to-site-configuratie maakt gebruik van certificaten voor verificatie bij de VPN-client. Daarnaast worden gebruikersreferenties gebruikt voor verificatie. Let op het volgende bij de point-to-site-verbinding met de lokale site:

- Gebruikers moeten hun Cyber Protect Cloud-referenties gebruiken voor verificatie bij de VPN-client. Ze moeten de gebruikersrol 'Bedrijfbeheerder' of 'Cyberbescherming' hebben.
- Als u de OpenVPN-configuratie opnieuw hebt gegenereerd, moet u de bijgewerkte configuratie verstrekken aan alle gebruikers die de point-to-site-verbinding met de cloudsite gebruiken.

Automatisch verwijderen van ongebruikte klantomgevingen op de cloudsite

In de noodherstelservice wordt het gebruik bijgehouden van de klantomgevingen die zijn gemaakt voor noodherstel en deze worden automatisch verwijderd indien ze niet worden gebruikt.

De volgende criteria worden gebruikt om te bepalen of de klanttenant actief is:

- Op dit moment is er minstens één cloudserver of er waren cloudserver(s) in de afgelopen zeven dagen.

  OF

- De optie **VPN-toegang tot lokale site** is ingeschakeld en de site-to-site OpenVPN-tunnel is tot stand gebracht of er worden gegevens van de VPN-toepassing voor de afgelopen 7 dagen gerapporteerd.

Alle overige tenants worden beschouwd als inactieve tenants. Voor dergelijke tenants wordt het automatisch het volgende uitgevoerd:

- De VPN-gateway en alle cloudresources voor de tenant worden verwijderd.
- De registratie van de VPN-toepassing wordt ongedaan gemaakt.

De inactieve tenants worden teruggezet naar hun status voordat de connectiviteit werd geconfigureerd.

Initiële connectiviteitsconfiguratie

In dit gedeelte worden de scenario's voor de connectiviteitsconfiguratie beschreven.

Modus Alleen cloud configureren

Een verbinding configureren in de modus Alleen cloud

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Connectiviteit**.
2. Selecteer **Alleen cloud** en klik op **Configureren**.
   De VPN-gateway en het cloudnetwerk met het gedefinieerde adres en masker worden dan geïmplementeerd op de cloudsite.

Zie 'Cloudnetwerken beheren' om te weten hoe u uw netwerken in de cloud beheert en de instellingen van de VPN-gateway configureert.

Site-to-site Open VPN configureren

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Vereisten voor de VPN-toepassing

Systeemvereisten

- 1 CPU
- 1 GB RAM
- 8 GB schijfruimte

Poorten

- TCP 443 (uitgaand) – voor VPN-verbinding
- TCP 80 (uitgaand) – voor automatische update van de toepassing

Controleer of uw firewalls en andere onderdelen van uw netwerkbeveiligingssysteem verbindingen naar elk IP-adres toestaan via deze poorten.

Een site-to-site Open VPN-verbinding configureren

De VPN-toepassing breidt uw lokale netwerk uit naar de cloud via een veilige VPN-tunnel. Dit soort verbinding wordt vaak een 'site-to-site'-verbinding (S2S) genoemd. U kunt de onderstaande procedure volgen of de videoles bekijken.

Een verbinding configureren via de VPN-toepassing

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Connectiviteit**.
2. Selecteer **Site-to-site Open VPN-verbinding** en klik op **Configureren**.
   De implementatie van de VPN-gateway in de cloud wordt dan automatisch gestart. Dit kan enige tijd duren. Ondertussen kunt u doorgaan naar de volgende stap.

   Opmerking
   De VPN-gateway wordt geleverd zonder extra kosten. Deze wordt verwijderd als de noodherstelfunctie niet wordt gebruikt, dat wil zeggen dat er gedurende zeven dagen geen primaire of herstelserver aanwezig is in de cloud.
3. Klik in het blok **VPN-toepassing** op **Downloaden en implementeren**. Afhankelijk van het virtualisatieplatform dat u gebruikt, downloadt u de VPN-toepassing voor VMware vSphere of Microsoft Hyper-V.
4. Implementeer de toepassing en verbind deze met de productienetwerken.
   In vSphere: controleer of **Promiscuous mode** en **Forged transmits** zijn ingeschakeld en stel deze in op **Accept** (Accepteren) voor alle virtuele switches die de VPN-toepassing verbinden met de productienetwerken. Als u deze instellingen wilt gebruiken, selecteert u in vSphere Client achtereenvolgens de host > **Summary** (Samenvatting) > **Network** (Netwerk), en dan de switch > **Edit settings...** (Instellingen bewerken ...) > **Security** (Beveiliging).
   In Hyper-V: maak een virtuele machine van **Generatie 1** met 1024 MB geheugen. We raden ook aan om **Dynamisch geheugen** in te schakelen voor de machine. Wanneer de machine is gemaakt, gaat u naar **Instellingen** > **Hardware** > **Netwerkadapter** > **Geavanceerde functies** en schakelt u het selectievakje **MAC-adresvervalsing (spoofing) inschakelen** in.
5. Schakel de toepassing in.
6. Ga naar de toepassingsconsole en meld u aan met de gebruikersnaam en het wachtwoord 'admin'/'admin'.
7. [Optioneel] Wijzig het wachtwoord.
8. [Optioneel] Wijzig de netwerkinstellingen indien nodig. Definieer welke interface u wilt gebruiken als WAN-interface voor de internetverbinding.
9. Gebruik de referenties van de bedrijfbeheerder om de toepassing te registreren in de Cyber Protection-service.
   Deze referenties worden slechts één keer gebruikt om het certificaat op te halen. De datacenter-URL is vooraf gedefinieerd.

Opmerking
Als tweeledige verificatie is geconfigureerd voor uw account, wordt u ook gevraagd om de TOTP-code in te voeren. Als tweeledige verificatie is ingeschakeld maar niet geconfigureerd voor uw account, kunt u de VPN-toepassing niet registreren. Eerst moet u naar de aanmeldingspagina van de Cyber Protect-console gaan en de configuratie voor tweeledige verificatie voltooien voor uw account. Ga naar de Beheerdershandleiding voor beheerportal voor meer informatie over tweeledige verificatie.

Wanneer de configuratie is voltooid, wordt de toepassing weergegeven met de status **Online**. De toepassing maakt verbinding met de VPN-gateway en begint informatie over netwerken van alle actieve interfaces te rapporteren aan de Cyber Disaster Recovery Cloud-service. In de Cyber Protect-console worden de interfaces weergegeven, gebaseerd op de informatie van de VPN-toepassing.

Multi-site IPsec VPN configureren

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

U kunt een multi-site IPsec VPN-verbinding op de volgende twee manieren configureren:

- vanaf het tabblad **Noodherstel** > **Connectiviteit**.
- door een beschermingsschema toe te passen op één of meer apparaten, en vervolgens handmatig over te schakelen van de automatisch gemaakte site-to-site Open VPN-verbinding naar een multi-site IPsec VPN-verbinding, en dan de multi-site IPsec VPN-instellingen te configureren en de IP-adressen opnieuw toe te wijzen.

Een multi-site IPsec VPN-verbinding configureren vanaf het tabblad Connectiviteit

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Connectiviteit**.
2. Klik in het gedeelte **Multi-site VPN-verbinding** op **Configureren**.
   Een VPN-gateway wordt geïmplementeerd op de cloudsite.
3. Configureer de Multi-site IPsec VPN-instellingen.

Een multi-site IPsec VPN-verbinding configureren vanuit een beschermingsschema

1. Ga in de Cyber Protect-console naar **Apparaten**.
2. Pas een beschermingsschema toe op een of meerdere apparaten uit de lijst.
   De instellingen voor de herstelserver en de cloudinfrastructuur worden automatisch geconfigureerd voor site-to site OpenVPN-connectiviteit.
3. Ga naar **Noodherstel** > **Connectiviteit**.
4. Klik op **Eigenschappen weergeven**.
5. Klik op **Overschakelen naar multi-site IPsec VPN**.

6. Configureer de multi-site IPsec VPN-instellingen.
7. Wijs de IP-adressen van het cloudnetwerk en de cloudservers opnieuw toe.

De multi-site IPsec VPN-instellingen configureren

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Wanneer u een multi-site IPsec VPN hebt geconfigureerd, moet u de instellingen voor de cloudsite en de lokale sites configureren op het tabblad **Noodherstel** > **Connectiviteit**.

Vereisten

- Multi-site IPsec VPN-connectiviteit is geconfigureerd. Zie "Multi-site IPsec VPN configureren" (p. 798) voor meer informatie over het configureren van de multi-site IPsec VPN-connectiviteit.
- Elke lokale IPsec VPN-gateway heeft een openbaar IP-adres.
- Uw cloudnetwerk heeft voldoende IP-adressen voor de cloudservers die kopieën zijn van uw beschermde machines (in het productienetwerk), en voor de herstelservers (met één of twee IP-adressen, afhankelijk van uw behoeften).
- [Als u een firewall gebruikt tussen de lokale sites en de cloudsite] De volgende IP-protocollen en UDP-poorten zijn toegestaan op de lokale sites: IP Protocol ID 50 (ESP), UDP-poort 500 (IKE) en UDP-poort 4500.
- De NAT-T-configuratie op de lokale sites is uitgeschakeld.

Een multi-site IPsec VPN-verbinding configureren

1. Voeg een of meer netwerken toe aan de cloudsite.
   a. Klik op **Netwerk toevoegen**.

      Opmerking
      Wanneer u een cloudnetwerk toevoegt, wordt er automatisch een overeenkomstig testnetwerk toegevoegd met hetzelfde netwerkadres en masker voor het uitvoeren van testfailovers. De cloudservers in het testnetwerk hebben dezelfde IP-adressen als in het productienetwerk in de cloud. Als u tijdens een testfailover toegang nodig hebt tot een cloudserver vanaf het productienetwerk, wijst u een tweede test-IP-adres toe wanneer u een herstelserver maakt.

   b. Typ het IP-adres van het netwerk in het veld **Netwerkadres**.

      Opmerking
      Controleer of de cloudnetwerken niet overlappen met een lokaal netwerk in uw omgeving. Anders kan er geen tunnel worden gemaakt.

c. Typ in het veld **Netwerkmasker** het masker van het netwerk.

d. Klik op **Toevoegen**.

2. Configureer de instellingen voor elke lokale site die u wilt verbinden met de cloudsite, volgens de aanbevelingen voor de lokale sites. Zie "Algemene aanbevelingen voor lokale sites" (p. 800) voor meer informatie over deze aanbevelingen.

   a. Klik op **Verbinding toevoegen**.

   b. Voer een naam in voor de lokale VPN-gateway.

   c. Voer het openbare IP-adres van de lokale VPN-gateway in.

   d. [Optioneel] Voer een beschrijving in voor de lokale VPN-gateway.

   e. Klik op **Volgende**.

   f. Typ in het veld **Vooraf gedeelde sleutel** de vooraf gedeelde sleutel of klik op **Een nieuwe vooraf gedeelde sleutel genereren** om een automatisch gegenereerde waarde te gebruiken.

   Opmerking
   U moet dezelfde vooraf gedeelde sleutel gebruiken voor de lokale en de Cloud VPN-gateways.

   g. Klik op **IPsec/IKE-beveiligingsinstellingen** om de instellingen te configureren. Zie "IPsec/IKE-beveiligingsinstellingen" (p. 801) voor meer informatie over de instellingen die u kunt configureren.

   Opmerking
   U kunt de standaardinstellingen gebruiken, die automatisch worden ingevuld, of aangepaste waarden gebruiken. Alleen verbindingen volgens het IKEv2-protocol worden ondersteund. De standaard **Opstartactie** bij het tot stand brengen van het VPN is **Toevoegen** (uw lokale VPN-gateway initieert de verbinding), maar u kunt dit wijzigen in **Starten** (de Cloud VPN-gateway initieert de verbinding) of in **Routeren** (geschikt voor firewalls die de opties voor Routeren ondersteunen).

   h. Configureer het **Netwerkbeleid**.
   Het netwerkbeleid geeft aan met welke netwerken het IPsec VPN verbinding maakt. Geef het IP adres en het masker van het netwerk op in de CIDR-indeling. De lokale en cloudnetwerksegmenten moeten niet overlappen.

   i. Klik op **Opslaan**.

Algemene aanbevelingen voor lokale sites

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Wanneer u de lokale sites voor uw multi-site IPsec VPN-connectiviteit configureert, houd dan rekening met de volgende aanbevelingen:

- Stel voor elke IKE-fase ten minste één van de waarden in die op de cloudsite zijn geconfigureerd voor de volgende parameters: Versleutelingsalgoritme, Hash-algoritme en Diffie-Hellman-groepsnummers.
- Schakel Perfect forward secrecy in met ten minste één van de waarden voor Diffie-Hellman-groepsnummers die op de cloudsite zijn geconfigureerd voor IKE fase 2.
- Configureer dezelfde waarde als op de cloudsite voor **Levensduur** voor IKE fase 1 en IKE fase 2.
- Configuraties met NAT traversal (NAT-T) worden niet ondersteund. Schakel de NAT-T-configuratie uit op de lokale site. Anders kan niet worden onderhandeld over de aanvullende UDP-inkapseling.
- De configuratie van de **Opstartactie** bepaalt door welke kant de verbinding wordt geïnitieerd. De standaardwaarde **Toevoegen** betekent dat de lokale site de verbinding initieert en de cloudsite wacht op het initiëren van de verbinding. Wijzig de waarde in **Start** als u wilt dat de cloudsite de verbinding initieert, of in **Route** als u wilt dat beide kanten de verbinding kunnen initiëren (geschikt voor firewalls die de Route-optie ondersteunen).

Voor meer informatie en configuratievoorbeelden voor verschillende oplossingen, zie:

- Deze reeks Knowledge Base-artikelen
- Dit videovoorbeeld

IPsec/IKE-beveiligingsinstellingen

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

De volgende tabel bevat meer informatie over de IPsec/IKE-beveiligingsparameters.

Parameter	Beschrijving
Versleutelingsalgoritme	Selecteer het versleutelingsalgoritme dat u wilt gebruiken, zodat de gegevens-in-transit niet zichtbaar zijn. Standaard worden alle algoritmen geselecteerd. U moet ten minste één van de geselecteerde algoritmen op uw lokale gatewayapparaat configureren voor elke IKE-fase.
Hash-algoritme	Het hash-algoritme dat moet worden gebruikt om de integriteit en authenticiteit van de gegevens te verifiëren. Standaard worden alle algoritmen geselecteerd. U moet ten minste één van de geselecteerde algoritmen op uw lokale gatewayapparaat configureren voor elke IKE-fase.

Parameter	Beschrijving
Diffie-Hellman-groepsnummers	Met Diffie-Hellman-groepsnummers wordt de sterkte bepaald van de sleutel die wordt gebruikt in het Internet Key Exchange-proces (IKE). Hogere groepsnummers zijn veiliger, maar de berekening van de sleutel duurt langer. Standaard zijn alle groepen geselecteerd. U moet ten minste één van de geselecteerde groepen op uw lokale gatewayapparaat configureren voor elke IKE-fase.
Levensduur (seconden)	De levensduur bepaalt de duur van een verbindingssessie met een set versleutelings-/verificatiesleutels voor gebruikerspakketten, vanaf de succesvolle onderhandeling tot het verstrijken ervan. Bereik voor fase 1: 900-28800 seconden (standaard 28800). Bereik voor fase 2: 900-3600 seconden (standaard 3600). De levensduur voor fase 2 moet korter zijn dan de levensduur voor fase 1. De verbinding wordt opnieuw tot stand gebracht via het sleutelkanaal voordat deze verloopt (zie **Margetijd voor opnieuw versleutelen**). Als de lokale en externe kant het niet eens zijn over de levensduur, ontstaat er een warboel van achterhaalde verbindingen aan de kant met de langste levensduur. Zie ook **Margetijd voor opnieuw versleutelen** en **Fuzz voor opnieuw versleutelen**.
Margetijd voor opnieuw versleutelen (seconden)	De margetijd gedurende welke de lokale kant van de VPN-verbinding probeert te onderhandelen over een vervanging voordat de verbinding of het sleutelkanaal verloopt. De exacte tijd voor opnieuw versleutelen wordt willekeurig gekozen op basis van de waarde van **Fuzz voor opnieuw versleutelen**. Alleen lokaal relevant, de externe kant hoeft er niet mee in te stemmen. Bereik: 900-3600 seconden. De standaardwaarde is 3600.
Grootte van venster voor opnieuw afspelen (pakket)	De grootte van het IPsec-venster voor opnieuw afspelen voor deze verbinding.

Parameter	Beschrijving
	De standaardwaarde -1 gebruikt de waarde die is geconfigureerd met charon.replay_window in het bestand strongswan.conf. Waarden groter dan 32 worden alleen ondersteund bij gebruik van de Netlink-backend. Met een waarde van 0 wordt de bescherming voor IPsec opnieuw afspelen uitgeschakeld.
Fuzz voor opnieuw versleutelen (%)	Het maximale percentage waarmee margebytes, margepakketten en margetijd willekeurig worden verhoogd om de intervallen voor opnieuw versleutelen te randomiseren (belangrijk voor hosts met veel verbindingen). De waarde van de fuzz voor opnieuw versleutelen kan meer zijn dan 100%. De waarde van marginTYPE, na de willekeurige verhoging, mag niet groter zijn dan lifeTYPE, waarbij TYPE bytes, pakketten of tijd kan zijn. Met de waarde 0% wordt randomiseren uitgeschakeld. Alleen lokaal relevant, de externe kant hoeft er niet mee in te stemmen.
DPD-time-out (seconden)	De tijd waarna er een time-out voor Dead Peer Detection (DPD) optreedt. U kunt een waarde van 30 of hoger opgeven. De standaardwaarde is 30.
Actie na time-out voor Dead Peer Detection (DPD)	De actie die moet worden ondernomen nadat een time-out voor DPD (Dead Peer Detection) is opgetreden. **Opnieuw starten**: Start de sessie opnieuw op wanneer er een time-out voor DPD optreedt. **Wissen**: Beëindig de sessie wanneer er een time-out voor DPD optreedt. **Geen**: Onderneem geen actie wanneer er een time-out voor DPD optreedt.
Opstartactie	Bepaalt welke kant de verbinding initieert en de tunnel voor de VPN-verbinding tot stand brengt. **Toevoegen**: Uw lokale VPN-gateway initieert de verbinding. **Starten**: De Cloud VPN-gateway initieert de verbinding.

Parameter	Beschrijving
	Routeren: Geschikt voor VPN-gateways die de optie Routeren ondersteunen. De tunnel is alleen actief als er verkeer is dat wordt geïnitieerd door de lokale VPN-gateway of de Cloud VPN-gateway.

Aanbevelingen voor de beschikbaarheid van Active Directory Domain Services

Als uw beschermde workloads zich moeten verifiëren bij een domeincontroller, raden wij u aan een Active Directory Domain Controller (AD DC)-exemplaar te hebben op de locatie voor noodherstel.

Active Directory Domain Controller voor L2 Open VPN-connectiviteit

Met de L2 Open VPN-connectiviteit blijven de IP-adressen van de beschermde workloads behouden op de cloudlocatie tijdens een testfailover of een productiefailover. Daarom heeft de AD DC tijdens een testfailover of een productiefailover hetzelfde IP-adres als op de lokale site.

Met een aangepast DNS kunt u uw eigen aangepaste DNS-server instellen voor alle cloudservers. Zie "Aangepaste DNS-servers configureren" (p. 814) voor meer informatie.

Active Directory Domain Controller voor L3 IPsec VPN-connectiviteit

Met L3 IPsec VPN-connectiviteit blijven de IP-adressen van de beschermde workloads niet behouden op de cloudlocatie. Daarom raden wij aan een aanvullend speciaal AD DC-exemplaar als primaire server op de cloudsite te hebben voordat u een productiefailover uitvoert.

De aanbevelingen voor een speciaal AD DC-exemplaar dat wordt geconfigureerd als primaire server op de cloudsite, zijn als volgt:

- Zet de Windows-firewall uit.
- Sluit de primaire server aan op de Active Directory-service.
- Controleer of de primaire server toegang heeft tot internet.
- Voeg de Active Directory-functie toe.

Met een aangepast DNS kunt u uw eigen aangepaste DNS-server instellen voor alle cloudservers. Zie "Aangepaste DNS-servers configureren" (p. 814) voor meer informatie.

Externe point-to-site-VPN-toegang configureren

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Als u op afstand verbinding wilt maken met uw lokale site, kunt u de point-to-site-verbinding met de lokale site configureren. U kunt de onderstaande procedure volgen of de videoles bekijken.

Vereisten

- Site-to-site Open VPN-connectiviteit is geconfigureerd.
- De VPN-toepassing is geïnstalleerd op de lokale site.

De point-to-site-verbinding met de lokale site configureren

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Connectiviteit**.
2. Klik op **Eigenschappen weergeven**.
3. Schakel de optie **VPN-toegang tot lokale site** in.
4. Controleer of gebruikers die de point-to-site-verbinding met de lokale site tot stand willen brengen, over het volgende beschikken:
   - een gebruikersaccount in Cyber Protect Cloud. Deze referenties worden gebruikt voor verificatie bij de VPN-client. Als dat niet het geval is, dan kunt u een gebruikersaccount maken in Cyber Protect Cloud.
   - de gebruikersrol 'Bedrijfbeheerder' of 'Cyberbescherming'.
5. De OpenVPN-client configureren:
   a. Download de OpenVPN-client versie 2.4.0 of later vanaf de volgende locatie: https://openvpn.net/community-downloads/.

      Opmerking
      OpenVPN Connect-client wordt niet ondersteund.

   b. Installeer de OpenVPN-client op de machine van waaruit u verbinding wilt maken met de lokale site.
   c. Klik op **Configuratie voor OpenVPN downloaden**. Het configuratiebestand is geldig voor gebruikers in uw organisatie die de rol 'Bedrijfbeheerder' of 'Cyberbescherming' hebben.
   d. Importeer de gedownloade configuratie naar de OpenVPN-client.
   e. Meld u aan bij de OpenVPN-client met de Cyber Protect Cloud-gebruikersreferenties (zie stap 4 hierboven).
   f. [Optioneel] Als tweeledige verificatie is ingeschakeld voor uw organisatie, moet u de eenmalig gegenereerde TOTP-code opgeven.

Belangrijk
Als u tweeledige verificatie hebt ingeschakeld voor uw account, moet u het configuratiebestand opnieuw genereren en dit vernieuwen voor uw bestaande OpenVPN-clients. Gebruikers moeten zich opnieuw aanmelden bij Cyber Protect Cloud om tweeledige verificatie in te stellen voor hun accounts.

Als gevolg hiervan kunt u verbinding maken met machines op de lokale site.

Netwerkbeheer

In dit gedeelte worden scenario's voor netwerkbeheer beschreven.

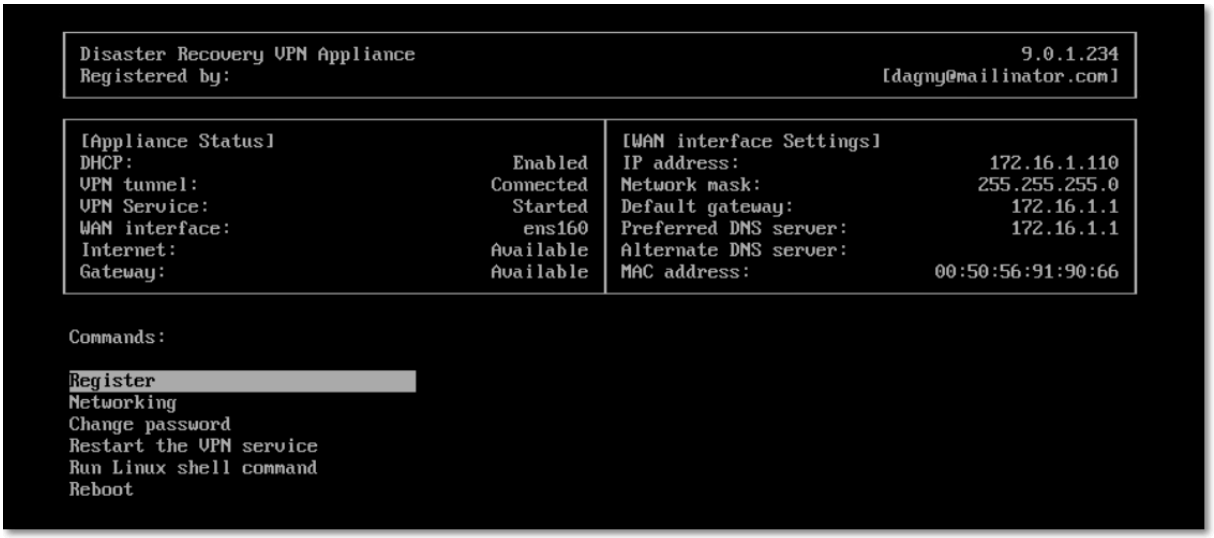
Netwerken beheren

Opmerking
Voor sommige functies zijn mogelijk extra licenties vereist, afhankelijk van het toegepaste licentiemodel.

Site-to-site OpenVPN-verbinding

Een netwerk toevoegen op de lokale site en uitbreiden naar de cloud

1. Stel op de VPN-toepassing de nieuwe netwerkinterface in met het lokale netwerk dat u wilt uitbreiden in de cloud.
2. Meld u aan bij de VPN-toepassingsconsole.
3. Configureer in het gedeelte **Netwerken** de netwerkinstellingen in voor de nieuwe interface.



De VPN-toepassing begint informatie over netwerken van alle actieve interfaces te rapporteren aan Cyber Disaster Recovery Cloud. In de Cyber Protect-console worden de interfaces weergegeven, gebaseerd op de informatie van de VPN-toepassing.

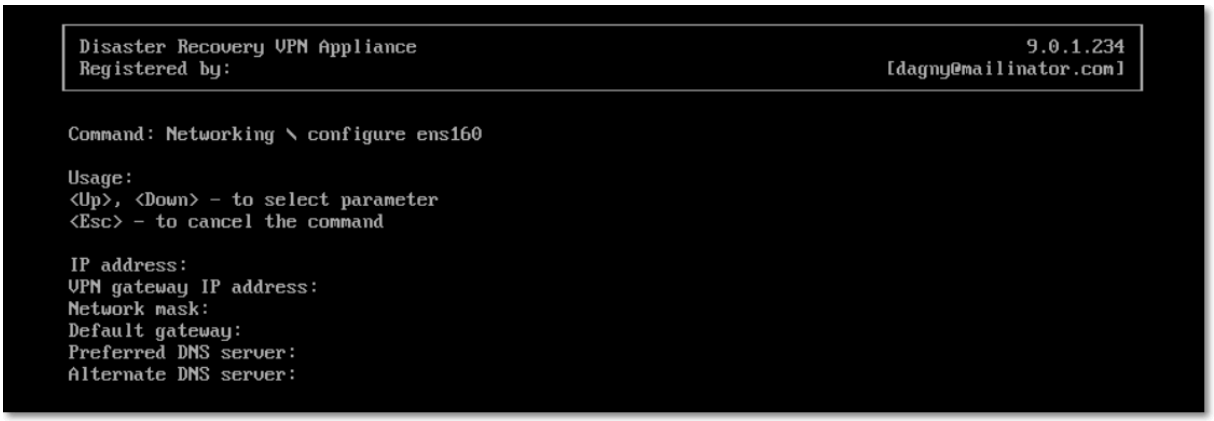
Een netwerk verwijderen dat is uitgebreid naar de cloud

1. Meld u aan bij de VPN-toepassingsconsole.
2. Selecteer in het gedeelte **Netwerken** de interface die u wilt verwijderen en klik vervolgens op **Netwerkinstellingen wissen**.
3. Bevestig de bewerking.

De uitbreiding van het lokale netwerk naar de cloud via een veilige VPN-tunnel wordt dan gestopt. Dit netwerk zal dan functioneren als onafhankelijk cloudsegment. Als deze interface wordt gebruikt om het verkeer van (naar) de cloudsite door te geven, worden al uw netwerkverbindingen van (naar) de cloudsite verbroken.

De netwerkparameters wijzigen

1. Meld u aan bij de VPN-toepassingsconsole.
2. Selecteer in het gedeelte **Netwerken** de interface die u wilt bewerken.
3. Klik op **Netwerkinstellingen**.
4. Selecteer een van de twee mogelijke opties:
   - Klik op **DHCP gebruiken** voor automatische netwerkconfiguratie via DHCP. Bevestig de bewerking.
   - Klik op **Statisch IP-adres instellen** voor handmatige netwerkconfiguratie. De volgende instellingen kunnen worden bewerkt:
     - **IP-adres**: het IP-adres van de interface in het lokale netwerk.
     - **IP-adres van VPN-gateway**: het speciale IP-adres dat is gereserveerd voor het cloudsegment van het netwerk om te zorgen voor een juiste werking van de Cyber Disaster Recovery Cloud-service.
     - **Netwerkmasker**: netwerkmasker van het lokale netwerk.
     - **Standaardgateway**: standaardgateway op de lokale site.
     - **Voorkeurs-DNS-server**: primaire DNS-server op de lokale site.
     - **Alternatieve DNS-server**: secundaire DNS-server op de lokale site.



- Breng de nodige wijzigingen aan en bevestig deze door op Enter te drukken.

Modus Alleen cloud

U kunt tot 23 netwerken hebben in de cloud.

Nieuw cloudnetwerk toevoegen

1. Ga naar **Noodherstel** > **Connectiviteit**.
2. Klik op de **Cloudsite** op **Cloudnetwerk toevoegen**.
3. Definieer de parameters voor het cloudnetwerk: het netwerkadres en het masker. Wanneer u klaar bent, klikt u op **Gereed**.

Het aanvullende cloudnetwerk met het gedefinieerde adres en masker wordt dan gemaakt op de cloudsite.

Een cloudnetwerk verwijderen

Opmerking
U kunt een cloudnetwerk niet verwijderen als er ten minste één cloudserver in het netwerk aanwezig is. Verwijder eerst de cloudserver en vervolgens het netwerk.

1. Ga naar **Noodherstel** > **Connectiviteit**.
2. Klik op de **Cloudsite** op het netwerkadres dat u wilt verwijderen.
3. Klik op **Verwijderen** en bevestig de bewerking.

Parameters voor cloudnetwerk wijzigen

1. Ga naar **Noodherstel** > **Connectiviteit**.
2. Klik op de **Cloudsite** op het netwerkadres dat u wilt bewerken.
3. Klik op **Bewerken**.
4. Definieer het netwerkadres en masker en klik vervolgens op **Gereed**.

IP-adres opnieuw configureren

Voor goede prestaties van noodherstel moeten de IP-adressen die aan de lokale en cloudservers zijn toegewezen, consistent zijn. Als er sprake is van inconsistente of niet-overeenkomende IP-adressen, ziet u een uitroepteken naast het betreffende netwerk in **Noodherstel** > **Connectiviteit**.

Hieronder ziet u enkele van de algemeen bekende redenen voor inconsistentie van IP-adressen:

1. Een herstelserver is gemigreerd naar een ander netwerk of het netwerkmasker van het cloudnetwerk is gewijzigd. Daardoor hebben cloudservers IP-adressen van netwerken waarmee ze niet zijn verbonden.
2. Het connectiviteitstype is omgezet van zonder site-to-site-verbinding naar site-to-site-verbinding. Daardoor wordt een lokale server geplaatst in een ander netwerk dan het netwerk dat is gemaakt voor de herstelserver op de cloudsite.
3. Het connectiviteitstype is omgezet van site-to-site OpenVPN naar multi-site IPsec VPN, of van multi-site IPsec VPN naar site-to-site OpenVPN. Zie Verbindingen omschakelen en IP-adressen opnieuw toewijzen voor meer informatie over dit scenario.
4. De volgende netwerkparameters bewerken op de site van de VPN-toepassing:

- Een interface toevoegen via de netwerkinstellingen
- Het netwerkmasker handmatig bewerken via de interface-instellingen
- Het netwerkmasker bewerken via DHCP
- Het netwerkadres en masker handmatig bewerken via de interface-instellingen
- Het netwerkmasker en adres bewerken via DHCP

Als gevolg van de bovenstaande acties kan het netwerk op de cloudsite een subset of superset van het lokale netwerk worden, of kan de interface van de VPN-toepassing dezelfde netwerkinstellingen rapporteren voor verschillende interfaces.

Het probleem met de netwerkinstellingen oplossen

1. Klik op het netwerk waarvoor het IP-adres opnieuw moet worden geconfigureerd.
   U ziet een lijst met servers in het geselecteerde netwerk, met hun status en IP-adressen. De servers waarvan de netwerkinstellingen inconsistent zijn, zijn gemarkeerd met een uitroepteken.
2. Klik op **Ga naar server** om de netwerkinstellingen voor een server te wijzigen. Klik op **Wijzigen** in het blok voor meldingen om de netwerkinstellingen voor alle servers tegelijk te wijzigen.
3. Wijzig de IP-adressen zoals gewenst door ze te definiëren in de velden **Nieuw IP** en **Nieuw test-IP**.
4. Wanneer u klaar bent, klikt u op **Bevestigen**.

Servers verplaatsen naar een geschikt netwerk

Wanneer u een beschermingsschema voor noodherstel maakt en dit toepast op geselecteerde apparaten, worden de IP-adressen van apparaten gecontroleerd en worden automatisch cloudnetwerken gemaakt als er geen bestaande cloudnetwerken zijn die passen bij het IP-adres. Standaard zijn de cloudnetwerken geconfigureerd met maximale bereiken, zoals door IANA aanbevolen voor privégebruik (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). U kunt uw netwerk verfijnen door het netwerkmasker te bewerken.

Als de geselecteerde apparaten zich in meerdere lokale netwerken bevinden, kan het netwerk op de cloudsite een superset van de lokale netwerken worden. In dit geval configureert u de cloudnetwerken opnieuw:

1. Klik op het cloudnetwerk waarvan u de netwerkgrootte opnieuw wilt configureren en klik vervolgens op **Bewerken**.
2. Configureer de netwerkgrootte opnieuw met de juiste instellingen.
3. Maak andere vereiste netwerken.
4. Klik op het meldingspictogram naast het aantal apparaten dat is verbonden met het netwerk.
5. Klik op **Verplaatsen naar een geschikt netwerk**.
6. Selecteer de servers die u wilt verplaatsen naar geschikte netwerken en klik vervolgens op **Verplaatsen**.

De instellingen van de VPN-toepassing beheren

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

In de Cyber Protect-console (**Noodherstel** > **Connectiviteit**) kunt u het volgende doen:

- Logboekbestanden downloaden.
- De registratie van de toepassing ongedaan maken (als u de VPN-toepassing opnieuw moet instellen of als u moet overschakelen naar de modus Alleen cloud).

Als u toegang wilt krijgen tot deze instellingen, klikt u op het **i**-pictogram in het blok **VPN-toepassing**.

In de VPN-toepassingsconsole kunt u:

- Het wachtwoord voor de toepassing wijzigen.
- De netwerkinstellingen bekijken/wijzigen en definiëren welke interface u als WAN wilt gebruiken voor de internetverbinding.
- Het registratieaccount registreren/wijzigen (door de registratie te herhalen).
- De VPN-service opnieuw starten.
- De VPN-toepassing opnieuw opstarten.
- De Linux-shell-opdracht uitvoeren (alleen voor geavanceerde probleemoplossing).

De VPN-gateway opnieuw installeren ...

Als er een probleem is met de VPN-gateway dat u niet kunt oplossen, kunt u de VPN-gateway misschien beter opnieuw installeren. Er kunnen bijvoorbeeld de volgende problemen optreden:

- De VPN-gateway heeft de status **Fout**.
- De VPN-gateway heeft gedurende lange tijd de status **In behandeling**.
- De status van de VPN-gateway kan gedurende lange tijd niet worden bepaald.

Het proces voor het opnieuw installeren van de VPN-gateway omvat de volgende automatische acties: de bestaande virtuele machine van de VPN-gateway volledig verwijderen, een nieuwe virtuele machine installeren vanaf de sjabloon, en de instellingen van de vorige VPN-gateway toepassen op de nieuwe virtuele machine.

Vereisten:

Een van de typen connectiviteit met de cloudsite moet worden ingesteld.

VPN-gateway opnieuw installeren

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Connectiviteit**.
2. Klik op het tandwielpictogram van de VPN-gateway en selecteer **VPN-gateway opnieuw installeren**.
3. Geef uw gebruikersnaam op in het dialoogvenster **VPN-gateway opnieuw installeren**.
4. Klik op **Opnieuw installeren**.

De site-to-site-verbinding inschakelen en uitschakelen

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

U kunt de site-to-site-verbinding inschakelen in de volgende gevallen:

- Als u wilt dat de cloudservers op de cloudsite kunnen communiceren met servers op de lokale site.
- Na een failover naar de cloud wordt de lokale infrastructuur hersteld en u wilt de servers terugzetten naar de lokale site (failback).

De site-to-site-verbinding inschakelen

1. Ga naar **Noodherstel** > **Connectiviteit**.
2. Klik op **Eigenschappen weergeven** en schakel de optie **Site-to-site-verbinding** in.

De site-to-site-VPN-verbinding tussen de lokale site en de cloudsite wordt dan tot stand gebracht. De Cyber Disaster Recovery Cloud-service krijgt de netwerkinstellingen van de VPN-toepassing en breidt de lokale netwerken uit naar de cloudsite.

Als u geen cloudservers op de cloudsite nodig hebt om te communiceren met servers op de lokale site, kunt u de site-to-site-verbinding uitschakelen.

De site-to-site-verbinding uitschakelen

1. Ga naar **Noodherstel** > **Connectiviteit**.
2. Klik op **Eigenschappen weergeven** en schakel de optie **Site-to-site-verbinding** uit.

De verbinding tussen de lokale site en de cloudsite wordt dan verbroken.

Het site-to-site-verbindingstype overschakelen

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

U kunt gemakkelijk overschakelen van een site-to-site OpenVPN-verbinding naar een multi-site IPsec VPN-verbinding, en van een multi-site IPsec VPN-verbinding naar een site-to-site Open VPN-verbinding.

Wanneer u het connectiviteitstype wijzigt, worden de actieve VPN-verbindingen verwijderd, maar de cloudservers en netwerkconfiguraties blijven behouden. U moet echter nog wel de IP-adressen van de cloudnetwerken en -servers opnieuw toewijzen.

De volgende tabel bevat een vergelijking van de basiskenmerken van de site-to-site OpenVPN-verbinding en de multi-site IPsec VPN-verbinding.

	Site-to-site OpenVPN	**Multi-site IPsec VPN**
Ondersteuning voor lokale site	Enkele	Enkele, meerdere
VPN-gateway	L2 Open VPN	L3 IPsec VPN
Netwerksegmenten	Breidt het lokale netwerk uit naar het cloudnetwerk	Lokale en cloudnetwerksegmenten mogen elkaar niet overlappen
Ondersteunt point-to-site-toegang tot lokale site	Ja	Nee
Ondersteunt point-to-site-toegang tot cloudsite	Ja	Ja
Vereist een optie voor openbaar IP	Nee	Ja

Overschakelen van een site-to-site OpenVPN-verbinding naar een multi-site IPsec VPN-verbinding

1. Ga in de Cyber Protect-console naar **Noodherstel** -> **Connectiviteit**.
2. Klik op **Eigenschappen weergeven**.
3. Klik op **Overschakelen naar multi-site IPsec VPN**.
4. Klik op **Opnieuw configureren**.
5. Wijs de IP-adressen van het cloudnetwerk en de cloudservers opnieuw toe.
6. Configureer de multi-site IPsec-verbindingsinstellingen.

Overschakelen van een multi-site IPsec VPN-verbinding naar een site-to-site OpenVPN-verbinding

1. Ga in de Cyber Protect-console naar **Noodherstel** -> **Connectiviteit**.
2. Klik op **Eigenschappen weergeven**.
3. Klik op **Overschakelen naar site-to-site OpenVPN**.

4. Klik op **Opnieuw configureren**.
5. Wijs de IP-adressen van het cloudnetwerk en de cloudservers opnieuw toe.
6. De site-to-site-verbindingsinstellingen configureren.

IP-adressen opnieuw toewijzen

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

In de volgende gevallen moet u de IP-adressen van de cloudnetwerken en de cloudservers opnieuw toewijzen om de configuratie te voltooien:

- Wanneer u bent overgeschakeld van site-to-site OpenVPN naar multi-site IPsec VPN, of omgekeerd.
- Wanneer u een beschermingsschema hebt toegepast (als de multi-site IPsec VPN-connectiviteit is geconfigureerd).

De IP-adressen van een cloudnetwerk opnieuw toewijzen

1. Klik op het tabblad **Connectiviteit** op de IP-adressen van het cloudnetwerk.
2. Klik in het pop-upvenster **Netwerk** op **Bewerken**.
3. Typ het nieuwe netwerkadres en netwerkmasker.
4. Klik op **Gereed**.

Nadat u het IP-adres van een cloudnetwerk opnieuw hebt toegewezen, moet u ook de cloudservers opnieuw toewijzen die horen bij het opnieuw toegewezen cloudnetwerk.

Het IP-adres van een server opnieuw toewijzen

1. Klik op het tabblad **Connectiviteit** op de IP-adressen van de server in het cloudnetwerk.
2. Klik in het pop-upvenster **Servers** op **IP-adres wijzigen**.
3. Geef in het pop-upvenster **IP-adres wijzigen** het nieuwe IP-adres van de server op of gebruik het automatisch gegenereerde IP-adres dat deel uitmaakt van het opnieuw toegewezen cloudnetwerk.

   Opmerking
   Cyber Disaster Recovery Cloud wijst automatisch IP-adressen van het cloudnetwerk toe aan alle cloudservers die deel uitmaakten van het cloudnetwerk voordat het IP-adres van het netwerk opnieuw werd toegewezen. U kunt de voorgestelde IP-adressen gebruiken om de IP-adressen van alle cloudservers in één keer opnieuw toe te wijzen.

4. Klik op **Bevestigen**.

Aangepaste DNS-servers configureren

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Wanneer u een connectiviteit configureert, wordt uw cloudnetwerkinfrastructuur gemaakt door Cyber Disaster Recovery Cloud. De DHCP-server in de cloud wijst automatisch standaard DNS-servers toe aan de herstelservers en primaire servers, maar u kunt de standaardinstellingen wijzigen en aangepaste DNS-servers configureren. De nieuwe DNS-instellingen worden toegepast bij de volgende aanvraag op de DHCP-server.

Vereisten:

Een van de typen connectiviteit met de cloudsite moet worden ingesteld.

Een aangepaste DNS-server configureren

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Connectiviteit**.
2. Klik op **Eigenschappen weergeven**.
3. Klik op **Standaard (geleverd door cloudsite)**.
4. Selecteer **Aangepaste servers**.
5. Typ het IP-adres van de DNS-server.
6. [Optioneel] Als u nog een DNS-server wilt toevoegen, klikt u op **Toevoegen** en typt u het IP-adres van de DNS-server.

   Opmerking
   Wanneer u de aangepaste DNS-servers hebt toegevoegd, kunt u ook de standaard DNS-servers toevoegen. Als de aangepaste DNS-servers dan niet beschikbaar zijn, zullen de standaard DNS-servers worden gebruikt door Cyber Disaster Recovery Cloud.

7. Klik op **Gereed**.

Aangepaste DNS-servers verwijderen

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

U kunt DNS-servers verwijderen uit de aangepaste DNS-lijst.

Vereisten:

Aangepaste DNS-servers zijn geconfigureerd.

Een aangepaste DNS-server verwijderen

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Connectiviteit**.
2. Klik op **Eigenschappen weergeven**.
3. Klik op **Aangepaste servers**.
4. Klik op het pictogram Verwijderen naast de DNS-server.

   Opmerking
   De bewerking voor verwijderen is uitgeschakeld wanneer slechts één aangepaste DNS-server beschikbaar is. Als u alle aangepaste DNS-servers wilt verwijderen, selecteert u **Standaard (geleverd door cloudsite)**.

5. Klik op **Gereed**.

Lokale routering configureren

Naast uw lokale netwerken die via de VPN-toepassing naar de cloud worden uitgebreid, kunt u ook andere lokale netwerken hebben die niet in de VPN-toepassing zijn geregistreerd, terwijl de servers in het netwerk wel met cloudservers moeten communiceren. Als u de connectiviteit tussen dergelijke lokale servers en cloudservers tot stand wilt brengen, moet u de instellingen voor de lokale routering configureren.

De lokale routering configureren

1. Ga naar **Noodherstel** > **Connectiviteit**.
2. Klik op **Eigenschappen weergeven** en klik vervolgens op **Lokale routering**.
3. Geef de lokale netwerken op in de CIDR-indeling.
4. Klik op **Opslaan**.

De servers van de opgegeven lokale netwerken kunnen dan communiceren met de cloudservers.

DHCP-verkeer via L2 VPN toestaan

Als apparaten op uw lokale site een IP-adres krijgen van een DHCP-server, kunt u de DHCP-server beschermen met Noodherstel, een failover naar de cloud uitvoeren, en vervolgens toestaan dat het DHCP-verkeer wordt uitgevoerd via L2 VPN. Uw DHCP-server zal dus in de cloud worden uitgevoerd, maar nog wel IP-adressen toewijzen aan uw lokale apparaten.

Vereisten:

U moet een site-to-site L2 VPN-connectiviteitstype naar de cloudsite instellen.

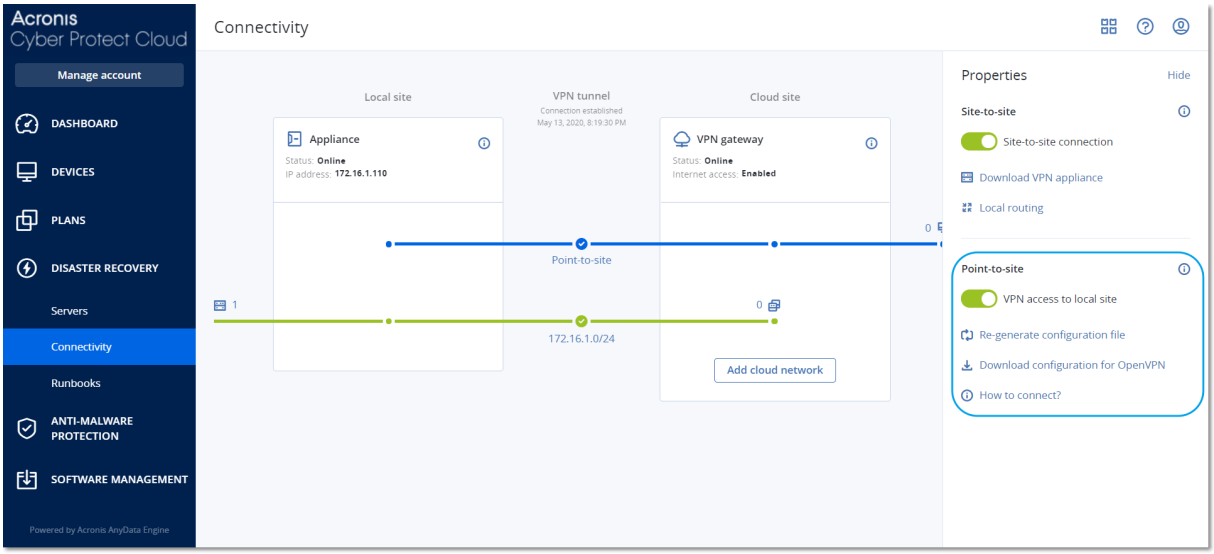
DHCP-verkeer via de L2 VPN-verbinding toestaan

1. Ga naar **Noodherstel** > tabblad **Connectiviteit**.
2. Klik op **Eigenschappen weergeven**.
3. Schakel de schakelaar **DHCP-verkeer via L2 VPN toestaan** in.

Instellingen voor point-to-site-verbindingen beheren

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Ga in de Cyber Protect-console naar **Noodherstel** > **Connectiviteit** en klik vervolgens op **Eigenschappen weergeven** in de rechterbovenhoek.



VPN-toegang tot lokale site

Deze optie wordt gebruikt voor het beheren van VPN-toegang tot de lokale site. Standaard is deze ingeschakeld. Als deze is uitgeschakeld, wordt de point-to-site-toegang tot de lokale site niet toegestaan.

Configuratie voor OpenVPN downloaden

Hiermee wordt het configuratiebestand voor de OpenVPN-client gedownload. Het bestand is vereist om een point-to-site-verbinding tot stand te brengen met de cloudsite.

Configuratie opnieuw genereren

U kunt het configuratiebestand voor de OpenVPN-client opnieuw genereren.

Dit is vereist in de volgende gevallen:

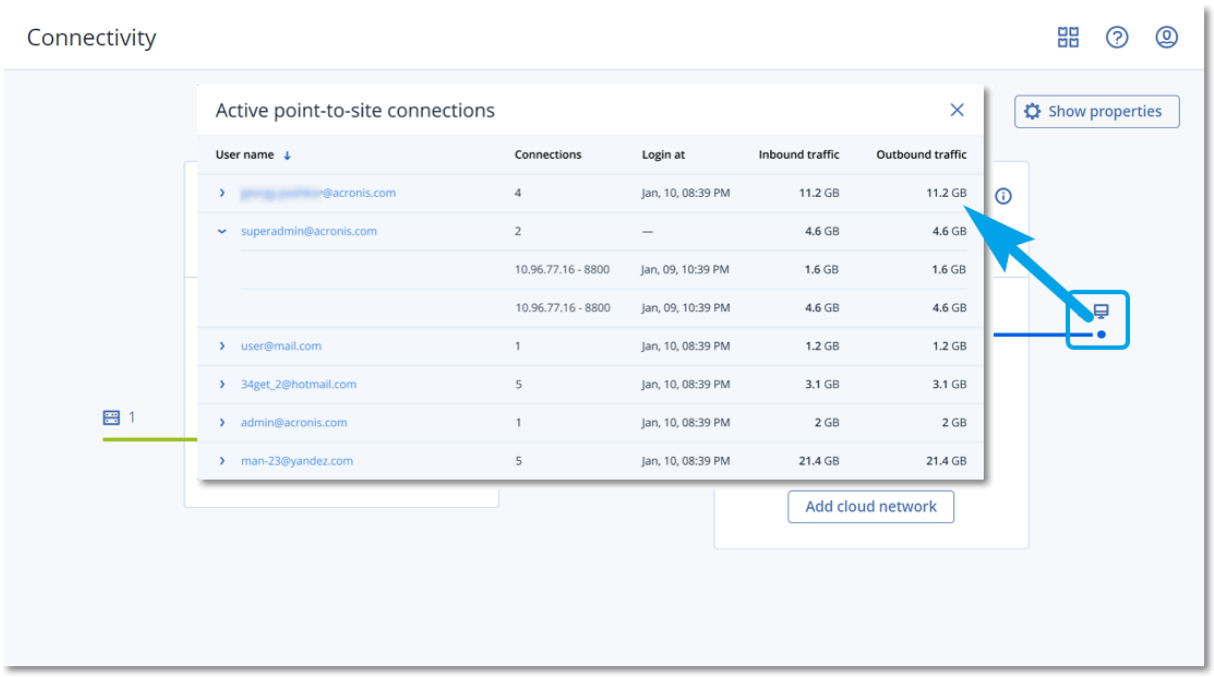
- Als u vermoedt dat het configuratiebestand is beschadigd.
- Als tweeledige verificatie is ingeschakeld voor uw account.

Wanneer het configuratiebestand is bijgewerkt, is het niet meer mogelijk verbinding te maken met het oude configuratiebestand. Zorg ervoor dat u het nieuwe bestand distribueert onder de gebruikers die de point-to-site-verbinding mogen gebruiken.

Actieve point-to-site-verbindingen

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

U kunt alle actieve point-to-site-verbindingen bekijken in **Noodherstel** > **Connectiviteit**. Klik op het machinepictogram op de blauwe regel **Point-to-site**. U ziet dan gedetailleerde informatie over actieve point-to-site-verbindingen, gegroepeerd op gebruikersnaam.



Werken met logboeken

Noodherstel verzamelt logboeken voor de VPN-toepassing en de VPN-gateway. De logboeken worden opgeslagen als .txt-bestanden, die worden gecomprimeerd in een .zip-archief. U kunt het archief downloaden en uitpakken, en de informatie gebruiken voor probleemoplossing of bewaking.

De volgende lijst bevat een beschrijving van de logbestanden in het .zip-archief en de gegevens die ze bevatten.

`dnsmasq.config.txt` - Het bestand bevat informatie over de configuratie van de service die DNS- en DHCP-adressen levert.

`dnsmsq.leases.txt` - Het bestand bevat informatie over de huidige DHCP-adresleases.

`dnsmasq_log.txt` - Het bestand bevat logboeken van de dnsmasq-service.

`ebtables.txt` - Het bestand bevat informatie over de firewall-tabellen.

`free.txt` - Het bestand bevat informatie over het vrije geheugen.

`ip.txt` - Het bestand bevat de logboeken van de configuratie van de netwerkinterfaces, inclusief de namen die kunnen worden gebruikt in de configuratie van de instellingen voor **Netwerkpakketten vastleggen**.

`NetworkManager_log.txt` - Het bestand bevat logboeken van de NetworkManager-service.

`NetworkManager_status.txt` - Het bestand bevat informatie over de status van de NetworkManager-service.

`openvpn@p2s_log.txt` - Het bestand bevat logboeken van de OpenVPN-service.

`openvpn@p2s_status.txt` - Het bestand bevat informatie over de status van de VPN-tunnels.

`ps.txt` - Het bestand bevat informatie over de huidige actieve processen op de VPN-gateway of in de VPN-toepassing.

`resolf.conf.txt` - Het bestand bevat informatie over de configuratie van de DNS-servers.

`routes.txt` - Het bestand bevat informatie over de netwerkroutes.

`uname.txt` - Het bestand bevat informatie over de huidige versie van de kernel van het besturingssysteem.

`uptime.txt` - Het bestand bevat informatie over hoe lang het besturingssysteem niet opnieuw is opgestart.

`vpnserver_log.txt` - Het bestand bevat logboeken van de VPN-service.

`vpnserver_status.txt` - Het bestand bevat informatie over de status van de VPN-server.

Zie "Multi-site IPsec VPN-logbestanden" (p. 823) voor meer informatie over logbestanden die specifiek zijn voor de IPsec VPN-connectiviteit.

De logboeken van de VPN-toepassing downloaden

U kunt het archief met de logboeken van de VPN-toepassing downloaden en uitpakken, en de informatie gebruiken voor probleemoplossing of bewaking.

De logboeken van de VPN-toepassing downloaden

1. Klik op de pagina **Connectiviteit** op het tandwielpictogram naast de VPN-toepassing.
2. Klik op **Logboek downloaden**.
3. [Optioneel] Selecteer **Netwerkpakketten vastleggen** en configureer de instellingen. Zie "Netwerkpakketten vastleggen" (p. 819) voor meer informatie.
4. Klik op **Gereed**.
5. Wanneer het .zip-archief klaar is om te downloaden, klikt u op **Logboek downloaden** en slaat u dit lokaal op.

De logboeken van de VPN-gateway downloaden

U kunt het archief met de logboeken van de VPN-gateway downloaden en uitpakken, en de informatie gebruiken voor probleemoplossing of bewaking.

De logboeken van de VPN-gateway downloaden

1. Klik op de pagina **Connectiviteit** op het tandwielpictogram naast de VPN-gateway.
2. Klik op **Logboek downloaden**.
3. [Optioneel] Selecteer **Netwerkpakketten vastleggen** en configureer de instellingen. Zie "Netwerkpakketten vastleggen" (p. 819) voor meer informatie.
4. Klik op **Gereed**.
5. Wanneer het .zip-archief klaar is om te downloaden, klikt u op **Logboek downloaden** en slaat u dit lokaal op.

Netwerkpakketten vastleggen

Als u problemen wilt oplossen en de communicatie wilt analyseren tussen de lokale productiesite en een primaire of herstelserver, kunt u ervoor kiezen om netwerkpakketten te verzamelen van de VPN-gateway of VPN-toepassing.

Wanneer er 32.000 netwerkpakketten zijn verzameld, of de tijdlimiet is verstreken, worden er geen netwerkpakketten meer vastgelegd en worden de resultaten weggeschreven naar een .libpcap-bestand dat wordt toegevoegd aan het .zip-archief voor logboeken.

De volgende tabel geeft meer informatie over de instellingen voor **Netwerkpakketten vastleggen** die u kunt configureren.

Instelling	Beschrijving
Naam van netwerkinterface	De netwerkinterface waarin netwerkpakketten moeten worden vastgelegd. Als u netwerkpakketten wilt vastleggen voor alle netwerkinterfaces, selecteert u **Alle**.
Tijdlimiet (seconden)	De tijdlimiet voor het vastleggen van netwerkpakketten. De maximale waarde die u kunt instellen, is 1800.
Filteren	Een extra filter om toe te passen op de vastgelegde netwerkpakketten. U kunt een tekenreeks invoeren met protocollen, poorten, richtingen, en de combinaties hiervan, gescheiden door spaties, bijvoorbeeld: 'and', 'or', 'not', ' (', ') ', 'src', 'dst', 'net', 'host', 'port', 'ip', 'tcp', 'udp', 'icmp', 'arp', 'esp'. Als u haakjes wilt gebruiken, moet u een spatie invoegen voor en na elk haakje. U kunt ook IP-adressen en netwerkadressen invoeren, bijvoorbeeld: 'icmp or arp' en 'port 67 or 68'. Voor meer informatie over de waarden die u kunt invoeren, raadpleegt u de Help van Linux-tcpdump.

Problemen met de IPsec VPN-configuratie oplossen

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Wanneer u de IPsec VPN-verbinding configureert of gebruikt, kunt u problemen ondervinden.

Bekijk de IPsec logbestanden om meer te weten te komen over de problemen die u bent tegengekomen. Kijk in het onderwerp Problemen met IPsec VPN-configuratie oplossen voor mogelijke oplossingen van enkele van de veelvoorkomende problemen die zich kunnen voordoen.

Problemen met IPsec VPN-configuratie oplossen

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

De volgende tabel bevat een beschrijving van de IPsec VPN-configuratieproblemen die het vaakst voorkomen, met uitlegt over hoe u deze problemen kunt oplossen.

Probleem	Mogelijke oplossing
Ik zie de volgende foutmelding: **Fout bij de IKE fase 1-onderhandeling. Controleer de IPsec IKE-instellingen in de cloud en op de lokale sites.**	Klik op **Opnieuw proberen** en controleer of er een specifiekere foutmelding wordt weergegeven. Een meer specifieke foutmelding kan bijvoorbeeld een foutmelding zijn over algoritmen die niet overeenkomen of een onjuiste vooraf gedeelde sleutel.

Probleem	Mogelijke oplossing
	Opmerking Om veiligheidsredenen zijn de volgende beperkingen van toepassing op de IPsec VPN-connectiviteit: • IKEv1 zal worden afgeschaft in RFC8247 en wordt niet ondersteund vanwege beveiligingsrisico's. Alleen verbindingen volgens het IKEv2-protocol worden ondersteund. • De volgende versleutelingsalgoritmen worden niet als veilig beschouwd en worden niet ondersteund: DES en 3DES. • De volgende hash-algoritmen worden niet als veilig beschouwd en worden niet ondersteund: SHA1 en MD5. • Diffie-Hellman-groepsnummer 2 wordt niet als veilig beschouwd en wordt niet ondersteund.
De verbinding tussen mijn lokale site en de cloudsite blijft de status **Verbinding maken** hebben.	Controleer: • Of de UDP-poort 500 open is (wanneer u een firewall gebruikt). • De connectiviteit tussen de lokale site en de cloudsite. • Of het IP-adres van de lokale site juist is.
De verbinding tussen mijn lokale site en de cloudsite blijft de status **Wachten op een verbinding** hebben.	U ziet deze status wanneer de **opstartactie** voor de cloudsite is ingesteld op **Toevoegen**, dat wil zeggen dat de cloudsite wacht op de lokale site om de verbinding te initiëren. Initieer de verbinding vanaf de lokale site.
De verbinding tussen mijn lokale site en de cloudsite blijft de status **Wachten op verkeer** hebben.	U ziet deze status wanneer de **opstartactie** voor de cloudsite is ingesteld op **Routeren**. Als u een verbinding verwacht van de lokale site, doe dan het volgende: • Probeer vanaf de lokale site de virtuele machine op de cloudsite te pingen. Dit is een standaardgedrag dat nodig is om een tunnel tot stand te brengen voor sommige apparaten, bijvoorbeeld Cisco ASA. (Modus Routeren) • Zorg ervoor dat de lokale site een tunnel tot stand heeft gebracht door de **opstartactie** van de lokale site in te stellen op **Start**.

Probleem	Mogelijke oplossing
De verbinding tussen mijn lokale site en de cloudsite is tot stand gebracht, maar ik kan zien dat een of meer van de netwerkbeleidsregels niet actief zijn.	Dit probleem kan de volgende oorzaken hebben: • De netwerktoewijzing op de Cloud IPsec-site is verschillend van de netwerktoewijzing op de lokale site. Zorg ervoor dat de netwerktoewijzingen en de volgorde van de netwerkbeleidsregels op de lokale en cloudsites exact overeenkomen. • Deze status is juist wanneer de **opstartactie** van de lokale site en/of van de cloudsite is ingesteld op **Routeren** (bijvoorbeeld op Cisco ASA-apparaten) en er momenteel geen verkeer is. U kunt proberen te pingen om te controleren of de tunnel tot stand is gebracht. Als de ping niet werkt, controleer dan de netwerktoewijzing op de lokale en de cloudsite.
Ik wil een specifieke IPsec-verbinding opnieuw starten.	Een specifieke IPsec-verbinding opnieuw starten: 1. Klik op het scherm **Noodherstel** > **Connectiviteit** op de IPsec-verbinding. 2. Klik op **Verbinding uitschakelen**. 3. Klik opnieuw op de IPsec-verbinding. 4. Klik op **Verbinding inschakelen**.

De IPsec VPN-logbestanden downloaden

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

U kunt aanvullende informatie over de IPsec-connectiviteit vinden in de logbestanden op de VPN-server. De logbestanden zijn gecomprimeerd in een .zip-archief dat u kunt downloaden en uitpakken.

Vereisten

Multi-site IPsec VPN-connectiviteit is geconfigureerd.

Het .zip-archief met de logbestanden downloaden

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Connectiviteit**.
2. Klik op het tandwielpictogram naast de VPN-gateway van de cloudsite.
3. Klik op **Logbestand downloaden**.
4. Klik op **Gereed**.

5. Wanneer het .zip-archief klaar is om te downloaden, klikt u op **Logboek downloaden** en slaat u dit lokaal op.

Multi-site IPsec VPN-logbestanden

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

De volgende lijst bevat een beschrijving van de IPsec VPN-logbestanden in het zip-archief en de gegevens die ze bevatten.

- `ip.txt`: Het bestand bevat de logboeken van de configuratie van de netwerkinterfaces. U moet twee IP adressen zien: een openbaar IP-adres en een lokaal IP-adres. Als u deze IP-adressen niet in het logboek ziet, is er een probleem. Neem contact op met het ondersteuningsteam.

  Opmerking
  Het masker voor het openbare IP-adres moet 32 zijn.

- `swanctl-list-loaded-config.txt`: Het bestand bevat informatie over alle IPsec-sites.
  Als u geen site in het bestand ziet, dan is de IPsec-configuratie niet toegepast. Probeer de configuratie bij te werken en op te slaan, of neem contact op met het ondersteuningsteam.
- `swanctl-list-active-sas.txt`: Het bestand bevat verbindingen en beleidsregels die de status 'actief' of 'verbinding maken' hebben.

Herstelservers instellen

In dit gedeelte wordt het volgende beschreven: de concepten van failover en failback, het maken van een herstelserver en de bewerkingen in het geval van noodherstel.

Herstelserver maken

Volg de onderstaande procedure om een herstelserver te maken die een kopie zal zijn van uw workload. U kunt ook de videoles over dit proces bekijken.

Belangrijk
Wanneer u een failover uitvoert, kunt u alleen herstelpunten selecteren die zijn gemaakt nadat de herstelserver is gemaakt.

Vereisten

- Er moet een beschermingsschema worden toegepast op de oorspronkelijke machine die u wilt beschermen. Dit schema moet een back-up maken van de volledige machine of alleen van de schijven die vereist zijn om de nodige services op te starten en te leveren naar een cloudopslag.
- Een van de typen connectiviteit met de cloudsite moet worden ingesteld.

Een herstelserver maken

1. Ga naar het tabblad **Alle apparaten** en selecteer de machine die u wilt beschermen.
2. Klik op **Noodherstel** en klik vervolgens op **Herstelserver maken**.
3. Selecteer het aantal virtuele kernen en de grootte van het RAM.

   Opmerking
   U kunt de compute-punten voor elke optie zien. Het aantal compute-punten geeft de kosten per uur weer voor het uitvoeren van de herstelserver. Zie "Compute-punten" (p. 779) voor meer informatie.

4. Geef het cloudnetwerk op waarmee de server wordt verbonden.
5. Selecteer de optie **DHCP**.

De optie DHCP	Beschrijving
Geleverd door cloudsite	Standaardinstelling. Het IP-adres van de server wordt geleverd door een automatisch geconfigureerde DHCP-server in de cloud.
Aangepast	Het IP-adres van de server wordt geleverd door uw eigen DHCP-server in de cloud.

6. [Optioneel] Geef het **MAC-adres** op.
   Het MAC-adres is een unieke identificatie die wordt toegewezen aan de netwerkadapter van de server. Als u aangepast DHCP gebruikt, kunt u configureren dat er altijd een specifiek IP-adres wordt toegewezen aan een specifiek MAC-adres, zodat de herstelserver altijd hetzelfde IP-adres krijgt. U kunt toepassingen uitvoeren met licenties die zijn geregistreerd met het MAC-adres.
7. Geef het IP-adres op voor de server in het productienetwerk. Standaard wordt het IP-adres van de oorspronkelijke machine ingesteld.

   Opmerking
   Als u een DHCP-server gebruikt, moet u dit IP-adres toevoegen aan de uitsluitingslijst voor de server om IP-adresconflicten te vermijden.
   Als u een aangepaste DHCP-server gebruikt, moet u in **IP-adres in productienetwerk** hetzelfde IP-adres opgeven als het IP-adres dat is geconfigureerd op de DHCP-server. Anders werkt de testfailover niet correct en is de server niet bereikbaar via een openbaar IP-adres.

8. [Optioneel] Schakel het selectievakje **Test-IP-adres** in en geef vervolgens het IP-adres op.
   Op die manier kunt u een failover testen in het geïsoleerde testnetwerk en verbinding maken met de herstelserver via RDP of SSH tijdens een testfailover. In de testfailovermodus vervangt de VPN-gateway het test-IP-adres door het productie-IP-adres via het NAT-protocol.
   Als u het selectievakje uitgeschakeld laat, is de console de enige manier om toegang te krijgen tot de server tijdens een test-failover.

Opmerking
Als u een DHCP-server gebruikt, moet u dit IP-adres toevoegen aan de uitsluitingslijst voor de server om IP-adresconflicten te vermijden.

U kunt een van de voorgestelde IP-adressen selecteren of een ander IP-adres typen.

9. [Optioneel] Schakel het selectievakje **Internettoegang** in.
   Hierdoor krijgt de herstelserver toegang tot internet tijdens een echte of test-failover. Standaard staat de TCP-poort 25 open voor uitgaande verbindingen naar openbare IP-adressen.
10. [Optioneel] Stel de **RPO-drempel** in.
    De RPO-drempel bepaalt het maximaal toegestane tijdsinterval tussen het laatste geschikte herstelpunt voor een failover en de huidige tijd. De waarde kan worden ingesteld op 15 - 60 minuten, 1 - 24 uur, 1 - 14 dagen.
11. [Optioneel] Schakel het selectievakje **Openbaar IP-adres gebruiken** in.
    Als u een openbaar IP-adres hebt, is de herstelserver beschikbaar via internet tijdens een failover of test-failover. Als u het selectievakje uitgeschakeld laat, is de server alleen beschikbaar in uw productienetwerk.
    Voor de optie **Openbaar IP-adres gebruiken** moet de optie **Internettoegang** zijn ingeschakeld.
    Het openbare IP-adres wordt weergegeven wanneer u de configuratie hebt voltooid. Standaard staat TCP-poort 443 open voor inkomende verbindingen naar openbare IP-adressen.

    Opmerking
    Als u het selectievakje **Openbaar IP-adres gebruiken** uitschakelt of de herstelserver verwijdert, wordt het openbare IP-adres niet gereserveerd.

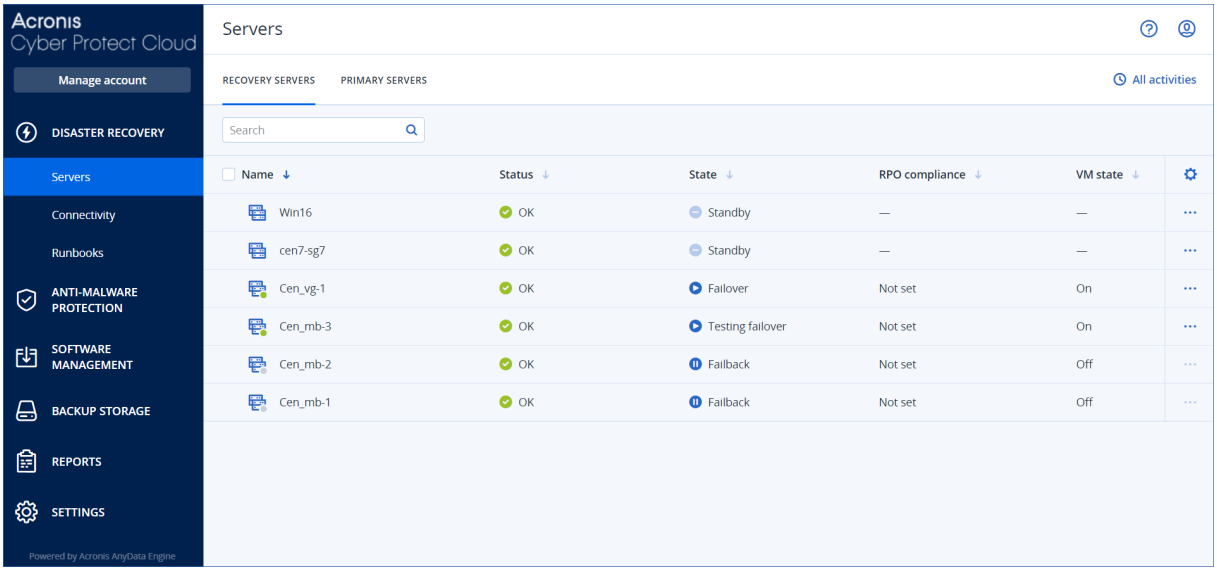
12. [Optioneel] [Als de back-ups voor de geselecteerde machine zijn versleuteld als machine-eigenschap]: geef het wachtwoord op dat automatisch wordt gebruikt wanneer een virtuele machine voor de herstelserver wordt gemaakt vanaf de versleutelde back-up.
    a. Klik op **Opgeven**, voer vervolgens het wachtwoord voor de versleutelde back-up in en definieer een naam voor de referenties.
       Standaard ziet u de meest recente back-up in de lijst.
    b. [Optioneel] Als u alle back-ups wilt bekijken, selecteert u **Alle back-ups weergeven**.
    c. Klik op **Gereed**.

    Opmerking
    Hoewel het wachtwoord dat u opgeeft, wordt opgeslagen in een veilige opslagplaats voor referenties, kan het opslaan van wachtwoorden in strijd zijn met uw nalevingsverplichtingen.

13. [Optioneel] Wijzig de naam van de herstelserver.
14. [Optioneel] Typ een beschrijving voor de herstelserver.
15. [Optioneel] Klik op het tabblad **Cloudfirewallregels** om de standaardfirewallregels te bewerken. Zie "Firewallregels instellen voor cloudservers" (p. 852) voor meer informatie.

16. Klik op **Maken**.

De herstelserver wordt weergegeven op het tabblad **Noodherstel** > **Servers** > **Herstelservers** van de Cyber Protect-console. U kunt de instellingen ook zien als u de oorspronkelijke machine selecteert en op **Noodherstel** klikt.



Hoe failover werkt

Productiefailover

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Wanneer u een herstelserver maakt, blijft deze de status **Stand-by** behouden. De betreffende virtuele machine bestaat pas als u een failover start. Voordat u een failoverproces start, moet u ten minste één back-up van een schijfimage (met opstartvolume) van de oorspronkelijke machine maken.

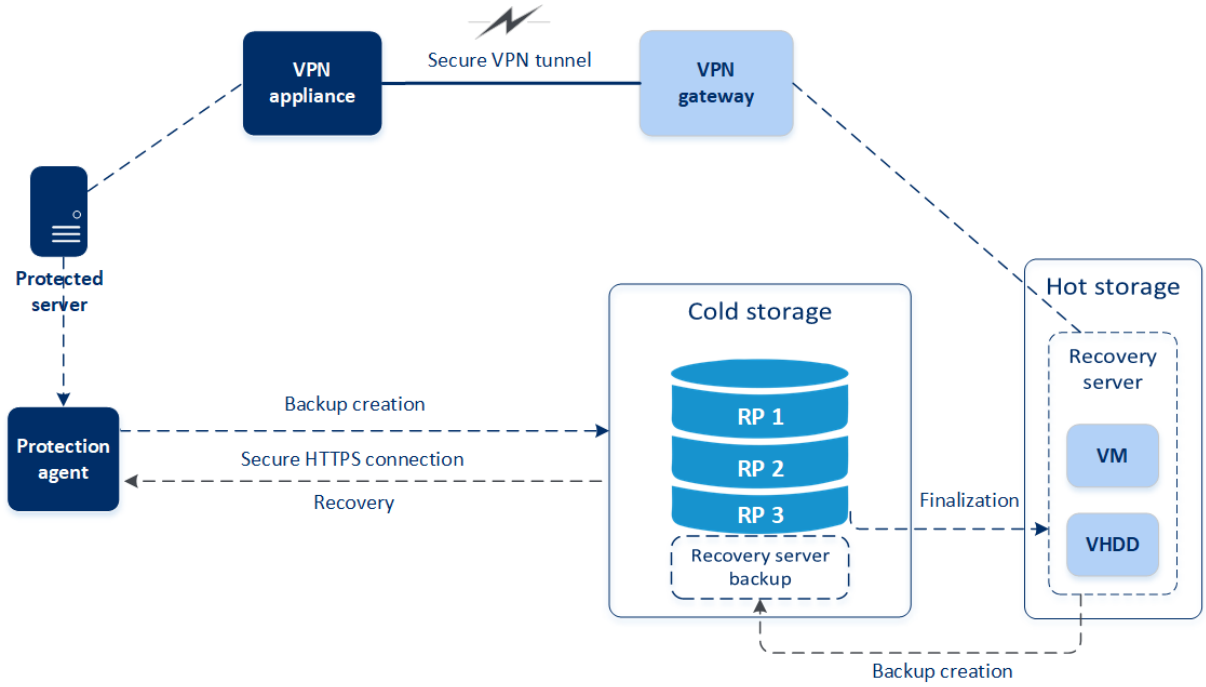
Bij het starten van het failoverproces selecteert u het herstelpunt (back-up) van de oorspronkelijke machine van waaruit een virtuele machine met de vooraf gedefinieerde parameters wordt gemaakt. Bij de failover wordt gebruikgemaakt van de functionaliteit 'VM uitvoeren vanuit back-up'. De herstelserver krijgt de overgangsstatus **Voltooien**. Met dit proces worden de virtuele schijven van de server overgebracht van de back-upopslag (niet-dynamische opslag) naar de noodherstelopslag (dynamische opslag).

Opmerking
Tijdens de fase van **Voltooien** is de server toegankelijk en bruikbaar, maar de prestaties zijn minder dan normaal. U kunt de serverconsole openen door op de link **Console is gereed** te klikken. De link is beschikbaar in de kolom **VM-status** op het scherm **Noodherstel** > **Servers** en in de weergave **Details** van de server.

Na afloop van de fase van **Voltooien** bereikt de serverprestatie de normale waarde. De serverstatus verandert in **Failover**. De workload wordt nu overgeschakeld van de oorspronkelijke machine naar de herstelserver op de cloudsite.

Als de herstelserver een beveiligingsagent heeft, wordt de agentservice gestopt om interferentie te voorkomen (zoals het starten van een back-up of het rapporteren van verouderde statussen aan het back-uponderdeel).

In het diagram hieronder ziet u het failover- en failbackproces.



Failover testen

Tijdens een **test-failover** wordt de virtuele machine niet voltooid. Dit betekent dat de agent de inhoud van de virtuele schijven rechtstreeks uit de back-up leest, waarbij willekeurige toegang tot verschillende delen van de back-up wordt verkregen. De prestaties kunnen daardoor langzamer zijn dan de normale prestaties. Zie "Een testfailover uitvoeren" (p. 828) voor meer informatie over het testfailoverproces.

Automatische testfailover

Wanneer automatisch e testfailover is geconfigureerd, wordt deze één keer per maand uitgevoerd zonder enige handmatige actie. Zie "Automatische testfailover" (p. 830) en "Automatische testfailover configureren" (p. 831) voor meer informatie.

Een testfailover uitvoeren

Bij het uitvoeren van een testfailover wordt een herstelserver gestart in een test-VLAN dat is geïsoleerd van uw productienetwerk. U kunt meerdere herstelservers tegelijk testen en de onderlinge interactie controleren. In het testnetwerk communiceren de servers via de productie-IP-adressen, maar er kunnen geen TCP- of UDP-verbindingen tot stand worden gebracht met de workloads in uw lokale netwerk.

Tijdens de testfailover wordt de virtuele machine (herstelserver) niet voltooid. De agent leest de inhoud van de virtuele schijven rechtstreeks uit de back-up en opent willekeurig verschillende delen van de back-up. Hierdoor kunnen de prestaties van de herstelserver in de testfailoverstatus langzamer zijn dan de normale prestaties.

Hoewel het uitvoeren van een failover optioneel is, raden we u aan om dit regelmatig te doen. Maak een afweging van kosten en veiligheid en kies een frequentie die geschikt voor u is. Het is verstandig gebruik te maken van een runbook: een set instructies die beschrijven hoe de productieomgeving in de cloud bedrijfsklaar kan worden gemaakt.

Belangrijk
U moet van te voren een herstelserver maken om uw apparaten te beschermen tegen een noodgeval.

U kunt alleen een failover uitvoeren vanaf herstelpunten die zijn gemaakt nadat de herstelserver van het apparaat is gemaakt.

Er moet ten minste één herstelpunt worden gemaakt voordat er wordt overgeschakeld naar een herstelserver. Maximaal worden 100 herstelpunten ondersteund.

Een testfailover uitvoeren:

1. Selecteer de oorspronkelijke machine of selecteer de herstelserver die u wilt testen.
2. Klik op **Noodherstel**.
   De beschrijving van de herstelserver wordt geopend.
3. Klik op **Failover**.
4. Selecteer het type failover **Testfailover**.
5. Selecteer het herstelpunt (back-up) en klik vervolgens op **Starten**.
6. Als de back-up die u hebt geselecteerd, is versleuteld als machine-eigenschap:

a. Voer het versleutelingswachtwoord voor de back-upset in.

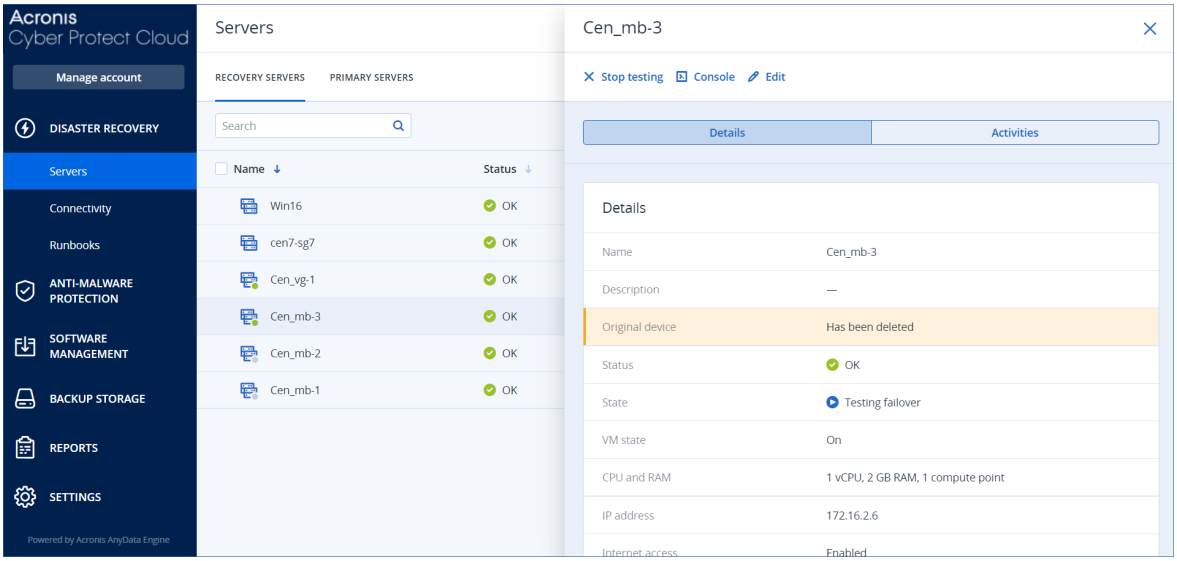
> **Opmerking**
> Het wachtwoord wordt alleen tijdelijk opgeslagen en alleen gebruikt voor de huidige testfailoverbewerking. Het wachtwoord wordt automatisch verwijderd uit de opslagplaats voor referenties als de testfailover wordt gestopt of is voltooid.

b. [Optioneel] Als u het wachtwoord voor de back-upset wilt opslaan en gebruiken voor latere failoverbewerkingen, schakelt u het selectievakje **Sla wachtwoord op in een veilige opslagplaats voor referenties...** in en voert u vervolgens in het veld **Naam van referenties** een naam in voor de referenties.

> **Belangrijk**
> Het wachtwoord wordt opgeslagen in een veilige opslagplaats voor referenties en wordt automatisch toegepast bij latere failoverbewerkingen. Denk er wel aan dat het opslaan van wachtwoorden mogelijk in strijd is met uw nalevingsverplichtingen.

c. Klik op **Gereed**.

Wanneer de herstelserver start, wordt de status gewijzigd in **Failover testen**.



7. Test de herstelserver op een van de volgende manieren:
   - Klik op **Noodherstel** > **Servers**, selecteer de herstelserver en klik vervolgens op **Console**.
   - Maak verbinding met de herstelserver via RDP of SSH en het test-IP-adres dat u hebt opgegeven bij het maken van de herstelserver. Probeer de verbinding zowel binnen als buiten het productienetwerk (zoals beschreven in 'Point-to-site-verbinding').
   - Voer een script uit binnen de herstelserver.
     Het script kan het aanmeldingsscherm en de internetverbinding controleren, en verifiëren of toepassingen worden gestart en of andere machines verbinding kunnen maken met de herstelserver.

- Als de herstelserver toegang heeft tot internet en een openbaar IP-adres heeft, kunt u TeamViewer gebruiken.

8. Wanneer de test is voltooid, klikt u op **Testen stoppen**.

   De herstelserver wordt gestopt. Alle wijzigingen die zijn aangebracht in de herstelserver tijdens de testfailover, gaan verloren.

Opmerking
De acties **Server starten** en **Server stoppen** zijn niet van toepassing op testfailoverbewerkingen, zowel in runbooks als bij het handmatig starten van een testfailover. Als u een dergelijke actie probeert uit te voeren, zal deze mislukken met de volgende foutmelding:
Mislukt: De actie is niet van toepassing op de huidige serverstatus.

Automatische testfailover

Met automatische testfailover wordt de herstelserver één keer per maand automatisch getest zonder enige handmatige actie.

Het proces van de automatische testfailover bestaat uit de volgende stappen:

1. een virtuele machine maken vanaf het laatste herstelpunt
2. een momentopname maken van de virtuele machine
3. analyseren of het besturingssysteem van de virtuele machine correct opstart
4. een melding ontvangen over de status van de testfailover

Opmerking
Er worden compute-punten verbruikt voor een automatische testfailover.

U kunt de automatische testfailover configureren in de instellingen van de herstelserver. Zie "Automatische testfailover configureren" (p. 831) voor meer informatie.

Let op: Het kan in zeldzame gevallen voorkomen dat de automatische testfailover wordt overgeslagen en mogelijk niet op het geplande tijdstip wordt uitgevoerd. Dit komt omdat productiefailover een hogere prioriteit heeft dan automatische testfailover, dus de hardwareresources (CPU en RAM) die zijn toegewezen voor automatische testfailover, kunnen tijdelijk beperkt zijn om te waarborgen dat er voldoende resources zijn voor een gelijktijdige productiefailover.

Als de automatische testfailover om de een of andere reden wordt overgeslagen, wordt er een waarschuwing weergegeven.

Opmerking
Automatische testfailover mislukt als de back-ups van de oorspronkelijke machine zijn versleuteld als machine-eigenschap en het versleutelingswachtwoord niet is opgegeven bij het maken van de herstelserver. Zie "Herstelserver maken" (p. 823) voor meer informatie over het opgeven van het versleutelingswachtwoord.

Automatische testfailover configureren

Als u automatische testfailover configureert, kunt u uw herstelserver elke maand testen zonder enige handmatige actie.

Automatische testfailover configureren:

1. Ga in de console naar **Noodherstel** > **Servers** > **Herstelservers** en selecteer de herstelserver.
2. Klik op **Bewerken**.
3. Ga in het gedeelte **Automatische testfailover** naar het veld **Planning** en selecteer **Maandelijks**.
4. [Optioneel] Ga naar **Time-out voor momentopname** en wijzig de standaardwaarde van de maximale periode (in minuten) gedurende welke wordt geprobeerd de automatische testfailover uit te voeren.
5. [Optioneel] Als u de waarde van **Time-out voor momentopname** wilt opslaan als de standaardwaarde en deze automatisch wilt laten invullen wanneer u automatisch e testfailover inschakelt voor de andere herstelservers, selecteert u **Instellen als standaardtime-out**.
6. Klik op **Opslaan**.

De status van de automatisch e testfailover bekijken

U kunt de details bekijken van een voltooide automatisch e testfailover, zoals status, begintijd, eindtijd, duur en de momentopname van de virtuele machine.

De status van een automatisch e testfailover van een herstelserver bekijken

1. Ga in de console naar **Noodherstel** > **Servers** > **Herstelservers** en selecteer de herstelserver.
2. Controleer in het gedeelte **Automatiseerde testfailover** de details van de laatste automatisch e testfailover.
3. [Optioneel] Klik op **Momentopname weergeven** om de momentopname van de virtuele machine te bekijken.

Automatische testfailover uitschakelen

U kunt automatisch e testfailover uitschakelen als u resources wilt besparen of als u geen automatisch e testfailover nodig hebt voor een bepaalde herstelserver.

Automatische testfailover uitschakelen:

1. Ga in de console naar **Noodherstel** > **Servers** > **Herstelservers** en selecteer de herstelserver.
2. Klik op **Bewerken**.
3. Ga in het gedeelte **Automatische testfailover** naar het veld **Planning** en selecteer **Nooit**.
4. Klik op **Opslaan**.

Failover uitvoeren

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Een failover is een proces waarbij een workload van uw locatie naar de cloud wordt verplaatst, en ook de status wanneer de workload in de cloud blijft.

Wanneer u een failover start, wordt de herstelserver in het productienetwerk gestart. Als u interferentie en ongewenste problemen wilt voorkomen, controleert u of de oorspronkelijke workload niet online is en niet toegankelijk is via VPN.

Als u een back-upinterferentie in hetzelfde cloudarchief wilt voorkomen, trekt u het beschermingsschema handmatig in voor de workload die momenteel de status **Failover** heeft. Zie Een beschermingsschema intrekken voor meer informatie over het intrekken van schema's.

Belangrijk
U moet van te voren een herstelserver maken om uw apparaten te beschermen tegen een noodgeval.

U kunt alleen een failover uitvoeren vanaf herstelpunten die zijn gemaakt nadat de herstelserver van het apparaat is gemaakt.

Er moet ten minste één herstelpunt worden gemaakt voordat er wordt overgeschakeld naar een herstelserver. Maximaal worden 100 herstelpunten ondersteund.

U kunt de onderstaande instructies volgen of de videoles bekijken.

Een failover uitvoeren

1. Zorg ervoor dat de oorspronkelijke machine niet beschikbaar is op het netwerk.
2. Ga in de Cyber Protect-console naar **Noodherstel** > **Servers** > **Herstelservers** en selecteer de herstelserver.
3. Klik op **Failover**.
4. Selecteer het type failover **Productiefailover**.
5. Selecteer het herstelpunt (back-up) en klik vervolgens op **Starten**.
6. [Als de back-up die u hebt geselecteerd, is versleuteld als machine-eigenschap]

a. Voer het versleutelingswachtwoord voor de back-upset in.

Opmerking
Het wachtwoord wordt alleen tijdelijk opgeslagen en alleen gebruikt voor de huidige failoverbewerking. Het wachtwoord wordt automatisch verwijderd uit de opslagplaats voor referenties nadat de failoverbewerking is voltooid en de server weer de status **Stand-by** heeft.

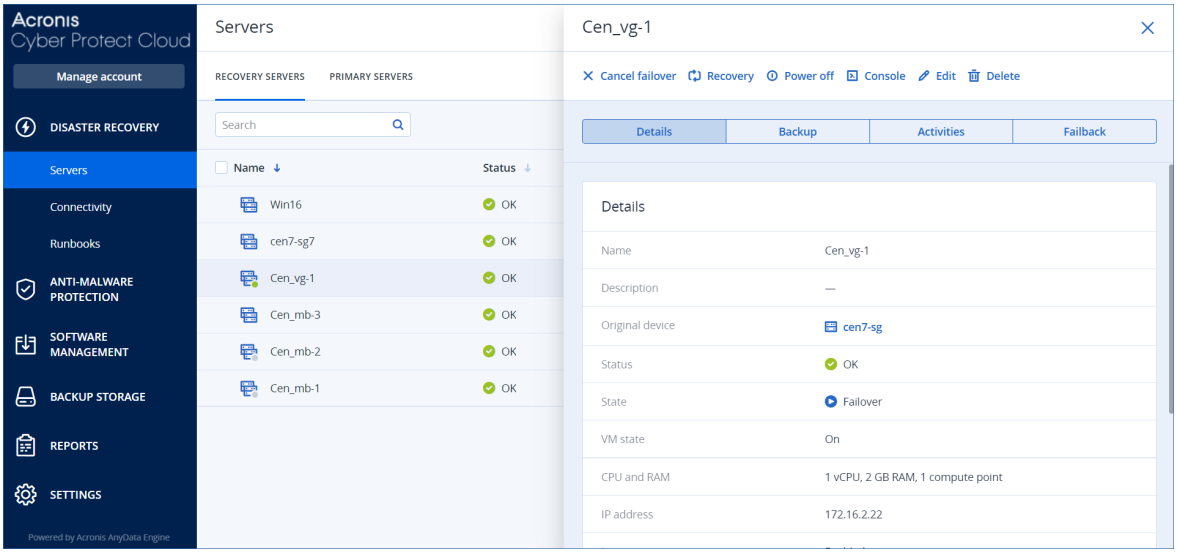
b. [Optioneel] Als u het wachtwoord voor de back-upset wilt opslaan en gebruiken voor latere failoverbewerkingen, schakelt u het selectievakje **Sla wachtwoord op in een veilige opslagplaats voor referenties...** in en voert u vervolgens in het veld **Naam van referenties** een naam in voor de referenties.

Belangrijk
Het wachtwoord wordt opgeslagen in een veilige opslagplaats voor referenties en wordt automatisch toegepast bij latere failoverbewerkingen. Denk er wel aan dat het opslaan van wachtwoorden mogelijk in strijd is met uw nalevingsverplichtingen.

c. Klik op **Gereed**.

Wanneer de herstelserver start, verandert de status ervan in **Voltooien** en na verloop van tijd in **Failover.**

Belangrijk
Het is belangrijk om te weten dat de server beschikbaar is tijdens zowel de fase van **Voltooien** als de fase van **Failover**. Tijdens de fase van **Voltooien** kunt u toegang krijgen tot de serverconsole door te klikken op de link **Console is gereed**. De link is beschikbaar in de kolom **VM-status** op het scherm **Noodherstel** > **Servers** en in de weergave **Details** van de server. Zie "Hoe failover werkt" (p. 826) voor meer details.



7. Controleer in de console of de herstelserver is gestart. Klik op **Noodherstel** > **Servers**, selecteer de herstelserver en klik vervolgens op **Console**.
8. Controleer of de herstelserver toegankelijk is met behulp van het productie-IP-adres dat u hebt opgegeven toen u de herstelserver maakte.

Wanneer de herstelserver is voltooid, wordt automatisch een nieuw beschermingsschema gemaakt en toegepast op de server. Dit beschermingsschema is gebaseerd op het beschermingsschema dat is gebruikt voor het maken van de herstelserver, maar met bepaalde beperkingen. In dit schema kunt u alleen het schema en de bewaarregels wijzigen. Zie 'Back-up maken van de cloudservers' voor meer informatie.

Als u de failover wilt annuleren, selecteert u de herstelserver en klikt u op **Failover annuleren**. Alle wijzigingen vanaf het failovermoment, behalve de back-ups van de herstelserver, gaan verloren. De herstelserver wordt teruggezet naar de **stand-bystatus**.

Als u een failback wilt uitvoeren, selecteert u de herstelserver en klikt u op **Failback**.

Een failover van servers uitvoeren met behulp van lokaal DNS

Als u DNS-servers op de lokale site gebruikt voor het oplossen van machinenamen, dan zullen de herstelservers die overeenkomen met de machines die afhankelijk zijn van het DNS, niet meer kunnen communiceren na een failover omdat ze verschillen van de DNS-servers die in de cloud worden gebruikt. Standaard worden de DNS-servers van de cloudsite gebruikt voor de nieuw gemaakte cloudservers. Als u aangepaste DNS-instellingen wilt toepassen, neemt u contact op met het ondersteuningsteam.

Een failover van een DHCP-server uitvoeren

In uw lokale infrastructuur kan de DHCP-server zich op een Windows- of Linux-host bevinden. Wanneer een failover van een dergelijke host naar de cloudsite wordt uitgevoerd, is er het probleem van DHCP-serverduplicatie omdat de VPN-gateway in de cloud ook de DHCP-rol vervult. U kunt dit probleem oplossen op een van de volgende manieren:

- Als alleen een failover van de DHCP-host naar de cloud is uitgevoerd, terwijl de rest van de lokale servers zich nog steeds op de lokale site bevindt, dan moet u zich aanmelden bij de DHCP-host in de cloud en de DHCP-server op de host uitschakelen. Er zullen dan geen conflicten ontstaan en alleen de VPN-gateway werkt als DHCP-server.
- Als uw cloudservers al de IP-adressen van de DHCP-host hebben, dan moet u zich aanmelden bij de DHCP-host in de cloud en de DHCP-server op de host uitschakelen. U moet u ook aanmelden bij de cloudservers en de DHCP-lease vernieuwen om nieuwe IP-adressen (toegewezen vanaf de juiste DHCP-server gehost op de VPN-gateway) toe te wijzen.

Opmerking
De instructies zijn niet geldig wanneer uw cloud-DHCP-server is geconfigureerd met de optie **Aangepast DHCP** en sommige herstel- of primaire servers hun IP-adres krijgen van deze DHCP-server.

Hoe failback werkt

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Een failback is een proces waarbij de workload vanuit de cloud wordt teruggeplaatst naar een fysieke of virtuele machine op uw lokale site. U kunt een failback uitvoeren op een herstelserver met de status **Failover** en tegelijkertijd de server op uw lokale site blijven gebruiken.

U kunt een automatische failover uitvoeren naar een virtuele of fysieke doelmachine op uw lokale site. Tijdens de failback kunt u de back-upgegevens overdragen naar uw lokale site terwijl de virtuele machine in de cloud actief blijft. Dankzij deze technologie blijft de downtimeperiode heel kort (de duur van deze periode wordt geschat en weergegeven in de Cyber Protect-console). U kunt deze informatie bekijken en gebruiken om uw activiteiten te plannen en, indien nodig, uw klanten te waarschuwen voor een komende downtimeperiode.

Er is een verschil tussen het failbackproces naar virtuele doelmachines en het failbackproces naar fysieke doelmachines. Zie "Failback naar een virtuele doelmachine" (p. 835) en "Failback naar een fysieke doelmachine" (p. 841) voor meer informatie over de fasen van het failbackproces.

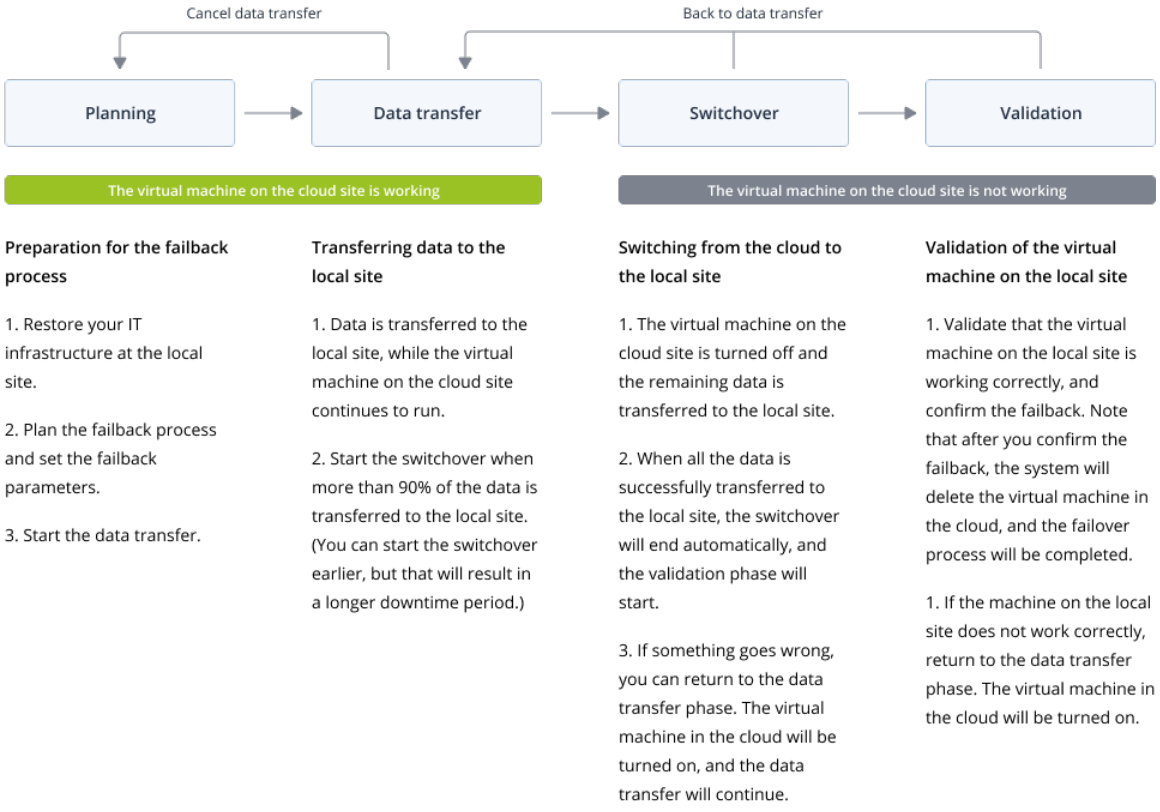
In specifieke gevallen waarin het niet mogelijk is de automatische failbackprocedure te gebruiken, kunt u een handmatige failback uitvoeren. Zie "Handmatige failback" (p. 844) voor meer informatie.

Opmerking
Runbookbewerkingen ondersteunen alleen de failback in handmatige modus. Dus als u het failbackproces start door een runbook uit te voeren dat een stap op de **failbackserver** bevat, dan is een handmatige interactie vereist: u moet de machine handmatig herstellen, en het failbackproces bevestigen of annuleren vanaf het tabblad **Noodherstel** > **Servers**.

Failback naar een virtuele doelmachine

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Het failbackproces naar een virtuele doelmachine bestaat uit vier fasen.



1. **Planning**. Tijdens deze fase herstelt u de IT-infrastructuur op uw lokale site (zoals de hosts en de netwerkconfiguraties), configureert u de failbackparameters en plant u wanneer u de gegevensoverdracht wilt starten.

   Opmerking
   Als u de totale tijd voor het failbackproces tot een minimum wilt beperken, raden wij u aan de fase van gegevensoverdracht te starten zodra u uw lokale servers hebt ingesteld, en vervolgens door te gaan met het configureren van het netwerk en de rest van de lokale infrastructuur tijdens de fase van gegevensoverdracht.

2. **Gegevensoverdracht**. Tijdens deze fase worden de gegevens van de cloudsite overgedragen naar de lokale site terwijl de virtuele machine in de cloud actief blijft. Switchover is de volgende fase en u kunt deze op elk moment starten tijdens de fase van gegevensoverdracht, maar u moet hierbij rekening houden met het volgende.
   Hoe langer de fase van gegevensoverdracht duurt,
   - hoe langer de virtuele machine in de cloud actief blijft.
   - hoe meer gegevens worden overgedragen naar uw lokale site.
   - hoe hoger de kosten die u moet betalen (u geeft meer compute-punten uit).
   - hoe korter de periode van downtime tijdens de switchoverfase.

Als u de downtime tot een minimum wilt beperken, start u de switchoverfase nadat meer dan 90% van de gegevens is overgedragen naar de lokale site.

Als een langere downtime geen probleem is en u niet meer compute-punten wilt uitgeven om de virtuele machine in de cloud actief te houden, dan kunt u de switchoverfase eerder starten.

Als u het failbackproces tijdens de fase van gegevensoverdracht annuleert, worden de overgedragen gegevens niet verwijderd van de lokale site. U kunt mogelijke problemen voorkomen door de overgedragen gegevens handmatig te verwijderen voordat u een nieuw failbackproces start. Het volgende gegevensoverdrachtproces start vanaf het begin.

3. **Switchover**. Tijdens deze fase wordt de virtuele machine in de cloud uitgeschakeld en worden de resterende gegevens, waaronder de laatste incrementele back-up, overgedragen naar de lokale site. Als er geen back-upschema is toegepast op de herstelserver, wordt tijdens de switchoverfase automatisch een back-up gemaakt, waardoor het proces wordt vertraagd.

   U kunt de geschatte tijd tot voltooiing (downtimeperiode) van deze fase bekijken in de Cyber Protect-console. Let op: wanneer alle gegevens zijn overgedragen naar de lokale site (er is geen gegevensverlies en de virtuele machine op de lokale site is een exacte kopie van de virtuele machine in de cloud), wordt de switchoverfase voltooid. De virtuele machine op de lokale site wordt hersteld en de validatiefase wordt automatisch gestart.
4. **Validatie**. Tijdens deze fase is de virtuele machine op de lokale site gereed en wordt deze automatisch gestart. U kunt controleren of de virtuele machine correct werkt, en:
   - Als alles werkt zoals verwacht, bevestigt u de failback. Na bevestiging van de failback wordt de virtuele machine in de cloud verwijderd en keert de herstelserver terug naar de status **Stand-by**. Dit is het einde van het failbackproces.
   - Als er iets misgaat, kunt u de switchover annuleren en terugkeren naar de fase van gegevensoverdracht.

Failback uitvoeren naar een virtuele machine

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

U kunt een failback uitvoeren naar een virtuele doelmachine op uw lokale site.

Vereisten

- De agent die u gaat gebruiken om de failback uit te voeren, is online en wordt momenteel niet gebruikt voor een andere failbackbewerking.
- Uw internetverbinding is stabiel.
- Er is ten minste één volledige back-up van de virtuele machine in de cloud.

Een failback uitvoeren naar een virtuele machine

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Servers**.
2. Selecteer de herstelserver die de status **Failover** heeft.
3. Klik op het tabblad **Failback**.
4. Open het gedeelte **Failbackparameters**. Selecteer de optie **Virtuele machine** als **Doel** en configureer de andere parameters.

   Let op: Sommige van de **Failbackparameters** worden standaard automatisch ingevuld met aanbevolen waarden, maar u kunt deze wijzigen.

   De volgende tabel bevat meer informatie over de **Failbackparameters**.

Parameter	Beschrijving
Grootte van back-up	De hoeveelheid gegevens die tijdens het failbackproces wordt overgedragen naar uw lokale site. Na het starten van het failbackproces naar een virtuele doelmachine neemt de **Grootte van back-up** toe tijdens de fase van gegevensoverdracht, omdat de virtuele machine in de cloud actief blijft en nieuwe gegevens genereert. Als u de geschatte downtimeperiode tijdens het failbackproces naar een virtuele doelmachine wilt berekenen, neemt u 10% van de waarde van de **Grootte van back-up** (omdat wij aanbevelen de switchoverfase te starten nadat 90% van de gegevens is overgedragen naar uw lokale site) en deelt u dit getal door de waarde van uw internetsnelheid. **Opmerking** De waarde van de internetsnelheid neemt af wanneer u meerdere failbackprocessen tegelijk uitvoert.
Doel	Type workload op uw lokale site waarnaar u de cloudserver wilt herstellen: **Virtuele machine** of **Fysieke machine**.
Locatie van doelmachine	Failbacklocatie: een VMware ESXi-host of een Microsoft Hyper-V-host. U kunt kiezen uit alle hosts die een agent hebben die is geregistreerd bij de Cyber Protection-service.
Agent	Agent waarmee de failbackbewerking wordt uitgevoerd. U kunt één agent gebruiken om één failbackbewerking tegelijk uit te voeren. U kunt een agent selecteren die online is en momenteel niet voor een ander failbackproces wordt gebruikt. Daarnaast moet de versie van de agent de failbackfunctionaliteit ondersteunen en toegangsrechten hebben voor de back-up. Let op: U kunt meerdere agenten op VMware ESXi-hosts installeren en met elke agent een afzonderlijk failbackproces starten. Deze failbackprocessen kunnen tegelijkertijd worden

Parameter	Beschrijving
	uitgevoerd.
Instellingen van doelmachine	Instellingen van virtuele machine: • **Virtuele processors**. Selecteer het aantal virtuele processors. • **Geheugen**. Selecteer hoeveel geheugen de virtuele machine zal hebben. • **Eenheden**. Selecteer de eenheden voor het geheugen. • [Optioneel] **Netwerkadapters**. Als u een netwerkadapter wilt toevoegen, klikt u op **Toevoegen** en selecteert u een netwerk in het veld **Netwerk**. Wanneer u klaar bent met de wijzigingen, klikt u op **Gereed**.
Pad	(Voor Microsoft Hyper-V hosts) Map op de host waarin uw machine wordt opgeslagen. Controleer of er voldoende vrije geheugenruimte is op de host voor de machine.
Gegevensopslag	(Voor VMware ESXi-hosts) Gegevensopslag op de host waarin uw machine wordt opgeslagen. Controleer of er voldoende vrije geheugenruimte is op de host voor de machine.
Inrichtingsmethode	Wijze van toewijzing van de virtuele schijf. Voor Microsoft Hyper-V-hosts: • **Dynamisch uitbreidbaar** (standaardwaarde). • **Vaste grootte**. Voor Microsoft Hyper-V-hosts: • **Thin** (standaardwaarde). • **Dik**.
Naam van doelmachine	Naam van de doelmachine. Standaard heeft de doelmachine dezelfde naam als de naam van de herstelserver. De naam van de doelmachine moet uniek zijn op de geselecteerde **Locatie van doelmachine**.

5. Klik op **Gegevensoverdracht starten** en klik vervolgens in het bevestigingsvenster op **Starten**.

Opmerking
Als er geen back-up van de virtuele machine in de cloud is, wordt er automatisch een back-up uitgevoerd voordat de gegevensoverdrachtfase begint.

De fase van **gegevensoverdracht** start. In de console wordt de volgende informatie weergegeven:

Veld	Beschrijving
Voortgang	Deze parameter geeft aan hoeveel gegevens al zijn overgedragen naar de lokale site en de totale hoeveelheid gegevens die nog moet worden overgedragen. De totale hoeveelheid gegevens omvat de gegevens van de laatste back-up voordat de fase van gegevensoverdracht werd gestart, plus de back-ups van de nieuw gegenereerde gegevens (incrementele back-ups), aangezien de virtuele machine actief blijft tijdens de fase van gegevensoverdracht. Daarom nemen beide waarden van de parameter **Voortgang** in de loop van de tijd toe.
Schatting van downtime	Deze parameter geeft aan hoelang de virtuele machine in de cloud niet beschikbaar zal zijn als u de switchoverfase op dat moment start. De waarde wordt berekend op basis van de waarden van de parameter **Voortgang** en deze neemt in de loop van de tijd af.

6. Klik op **Switchover** en vervolgens in het bevestigingsvenster nogmaals op **Switchover**.
   De switchoverfase start. In de console wordt de volgende informatie weergegeven:

Veld	Beschrijving
Voortgang	De parameter toont de voortgang van het herstel van de machine op de lokale site.
Geschatte tijd om te voltooien	Deze parameter geeft bij benadering het tijdstip aan waarop de switchoverfase zal zijn voltooid en u de machine op de lokale site kunt starten.

Opmerking
Als er geen back-upschema is toegepast op de virtuele machine in de cloud, wordt tijdens de switchoverfase automatisch een back-up gemaakt, waardoor de downtime langer duurt.

7. Nadat de **Switchover**fase is voltooid en de virtuele machine op uw lokale site automatisch is gestart, bevestig dan of deze werkt zoals verwacht.
8. Klik op **Failback bevestigen** en vervolgens in het bevestigingsvenster op **Bevestigen** om het proces te voltooien.
   De virtuele machine in de cloud wordt verwijderd en de herstelserver keert terug naar de status **Stand-by**.

Opmerking
Het toepassen van een beschermingsschema op de herstelde server maakt geen deel uit van het failbackproces. Wanneer het failbackproces is voltooid, past u een beschermingsschema toe op de herstelde server, zodat deze weer is beschermd. U kunt hetzelfde beschermingsschema toepassen dat was toegepast op de oorspronkelijke server, of een nieuw beschermingsschema waarvoor de module **Noodherstel** is ingeschakeld.

Failback naar een fysieke doelmachine

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Het automatische failbackproces naar een fysieke doelmachine omvat de volgende fasen:

1. **Planning**. Tijdens deze fase herstelt u de IT-infrastructuur op uw lokale site (zoals de hosts en de netwerkconfiguraties), configureert u de failbackparameters en plant u wanneer u de gegevensoverdracht wilt starten.
2. **Gegevensoverdracht**. Tijdens deze fase worden de gegevens van de cloudsite overgedragen naar de lokale site terwijl de virtuele machine in de cloud actief blijft. Switchover is de volgende fase en u kunt deze op elk moment starten tijdens de fase van gegevensoverdracht, maar u moet hierbij rekening houden met het volgende.

   Hoe langer de fase van gegevensoverdracht duurt,
   - hoe langer de virtuele machine in de cloud actief blijft.
   - hoe meer gegevens worden overgedragen naar uw lokale site.
   - hoe hoger de kosten die u moet betalen (u geeft meer compute-punten uit).
   - hoe korter de periode van downtime tijdens de switchoverfase.

   Als u de downtime tot een minimum wilt beperken, start u de switchoverfase nadat meer dan 90% van de gegevens is overgedragen naar de lokale site.

   Als een langere downtime geen probleem is en u niet meer compute-punten wilt uitgeven om de virtuele machine in de cloud actief te houden, dan kunt u de switchoverfase eerder starten.

   Opmerking
   Bij de gegevensoverdracht wordt gebruikgemaakt van flashback-technologie. Met deze technologie worden de gegevens die beschikbaar zijn op de doelmachine, vergeleken met de gegevens van de virtuele machine in de cloud. Als een deel van de gegevens al beschikbaar is op de doelmachine, worden deze niet opnieuw overgedragen. Dankzij deze technologie wordt de fase van gegevensoverdracht versneld.

   Daarom raden wij u aan de server te herstellen naar de oorspronkelijke machine op uw lokale site.
3. **Switchover**. Tijdens deze fase wordt de virtuele machine in de cloud uitgeschakeld en worden de resterende gegevens, waaronder de laatste incrementele back-up, overgedragen naar de lokale site. Als er geen back-upschema is toegepast op de herstelserver, wordt tijdens de switchoverfase automatisch een back-up gemaakt, waardoor het proces wordt vertraagd.
4. **Validatie**. Tijdens deze fase is de fysieke machine op de lokale site gereed en kunt u deze opnieuw opstarten met Linux-opstartmedia. U kunt controleren of de virtuele machine goed werkt, en:

- Als alles werkt zoals verwacht, bevestigt u de failback. Na bevestiging van de failback wordt de virtuele machine in de cloud verwijderd en keert de herstelserver terug naar de status **Stand-by**. Dit is het einde van het failbackproces.
- Als er iets misgaat, kunt u de failover annuleren en terugkeren naar de planningfase.

Opmerking
Nadat het opstartmedium opnieuw is opgestart, kunt u het niet meer gebruiken. Als u tijdens de validatiefase ontdekt dat er iets verkeerd is, moet u een nieuw opstartmedium registreren en het failbackproces opnieuw starten.

Maar omdat flashback-technologie wordt gebruikt, worden de gegevens die al op de lokale site beschikbaar zijn, niet opnieuw overgedragen, zodat het failbackproces veel sneller verloopt.

Failback uitvoeren naar een fysieke machine

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

U kunt een failback naar een fysieke doelmachine op uw lokale site automatisch laten uitvoeren.

Opmerking
Bij de gegevensoverdracht wordt gebruikgemaakt van flashback-technologie. Met deze technologie worden de gegevens die beschikbaar zijn op de doelmachine, vergeleken met de gegevens van de virtuele machine in de cloud. Als een deel van de gegevens al beschikbaar is op de doelmachine, worden deze niet opnieuw overgedragen. Dankzij deze technologie wordt de fase van gegevensoverdracht versneld.

Daarom raden wij u aan de server te herstellen naar de oorspronkelijke machine op uw lokale site.

Vereisten

- De agent die u gaat gebruiken om de failback uit te voeren, is online en wordt momenteel niet gebruikt voor een andere failbackbewerking.
- Uw internetverbinding is stabiel.
- Er is een geregistreerd opstartmedium beschikbaar. Zie 'Opstartmedia maken om besturingssystemen te herstellen' in de Gebruikershandleiding van Cyber Protection voor meer informatie.
- De fysieke doelmachine is de oorspronkelijke machine op uw lokale site, of heeft dezelfde firmware als de oorspronkelijke machine.
- Er is ten minste één volledige back-up van de virtuele machine in de cloud.

Een failback uitvoeren naar een fysieke machine

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Servers**.
2. Selecteer de herstelserver die de status **Failover** heeft.
3. Klik op het tabblad **Failback**.
4. Ga naar het veld **Doel** en selecteer **Fysieke machine**.
5. Klik in het veld **Doel-opstartmedia**, klik op **Opgeven**, selecteer de opstartmedia en klik vervolgens op **Gereed**.

   Opmerking
   We raden u aan kant-en-klare opstartmedia te gebruiken, aangezien deze al zijn geconfigureerd. Zie 'Opstartmedia maken om besturingssystemen te herstellen' in de Gebruikershandleiding van Cyber Protection voor meer informatie.

6. [Optioneel] Als u de standaardschijftoewijzing wilt wijzigen, klikt u in het veld **Schijftoewijzing** op **Opgeven**, wijst u de schijven van de back-up toe aan de schijven van de doelmachine en klikt u vervolgens op **Gereed**.
7. Klik op **Gegevensoverdracht starten** en klik vervolgens in het bevestigingsvenster op **Starten**.

   Opmerking
   Als er geen back-up van de virtuele machine in de cloud is, wordt er automatisch een back-up uitgevoerd voordat de gegevensoverdrachtfase begint.

   De fase van gegevensoverdracht start. In de console wordt de volgende informatie weergegeven:

Veld	Beschrijving
Voortgang	Deze parameter geeft aan hoeveel gegevens al zijn overgedragen naar de lokale site en de totale hoeveelheid gegevens die nog moet worden overgedragen. De totale hoeveelheid gegevens omvat de gegevens van de laatste back-up voordat de fase van gegevensoverdracht werd gestart, plus de back-ups van de nieuw gegenereerde gegevens (incrementele back-ups), aangezien de virtuele machine actief blijft tijdens de fase van gegevensoverdracht. Daarom nemen de waarden van **Voortgang** in de loop van de tijd toe. Tijdens de gegevensoverdracht wordt gebruikgemaakt van flashback-technologie, dus de gegevens die al beschikbaar zijn op de doelmachine, worden niet overgedragen. De voortgang kan daarom sneller zijn dan wat aanvankelijk door de console is berekend.
Schatting van downtime	Deze parameter geeft aan hoelang de virtuele machine in de cloud niet beschikbaar zal zijn als u de switchoverfase op dat moment start. De waarde wordt berekend op basis van de waarden van de parameter **Voortgang** en deze neemt in de loop van de tijd af. Tijdens de gegevensoverdracht wordt gebruikgemaakt van flashback-technologie, dus de gegevens die al beschikbaar zijn op de doelmachine, worden niet overgedragen. De downtime kan daarom veel korter zijn dan

Veld	Beschrijving
	de aanvankelijk weergegeven waarde in de console.

8. Klik op **Switchover** en vervolgens in het bevestigingsvenster nogmaals op **Switchover**.
   De switchoverfase start. In de console wordt de volgende informatie weergegeven:

Veld	Beschrijving
Voortgang	De parameter toont de voortgang van het herstel van de machine op de lokale site.
Geschatte tijd om te voltooien	Deze parameter geeft bij benadering het tijdstip aan waarop de switchoverfase zal zijn voltooid en u de machine op de lokale site kunt starten.

Opmerking
Als er geen back-upschema is toegepast op de virtuele machine in de cloud, wordt tijdens de switchoverfase automatisch een back-up gemaakt, waardoor de downtime langer duurt.

9. Nadat de fase van **Switchover** is voltooid, start u opstartmedia opnieuw op en verifieert u of de fysieke machine op uw lokale site werkt zoals verwacht.
   Zie 'Schijven herstellen met opstartmedia' in de Gebruikershandleiding van Cyber Protection voor meer informatie.
10. Klik op **Failback bevestigen** en vervolgens in het bevestigingsvenster op **Bevestigen** om het proces te voltooien.
    De virtuele machine in de cloud wordt verwijderd en de herstelserver keert terug naar de status **Stand-by**.

Opmerking
Het toepassen van een beschermingsschema op de herstelde server maakt geen deel uit van het failbackproces. Wanneer het failbackproces is voltooid, past u een beschermingsschema toe op de herstelde server, zodat deze weer is beschermd. U kunt hetzelfde beschermingsschema toepassen dat was toegepast op de oorspronkelijke server, of een nieuw beschermingsschema waarvoor de module **Noodherstel** is ingeschakeld.

Handmatige failback

Opmerking
We raden u aan de handmatige modus van het failbackproces alleen te gebruiken wanneer het ondersteuningsteam dit adviseert.

U kunt een failbackproces ook starten in een handmatige modus. In dit geval wordt de gegevensoverdracht van de back-up in de cloud naar de lokale site niet automatisch uitgevoerd. Deze moet handmatig worden uitgevoerd nadat de virtuele machine in de cloud is uitgeschakeld.

Dit maakt het failbackproces in een handmatige modus veel langzamer en u kunt een langere downtime verwachten.

Het failbackproces in een handmatige modus omvat de volgende fasen:

1. **Planning**. Tijdens deze fase herstelt u de IT-infrastructuur op uw lokale site (zoals de hosts en de netwerkconfiguraties), configureert u de failbackparameters en plant u wanneer u de gegevensoverdracht wilt starten.
2. **Switchover**. Tijdens deze fase wordt de virtuele machine in de cloud uitgeschakeld en wordt er een back-up gemaakt van de meest recentelijk gegenereerde gegevens. Als er geen back-upschema is toegepast op de herstelserver, wordt tijdens de switchoverfase automatisch een back-up gemaakt, waardoor het proces wordt vertraagd. Wanneer de back-up is voltooid, herstelt u de machine handmatig naar de lokale site. U kunt de schijf herstellen via opstartmedia of de hele machine herstellen vanaf de back-upopslag in de cloud.
3. **Validatie**. Tijdens deze fase verifieert u of de fysieke of virtuele machine op de lokale site goed werkt en bevestigt u de failback. Na de bevestiging wordt de virtuele machine op de cloudsite verwijderd en keert de herstelserver terug naar de status **Stand-by**.

Handmatige failback uitvoeren

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

U kunt een handmatige failback uitvoeren naar een fysieke of virtuele doelmachine op uw lokale site.

Een handmatige failback uitvoeren:

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Servers**.
2. Selecteer de herstelserver die de status **Failover** heeft.
3. Klik op het tabblad **Failback**.
4. Ga naar het veld **Doel** en selecteer **Fysieke machine**.
5. Klik op het tandwielpictogram en schakel vervolgens **Handmatige modus gebruiken** in.
6. [Optioneel] Bereken de geschatte downtimeperiode tijdens het failbackproces door de waarde van de **back-upgrootte** te delen door de waarde van uw internetsnelheid.

   Opmerking
   De waarde van de internetsnelheid neemt af wanneer u meerdere failbackprocessen tegelijk uitvoert.

7. Klik op **Switchover** en vervolgens in het bevestigingsvenster nogmaals op **Switchover**.
   De virtuele machine op de cloudsite wordt uitgeschakeld.

Opmerking
Als er geen back-upschema is toegepast op de virtuele machine in de cloud, wordt tijdens de switchoverfase automatisch een back-up gemaakt, waardoor de downtime langer duurt.

8. Herstel de server vanaf de cloudback-up naar de fysieke of virtuele machine op uw lokale site. Zie 'Een machine herstellen' in de gebruikershandleiding van Cyber Protection voor meer informatie.
9. Controleer of het herstelproces volledig is uitgevoerd en of de herstelde machine goed werkt. Klik vervolgens op **Machine is hersteld**.
10. Als alles werkt zoals verwacht, klik dan op **Failback bevestigen** en klik in het bevestigingsvenster nogmaals op **Bevestigen**.
    De herstelserver en herstelpunten zijn dan gereed voor de volgende failover. Als u nieuwe herstelpunten wilt maken, past u een beschermingsschema toe op de nieuwe lokale server.

Opmerking
Het toepassen van een beschermingsschema op de herstelde server maakt geen deel uit van het failbackproces. Wanneer het failbackproces is voltooid, past u een beschermingsschema toe op de herstelde server, zodat deze weer is beschermd. U kunt hetzelfde beschermingsschema toepassen dat was toegepast op de oorspronkelijke server, of een nieuw beschermingsschema waarvoor de module **Noodherstel** is ingeschakeld.

Werken met versleutelde back-ups

U kunt herstelservers maken vanaf de versleutelde back-ups. Voor uw gemak kunt u een automatische wachtwoordtoepassing instellen voor een versleutelde back-up tijdens de failover naar een herstelserver.

Bij het maken van een herstelserver kunt u het wachtwoord voor automatische noodherstelbewerkingen opgeven. Dit wordt opgeslagen in de referentieopslag, een beveiligde opslag van referenties die u kunt vinden in het gedeelte **Instellingen** > **Referenties**.

Een referentie kan worden gekoppeld aan meerdere back-ups.

De opgeslagen wachtwoorden in de referentieopslag beheren

1. Ga naar **Instellingen** > **referenties**.
2. Als u een specifieke referentie wilt beheren, klikt u op het pictogram in de laatste kolom. U kunt dan de items zien die aan dit certificaat zijn gekoppeld.
   - U kunt de back-up ontkoppelen van de geselecteerde referentie door te klikken op het pictogram van de prullenbak bij de back-up. Bij de failover naar de herstelserver moet u het wachtwoord dan handmatig opgeven.
   - Als u de referentie wilt bewerken, klikt u op **Bewerken** en geeft u de naam of het wachtwoord op.

- Als u de referentie wilt verwijderen, klikt u op **Verwijderen**. Let op: bij de failover naar de herstelserver moet u het wachtwoord dan handmatig opgeven.

Bewerkingen met virtuele Microsoft Azure-machines

Opmerking
Voor sommige functies zijn mogelijk extra licenties vereist, afhankelijk van het toegepaste licentiemodel.

U kunt failover van virtuele Microsoft Azure-machines naar Acronis Cyber Protect Cloud uitvoeren. Zie "Failover uitvoeren" (p. 832) voor meer informatie.

Daarna kunt u een failback uitvoeren vanuit Acronis Cyber Protect Cloud terug naar de virtuele Azure-machines. Het failbackproces is identiek aan het failbackproces naar een fysieke machine. Zie "Vereisten" (p. 842) voor meer informatie.

Opmerking
Als u een nieuwe virtuele Azure-machine wilt registreren voor failback, kunt u de Acronis Backup VM-extensie gebruiken die beschikbaar is in Azure.

U kunt Multisite IPsec VPN-connectiviteit configureren tussen Acronis Cyber Protect Cloud en de Azure VPN-gateway. Zie "Multi-site IPsec VPN configureren" (p. 798) voor meer informatie.

Primaire servers instellen

In dit gedeelte wordt beschreven hoe u uw primaire servers kunt maken en beheren.

Primaire server maken

Vereisten

- Een van de typen connectiviteit met de cloudsite moet worden ingesteld.

Een primaire server maken

1. Ga naar **Noodherstel** > **Servers** > tabblad **Primaire servers**.
2. Klik op **Maken**.
3. Selecteer een sjabloon voor de nieuwe virtuele machine.
4. Selecteer de variant van de configuratie (aantal virtuele kernen en de grootte van het RAM). De volgende tabel toont de maximale totale hoeveelheid schijfruimte (GB) voor elke variant.

Type	vCPU	RAM (GB)	Maximale totale hoeveelheid schijfruimte (GB)
F1	1	2	500

Type	vCPU	RAM (GB)	Maximale totale hoeveelheid schijfruimte (GB)
F2	1	4	1000
F3	2	8	2000
F4	4	16	4000
F5	8	32	8000
F6	16	64	16000
F7	16	128	32000
F8	16	256	64000

Opmerking
U kunt de compute-punten voor elke optie zien. Het aantal compute-punten geeft de kosten per uur weer voor het uitvoeren van de primaire server. Zie "Compute-punten" (p. 779) voor meer informatie.

5. [Optioneel] Wijzig de grootte van de virtuele schijf. Als u meer dan één harde schijf nodig hebt, klikt u op **Schijf toevoegen** en geeft u vervolgens de nieuwe schijfgrootte op. Momenteel kunt u niet meer dan 10 schijven toevoegen voor een primaire server.
6. Geef het cloudnetwerk op waarin de primaire server wordt opgenomen.
7. Selecteer de optie **DHCP**.

De optie DHCP	Beschrijving
Geleverd door cloudsite	Standaardinstelling. Het IP-adres van de server wordt geleverd door een automatisch geconfigureerde DHCP-server in de cloud.
Aangepast	Het IP-adres van de server wordt geleverd door uw eigen DHCP-server in de cloud.

8. [Optioneel] Geef het **MAC-adres** op.
   Het MAC-adres is een unieke identificatie die wordt toegewezen aan de netwerkadapter van de server. Als u aangepast DHCP gebruikt, kunt u configureren dat er altijd een specifiek IP-adres wordt toegewezen aan een specifiek MAC-adres, zodat de primaire server altijd hetzelfde IP-adres krijgt. U kunt toepassingen uitvoeren met licenties die zijn geregistreerd met het MAC-adres.
9. Geef het IP-adres op voor de server in het productienetwerk. Standaard wordt het eerste gratis IP-adres van uw productienetwerk ingesteld.

Opmerking
Als u een DHCP-server gebruikt, moet u dit IP-adres toevoegen aan de uitsluitingslijst voor de server om IP-adresconflicten te vermijden.

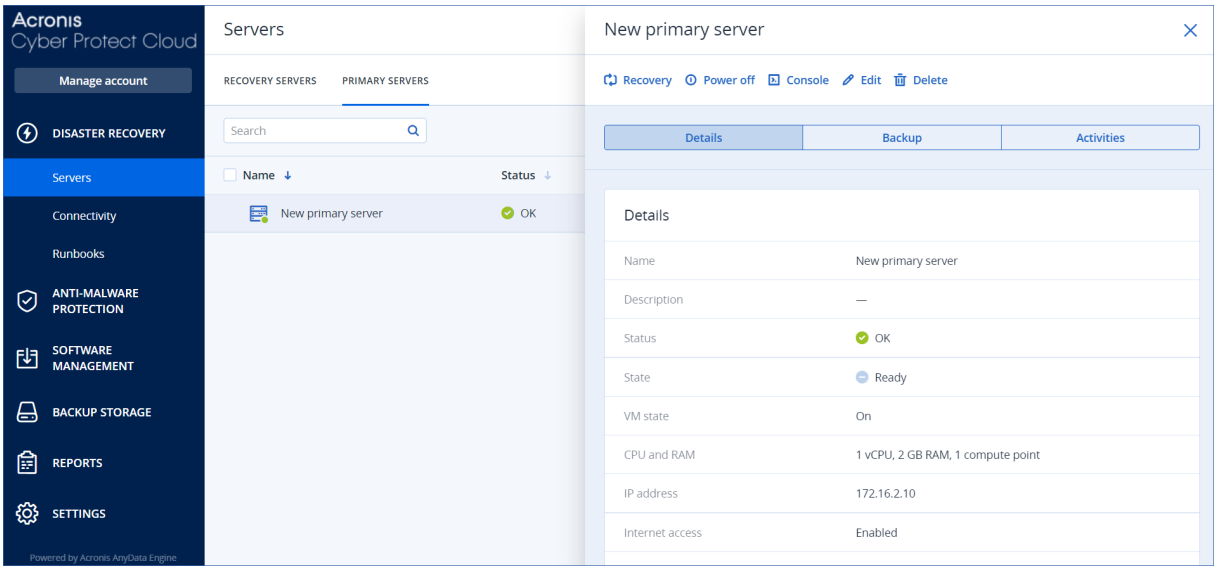
Als u een aangepaste DHCP-server gebruikt, moet u in **IP-adres in productienetwerk** hetzelfde IP-adres opgeven als het IP-adres dat is geconfigureerd op de DHCP-server. Anders werkt de testfailover niet correct en is de server niet bereikbaar via een openbaar IP-adres.

10. [Optioneel] Schakel het selectievakje **Internettoegang** in.
    Hierdoor krijgt de primaire server toegang tot internet. Standaard staat TCP-poort 25 open voor uitgaande verbindingen naar openbare IP-adressen.
11. [Optioneel] Schakel het selectievakje **Openbaar IP-adres gebruiken** in.
    Als u een openbaar IP-adres hebt, is de primaire server beschikbaar via internet. Als u het selectievakje uitgeschakeld laat, is de server alleen beschikbaar in uw productienetwerk.
    Het openbare IP-adres wordt weergegeven wanneer u de configuratie hebt voltooid. Standaard staat TCP-poort 443 open voor inkomende verbindingen naar openbare IP-adressen.

    Opmerking
    Als u het selectievakje **Openbaar IP-adres gebruiken** uitschakelt of de herstelserver verwijdert, wordt het openbare IP-adres niet gereserveerd.

12. [Optioneel] Selecteer **RPO-drempel instellen**.
    De RPO-drempel bepaalt het maximaal toegestane tijdsinterval tussen het laatste herstelpunt en de huidige tijd. De waarde kan worden ingesteld op 15 - 60 minuten, 1 - 24 uur, 1 - 14 dagen.
13. Definieer de naam van de primaire server.
14. [Optioneel] Typ een beschrijving voor de primaire server.
15. [Optioneel] Klik op het tabblad **Cloudfirewallregels** om de standaardfirewallregels te bewerken. Zie "Firewallregels instellen voor cloudservers" (p. 852) voor meer informatie.
16. Klik op **Maken**.

De primaire server wordt beschikbaar in het productienetwerk. U kunt de server beheren met behulp van de console, RDP, SSH of TeamViewer.



Bewerkingen met een primaire server

De primaire server wordt weergegeven in **Noodherstel** > **Servers** > tabblad **Primaire servers** van de Cyber Protect-console.

Als u de server wilt starten of te stoppen, klikt u op **Starten** of **Stoppen** in het deelvenster voor de primaire server.

Als u de instellingen van de primaire server wilt bewerken, stopt u de server en klikt u vervolgens op **Bewerken**.

Als u een beschermingsschema wilt toepassen op de primaire server, selecteert u de server, gaat u naar het tabblad **Schema** en klikt u op **Maken**. U ziet een vooraf gedefinieerd beschermingsschema waarin u alleen het schema en de bewaarregels kunt wijzigen. Zie 'Back-up maken van de cloudservers' voor meer informatie.

De cloudservers beheren

U kunt de cloudservers beheren via **Noodherstel** > **Servers**. Er zijn daar twee tabbladen: **Herstelservers** en **Primaire servers**. Klik op het tandwielpictogram om alle optionele kolommen in de tabel weer te geven.

Als u een cloudserver selecteert, ziet u de volgende informatie.

Kolomnaam	Beschrijving
Naam	Een door u gedefinieerde naam voor de cloudserver
Status	De status die het ernstigste probleem met een cloudserver weergeeft (gebaseerd op de actieve waarschuwingen)
Status	Status van een cloudserver

VM-status	De energiestatus van een virtuele machine die is gekoppeld aan een cloudserver
Actieve locatie	De locatie waar een cloudserver wordt gehost. Bijvoorbeeld **Cloud**.
RPO drempel	Het maximaal toegestane tijdsinterval tussen het laatste herstelpunt dat geschikt is voor failover, en de huidige tijd. De waarde kan worden ingesteld op 15 - 60 minuten, 1 - 24 uur, 1 - 14 dagen.
RPO compliance	De RPO-compliance is de ratio tussen de feitelijke RPO en RPO-drempel. De RPO-compliance wordt weergegeven als de RPO-drempel is gedefinieerd. Deze wordt als volgt berekend: **RPO-compliance = Werkelijke RPO / RPO-drempel** waarbij **Huidige RPO = huidige tijd - laatste tijd van herstelpunt** Statussen van **RPO-compliance** Afhankelijk van de waarde van de ratio tussen de huidige RPO en RPO-drempel worden de volgende statussen gebruikt: • **Voldoet**. RPO-compliance < 1x. Server voldoet aan de RPO-drempel. • **Overschreden**. RPO-compliance <= 2x. Server overschrijdt de RPO-drempel. • **Sterk overschreden**. RPO-compliance <= 4x. Server overschrijdt de RPO-drempel meer dan 2x keer. • **Kritisch overschreden**. RPO-compliance > 4x. Server overschrijdt de RPO-drempel meer dan 4x keer. • **In behandeling (geen back-ups)**. De server is beschermd met het beschermingsschema, maar de back-up wordt momenteel gemaakt en is nog niet voltooid.
Huidige RPO	De tijd die is verstreken sinds de laatste keer dat een herstelpunt is gemaakt
Laatste herstelpunt	De datum en tijd waarop het laatste herstelpunt is gemaakt

Firewallregels voor cloudservers

U kunt firewallregels configureren voor het beheer van het inkomende en uitgaande verkeer van de primaire server en de herstelservers op uw cloudsite.

U kunt regels configureren voor inkomend verkeer wanneer u een openbaar IP-adres voor de cloudserver hebt ingesteld. Standaard wordt TCP poort 443 toegestaan en alle andere inkomende verbindingen worden geweigerd. U kunt de standaardfirewallregels wijzigen en uitzonderingen voor inkomend verkeer toevoegen of verwijderen. Als geen openbaar IP is ingesteld, kunt u alleen de regels voor inkomend verkeer bekijken, maar u kunt deze niet configureren.

U kunt regels configureren voor uitgaand verkeer wanneer u internettoegang voor de cloudserver hebt ingesteld. Standaard wordt TCP poort 25 geweigerd en worden alle andere uitgaande verbindingen toegestaan. U kunt de standaardfirewallregels wijzigen en uitzonderingen voor uitgaand verkeer toevoegen of verwijderen. Als geen internettoegang is ingesteld, kunt u alleen de regels voor uitgaand verkeer bekijken, maar u kunt deze niet configureren.

Opmerking
Om veiligheidsredenen zijn er vooraf gedefinieerde firewallregels die u niet kunt wijzigen.

Voor inkomende en uitgaande verbindingen:

- Ping toestaan: ICMP echo-request (type 8, code 0) en ICMP echo-reply (type 0, code 0)
- ICMP need-to-frag (type 3, code 4) toestaan
- TTL exceeded (type 11, code 0) toestaan

Alleen voor inkomende verbindingen:

- Niet-configureerbaar gedeelte: Alles weigeren

Alleen voor uitgaande verbindingen:

- Niet-configureerbaar gedeelte: Alles weigeren

Firewallregels instellen voor cloudservers

U kunt de standaardfirewallregels voor de primaire server en herstelserver in de cloud bewerken.

De firewallregels van een server op uw cloudsite bewerken

1. Ga in de Cyber Protect-console naar **Noodherstel** > **Servers**.
2. Als u de firewallregels van een herstelserver wilt bewerken, klikt u op het tabblad **Herstelservers**. En als u de firewallregels van een primaire server wilt bewerken, klikt u op het tabblad **Primaire servers**.
3. Klik op de server en klik vervolgens op **Bewerken**.
4. Klik op het tabblad **Cloudfirewallregels**.
5. Als u de standaardactie voor de inkomende verbindingen wilt wijzigen:

a. Ga naar het vervolgkeuzeveld **Inkomend** en selecteer de standaardactie.

Actie	Beschrijving
Alles weigeren	Hiermee wordt elk inkomend verkeer geweigerd. U kunt uitzonderingen toevoegen en verkeer van specifieke IP-adressen, protocollen en poorten toestaan.
Alles toestaan	Hiermee wordt al het inkomende TCP- en UDP-verkeer toegestaan. U kunt uitzonderingen toevoegen en verkeer van specifieke IP-adressen, protocollen en poorten weigeren.

Opmerking
Door de standaardactie te wijzigen wordt de configuratie van bestaande regels voor inkomend verkeer ongeldig gemaakt en verwijderd.

b. [Optioneel] Als u de bestaande uitzonderingen wilt opslaan, selecteert u in het bevestigingsvenster de optie **Ingevulde uitzonderingen opslaan**.

c. Klik op **Bevestigen**.

6. Als u een uitzondering wilt toevoegen:

a. Klik op **Uitzondering toevoegen**.

b. Geef de firewallparameters op.

Firewallparameter	Beschrijving
Protocol	Selecteer het protocol voor de verbinding. De volgende opties worden ondersteund: • **TCP** • **UDP** • **TCP+UDP**
Serverpoort	Selecteer de poorten waarop de regel van toepassing is. U kunt het volgende opgeven: • een specifiek poortnummer (bijvoorbeeld `2298`) • een reeks poortnummers (bijvoorbeeld `6000-6700`) • elk poortnummer. Gebruik `*` als u wilt dat de regel wordt toegepast voor elk poortnummer.
IP-adres van client	Selecteer de IP-adressen waarop de regel van toepassing is. U kunt het volgende opgeven: • een specifiek IP-adres (bijvoorbeeld `192.168.0.0`) • een reeks IP-adressen met de CIDR-indeling (bijvoorbeeld `192.168.0.0/24`) • elk IP-adres. Gebruik `*` als u wilt dat de regel wordt toegepast voor elk IP-adres.

7. Als u een bestaande uitzondering voor inkomend verkeer wilt verwijderen, klikt u op het pictogram van de prullenbak ernaast.
8. Als u de standaardactie voor de uitgaande verbindingen wilt wijzigen:
   a. Ga naar het vervolgkeuzeveld **Uitgaand** en selecteer de standaardactie.

Actie	Beschrijving
Alles weigeren	Hiermee wordt elk uitgaand verkeer geweigerd. U kunt uitzonderingen toevoegen en verkeer naar specifieke IP-adressen, protocollen en poorten toestaan.
Alles toestaan	Hiermee wordt al het uitgaande verkeer toegestaan. U kunt uitzonderingen toevoegen en verkeer van specifieke IP-adressen, protocollen en poorten weigeren.

Opmerking
Door de standaardactie te wijzigen wordt de configuratie van bestaande regels voor uitgaand verkeer ongeldig gemaakt en verwijderd.

   b. [Optioneel] Als u de bestaande uitzonderingen wilt opslaan, selecteert u in het bevestigingsvenster de optie **Ingevulde uitzonderingen opslaan**.
   c. Klik op **Bevestigen**.
9. Als u een uitzondering wilt toevoegen:
   a. Klik op **Uitzondering toevoegen**.
   b. Geef de firewallparameters op.

Firewallparameter	Beschrijving
Protocol	Selecteer het protocol voor de verbinding. De volgende opties worden ondersteund: • **TCP** • **UDP** • **TCP+UDP**
Serverpoort	Selecteer de poorten waarop de regel van toepassing is. U kunt het volgende opgeven: • een specifiek poortnummer (bijvoorbeeld `2298`) • een reeks poortnummers (bijvoorbeeld `6000-6700`) • elk poortnummer. Gebruik `*` als u wilt dat de regel wordt toegepast voor elk poortnummer.
IP-adres van client	Selecteer de IP-adressen waarop de regel van toepassing is. U kunt het volgende opgeven: • een specifiek IP-adres (bijvoorbeeld `192.168.0.0`) • een reeks IP-adressen met de CIDR-indeling (bijvoorbeeld `192.168.0.0/24`)

Firewallparameter	Beschrijving
	• elk IP-adres. Gebruik * als u wilt dat de regel wordt toegepast voor elk IP-adres.

10. Als u een bestaande uitzondering voor uitgaand verkeer wilt verwijderen, klikt u op het pictogram van de prullenbak ernaast.
11. Klik op **Opslaan**.

De activiteiten van de cloudfirewall controleren

Wanneer de configuratie van de firewallregels van een cloudserver is bijgewerkt, is er een logboek van de updateactiviteit beschikbaar in de Cyber Protect-console. U kunt het logboek bekijken en de volgende gegevens controleren:

- gebruikersnaam van de gebruiker die de configuratie heeft bijgewerkt
- datum en tijd van de update
- firewallinstellingen voor inkomende en uitgaande verbindingen
- de standaardacties voor inkomende en uitgaande verbindingen
- de protocollen, poorten en IP-adressen van de uitzonderingen voor inkomende en uitgaande verbindingen

De details van een gewijzigde configuratie van de cloudfirewallregels bekijken

1. Klik in de Cyber Protect-console op **Controle** > **Activiteiten**.
2. Klik op de betreffende activiteit en klik op **Alle eigenschappen**.
   De beschrijving van de activiteit moet zijn: **Configuratie van cloudserver bijwerken**.
3. Inspecteer in het **context**veld de informatie waarin u bent geïnteresseerd.

Back-up maken van de cloudservers

Op de cloudsite wordt een back-up zonder agent gemaakt van primaire en herstelservers. Voor deze back-ups gelden de volgende beperkingen.

- De enig mogelijke back-uplocatie is de cloudopslag. Back-ups van primaire servers worden opgeslagen in de opslag voor **Back-ups van primaire servers**.

  Opmerking
  Back-uplocaties van Microsoft Azure worden niet ondersteund.

- Een back-upschema kan niet worden toegepast op meerdere servers. Elke server moet een eigen back-upschema hebben, zelfs als alle back-upschema's dezelfde instellingen hebben.

- Er kan slechts één back-upschema worden toegepast op een server.
- Applicatiegerichte back-up wordt niet ondersteund.
- Versleuteling is niet beschikbaar.
- Back-upopties zijn niet beschikbaar.

Wanneer u een primaire server verwijdert, worden ook de bijbehorende back-ups verwijderd.

Van een herstelserver wordt alleen een back-up gemaakt als deze de failoverstatus heeft. Deze back-ups zetten de back-upreeks van de oorspronkelijke server voort. Wanneer een failback wordt uitgevoerd, kan de oorspronkelijke server deze back-upreeks weer voortzetten. De back-ups van de herstelserver kunnen dus alleen handmatig worden verwijderd of doordat de bewaarregels worden toegepast. Wanneer een herstelserver wordt verwijderd, worden de back-ups hiervan altijd bewaard.

Opmerking
De back-upschema's voor cloudservers worden uitgevoerd op een tijdstip in UTC-tijd.

Orchestration (runbooks)

Opmerking
Voor sommige functies zijn mogelijk extra licenties vereist, afhankelijk van het toegepaste licentiemodel.

Een draaiboek is een set instructies die beschrijft hoe u de productieomgeving in de cloud kunt inrichten. U kunt draaiboeken maken in de Cyber Protect-console. Voor toegang tot het scherm **Runbooks** selecteert u **Noodherstel** > **Runbooks**.

Waarom runbooks gebruiken?

Met draaiboeken kunt u het volgende doen:

- Een failover van een of meerdere servers automatiseren
- Het failoverresultaat automatisch laten controleren door het IP-adres van de server te pingen en de verbinding met de door u opgegeven poort te controleren
- De volgorde van bewerkingen instellen voor servers met gedistribueerde toepassingen
- Handmatige bewerkingen toevoegen aan de workflow
- Verifieer de integriteit van uw noodhersteloplossing door runbooks uit te voeren in de testmodus.

Runbook maken

Een draaiboek bestaat uit stappen die achtereenvolgens worden uitgevoerd. Een stap bestaat uit acties die tegelijkertijd starten.

U kunt de onderstaande instructie volgen of de videoles bekijken.

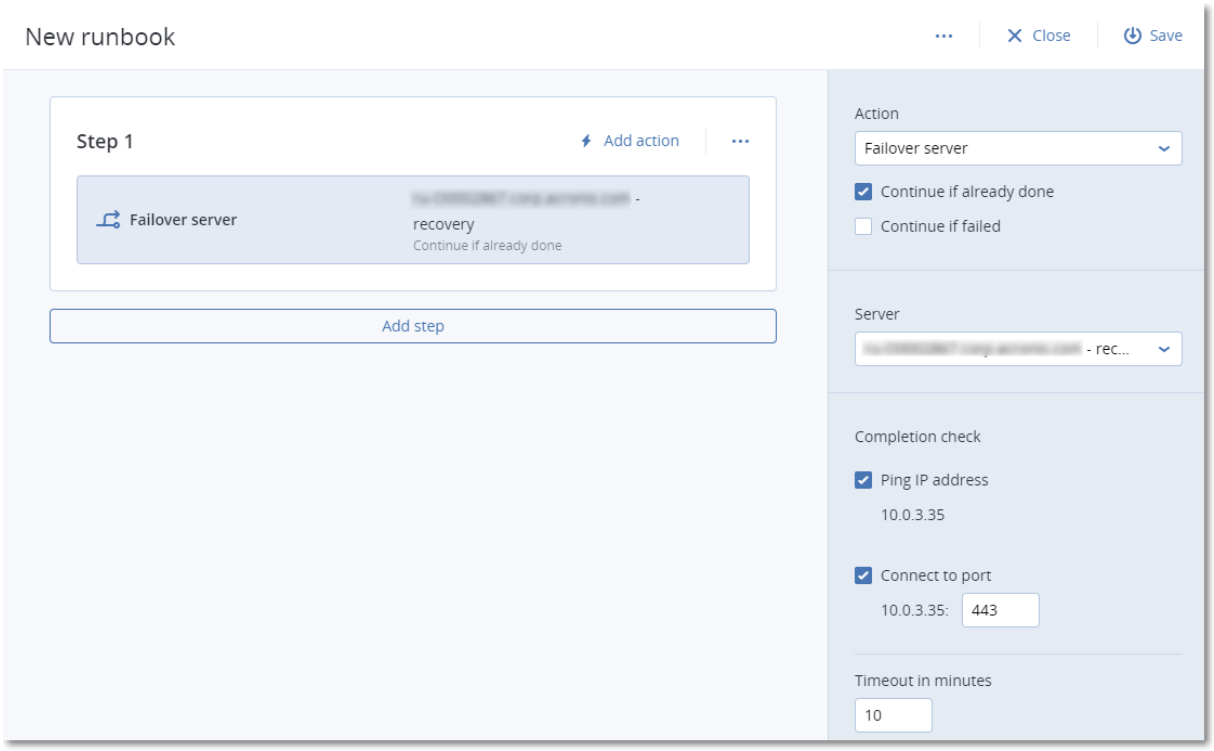
Een draaiboek maken:

1. Ga in de Cyber Protection-console naar **Noodherstel** > **Runbooks**.
2. Klik op **Draaiboek maken**.
3. Klik op **Stap toevoegen**.
4. Klik op **Actie toevoegen** en selecteer vervolgens de actie die u aan de stap wilt toevoegen.

Actie	Beschrijving
Failover van server uitvoeren	Voert een failover uit van een cloudserver. Als u deze actie wilt definiëren, moet u een cloudserver selecteren en de draaiboekparameters configureren die beschikbaar zijn voor deze actie. Voor meer informatie over deze parameters: zie "Draaiboekparameters" (p. 859). **Opmerking** Als de back-up van de server die u selecteert, is versleuteld als machine-eigenschap, wordt de actie **Failover van server uitvoeren** gepauzeerd en automatisch gewijzigd in **Interactie vereist**. Als u wilt doorgaan met de uitvoering van het draaiboek, moet u het wachtwoord voor de versleutelde back-up opgeven.
Failback van server uitvoeren	Voert een failback uit van een cloudserver. Als u deze actie wilt definiëren, moet u een cloudserver selecteren en de draaiboekparameters configureren die beschikbaar zijn voor deze actie. Voor meer informatie over deze instellingen: zie "Draaiboekparameters" (p. 859). **Opmerking** Runbookbewerkingen ondersteunen alleen de failback in handmatige modus. Dus als u het failbackproces start door een runbook uit te voeren dat een stap op de **Failback van server uitvoeren** bevat, dan is een handmatige interactie vereist: u moet de machine handmatig herstellen, en het failbackproces bevestigen of annuleren vanaf het tabblad **Noodherstel** > **Servers**.
Server starten	Start een cloudserver. Als u deze actie wilt definiëren, moet u een cloudserver selecteren en de draaiboekparameters configureren die beschikbaar zijn voor deze actie. Voor meer informatie over deze instellingen: zie "Draaiboekparameters" (p. 859). **Opmerking** De actie **Server starten** is niet van toepassing op testfailoverbewerkingen in draaiboeken. Als u probeert een dergelijke actie uit te voeren, mislukt deze met de volgende foutmelding: Mislukt: de actie is niet van toepassing op de huidige serverstatus.
Server stoppen	Stopt een cloudserver. Als u deze actie wilt definiëren, moet u een cloudserver selecteren en de draaiboekparameters configureren die beschikbaar zijn voor deze actie. Voor meer informatie over deze instellingen: zie "Draaiboekparameters" (p. 859).

Actie	Beschrijving
	Opmerking De actie **Server stoppen** is niet van toepassing op testfailoverbewerkingen in draaiboeken. Als u probeert een dergelijke actie uit te voeren, mislukt deze met de volgende foutmelding: Mislukt: de actie is niet van toepassing op de huidige serverstatus.
Handmatige bewerking	Een handmatige bewerking vereist interactie van een gebruiker. Als u deze actie wilt definiëren, moet u een beschrijving invoeren. Wanneer een draaiboeksequentie een handmatige bewerking bereikt, wordt het draaiboek gepauzeerd en pas weer voortgezet wanneer een gebruiker de vereiste handmatige bewerking uitvoert, bijvoorbeeld klikken op de bevestigingsknop.
Draaiboek uitvoeren	Voert een ander draaiboek uit. Als u deze actie wilt definiëren, moet u een draaiboek kiezen. Een runbook kan slechts één uitvoering van een bepaald runbook bevatten. Als u bijvoorbeeld de actie 'Runbook A uitvoeren' hebt toegevoegd, kunt u de actie 'Runbook B uitvoeren' toevoegen, maar kunt u geen andere actie 'Runbook A uitvoeren' toevoegen.

5. Definieer de draaiboekparameters voor de actie. Voor meer informatie over deze parameters: zie "Draaiboekparameters" (p. 859).
6. [Optioneel] Een beschrijving van de stap toevoegen:
   a. Klik op het ellipspictogram en klik vervolgens op **Beschrijving**.
   b. Voer een beschrijving van de stap in.
   c. Klik op **Gereed**.
7. Herhaal stappen 3-6 totdat u de gewenste reeks stappen en acties hebt gemaakt.
8. [Optioneel] De standaardnaam van het draaiboek wijzigen:
   a. Klik op het ellipspictogram.
   b. Voer de naam van het draaiboek in.
   c. Voer een beschrijving van het draaiboek in.
   d. Klik op **Gereed**.
9. Klik op **Opslaan**.
10. Klik op **Sluiten**.



Draaiboekparameters

Draaiboek \parameters zijn specifieke instellingen die u moet configureren om een draaiboekactie te definiëren. Er zijn twee categorieën draaiboekparameters: actieparameters en voltooiingscontroleparameters.

Actieparameters definiëren het gedrag van het draaiboek, afhankelijk van de initiële staat of het resultaat van de actie.

Voltooiingscontroleparameters zorgen ervoor dat de server beschikbaar is en de noodzakelijke services levert. Als een voltooiingscontrole mislukt, wordt de actie beschouwd als mislukt.

De volgende tabel beschrijft de configureerbare draaiboekparameters voor elke actie.

Draaiboekparameter	Categorie	Beschikbaar voor actie	Beschrijving
Doorgaan indien al uitgevoerd	Actieparameter	• **Failover van server uitvoeren** • **Server starten** • **Server stoppen** • **Failback van server uitvoeren**	Deze parameter definieert het gedrag van het draaiboek wanneer de vereiste actie al is uitgevoerd (bijvoorbeeld: een failover is al uitgevoerd of een server wordt al uitgevoerd). Wanneer de parameter is ingeschakeld, geeft het draaiboek een waarschuwing en gaat het verder. Wanneer de parameter is uitgeschakeld, mislukt de actie en

Draaiboekparameter	Categorie	Beschikbaar voor actie	Beschrijving
			mislukt ook het draaiboek. Standaard is deze parameter ingeschakeld.
Doorgaan indien mislukt	Actieparameter	• **Failover van server uitvoeren** • **Server starten** • **Server stoppen** • **Failback van server uitvoeren**	Deze parameter definieert het gedrag van het draaiboek wanneer de vereiste actie mislukt. Wanneer de parameter is ingeschakeld, geeft het draaiboek een waarschuwing en gaat het verder. Wanneer de parameter is uitgeschakeld, mislukt de actie en mislukt ook het draaiboek. Standaard is deze parameter uitgeschakeld.
IP-adres pingen	Voltooiingscontrole	• **Server starten**	Het programma pingt het productie-IP-adres van de cloudserver totdat de server antwoordt of een time-out optreedt, afhankelijk van wat zich het eerst voordoet.
Verbinding maken met poort (standaard 443)	Voltooiingscontrole	• **Failover van server uitvoeren** • **Server starten**	Het programma probeert verbinding te maken met de cloudserver door gebruik te maken van het productie-IP-adres en de poort die u opgeeft, totdat de verbinding tot stand is gebracht of een time-out optreedt, afhankelijk van wat zich het eerst voordoet. Op deze manier kunt u controleren of de toepassing die naar de opgegeven poort luistert, actief is.
Time-out in minuten	Voltooiingscontrole	• **Failover van server uitvoeren** • **Server starten**	De standaardtime-out is 10 minuten.

Bewerkingen met runbooks

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Voor toegang tot de lijst met bewerkingen wijst u een runbook aan en klikt u op het ellipspictogram. Wanneer een runbook niet wordt uitgevoerd, zijn de volgende bewerkingen beschikbaar:

- **Uitvoeren**
- **Bewerken**
- **Klonen**
- **Verwijderen**

Een runbook uitvoeren

Elke keer dat u op **Uitvoeren** klikt, wordt u om de uitvoeringsparameters gevraagd. Deze parameters zijn van toepassing op alle failover- en failbackbewerkingen die zijn opgenomen in het runbook. Deze parameters van het hoofdrunboek worden overgenomen voor de runbooks die zijn opgegeven in de bewerkingen voor **Runbook uitvoeren**.

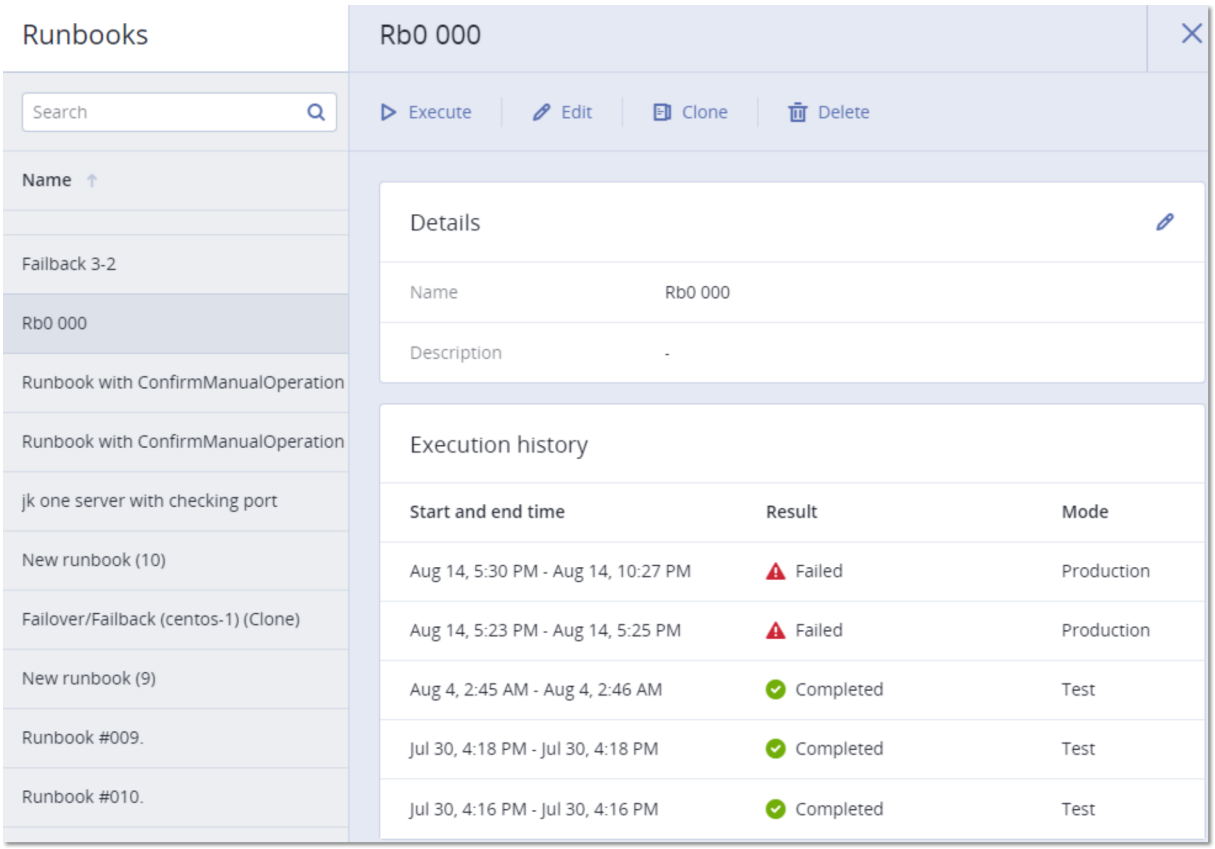
- **Failover- en failbackmodus**
  Kies of u een testfailover (standaard) of een echte (productie-)failover wilt uitvoeren. De failbackmodus komt overeen met de gekozen failovermodus.
- **Failover maken van herstelpunt**
  Kies het meest recente herstelpunt (standaard) of selecteer een tijdstip in het verleden. In dit laatste geval worden de herstelpunten die zich het dichtst bij de opgegeven datum en tijd bevinden, voor elke server geselecteerd.

Uitvoering van een runbook stoppen

Tijdens de uitvoering van een runbook kunt u **Stoppen** selecteren in de lijst met bewerkingen. Het programma voltooit alle reeds gestarte acties, behalve de acties waarvoor interactie met de gebruiker is vereist.

De uitvoeringsgeschiedenis weergeven

Wanneer u een runbook selecteert op het tabblad **Runbooks**, geeft het programma de details en de uitvoeringsgeschiedenis van het runbook weer. Klik op de regel die overeenkomt met een specifieke uitvoering om het uitvoeringslogboek te bekijken.



Antivirus- en antimalwarebeveiliging configureren

Opmerking
Voor de functie van antimalwarebeveiliging op Windows-machines is de installatie van Agent voor Antimalwarebeveiliging vereist, en voor de functie van URL-filtering is de installatie van Agent voor URL-filtering vereist. Deze agents worden automatisch geïnstalleerd voor beschermde workloads als de module **Antivirus- en Antimalwarebeveiliging** en/of **URL-filtering** is ingeschakeld in de betreffende beschermingsplannen.

Antimalwarebeveiliging in Cyber Protection biedt u de volgende voordelen:

- Uitmuntende bescherming in alle fasen: proactief, actief en reactief.
- Vier verschillende ingebouwde antimalwaretechnologieën voor optimale meerlaagse bescherming.
- Beheer van Microsoft Security Essentials en Microsoft Defender Antivirus.

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Belangrijk
Het EICAR-testbestand wordt alleen gedetecteerd wanneer de optie **Geavanceerde antimalware** is ingeschakeld in het beschermingsschema. Als het EICAR-bestand niet wordt gedetecteerd, heeft dit echter geen invloed op de antimalwaremogelijkheden van Cyber Protection.

Ondersteunde platforms

De functies Active Protection en Antivirus- en antimalwarebeveiliging worden ondersteund op de volgende platforms.

Besturingssysteem	Versie/Distributie
Windows	Windows 7 Service Pack 1 en later Windows Server 2008 R2 Service Pack 1 en later

Besturingssysteem	Versie/Distributie
	Opmerking Voor Windows 7 moet u de volgende updates van Microsoft installeren voordat u de beveiligingsagent installeert. • Windows 7 Extended Security Updates (ESU) • KB4474419 • KB4490628 Zie dit Knowledge Base-artikel voor meer informatie over de vereiste updates.
Linux	Red Hat Linux 7.x, 8.x, 9.x CloudLinux 6.10, 7.x, 8.x CentOS 6.5 en latere 6.x-versies, 7.x, 8.x Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 Debian 8.x, 9.x, 10,x, 11.x Oracle Linux 7.x, 8.x, 9.x SUSE Enterprise Linux 15.x openSUSE Leap 15.x
macOS	macOS 10.13.x en later

Ondersteunde functies per platform

Opmerking
Antimalwarebeveiliging voor Linux en macOS is beschikbaar met het Geavanceerde antimalware-pakket.

Functieset	Windows	Linux	macOS
Antivirus- en antimalwarebeveiliging			
Volledig geïntegreerde Active Protection-functionaliteit	Ja	Nee	Nee
Realtime antimalwarebeveiliging	Ja	Ja, met het Geavanceerde antimalware-pakket	Ja, met het Geavanceerde antimalware-pakket
Geavanceerde realtime antimalwarebeveiliging met lokale detectie op basis van handtekeningen	Ja	Ja	Ja

Functieset	Windows	Linux	macOS
Antivirus- en antimalwarebeveiliging			
Statische analyse voor draagbare uitvoerbare bestanden	Ja	Nee	Ja*
Antimalwarescan op aanvraag	Ja	Ja**	Ja
Netwerkmapbescherming	Ja	Ja	Nee
Bescherming op server	Ja	Nee	Nee
Scan van archiefbestanden	Ja	Nee	Ja
Scan van verwisselbare stations	Ja	Nee	Ja
Scan van alleen nieuwe en gewijzigde bestanden	Ja	Nee	Ja
Bestand-/mapuitsluitingen	Ja	Ja	Ja***
Procesuitsluitingen	Ja	Nee	Ja
Engine voor gedragsanalyse	Ja	Nee	Ja
Preventie tegen aanvallen	Ja	Nee	Nee
Quarantaine	Ja	Ja	Ja
Automatische opschoning in quarantaine	Ja	Ja	Ja
URL-filtering (http/https)	Ja	Nee	Nee
Witte lijst van het bedrijf	Ja	Nee	Ja
Firewallbeheer****	Ja	Nee	Nee
Microsoft Defender Antivirus-beheer*****	Ja	Nee	Nee
Microsoft Security Essentials-beheer	Ja	Nee	Nee
Antivirus- en antimalwarebeveiliging registreren en beheren via Windows Security Center	Ja	Nee	Nee
Zie "Ondersteunde platforms" (p. 863) voor meer informatie over de ondersteunde besturingssystemen en versies.			

* Statische analyse voor draagbare uitvoerbare bestanden wordt alleen ondersteund voor geplande scans op macOS.

** Startvoorwaarden worden niet ondersteund voor scannen op aanvraag in Linux.

*** Uitsluitingen van bestanden/mappen worden alleen ondersteund wanneer u bestanden en mappen opgeeft die niet worden gescand door realtime bescherming of geplande scans op macOS.

**** Firewallbeheer wordt ondersteund voor Windows 8 en later. Windows Server wordt niet ondersteund.

***** Microsoft Defender Antivirus-beheer wordt ondersteund voor Windows 8.1 en later.

Functieset	Windows	Linux	macOS
Active Protection			
Detectie van procesinjectie	Ja	Nee	Nee
Automatisch herstel van getroffen bestanden uit de lokale cache	Ja	Ja	Ja
Zelfverdediging voor Acronis Backup-bestanden	Ja	Nee	Nee
Zelfverdediging voor Acronis-software	Ja	Nee	Ja (Alleen Active Protection en antimalware-onderdelen)
Beheer van vertrouwde/geblokkeerde processen	Ja	Nee	Ja
Proces-/mapuitsluitingen	Ja	Ja	Ja
Detectie van ransomware op basis van procesgedrag (gebaseerd op AI)	Ja	Ja	Ja
Detectie van cryptomining-processen op basis van procesgedrag	Ja	Nee	Nee
Bescherming van externe stations (HDD, flashstations, SD-kaarten)	Ja	Nee	Ja
Netwerkmapbescherming	Ja	Ja	Ja
Bescherming op server	Ja	Nee	Nee
Bescherming van Zoom, Cisco Webex, Citrix Workspace en Microsoft Teams	Ja	Nee	Nee
Zie "Ondersteunde platforms" (p. 863) voor meer informatie over de ondersteunde besturingssystemen en versies.			

Antivirus- en antimalwarebeveiliging

Opmerking
Voor sommige functies zijn mogelijk extra licenties vereist, afhankelijk van het toegepaste licentiemodel.

Met de module **Antivirus- en antimalware** kunt u uw Windows-, Linux- en macOS-machines beschermen tegen alle recente malwarebedreigingen. Bekijk de volledige lijst met ondersteunde antimalwarefuncties in "Ondersteunde platforms" (p. 863).

Antivirus- en antimalwarebeveiliging wordt ondersteund en geregistreerd in Windows Security Center.

Antimalwarefuncties

- Detectie van malware in bestanden in de modi 'realtime bescherming' en 'op aanvraag'
- Detectie van kwaadaardig gedrag in processen (voor Windows)
- Toegang blokkeren tot schadelijke URL's (voor Windows)
- Gevaarlijke bestanden in quarantaine plaatsen
- Vertrouwde bedrijfstoepassingen toevoegen aan de acceptatielijst

Scantypen

U kunt de antivirus- en antimalwarebescherming zo configureren dat deze constant op de achtergrond of op aanvraag wordt uitgevoerd.

Realtime bescherming

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Met realtime bescherming wordt een controle uitgevoerd van alle bestanden die op een machine worden uitgevoerd of geopend, met de bedoeling om malwarebedreigingen te voorkomen.

Realtime bescherming kan niet parallel werken met andere antivirusoplossingen die ook gebruikmaken van functies voor realtime bescherming. Dit is om mogelijke compatibiliteits- en prestatieproblemen te voorkomen. De statussen van andere geïnstalleerde antivirusoplossingen worden bepaald via het Windows Security Center. Als de Windows-machine al is beschermd door een andere antivirusoplossing, wordt realtime bescherming automatisch uitgeschakeld.

Als u realtime bescherming wilt inschakelen, schakelt u de andere antivirusoplossing uit of verwijdert u deze. Realtime bescherming kan de realtime bescherming van Microsoft Defender automatisch vervangen.

Opmerking
Op machines met Windows Server-besturingssystemen wordt Microsoft Defender niet automatisch uitgeschakeld wanneer realtime bescherming is ingeschakeld. Een beheerder moet Microsoft Defender handmatig uitschakelen om mogelijke compatibiliteitsproblemen te voorkomen.

U kunt een van de volgende scanmodi kiezen:

- Detectie **Smart bij toegang** betekent dat het antimalwareprogramma op de achtergrond wordt uitgevoerd en dat het systeem van uw machine actief en constant wordt gescand op virussen en andere bedreigingen gedurende de hele tijd dat het systeem is ingeschakeld. Malware wordt in beide gevallen gedetecteerd wanneer een bestand wordt uitgevoerd en tijdens verschillende bewerkingen met het bestand, zoals het bestand openen voor lezen of bewerken.
- Detectie **bij uitvoering** betekent dat alleen uitvoerbare bestanden worden gescand wanneer ze worden uitgevoerd om te waarborgen dat ze schoon zijn en geen schade aan uw machine of gegevens kunnen veroorzaken. Het kopiëren van een geïnfecteerd bestand wordt niet opgemerkt.

Geplande scan

De antimalwarescan wordt uitgevoerd volgens een schema.

U kunt een van de volgende scanmodi kiezen.

- **Snelle scan**: hiermee worden alleen systeembestanden van de workload gecontroleerd.
- **Volledige scan**: hiermee worden alle bestanden van de workload gecontroleerd.
- **Aangepaste scan**: hiermee worden de bestanden/mappen gecontroleerd die door de beheerder zijn toegevoegd aan het beschermingsschema.

Wanneer de scan van antimalware is voltooid, kunt u naar **Controle** > **Overzicht** > widget Onlangs beïnvloed gaan voor details over de workloads die zijn getroffen door bedreigingen.

Instellingen voor Antivirus- en antimalwarebeveiliging

In dit gedeelte worden de functies beschreven die u kunt configureren in de module **Antivirus- en antimalwarebeveiliging** in een beschermingsschema. Zie "Een beschermingsschema maken" (p. 217) voor meer informatie over het maken van een beschermingsschema.

In de module Antivirus- en antimalwarebeveiliging kunnen de volgende functies worden geconfigureerd voor een beschermingsschema:

- "Active Protection" (p. 869)
- "Geavanceerde antimalware" (p. 870)

- "Netwerkmapbescherming" (p. 870)
- "Bescherming op server" (p. 871)
- "Zelfbescherming" (p. 872)
- "Detectie van cryptomining-processen" (p. 873)
- "Quarantaine" (p. 874)
- "Gedragengine" (p. 874)
- "Preventie tegen aanvallen" (p. 875)
- "Realtime bescherming" (p. 877)
- "Scan plannen" (p. 878)
- "Uitsluitingen voor bescherming" (p. 881)

Opmerking
Niet alle besturingssystemen ondersteunen de functies van Antivirus- en antimalwarebeveiliging. Voor meer informatie over de ondersteunde besturingssystemen en functies: zie "Ondersteunde platforms" (p. 863). Sommige functies zijn alleen beschikbaar in uw beschermingsplan als u een bepaalde licentie hebt.

Active Protection

Active Protection beschermt uw systeem tegen schadelijke software, ook wel ransomware genoemd, waarmee bestanden worden versleuteld en er vervolgens om losgeld wordt gevraagd voor de versleutelingssleutel.

Standaardinstelling: **Ingeschakeld**.

Opmerking
Er moet een beveiligingsagent zijn geïnstalleerd op de beschermde machine. Zie "Ondersteunde platforms" (p. 863) voor meer informatie over de ondersteunde besturingssystemen en functies.

Active Protection configureren:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Active Protection**.
3. Ga naar het gedeelte **Actie bij detectie** en selecteer een van de beschikbare opties:

   Standaardinstelling: **Terugdraaien met cache**

   - **Alleen melden**: er wordt een waarschuwing gegenereerd over het proces met verdachte ransomwareactiviteit.
   - **Het proces stoppen**: er wordt een waarschuwing gegenereerd en het proces met verdachte ransomwareactiviteit wordt gestopt.

- **Terugdraaien met cache**: er wordt een waarschuwing gegenereerd, het proces wordt gestopt en de bestandswijzigingen worden teruggedraaid met behulp van de servicecache.

4. Klik op **Gereed** om de geselecteerde opties toe te passen op uw beschermingsschema.

Geavanceerde antimalware

Deze engine gebruikt een verbeterde database van virushandtekeningen om de efficiëntie van antimalwaredetectie te verbeteren voor zowel snelle als volledige scans.

Belangrijk
Deze functie is alleen beschikbaar als het Advanced Security-beschermingspakket is ingeschakeld. Zie https://www.acronis.com/en-us/products/cloud/cyber-protect/security/ voor meer informatie

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Geavanceerde antimalware configureren:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Gebruik de schakelaar in het gedeelte **Geavanceerde antimalware** om de lokale, op handtekeningen gebaseerde engine in te schakelen.

Opmerking
De lokale engine op basis van handtekeningen is ook vereist voor antivirus- en antimalwarebeveiliging voor macOS en Linux. Antivirus- en antimalwarebeveiliging voor Windows is beschikbaar met of zonder deze engine.

Netwerkmapbescherming

Met de functie **Netwerkmapbescherming** bepaalt u of Antivirus- en antimalwarebeveiliging ook netwerkmappen beschermt die zijn toegewezen als lokale stations. De bescherming is van toepassing op mappen die worden gedeeld via SMB- of NFS-protocollen.

Netwerkmapbescherming configureren:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Netwerkmapbescherming**.
3. Voeg de bestanden toe waar u een back-up van de netwerkmappen wilt maken:
   - Als uw workload bijvoorbeeld Windows is, voert u in het veld **Windows** het pad in voor het Windows-bestand waar u een back-up van de netwerkmappen wilt maken. Standaardwaarde: C:\ProgramData\Acronis\Restored Network Files.

- Als uw workload bijvoorbeeld macOS is, voert u in het veld **macOS** het pad in voor de macOS-bestanden waar u een back-up van de netwerkmappen wilt maken. Standaardwaarde: /Library/Application Support/Acronis/Restored Network Files/.

Opmerking
Voer het pad van een lokale map in. Netwerkmappen, inclusief mappen op gekoppelde stations, worden niet ondersteund als back-upbestemming voor de netwerkmappen.

4. Klik op **Gereed** om de geselecteerde opties toe te passen op uw beschermingsschema.

Bescherming op server

Met deze functie bepaalt u of Active Protection ook de door u gedeelde netwerkmappen beschermt tegen de externe inkomende verbindingen van andere servers in het netwerk die mogelijk bedreigingen kunnen veroorzaken.

Standaardinstelling: **Uit**.

Opmerking
Bescherming op server wordt niet ondersteund voor Linux.

Vertrouwde verbindingen instellen:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Bescherming op server**.
3. Gebruik de schakelaar **Bescherming op server** om deze functie in te schakelen.
4. Selecteer het tabblad **Vertrouwd**.
5. Ga naar het veld **Vertrouwde verbindingen** en klik op **Toevoegen** om te definiëren welke verbindingen toestemming hebben om gegevens te wijzigen.
6. Ga naar het veld **Computernaam/Account** en typ de naam van de computer en het account van de machine waarop de beveiligingsagent is geïnstalleerd. Bijvoorbeeld: `MijnComputer\Testgebruiker`.
7. Ga naar het veld **Hostnaam** en typ de hostnaam van de machine die verbinding mag maken met de machine via de beveiligingsagent.
8. Klik op het vinkje rechts om de verbindingsdefinitie op te slaan.
9. Klik op **Gereed**.

Geblokkeerde verbindingen instellen:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Bescherming op server**.

3. Gebruik de schakelaar **Bescherming op server** om deze functie in te schakelen.
4. Selecteer het tabblad **Geblokkeerd**.
5. Ga naar het veld **Geblokkeerde verbindingen** en klik op **Toevoegen** om te definiëren welke verbindingen geen toestemming hebben om gegevens te wijzigen.
6. Ga naar het veld **Computernaam/Account** en typ de naam van de computer en het account van de machine waarop de beveiligingsagent is geïnstalleerd. Bijvoorbeeld: `MijnComputer\Testgebruiker`.
7. Ga naar het veld **Hostnaam** en typ de hostnaam van de machine die verbinding mag maken met de machine via de beveiligingsagent.
8. Schakel het selectievakje rechts in om de definitie van de verbinding op te slaan.
9. Klik op **Gereed**.

Zelfbescherming

Met Zelfbescherming voorkomt u ongeautoriseerde wijzigingen in softwareprocessen, registerrecords, uitvoerbare bestanden, configuratiebestanden, en in back-ups in lokale mappen.

Beheerders kunnen **Zelfbescherming** inschakelen zonder **Active Protection** in te schakelen.

Standaardinstelling: **Aan**.

Opmerking
Zelfbescherming wordt niet ondersteund voor Linux.

Zelfbescherming inschakelen:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Zelfbescherming**.
3. Gebruik de schakelaar **Zelfbescherming** om deze functie in te schakelen.

Wachtwoordbescherming inschakelen

1. Wanneer de functie **Zelfbescherming** is ingeschakeld, kunt u de schakelaar gebruiken om de functie **Wachtwoordbescherming** in te schakelen.
2. Klik op **Nieuw wachtwoord genereren** om een wachtwoord te genereren waarmee u lokale agents kunt wijzigen of verwijderen.
3. Klik op **Kopiëren** en plak het vervolgens op een veilige plaats, want u moet dit opgeven wanneer u de lijst met onderdelen lokaal wilt wijzigen.

Belangrijk
Het wachtwoord is niet meer beschikbaar nadat u het venster hebt gesloten. Als u dit wachtwoord wilt toepassen op apparaten, moeten de instellingen van het beschermingsschema worden opgeslagen.

4. Klik op **Sluiten**.

Met **Wachtwoordbescherming** voorkomt u dat niet-geautoriseerde gebruikers of software de Agent voor Windows kunnen verwijderen of de onderdelen ervan kunnen wijzigen. Deze acties zijn alleen mogelijk met een wachtwoord dat een beheerder kan verstrekken.

Voor de volgende acties is nooit een wachtwoord vereist:

- De installatie bijwerken door het installatieprogramma lokaal uit te voeren
- De installatie bijwerken met de Cyber Protect-console
- De installatie herstellen

Standaardinstelling: **Uitgeschakeld**

Meer informatie over het inschakelen van **Wachtwoordbescherming** vindt u in Voorkomen van niet-geautoriseerde verwijdering of wijziging van agents.

Detectie van cryptomining-processen

Cryptomining-malware kan leiden tot mindere prestaties van nuttige toepassingen, een hogere elektriciteitsrekening, systeemcrashes en zelfs schade aan de hardware als gevolg van misbruik. De functie **Detectie van cryptomining-processen** beschermt uw apparaten tegen crytomining-malware en voorkomt niet-goedgekeurd gebruik van computerresources.

Beheerders kunnen **Detectie van cryptomining-processen** inschakelen zonder **Active Protection** in te schakelen. Standaardinstelling: **Ingeschakeld**.

Opmerking
Detectie van cryptomining-processen wordt niet ondersteund voor Linux.

Netwerkmapbescherming configureren:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Detectie van cryptomining-processen**.
3. Gebruik de schakelaar **Cryptomining-processen detecteren** om de functie in of uit te schakelen.
4. Selecteer wat u wilt doen met processen die verdacht worden van cryptomining-activiteiten:

   Standaardinstelling: **Het proces stoppen**

- **Alleen melden**: er wordt een waarschuwing gegenereerd.
- **Het proces stoppen**: er wordt een waarschuwing gegenereerd en het proces wordt gestopt.

5. Klik op **Gereed** om de geselecteerde opties toe te passen op uw beschermingsschema.

Quarantaine

Quarantaine is een map waar u verdachte (waarschijnlijk geïnfecteerde) of potentieel gevaarlijke bestanden kunt isoleren.

Quarantaine configureren:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Quarantaine**.
3. In het veld **Bestanden in quarantaine verwijderen na** kunt u definiëren na hoeveel dagen de bestanden in quarantaine worden verwijderd.
   Standaardinstelling: **30 dagen**
4. Klik op **Gereed**.

Zie Quarantaine voor meer informatie over deze functie.

Gedragengine

De functie **Gedragengine** beschermt een systeem tegen malware door gebruik te maken van gedragsheuristiek om schadelijke processen te detecteren.

Standaardinstelling: **Ingeschakeld**.

Opmerking
Gedragengine wordt niet ondersteund voor Linux.

Netwerkmapbescherming configureren:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Gedragengine**.
3. Gebruik de schakelaar **Gedragengine** om de functie in of uit te schakelen.
4. Ga naar **Actie bij detectie** en selecteer de actie die moet worden uitgevoerd wanneer een malwareactiviteit wordt gedetecteerd:
   Standaardinstelling: **Quarantaine**
   - **Alleen melden**: er wordt een waarschuwing gegenereerd over het proces met verdachte malwareactiviteit.
   - **Het proces stoppen**: er wordt een waarschuwing gegenereerd en het proces met verdachte malwareactiviteit wordt gestopt.

- **Quarantaine**: er wordt een waarschuwing gegenereerd, het proces wordt gestopt en de uitvoerbare bestanden worden verplaatst naar de quarantainemap.

5. Klik op **Gereed** om de geselecteerde opties toe te passen op uw beschermingsschema.

Preventie tegen aanvallen

Belangrijk
Deze functie is alleen beschikbaar als het Advanced Security-beschermingspakket is ingeschakeld. Zie https://www.acronis.com/en-us/products/cloud/cyber-protect/security/ voor meer informatie

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Met Preventie tegen aanvallen detecteert u schadelijke processen en voorkomt u dat deze zich verspreiden en gebruikmaken van beveiligingsproblemen in een systeem. Wanneer een aanval wordt gedetecteerd, kan een waarschuwing worden gegenereerd en wordt het proces gestopt dat wordt verdacht van de aanval.

Preventie tegen aanvallen is alleen beschikbaar met agentversie 12.5.23130 (21.08, uitgebracht in augustus 2020) of later.

Standaardinstelling: **Ingeschakeld** voor nieuw gemaakte beschermingsschema's, en **Uitgeschakeld** voor bestaande beschermingsschema's die zijn gemaakt met eerdere agentversies.

Opmerking
Preventie tegen aanvallen wordt niet ondersteund voor Linux.

U kunt kiezen wat het programma moet doen wanneer een aanval wordt gedetecteerd en welke methoden voor preventie tegen aanvallen moeten worden toegepast door het programma.

Preventie tegen aanvallen configureren:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Preventie tegen aanvallen**.
3. Ga naar het gedeelte **Actie bij detectie** en selecteer een van de beschikbare opties:

   Standaardinstelling: **Het proces stoppen**

   - **Alleen melden**
     Er wordt een waarschuwing gegenereerd over het proces met verdachte aanvalsactiviteiten.
   - **Het proces stoppen**
     Er wordt een waarschuwing gegenereerd en het proces met verdachte aanvalsactiviteiten wordt gestopt.

4. Ga naar het gedeelte **Ingeschakelde technieken voor preventie tegen aanvallen** en selecteer (een van) de opties die u wilt toepassen:

   Standaardinstelling: **Alle methoden zijn ingeschakeld**

   - **Geheugenbescherming**

     Detecteert en voorkomt verdachte wijzigingen van de uitvoeringsrechten voor geheugenpagina's. Schadelijke processen passen zulke wijzigingen toe op de pagina-eigenschappen om de uitvoering van shellcodes uit niet-uitvoerbare geheugengebieden, zoals stack en heaps, mogelijk te maken.
   - **Bescherming tegen return-oriented programming (ROP)**

     Detecteert en voorkomt pogingen om de ROP-aanvalstechniek te gebruiken.
   - **Bescherming tegen escalatie van bevoegdheden**

     Detecteert en voorkomt pogingen tot onrechtmatige uitbreiding van rechten door een ongeoorloofde code of applicatie. Escalatie van bevoegdheden wordt gebruikt door schadelijke code om volledige toegang te krijgen tot de aangevallen machine en vervolgens kritieke en gevoelige taken uit te voeren. Ongeoorloofde code krijgt geen toegang tot kritieke systeembronnen en kan geen systeeminstellingen wijzigen.
   - **Bescherming tegen code-injecties**

     Detecteert en voorkomt het injecteren van schadelijke code in externe processen. Code-injectie wordt gebruikt om de kwaadaardige bedoeling van een applicatie te verbergen achter schone of goedaardige processen, zodat de detectie door antimalwareproducten wordt omzeild.
5. Klik op **Gereed** om de geselecteerde opties toe te passen op uw beschermingsschema.

Opmerking
Processen die als vertrouwde processen in de lijst met uitsluitingen zijn opgenomen, worden niet gescand op aanvallen.

Toestaan dat back-ups worden gewijzigd door processen

De instelling **Specifieke processen toestaan om back-ups te wijzigen** is alleen beschikbaar wanneer de instelling **Zelfbescherming** is ingeschakeld.

De optie is van toepassing op bestanden met de extensies .tibx, .tib, .tia in lokale mappen.

Met deze instelling kunt u de processen opgeven die de back-upbestanden mogen wijzigen, ook al zijn deze bestanden beveiligd met zelfbescherming. Dit is bijvoorbeeld handig als u back-upbestanden verwijdert of ze met een script naar een andere locatie verplaatst.

Als deze instelling is uitgeschakeld, kunnen de back-upbestanden alleen worden gewijzigd door processen die zijn ondertekend door de leverancier van de back-upsoftware. Hierdoor kan de software bewaarregels toepassen en back-ups verwijderen wanneer een gebruiker hierom verzoekt via de webinterface. Andere processen, ongeacht of ze verdacht zijn of niet, kunnen de back-ups niet wijzigen.

Als deze instelling is ingeschakeld, kunt u toestaan dat andere processen de back-ups wijzigen. Geef het volledige pad naar het uitvoerbare bestand voor het proces op. Het pad begint met de stationsletter.

Standaardinstelling: **Uitgeschakeld**.

Realtime bescherming

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Met **Realtime bescherming** wordt uw computersysteem continu gecontroleerd op virussen en andere bedreigingen gedurende de hele tijd dat uw systeem is ingeschakeld, tenzij de computergebruiker het proces onderbreekt.

Standaardinstelling: **Ingeschakeld**.

Belangrijk
Deze functie is alleen beschikbaar als het Advanced Security-beschermingspakket is ingeschakeld. Zie https://www.acronis.com/en-us/products/cloud/cyber-protect/security/ voor meer informatie

Realtime bescherming configureren:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Realtime bescherming**.
3. Ga naar het vervolgkeuzemenu **Actie bij detectie** en selecteer een van de beschikbare opties:

   Standaardinstelling: **Quarantaine**

   - **Alleen melden**

     De software genereert een waarschuwing over het proces dat wordt verdacht van ransomwareactiviteit.

   - **Blokkeren en melden**

     Het proces wordt geblokkeerd en er wordt een waarschuwing gegenereerd over het proces dat wordt verdacht van malwareactiviteit.

   - **Quarantaine**
4. Er wordt een waarschuwing gegenereerd, het proces wordt gestopt en het uitvoerbare bestand wordt verplaatst naar de quarantainemap.
5. Selecteer in het gedeelte **Scanmodus** de actie die moet worden uitgevoerd wanneer een virus of andere bedreiging wordt gedetecteerd:

   Standaardinstelling: **Smart bij toegang**

- **Smart bij toegang**: alle systeemactiviteiten worden gecontroleerd en bestanden worden automatisch gescand wanneer ze worden geopend met lees- of schrijftoegang of wanneer een programma wordt gestart.
- **Bij uitvoering**: alleen uitvoerbare bestanden worden automatisch gescand wanneer ze worden gestart om te waarborgen dat ze veilig zijn en geen schade aan uw computer of gegevens kunnen veroorzaken.

6. Klik op **Gereed**.

Scan plannen

Met Scannen op aanvraag wordt uw computersysteem gecontroleerd op virussen volgens het opgegeven schema. Met een volledige scan worden alle bestanden op uw machine gecontroleerd. Met een snelle scan worden alleen de systeembestanden van de machine gecontroleerd.

Scan plannen configureren:

Standaardinstellingen:

- **Aangepaste scan** is uitgeschakeld.
- **Snel** en **Volledig** zijn gepland.

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Scan plannen**.
3. Gebruik de schakelaar om het type scan in te schakelen dat u wilt toepassen voor uw machine.

Beschikbare typen scans:

- **Volledig**: duurt veel langer dan de snelle scan omdat elk bestand wordt gecontroleerd.
- **Snel**: alleen de gebieden worden gescand waar malware zich doorgaans bevindt op de machine.
- **Aangepast**: de bestanden/mappen die door de beheerder van het Bescherming-schema zijn geselecteerd, worden gecontroleerd.

> **Opmerking**
> U kunt de drie scans (**Snel**, **Volledig** en **Aangepast**) plannen in één beschermingsschema.

Aangepaste scan configureren:

- Gebruik de **schakelaar Aangepaste scan** om dit type scan in of uit te schakelen.
- Ga naar de vervolgkeuzelijst **Actie bij detectie** en selecteer een van de beschikbare opties:

Standaardinstelling: **Quarantaine**

Quarantaine

Er wordt een waarschuwing gegenereerd en het uitvoerbare bestand wordt verplaatst naar de quarantainemap.

Alleen melden

Er wordt een waarschuwing gegenereerd over het proces dat vermoedelijk malware is.

Veld	Beschrijving
De taakuitvoering plannen met de volgende gebeurtenissen	Met deze instelling definieert u wanneer de taak wordt uitgevoerd. De volgende waarden zijn beschikbaar: • **Schema op tijd**: dit is de standaardinstelling. De taak wordt uitgevoerd volgens de opgegeven tijd. • **Wanneer de gebruiker zich aanmeldt bij het systeem**: standaard wordt de taak geactiveerd wanneer een gebruiker zich aanmeldt. U kunt deze instelling ook wijzigen, zodat alleen een specifiek gebruikersaccount de taak kan activeren. • **Wanneer de gebruiker zich afmeldt bij het systeem**: standaard wordt de taak geactiveerd wanneer een gebruiker zich afmeldt. U kunt deze instelling ook wijzigen, zodat alleen een specifiek gebruikersaccount de taak kan activeren. **Opmerking** De taak wordt niet uitgevoerd bij het afsluiten van het systeem. Afsluiten en afmelden zijn verschillende gebeurtenissen in de planningsconfiguratie. • **Wanneer het systeem wordt opgestart**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt gestart. • **Wanneer het systeem wordt afgesloten**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt afgesloten.
Type schema	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd. De volgende waarden zijn beschikbaar: • **Maandelijks**: selecteer de maanden en de weken of dagen van de maand wanneer de taak zal worden uitgevoerd. • **Dagelijks**: dit is de standaardinstelling. Selecteer de dagen van de week waarop de taak wordt uitgevoerd. • **Elk uur**: selecteer de dagen van de week, het aantal herhalingen en het tijdinterval waarin de taak wordt uitgevoerd.
Starten om	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd. Selecteer het exacte tijdstip waarop de taak wordt uitgevoerd.
Uitvoeren binnen een datumbereik	Dit veld wordt weergegeven als u in **De taakuitvoering plannen**

Veld	Beschrijving
	met de volgende gebeurtenissen de optie **Schema op tijd** hebt geselecteerd. Stel een bereik in waarin het geconfigureerde schema van kracht is.
Geef een gebruikersaccount op waarvoor een taak wordt geïnitieerd zodra het account wordt aangemeld bij het besturingssysteem	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Wanneer de gebruiker zich aanmeldt bij het systeem** hebt geselecteerd. De volgende waarden zijn beschikbaar: • **Elke gebruiker**: gebruik deze optie als u wilt dat de taak wordt geactiveerd wanneer een willekeurige gebruiker zich aanmeldt. • **De volgende gebruiker**: gebruik deze optie als u wilt dat de taak alleen wordt geactiveerd wanneer een specifiek gebruikersaccount zich aanmeldt.
Geef een gebruikersaccount op waarvoor een taak wordt geïnitieerd zodra het account wordt afgemeld bij het besturingssysteem	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Wanneer de gebruiker zich afmeldt bij het systeem** hebt geselecteerd. De volgende waarden zijn beschikbaar: • **Elke gebruiker**: gebruik deze optie als u wilt dat de taak wordt geactiveerd wanneer een willekeurige gebruiker zich afmeldt. • **De volgende gebruiker**: gebruik deze optie als u wilt dat de taak alleen wordt geactiveerd wanneer een specifiek gebruikersaccount zich afmeldt.
Startvoorwaarden	Hiermee definieert u alle voorwaarden waaraan tegelijkertijd moet worden voldaan om de taak uit te voeren. De startvoorwaarden voor antimalwarescans zijn vergelijkbaar met de startvoorwaarden voor de **module Back-up** die worden beschreven in 'Startvoorwaarden'. U kunt de volgende aanvullende startvoorwaarden definiëren: • **Starttijd van taak binnen een tijdvenster distribueren**: met deze optie kunt u het tijdsbestek instellen voor de taak om knelpunten in het netwerk te voorkomen. U kunt de vertraging opgeven in uren of minuten. Als de standaardstarttijd bijvoorbeeld 10:00 uur en de vertraging 60 minuten is, dan zal de taak beginnen tussen 10:00 uur en 11:00 uur. • **Als de machine is uitgeschakeld, gemiste taken uitvoeren wanneer de machine wordt opgestart** • **De slaap- of sluimerstand voorkomen tijdens het uitvoeren van taken**: deze optie is alleen van toepassing op machines met Windows.

Veld	Beschrijving
	• **Voer de taak na de start uit, zelfs als niet aan de startvoorwaarden wordt voldaan**: geef aan na hoeveel tijd de taak wordt uitgevoerd, ongeacht de andere startvoorwaarden. **Opmerking** Startvoorwaarden worden niet ondersteund voor Linux.

- Schakel het selectievakje **Alleen nieuwe en gewijzigde bestanden scannen** in als u alleen nieuw gemaakte en gewijzigde bestanden wilt scannen.

Standaardinstelling: **Ingeschakeld**

- Er worden twee extra opties voor **Aangepaste scan** weergegeven (alleen voor **Volledige scan**):

1. **Archiefbestanden scannen**

   Standaardinstelling: **Ingeschakeld**.

   Max. recursiediepte

   Standaardinstelling: **16**

   Hoeveel niveaus van ingesloten archieven kunnen worden gescand. Bijvoorbeeld MIME-document > ZIP-archief > Office-archief > documentinhoud.

   Maximale grootte

   Standaardinstelling: **100**

   Maximale grootte van een te scannen archiefbestand.

2. **Verwisselbare stations scannen**

Standaardinstelling: **Uitgeschakeld**

- **Toegewezen (externe) netwerkstations**
- **USB-opslagapparaten** (zoals pennen en externe harde schijven)
- **Cd's/dvd's**

Opmerking
Verwisselbare stations scannen wordt niet ondersteund voor Linux.

Uitsluitingen voor bescherming

Met Uitsluitingen voor bescherming kunt u fout-positieven elimineren wanneer een vertrouwd programma als ransomware of malware wordt beschouwd. U kunt vertrouwde en geblokkeerde items definiëren door ze toe te voegen aan de lijst met uitsluitingen voor bescherming.

In de lijst met vertrouwde items kunt u bestanden, processen en mappen toevoegen zodat ze als veilig worden beschouwd in het systeem en om toekomstige detecties hiervan te voorkomen.

In de lijst met geblokkeerde items kun je processen en hashes toevoegen. Deze optie garandeert dat deze processen worden geblokkeerd en dat uw workload veilig is.

Item uitgesloten voor beschermin g	Geblokkeerd	Vertrouwd
Hash	Wanneer een hash wordt toegevoegd aan de lijst met geblokkeerde items, wordt het proces automatisch gestopt op basis van de opgegeven hash. Wanneer u bijvoorbeeld de MD5-hash 938c2cc0dcc05f2b68c4287040cfcf71 toevoegt, wordt het aan deze hash gekoppelde proces geblokkeerd.	Wanneer een hash wordt toegevoegd aan de lijst met vertrouwde items, worden de betreffende processen, op basis van de opgegeven hash, automatisch genegeerd bij controles. Wanneer u bijvoorbeeld de MD5-hash 938c2cc0dcc05f2b68c4287040cfcf71 toevoegt, wordt het aan deze hash gekoppelde proces vertrouwd en uitgesloten van controles.
Proces	Wanneer een proces wordt toegevoegd aan de lijst met geblokkeerde items, worden de betreffende processen automatisch gecontroleerd en altijd geblokkeerd. Als u bijvoorbeeld het pad C:\Users\user1\application\nppInstaller.exe toevoegt aan de lijst met geblokkeerde items, wordt dit specifieke proces geblokkeerd en kan het niet worden gestart wanneer u het probeert te openen.	Wanneer een proces wordt toegevoegd aan de lijst met vertrouwde items, worden de betreffende processen automatisch uitgesloten van controles. **Opmerking** Processen ondertekend door Microsoft worden altijd vertrouwd. Als u bijvoorbeeld het pad C:\Users\user1\application\nppInstaller.exe toevoegt, wordt dit specifieke proces uitgesloten van controles en wordt het niet gecontroleerd door antivirusprogramma's.
Bestand/map		Wanneer een bestand of map wordt toegevoegd aan de lijst met vertrouwde items, worden die bestanden of mappen altijd als veilig beschouwd en worden ze niet gescand of gecontroleerd.

De items opgeven die altijd worden vertrouwd:

1. Open het beschermingsschema.
2. Vouw de module **Antivirus- en antimalwarebeveiliging** uit.
3. Selecteer de optie **Uitsluitingen**.
   Het venster **Uitsluitingen voor bescherming** wordt geopend.
4. Klik in het gedeelte **Vertrouwde items** op **Toevoegen** en selecteer een of meer van de beschikbare opties:
   - Als u bestanden, mappen of processen wilt vertrouwen, selecteert u de optie '**Bestand/map/proces**. Het venster **Bestand/map/proces toevoegen** wordt geopend.
     - Ga naar het veld **Bestand/proces/map** en voer het pad voor elk proces, map of bestand in op een nieuwe regel. Voer in het gedeelte **Beschrijving** een korte beschrijving in, zodat u uw wijziging kunt herkennen in de lijst met vertrouwde items.
     - Schakel het selectievakje **Toevoegen als bestand/map** in om het bestand/de map te vertrouwen.
       Voorbeeld van een mapbeschrijving: D:\map\, /home/Map/map2, F:\
     - Schakel het selectievakje **Toevoegen als proces** in om een proces te vertrouwen. De geselecteerde processen worden uitgesloten van controles.

       Opmerking
       Geef het volledige pad naar het uitvoerbare bestand voor het proces op. Het pad begint met de stationsletter. Bijvoorbeeld `C:\Windows\Temp\er76s7sdkh.exe`.

       Opmerking
       Lokale netwerkpaden worden ondersteund. bijvoorbeeld: \\localhost\folderpath\file.exe

   - Selecteer de optie **Hash** om MD5-hashes toe te voegen aan de lijst met vertrouwde items. Het venster **Hash toevoegen** wordt geopend.
     - Hier kunt u MD5-hashes op afzonderlijke regels invoegen, zodat deze als vertrouwd worden opgenomen in de lijst Uitsluitingen voor bescherming. Cyber Protection gebruikt deze hashes om de processen die worden beschreven door de MD5-hashes, uit te sluiten van controles.

Standaardinstelling: Standaard worden geen uitsluitingen gedefinieerd.

De items opgeven die altijd worden geblokkeerd:

1. Open het beschermingsschema.
2. Vouw de module **Antivirus- en antimalwarebeveiliging** uit.
3. Selecteer de optie **Uitsluitingen voor bescherming**. Het venster **Uitsluitingen voor bescherming** wordt geopend.

   Klik in het gedeelte **Geblokkeerde items** op **Toevoegen** en selecteer een of meer van de beschikbare opties:
   - Als u processen wilt blokkeren, selecteert u de optie **Proces**. Het venster **Proces toevoegen** wordt geopend.

- Ga naar het veld **Proces** en voer het pad voor elk proces in op een nieuwe regel. Voer in het veld **Beschrijving** een korte beschrijving in, zodat u uw wijziging kunt herkennen in de lijst met geblokkeerde items.

Opmerking
Deze processen kunnen niet worden gestart wanneer Active Protection is ingeschakeld op de machine.

- Als u hashes wilt blokkeren, selecteert u de optie **Hash**. Het venster **Hash toevoegen** wordt weergegeven.
  - Ga naar het veld **Hash** en voer de hash voor elk proces in op een nieuwe regel. Voer in het veld **Beschrijving** een korte beschrijving in, zodat u uw wijziging kunt herkennen in de lijst met geblokkeerde items.

Standaardinstelling: Standaard worden geen uitsluitingen gedefinieerd.

Jokertekens

U kunt de jokertekens * en ? gebruiken als u een map opgeeft. Het sterretje (*) vervangt nul of meer tekens. Het vraagteken (?) vervangt precies één teken. Omgevingsvariabelen, zoals `%AppData%`, kunnen niet worden gebruikt.

U kunt een jokerteken (*) gebruiken om items toe te voegen aan de uitsluitingslijsten.

- Jokertekens kunnen in het midden of aan het einde van een beschrijving worden gebruikt.

Voorbeelden van geaccepteerde jokertekens in beschrijvingen:

C:*.pdf

D:\folders\file.*

C:\Users*\AppData\Roaming

- Jokertekens kunnen niet aan het begin van een beschrijving worden gebruikt.

Voorbeelden van niet-geaccepteerde jokertekens in beschrijvingen:

*.docx

*:\folder\

Variabelen

U kunt ook variabelen gebruiken om items toe te voegen aan de lijst Uitsluitingen voor bescherming, met de volgende beperkingen:

- Voor Windows worden alleen SYSTEM-variabelen ondersteund. Gebruikersspecifieke variabelen, bijvoorbeeld %USERNAME%, %APPDATA%, worden niet ondersteund. Variabelen met {username} worden niet ondersteund. Zie https://ss64.com/nt/syntax-variables.html voor meer informatie.

- Omgevingsvariabelen worden niet ondersteund voor macOS.
- Omgevingsvariabelen worden niet ondersteund voor Linux.

  Voorbeelden van ondersteunde indelingen:

  - %WINDIR%\Media
  - %public%
  - %CommonProgramFiles%\Acronis\

Beschrijving

U kunt het veld **Beschrijving** gebruiken om notities te maken over de uitsluitingen die u hebt toegevoegd in de lijst met uitsluitingen voor bescherming. Enkele suggesties voor de opmerkingen die u kunt maken:

- Redenen en doeleinden van de uitsluiting.
- Werkelijke bestandsnaam van een hash-uitsluiting.
- Tijdstempels.

Als er meerdere items zijn toegevoegd aan één vermelding, kan er slechts 1 opmerking worden vastgelegd voor de meerdere items.

Active Protection in de Cyber Backup Standard-editie

Active Protection is een afzonderlijke module in het beschermingsschema van de Cyber Backup Standard-editie. Op die manier kan deze afzonderlijk worden geconfigureerd en worden toegepast op verschillende apparaten of een groep apparaten.

In alle andere edities van de Cyber Protection-service maakt Active Protection deel uit van de module **Antivirus en Antimalware** van het beschermingsschema.

Standaardinstelling: **Ingeschakeld**.

Opmerking
Er moet een beveiligingsagent zijn geïnstalleerd op de beschermde machine. Zie "Ondersteunde platforms" (p. 863) voor meer informatie over de ondersteunde besturingssystemen en functies.

Zo werkt het

Active Protection controleert de processen die op de beveiligde machine worden uitgevoerd. Wanneer een extern proces bestanden probeert te versleutelen of een poging doet tot cryptomining, genereert Active Protection een waarschuwing en worden er extra acties uitgevoerd zoals opgegeven in het beschermingsschema.

Daarnaast voorkomt Active Protection dat ongeautoriseerde wijzigingen worden doorgevoerd in softwareprocessen, registerrecords, uitvoerbare bestanden, configuratiebestanden en back-ups in lokale mappen.

Active Protection maakt gebruik van gedragsheuristiek om schadelijke processen te identificeren. Active Protection vergelijkt de acties die worden uitgevoerd door een proces, met de gebeurtenisreeksen die zijn opgenomen in de database van schadelijke gedragspatronen. Via deze aanpak kan Active Protection nieuwe malware detecteren aan de hand van het typische gedrag ervan.

Instellingen voor Active Protection in Cyber Backup Standard

In de Cyber Backup Standard-editie kunt u de volgende Active Protection-functies configureren:

- Actie bij detectie
- Zelfbescherming
- Netwerkmapbescherming
- Bescherming op server
- Detectie van cryptomining-processen
- Uitsluitingen

Opmerking
Active Protection voor Linux ondersteunt de volgende instellingen: Actie bij detectie, Netwerkmapbescherming en Uitsluitingen. De netwerkmapbescherming is altijd ingeschakeld en kan niet worden geconfigureerd.

Actie bij detectie

Ga naar het gedeelte **Actie bij detectie** en selecteer een van de beschikbare opties:

- **Alleen melden**
  Er wordt een waarschuwing gegenereerd over het proces met verdachte ransomwareactiviteit.
- **Het proces stoppen**
  Er wordt een waarschuwing gegenereerd en het proces met verdachte ransomwareactiviteit wordt gestopt.
- **Terugdraaien met cache**
  De software genereert een waarschuwing, stopt het proces en draait bestandswijzigingen terug door gebruik te maken van de servicecache.

Standaardinstelling: **Terugdraaien met cache**.

Met Zelfbescherming voorkomt u ongeautoriseerde wijzigingen in softwareprocessen, registerrecords, uitvoerbare bestanden, configuratiebestanden, en in back-ups in lokale mappen.

Beheerders kunnen **Zelfbescherming** inschakelen zonder **Active Protection** in te schakelen.

Standaardinstelling: **Aan**.

Opmerking
Zelfbescherming wordt niet ondersteund voor Linux.

Zelfbescherming inschakelen:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Zelfbescherming**.
3. Gebruik de schakelaar **Zelfbescherming** om deze functie in te schakelen.

Wachtwoordbescherming inschakelen

1. Wanneer de functie **Zelfbescherming** is ingeschakeld, kunt u de schakelaar gebruiken om de functie **Wachtwoordbescherming** in te schakelen.
2. Klik op **Nieuw wachtwoord genereren** om een wachtwoord te genereren waarmee u lokale agents kunt wijzigen of verwijderen.
3. Klik op **Kopiëren** en plak het vervolgens op een veilige plaats, want u moet dit opgeven wanneer u de lijst met onderdelen lokaal wilt wijzigen.

   Belangrijk
   Het wachtwoord is niet meer beschikbaar nadat u het venster hebt gesloten. Als u dit wachtwoord wilt toepassen op apparaten, moeten de instellingen van het beschermingsschema worden opgeslagen.

4. Klik op **Sluiten**.

Met **Wachtwoordbescherming** voorkomt u dat niet-geautoriseerde gebruikers of software de Agent voor Windows kunnen verwijderen of de onderdelen ervan kunnen wijzigen. Deze acties zijn alleen mogelijk met een wachtwoord dat een beheerder kan verstrekken.

Voor de volgende acties is nooit een wachtwoord vereist:

- De installatie bijwerken door het installatieprogramma lokaal uit te voeren
- De installatie bijwerken met de Cyber Protect-console
- De installatie herstellen

Standaardinstelling: **Uitgeschakeld**

Meer informatie over het inschakelen van **Wachtwoordbescherming** vindt u in Voorkomen van niet-geautoriseerde verwijdering of wijziging van agents.

Netwerkmapbescherming

Met de instelling **Netwerkmappen beschermen die zijn toegewezen als lokale stations** bepaalt u of Active Protection bescherming biedt tegen schadelijke lokale processen voor netwerkmappen die zijn toegewezen als lokale stations.

Deze instelling is van toepassing op mappen die worden gedeeld via SMB- of NFS-protocollen.

Als een bestand zich oorspronkelijk op een toegewezen station bevond, kan het niet worden opgeslagen op de oorspronkelijke locatie wanneer het uit de cache wordt opgehaald met de actie

Terugdraaien met cache. In plaats daarvan wordt het opgeslagen in de map die is opgegeven in deze instelling. De standaardmap is `C:\ProgramData\Acronis\Restored Network Files` voor Windows en `Library/Application Support/Acronis/Restored Network Files/` voor macOS. Als deze map niet bestaat, wordt deze gemaakt. Als u dit pad wilt wijzigen, geeft u een lokale map op. Netwerkmappen, inclusief mappen op toegewezen stations, worden niet ondersteund.

Standaardinstelling: **Aan**.

Met deze functie bepaalt u of Active Protection ook de door u gedeelde netwerkmappen beschermt tegen de externe inkomende verbindingen van andere servers in het netwerk die mogelijk bedreigingen kunnen veroorzaken.

Standaardinstelling: **Uit**.

Opmerking
Bescherming op server wordt niet ondersteund voor Linux.

Vertrouwde verbindingen instellen:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Bescherming op server**.
3. Gebruik de schakelaar **Bescherming op server** om deze functie in te schakelen.
4. Selecteer het tabblad **Vertrouwd**.
5. Ga naar het veld **Vertrouwde verbindingen** en klik op **Toevoegen** om te definiëren welke verbindingen toestemming hebben om gegevens te wijzigen.
6. Ga naar het veld **Computernaam/Account** en typ de naam van de computer en het account van de machine waarop de beveiligingsagent is geïnstalleerd. Bijvoorbeeld: `MijnComputer\Testgebruiker`.
7. Ga naar het veld **Hostnaam** en typ de hostnaam van de machine die verbinding mag maken met de machine via de beveiligingsagent.
8. Klik op het vinkje rechts om de verbindingsdefinitie op te slaan.
9. Klik op **Gereed**.

Geblokkeerde verbindingen instellen:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Bescherming op server**.
3. Gebruik de schakelaar **Bescherming op server** om deze functie in te schakelen.
4. Selecteer het tabblad **Geblokkeerd**.
5. Ga naar het veld **Geblokkeerde verbindingen** en klik op **Toevoegen** om te definiëren welke verbindingen geen toestemming hebben om gegevens te wijzigen.

6. Ga naar het veld **Computernaam/Account** en typ de naam van de computer en het account van de machine waarop de beveiligingsagent is geïnstalleerd. Bijvoorbeeld: `MijnComputer\Testgebruiker`.
7. Ga naar het veld **Hostnaam** en typ de hostnaam van de machine die verbinding mag maken met de machine via de beveiligingsagent.
8. Schakel het selectievakje rechts in om de definitie van de verbinding op te slaan.
9. Klik op **Gereed**.

Cryptomining-malware kan leiden tot mindere prestaties van nuttige toepassingen, een hogere elektriciteitsrekening, systeemcrashes en zelfs schade aan de hardware als gevolg van misbruik. De functie **Detectie van cryptomining-processen** beschermt uw apparaten tegen crytomining-malware en voorkomt niet-goedgekeurd gebruik van computerresources.

Beheerders kunnen **Detectie van cryptomining-processen** inschakelen zonder **Active Protection** in te schakelen. Standaardinstelling: **Ingeschakeld**.

Opmerking
Detectie van cryptomining-processen wordt niet ondersteund voor Linux.

Netwerkmapbescherming configureren:

1. Ga naar het venster **Beschermingsschema maken** en vouw de module **Antivirus- en antimalwarebeveiliging** uit.
2. Klik op **Detectie van cryptomining-processen**.
3. Gebruik de schakelaar **Cryptomining-processen detecteren** om de functie in of uit te schakelen.
4. Selecteer wat u wilt doen met processen die verdacht worden van cryptomining-activiteiten:

   Standaardinstelling: **Het proces stoppen**

   - **Alleen melden**: er wordt een waarschuwing gegenereerd.
   - **Het proces stoppen**: er wordt een waarschuwing gegenereerd en het proces wordt gestopt.
5. Klik op **Gereed** om de geselecteerde opties toe te passen op uw beschermingsschema.

Met Uitsluitingen voor bescherming kunt u fout-positieven elimineren wanneer een vertrouwd programma als ransomware of malware wordt beschouwd. U kunt vertrouwde en geblokkeerde items definiëren door ze toe te voegen aan de lijst met uitsluitingen voor bescherming.

In de lijst met vertrouwde items kunt u bestanden, processen en mappen toevoegen zodat ze als veilig worden beschouwd in het systeem en om toekomstige detecties hiervan te voorkomen.

In de lijst met geblokkeerde items kun je processen en hashes toevoegen. Deze optie garandeert dat deze processen worden geblokkeerd en dat uw workload veilig is.

Item uitgesloten voor beschermin g	Geblokkeerd	Vertrouwd
Hash	Wanneer een hash wordt toegevoegd aan de lijst met geblokkeerde items, wordt het proces automatisch gestopt op basis van de opgegeven hash. Wanneer u bijvoorbeeld de MD5-hash 938c2cc0dcc05f2b68c4287040cfcf71 toevoegt, wordt het aan deze hash gekoppelde proces geblokkeerd.	Wanneer een hash wordt toegevoegd aan de lijst met vertrouwde items, worden de betreffende processen, op basis van de opgegeven hash, automatisch genegeerd bij controles. Wanneer u bijvoorbeeld de MD5-hash 938c2cc0dcc05f2b68c4287040cfcf71 toevoegt, wordt het aan deze hash gekoppelde proces vertrouwd en uitgesloten van controles.
Proces	Wanneer een proces wordt toegevoegd aan de lijst met geblokkeerde items, worden de betreffende processen automatisch gecontroleerd en altijd geblokkeerd. Als u bijvoorbeeld het pad C:\Users\user1\application\nppInstall er.exe toevoegt aan de lijst met geblokkeerde items, wordt dit specifieke proces geblokkeerd en kan het niet worden gestart wanneer u het probeert te openen.	Wanneer een proces wordt toegevoegd aan de lijst met vertrouwde items, worden de betreffende processen automatisch uitgesloten van controles. **Opmerking** Processen ondertekend door Microsoft worden altijd vertrouwd. Als u bijvoorbeeld het pad C:\Users\user1\application\nppInstall er.exe toevoegt, wordt dit specifieke proces uitgesloten van controles en wordt het niet gecontroleerd door antivirusprogramma's.
Bestand/ma p		Wanneer een bestand of map wordt toegevoegd aan de lijst met vertrouwde items, worden die bestanden of mappen altijd als veilig beschouwd en worden ze niet gescand of gecontroleerd.

De items opgeven die altijd worden vertrouwd:

1. Open het beschermingsschema.
2. Vouw de module **Antivirus- en antimalwarebeveiliging** uit.
3. Selecteer de optie **Uitsluitingen**.
   Het venster **Uitsluitingen voor bescherming** wordt geopend.

4. Klik in het gedeelte **Vertrouwde items** op **Toevoegen** en selecteer een of meer van de beschikbare opties:
   - Als u bestanden, mappen of processen wilt vertrouwen, selecteert u de optie '**Bestand/map/proces**. Het venster **Bestand/map/proces toevoegen** wordt geopend.
     - Ga naar het veld **Bestand/proces/map** en voer het pad voor elk proces, map of bestand in op een nieuwe regel. Voer in het gedeelte **Beschrijving** een korte beschrijving in, zodat u uw wijziging kunt herkennen in de lijst met vertrouwde items.
     - Schakel het selectievakje **Toevoegen als bestand/map** in om het bestand/de map te vertrouwen.
       Voorbeeld van een mapbeschrijving: D:\map\, /home/Map/map2, F:\
     - Schakel het selectievakje **Toevoegen als proces** in om een proces te vertrouwen. De geselecteerde processen worden uitgesloten van controles.

       Opmerking
       Geef het volledige pad naar het uitvoerbare bestand voor het proces op. Het pad begint met de stationsletter. Bijvoorbeeld `C:\Windows\Temp\er76s7sdkh.exe`.

       Opmerking
       Lokale netwerkpaden worden ondersteund. bijvoorbeeld: \\localhost\folderpath\file.exe

   - Selecteer de optie **Hash** om MD5-hashes toe te voegen aan de lijst met vertrouwde items. Het venster **Hash toevoegen** wordt geopend.
     - Hier kunt u MD5-hashes op afzonderlijke regels invoegen, zodat deze als vertrouwd worden opgenomen in de lijst Uitsluitingen voor bescherming. Cyber Protection gebruikt deze hashes om de processen die worden beschreven door de MD5-hashes, uit te sluiten van controles.

Standaardinstelling: Standaard worden geen uitsluitingen gedefinieerd.

De items opgeven die altijd worden geblokkeerd:

1. Open het beschermingsschema.
2. Vouw de module **Antivirus- en antimalwarebeveiliging** uit.
3. Selecteer de optie **Uitsluitingen voor bescherming**. Het venster **Uitsluitingen voor bescherming** wordt geopend.

   Klik in het gedeelte **Geblokkeerde items** op **Toevoegen** en selecteer een of meer van de beschikbare opties:
   - Als u processen wilt blokkeren, selecteert u de optie **Proces**. Het venster **Proces toevoegen** wordt geopend.
     - Ga naar het veld **Proces** en voer het pad voor elk proces in op een nieuwe regel. Voer in het veld **Beschrijving** een korte beschrijving in, zodat u uw wijziging kunt herkennen in de lijst met geblokkeerde items.

Opmerking
Deze processen kunnen niet worden gestart wanneer Active Protection is ingeschakeld op de machine.

- Als u hashes wilt blokkeren, selecteert u de optie **Hash**. Het venster **Hash toevoegen** wordt weergegeven.
  - Ga naar het veld **Hash** en voer de hash voor elk proces in op een nieuwe regel. Voer in het veld **Beschrijving** een korte beschrijving in, zodat u uw wijziging kunt herkennen in de lijst met geblokkeerde items.

Standaardinstelling: Standaard worden geen uitsluitingen gedefinieerd.

Jokertekens

U kunt de jokertekens * en ? gebruiken als u een map opgeeft. Het sterretje (*) vervangt nul of meer tekens. Het vraagteken (?) vervangt precies één teken. Omgevingsvariabelen, zoals `%AppData%`, kunnen niet worden gebruikt.

U kunt een jokerteken (*) gebruiken om items toe te voegen aan de uitsluitingslijsten.

- Jokertekens kunnen in het midden of aan het einde van een beschrijving worden gebruikt.

Voorbeelden van geaccepteerde jokertekens in beschrijvingen:

C:*.pdf

D:\folders\file.*

C:\Users*\AppData\Roaming

- Jokertekens kunnen niet aan het begin van een beschrijving worden gebruikt.

Voorbeelden van niet-geaccepteerde jokertekens in beschrijvingen:

*.docx

*:\folder\

Variabelen

U kunt ook variabelen gebruiken om items toe te voegen aan de lijst Uitsluitingen voor bescherming, met de volgende beperkingen:

- Voor Windows worden alleen SYSTEM-variabelen ondersteund. Gebruikersspecifieke variabelen, bijvoorbeeld %USERNAME%, %APPDATA%, worden niet ondersteund. Variabelen met {username} worden niet ondersteund. Zie https://ss64.com/nt/syntax-variables.html voor meer informatie.
- Omgevingsvariabelen worden niet ondersteund voor macOS.
- Omgevingsvariabelen worden niet ondersteund voor Linux.

Voorbeelden van ondersteunde indelingen:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Beschrijving

U kunt het veld **Beschrijving** gebruiken om notities te maken over de uitsluitingen die u hebt toegevoegd in de lijst met uitsluitingen voor bescherming. Enkele suggesties voor de opmerkingen die u kunt maken:

- Redenen en doeleinden van de uitsluiting.
- Werkelijke bestandsnaam van een hash-uitsluiting.
- Tijdstempels.

Als er meerdere items zijn toegevoegd aan één vermelding, kan er slechts 1 opmerking worden vastgelegd voor de meerdere items.

URL-filtering

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Malware wordt vaak verspreid door schadelijke of geïnfecteerde sites, waarbij gebruik wordt gemaakt van de zogenaamde Drive-by-download-infectiemethode.

Met de functie URL-filtering kunt u uw machines beschermen tegen bedreigingen via internet, zoals malware en phishing. U kunt uw organisatie beschermen door gebruikerstoegang tot websites met mogelijk schadelijke inhoud te blokkeren.

Met URL-filtering kunt u ook het webgebruik beheren om te voldoen aan de externe voorschriften en het interne bedrijfsbeleid. U kunt de toegang tot de websites configureren, afhankelijk van de categorie waarop ze betrekking hebben. URL-filtering ondersteunt momenteel 44 websitecategorieën en maakt het mogelijk om de toegang hiertoe te beheren.

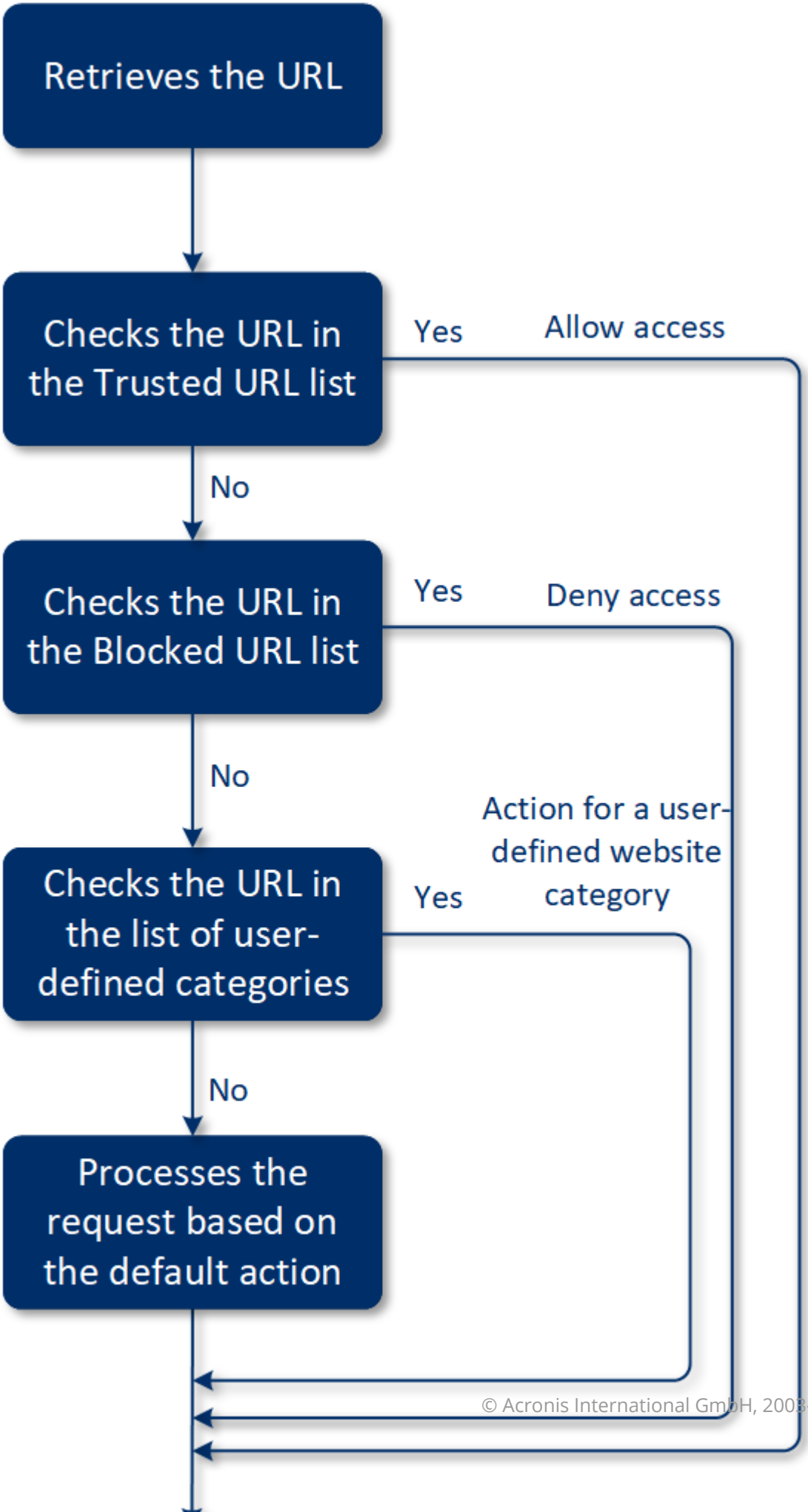
Momenteel worden de HTTP/HTTPS-verbindingen op Windows-machines gecontroleerd door de beveiligingsagent.

De functie URL-filtering werkt alleen als er een internetverbinding is.

Opmerking
Mogelijke compatibiliteitsproblemen met builds 15.0.26692 (release C21.03 HF1) en eerder van de beveiligingsagent worden voorkomen doordat de functionaliteit voor URL-filtering automatisch wordt uitgeschakeld als een andere antivirusoplossing wordt gedetecteerd, of als de Windows Security Center-service niet aanwezig is op het systeem.
In latere beveiligingsagents zijn de compatibiliteitsproblemen opgelost, zodat URL-filtering altijd is ingeschakeld volgens het beleid.

Zo werkt het

Een gebruiker voert een URL-link in een browser in. De interceptor krijgt de link en stuurt deze naar de beveiligingsagent. De agent haalt de URL op, parseert deze en controleert vervolgens het resultaat. De interceptor leidt een gebruiker om naar de pagina met een bericht over beschikbare acties om handmatig naar de gevraagde pagina te gaan.

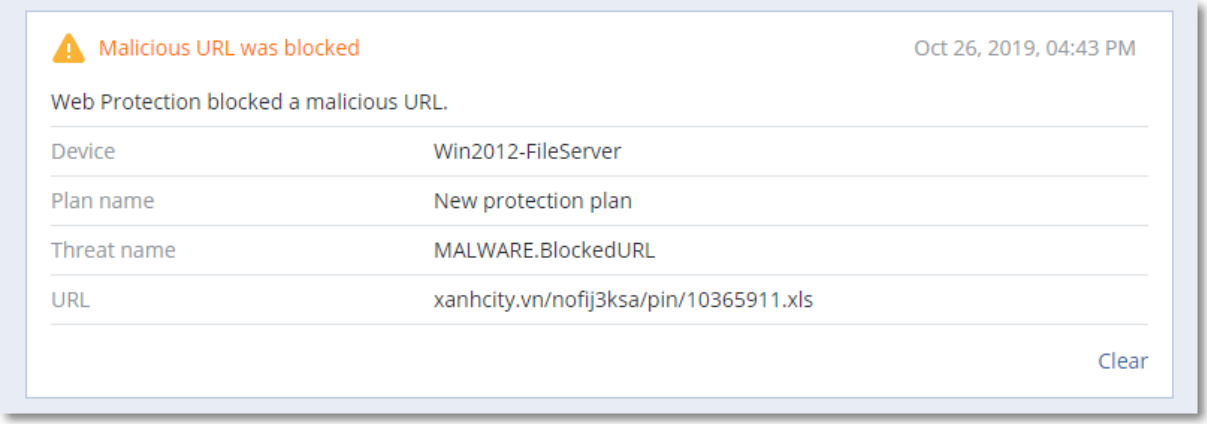


Workflow voor de configuratie van URL-filtering

Over het algemeen bestaat de configuratie voor URL-filtering uit de volgende stappen:

1. U maakt een beschermingsschema terwijl de module **URL-filtering** is ingeschakeld.
2. Geef de instellingen voor URL-filtering op (zie hieronder).
3. Wijs het beveiligingsschema toe aan de machines.

Als u wilt controleren welke URL's zijn geblokkeerd, gaat u naar **Controle** > **Waarschuwingen**.



Instellingen voor URL-filtering

De volgende instellingen kunnen worden opgegeven voor de module URL-filtering.

Toegang via schadelijke website

Geef op welke actie wordt uitgevoerd wanneer een gebruiker een schadelijke website opent:

- **Alleen melden**: er wordt een waarschuwing gegenereerd over het proces met verdachte ransomwareactiviteit.
- **Blokkeren**: blokkeert de toegang tot de schadelijke website. De gebruiker heeft geen toegang tot de website en er wordt een waarschuwing gegenereerd.
- **Altijd vragen aan gebruiker**: vraagt de gebruiker of deze toch wil doorgaan naar de website of terug wil gaan.

Categorieën om te filteren

Er zijn 44 websitecategorieën waarvoor u toegang kunt configureren:

- **Toestaan**: toegang tot websites voor de geselecteerde categorie toestaan.
- **Weigeren**: toegang tot websites voor de geselecteerde categorie weigeren.

Standaard zijn alle categorieën toegestaan.

Alle meldingen voor geblokkeerde URL's per categorie weergeven: indien deze optie is ingeschakeld, worden alle meldingen weergegeven in het vak voor geblokkeerde URL's per categorie. Als een website meerdere subdomeinen heeft, worden ook daarvoor meldingen gegenereerd, dus dit kan resulteren in een groot aantal meldingen.

In de onderstaande tabel vindt u beschrijvingen van de categorieën:

	Websitecategorie	Beschrijving
1	**Reclame**	Deze categorie omvat domeinen waarvan het belangrijkste doel is om advertenties weer te geven.
2	**Prikborden**	Deze categorie omvat forums, discussieborden en websites van het type vraag-antwoord. Deze categorie omvat niet de specifieke gedeelten van bedrijfswebsites waar klanten vragen stellen.
3	**Persoonlijke websites**	Deze categorie omvat persoonlijke websites en alle typen blogs: individuele blogs, groepsblogs en bedrijfsblogs. Een blog is een dagboek gepubliceerd op internet. Het bestaat uit items ('posts'), meestal weergegeven in omgekeerde chronologische volgorde, zodat de meest recente post als eerste wordt getoond.
4	**Zakelijke/bedrijfswebsites**	Dit is een brede categorie die bedrijfswebsites omvat die meestal niet tot een andere categorie behoren.
5	**Computersoftware**	Deze categorie omvat websites die computersoftware aanbieden, meestal open-source, freeware en shareware. Omvat ook sommige online softwarewinkels.
6	**Geneesmiddelen**	Deze categorie omvat websites over medicijnen/alcohol/rookwaar en websites met discussies over het gebruik of de verkoop van (legale) medicijnen of toebehoren, alcohol of tabaksproducten. Let op: illegale drugs worden weergegeven bij de categorie Verdovende middelen.
7	**Onderwijs**	Deze categorie omvat websites die behoren tot officiële onderwijsinstellingen, inclusief websites buiten het .edu-domein. Omvat ook educatieve websites, zoals een encyclopedie.
8	**Entertainment**	Deze categorie omvat websites met informatie over artistieke activiteiten en musea en websites met recensies en beoordelingen van inhoud zoals films, muziek of kunst.
9	**Bestanden delen**	Deze categorie omvat websites voor het delen van bestanden waar een gebruiker bestanden kan uploaden en delen met anderen. Omvat ook websites voor het delen van torrents en torrent-trackers.
10	**Financiën**	Deze categorie omvat websites van alle banken over de hele wereld die online toegang bieden. Omvat ook sommige kredietverenigingen en andere financiële instellingen. Lokale

		banken zijn echter mogelijk uitgesloten.
11	**Gokken**	Deze categorie omvat gokwebsites. Dit zijn websites van het type 'online casino' of 'online loterij', waar doorgaans betaling is vereist is voordat een gebruiker kan gokken om geld in online roulette, poker, blackjack en dergelijke spellen. Sommige zijn legitiem, dat wil zeggen dat er een kans is om te winnen. Andere zijn frauduleus, dat wil zeggen dat er geen kans is om te winnen. Ook worden websites gedetecteerd die 'tips en cheats' bevatten en beschrijvingen geven van manieren om geld te verdienen op goksites en online loterijwebsites.
12	**Games**	Deze categorie omvat websites die online games aanbieden, meestal gebaseerd op Adobe Flash- of Java-applets. Omvat zowel gratis games als games waarvoor een abonnement is vereist, maar casinoachtige websites worden gedetecteerd in de categorie Gokken. Deze categorie omvat niet: • Officiële websites van bedrijven die videogames ontwikkelen (tenzij ze online games produceren) • Discussiewebsites waar games worden besproken • Websites waar niet-online games kunnen worden gedownload (sommige hiervan worden weergegeven bij de categorie Illegaal) • Games waarvoor een gebruiker een uitvoerbaar bestand moet downloaden en uitvoeren, zoals World of Warcraft, kunnen op andere manieren worden voorkomen, bijvoorbeeld met een firewall
13	**Overheid**	Deze categorie omvat websites van de overheid, zoals overheidsinstellingen, ambassades en kantoorwebsites.
14	**Hacking**	Deze categorie omvat websites die tools, artikelen en discussieplatforms voor hackers bieden. Omvat ook websites die aanvallen voor bekende platforms aanbieden om het hacken van Facebook- of Gmail-accounts te vergemakkelijken.
15	**Illegale activiteiten**	Deze categorie is een brede categorie die haat, geweld en racisme omvat, en is bedoeld om de volgende categorieën websites te blokkeren: • Websites van terroristische organisaties • Websites met racistische of xenofobische inhoud • Websites die agressieve sporten bespreken en/of geweld promoten
16	**Gezondheid en fitness**	Deze categorie omvat websites van en over medische instellingen, websites met betrekking tot ziektepreventie en -behandeling,

		websites met informatie over of producten voor gewichtsverlies, diëten, steroïden, anabole of HGH-producten, en websites met informatie over plastische chirurgie.
17	**Hobby's**	Deze categorie omvat websites met bronnen over activiteiten die doorgaans worden uitgevoerd in de vrije tijd, zoals verzamelen, kunstnijverheid en fietsen.
18	**Webhosting**	Deze categorie omvat gratis en commerciële websitehostingservices waarmee particuliere gebruikers en organisaties webpagina's kunnen maken en publiceren.
19	**Illegale downloads**	Deze categorie omvat websites over softwarepiraterij, zoals: • peer-to-peer-trackerwebsites (BitTorrent, emule, DC++) tracker-websites waarvan bekend is dat ze helpen bij het verspreiden van auteursrechtelijk beschermde inhoud zonder toestemming van de houder van het auteursrecht • Warez (illegale commerciële software)-websites en -discussieborden • Websites die gebruikers cracks, sleutelgeneratoren en serienummers bieden om het illegaal gebruik van software te vergemakkelijken Sommige van deze websites kunnen ook worden gedetecteerd als pornografie of alcohol/rookwaar, omdat ze vaak advertenties voor porno of alcohol gebruiken om geld te verdienen.
20	**Chatberichten**	Deze categorie omvat instant messaging- en chatwebsites waarmee gebruikers in real time kunnen chatten. Ook yahoo.com en gmail.com worden gedetecteerd, omdat ze allebei een ingebouwde chatservice bevatten.
21	**Banen/werkgelegenheid**	Deze categorie omvat websites met vacaturebanken, advertenties over banen en carrièremogelijkheden, en aggregators van dergelijke diensten. Omvat geen wervingsbureaus of de 'banen'-pagina's op reguliere bedrijfswebsites.
22	**Inhoud voor volwassenen**	Deze categorie omvat inhoud die door de maker van de website is aangeduid als bedoeld voor een volwassen publiek. Omvat uiteenlopende websites, van websites over het Kama Sutra-boek en websites over seksuele voorlichting tot hardporno.
23	**Verdovende middelen**	Deze categorie omvat websites die informatie delen over recreatieve en illegale drugs. Deze categorie omvat ook websites over de ontwikkeling of het telen van drugs.
24	**Nieuws**	Deze categorie omvat nieuwswebsites die tekst- en videonieuws bieden. Omvat in principe zowel wereldwijde als lokale nieuwswebsites, maar mogelijk met uitzondering van sommige kleine lokale nieuwssites.

25	**Online dating**	Deze categorie omvat online datingsites, zowel betaald als gratis, waar gebruikers naar andere mensen kunnen zoeken via bepaalde criteria. Ze kunnen ook hun profielen posten zodat anderen deze kunnen doorzoeken. Deze categorie bevat zowel gratis als betaalde online datingwebsites. Omdat de meeste populaire sociale netwerken kunnen worden gebruikt als online datingwebsites, worden ook enkele populaire websites zoals Facebook gedetecteerd in deze categorie. We raden aan om deze categorie te gebruiken in combinatie met de categorie Sociale netwerken.
26	**Online betalingen**	Deze categorie omvat websites die online betalingen of overboekingen aanbieden. Populaire betalingswebsites zoals PayPal of Moneybookers worden gedetecteerd. Ook is er heuristische detectie van de webpagina's op reguliere websites waar creditcardgegevens worden gevraagd, zodat verborgen, onbekende of illegale online winkels kunnen worden opgespoord.
27	**Foto's delen**	Deze categorie omvat websites voor het delen van foto's waarvan het primaire doel is om gebruikers foto's te laten uploaden en delen.
28	**Online winkels**	Deze categorie omvat bekende online winkels. Een website wordt als een online winkel beschouwd als deze goederen of diensten online verkoopt.
29	**Pornografie**	Deze categorie omvat websites met erotische inhoud en pornografie. Omvat zowel betaalde als gratis websites. Omvat websites met afbeeldingen, verhalen en video's, en ook pornografische inhoud op websites met gemengde inhoud wordt gedetecteerd.
30	**Portals**	Deze categorie omvat websites die informatie uit meerdere bronnen en verschillende domeinen samenvoegen en die gewoonlijk functies bieden zoals zoekmachines, e-mail, nieuws en entertainmentinformatie.
31	**Radio**	Deze categorie omvat websites die internetstreamingdiensten voor muziek aanbieden, zoals online radiostations en streamingwebsites voor gratis of betaalde audio-inhoud.
32	**Religie**	Deze categorie omvat websites die religie of een sekte promoten. Omvat ook de discussieforums over een of meerdere religies.
33	**Zoekprogramma's**	Deze categorie omvat websites van zoekmachines, zoals Google, Yahoo en Bing.
34	**Sociale netwerken**	Deze categorie omvat websites van sociale netwerken. Omvat MySpace.com, Facebook.com, Bebo.com, enzovoort. Gespecialiseerde sociale netwerken, zoals YouTube.com, worden

		echter vermeld in de categorie Video/Foto.
35	**Sport**	Deze categorie omvat websites met sportinformatie, nieuws en zelfstudies.
36	**Zelfdoding**	Deze categorie omvat websites die zelfdoding promoten, aanbieden of bepleiten. Omvat geen klinieken voor zelfmoordpreventie.
37	**Tabloids**	Deze categorie is voornamelijk bedoeld voor websites met softporno en roddels over beroemdheden. Subcategorieën die hier worden vermeld, zijn mogelijk van toepassing voor veel van de nieuwswebsites in tabloidstijl. Detectie voor deze categorie is ook gebaseerd op heuristiek.
38	**Tijdverdrijf**	Deze categorie omvat websites waar bezoekers vaak veel tijd doorbrengen. Dit kunnen websites zijn uit andere categorieën, zoals sociale netwerken of entertainment.
39	**Reizen**	Deze categorie omvat websites met reisaanbiedingen en reisbenodigdheden, en recensies en beoordelingen van reisbestemmingen.
40	**Video's**	Deze categorie omvat websites die diverse video's of foto's hosten, geüpload door gebruikers of geleverd door diverse inhoudsproviders. Omvat websites zoals YouTube, Metacafe, Google Video en fotowebsites zoals Picasa of Flickr. Ook video's die zijn ingesloten in andere websites of blogs, worden gedetecteerd.
41	**Gewelddadige cartoons**	Deze categorie omvat websites die gewelddadige cartoons of manga's bespreken, delen en aanbieden en die mogelijk ongepast zijn voor minderjarigen vanwege geweld, expliciete taal of seksuele inhoud. Deze categorie omvat niet de websites die reguliere cartoons aanbieden zoals 'Tom en Jerry'.
42	**Wapens**	Deze categorie omvat websites die wapens aanbieden voor verkoop of ruil, fabricage of gebruik. Omvat ook de hulpbronnen voor de jacht en het gebruik van luchtdrukwapens, BB-wapens en contactwapens.
43	**E-mail**	Deze categorie omvat websites die e-mailfunctionaliteit bieden als webtoepassing.
44	**Webproxy**	Deze categorie omvat websites die webproxyservices aanbieden. Dit zijn websites van het type 'browser in een browser': wanneer een gebruiker een webpagina opent, de gevraagde URL in een formulier invoert en op 'Verzenden' klikt. De webproxysite downloadt de werkelijke pagina en geeft deze weer in de

		gebruikersbrowser. Hier zijn redenen waarom dit type wordt gedetecteerd (en mogelijk moet worden geblokkeerd): • Voor anoniem browsen. Aanvragen voor de bestemmingswebserver worden gedaan vanaf de proxywebserver, dus alleen het IP-adres is zichtbaar en als de serverbeheerders de gebruiker traceren, eindigt de tracering op de webproxy, waar mogelijk logboeken worden bijgehouden om de oorspronkelijke gebruiker te lokaliseren. • Voor locatievervalsing (spoofing). IP-adressen van gebruikers worden vaak gebruikt voor het profileren van de service op basis van de bronlocatie (sommige websites van de nationale overheid zijn mogelijk alleen beschikbaar vanaf lokale IP-adressen), en het gebruik van die services kan gebruikers helpen hun echte locatie te vervalsen. • Voor toegang tot verboden inhoud. Als een eenvoudig URL-filter wordt gebruikt, worden alleen de webproxy-URL's weergegeven en niet de daadwerkelijke servers die de gebruiker bezoekt. • Voor omzeiling van bedrijfsbewaking. Een zakelijk beleid vereist mogelijk toezicht op het internetgebruik van werknemers. Door alles te benaderen via een webproxy kan een gebruiker ontsnappen aan het toezicht zodat niet de juiste informatie wordt geleverd. Aangezien de SDK de HTML-pagina (indien aanwezig) analyseert, en niet alleen URL's, kan de SDK voor sommige categorieën nog steeds de inhoud detecteren. Andere redenen kunnen echter niet worden vermeden door alleen de SDK te gebruiken.

Uitsluitingen van URL's

URL's die bekend staan als veilig, kunnen worden toegevoegd aan de lijst met vertrouwde domeinen. URL's die een bedreiging inhouden, kunnen worden toegevoegd aan de lijst met geblokkeerde domeinen.

De URL's opgeven die altijd worden vertrouwd of geblokkeerd:

1. Klik op **Uitsluitingen van URL's** in de module URL-filtering van een beschermingsschema.
   Het venster **Uitsluitingen van URL's** wordt geopend.
   De volgende opties worden weergegeven:

Vertrouwde items: klik op **Toevoegen** en selecteer een van de beschikbare opties:

- **Domein**: wanneer u deze optie selecteert, wordt het venster **Domein toevoegen** geopend.
  - Voer in het veld **Domein** elk domein in op een nieuwe regel. Voer in het veld **Beschrijving** een korte beschrijving in, zodat u uw wijziging kunt herkennen in de lijst met vertrouwde items.

- **Proces**: wanneer u deze optie selecteert, wordt het venster **Proces toevoegen** weergegeven.
  - Ga naar het veld **Proces** en voer het pad voor elk proces in op een nieuwe regel. Voer in het gedeelte **Beschrijving** een korte beschrijving in, zodat u uw wijziging kunt herkennen in de lijst met vertrouwde items.

Geblokkeerde items: klik op **Toevoegen**. Het venster **Domein toevoegen** wordt weergegeven.

Voer in het veld **Domein** elk domein in op een nieuwe regel. Voer in het veld **Beschrijving** een korte beschrijving in, zodat u uw wijziging kunt herkennen in de lijst met geblokkeerde items.

Opmerking
Lokale netwerkpaden worden ondersteund. Bijvoorbeeld: \\localhost\folderpath\file.exe.

Beschrijving

U kunt het veld **Beschrijving** gebruiken om notities te maken over de uitsluitingen die u hebt toegevoegd in de lijst Uitsluitingen van URL's. Enkele suggesties voor de notities die u kunt maken:

- Redenen en doeleinden van de uitsluiting.
- Tijdstempels.

Als er meerdere items zijn toegevoegd aan één vermelding, kan er slechts 1 opmerking worden vastgelegd voor de meerdere items.

Microsoft Defender Antivirus en Microsoft Security Essentials

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Microsoft Defender Antivirus

Microsoft Defender Antivirus is een ingebouwd antimalwareonderdeel van Microsoft Windows dat wordt geleverd vanaf Windows 8.

Met de Microsoft Defender Antivirus-module (WDA) kunt u het Microsoft Defender Antivirus-beveiligingsbeleid configureren en de status ervan volgen via de Cyber Protect-console.

Deze module is van toepassing op de workloads waarop Microsoft Defender Antivirus is geïnstalleerd.

Microsoft Security Essentials

Microsoft Security Essentials is een ingebouwd antimalwareonderdeel van Microsoft Windows dat wordt geleverd bij Windows-versies die ouder zijn dan Windows 8.

Met de Microsoft Security Essentials-module kunt u het beveiligingsbeleid van Microsoft Security Essentials configureren en de status ervan volgen via de Cyber Protect-console.

Deze module is van toepassing op de workloads waarop Microsoft Security Essentials is geïnstalleerd.

De instellingen voor Microsoft Security Essentials zijn vergelijkbaar met de instellingen voor Microsoft Defender Antivirus, maar u kunt geen realtime bescherming configureren en geen uitsluitingen definiëren via de Cyber Protect-console.

Scan plannen

Geef het schema op voor geplande scans.

Scanmodus:

- **Volledig**: volledige controle van alle bestanden en mappen, inclusief de items die zijn gescand met de snelle scan. De uitvoering hiervan vereist meer machineresources dan de snelle scan.
- **Snel**: een snelle controle van de processen in het geheugen en de mappen waar doorgaans malware wordt aangetroffen. De uitvoering hiervan vereist minder machineresources.

Definieer het tijdstip en de dag van de week waarop de scan wordt uitgevoerd.

Dagelijkse snelle scan: definieer de tijd voor de dagelijkse snelle scan.

U kunt de volgende opties instellen, afhankelijk van uw behoeften:

De geplande scan starten wanneer de machine aan staat maar niet in gebruik is

Controleren op de nieuwste virus- en spywaredefinities voordat een geplande scan wordt uitgevoerd

CPU-gebruik beperken tijdens de scan tot

Zie https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings voor meer informatie over de instelling voor Microsoft Defender Antivirus

Standaardacties

Definieer de standaardacties die moeten worden uitgevoerd voor de gedetecteerde bedreigingen van verschillende ernstniveaus:

- **Opschonen**: de gedetecteerde malware in een workload opschonen.
- **Quarantaine**: de gedetecteerde malware in de quarantainemap plaatsen maar niet verwijderen.
- **Verwijderen**: de gedetecteerde malware verwijderen uit een workload.
- **Toestaan**: de gedetecteerde malware niet verwijderen of in quarantaine plaatsen.
- **Door de gebruiker gedefinieerd**: de gebruiker wordt gevraagd elke actie moet worden uitgevoerd voor de gedetecteerde malware.

- **Geen actie**: er worden geen acties ondernomen.
- **Blokkeren**: de gedetecteerde malware blokkeren.

Zie https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings voor meer informatie over de standaardinstellingen voor acties voor Microsoft Defender Antivirus

Realtime bescherming

Realtime bescherming: schakel dit in om malware te detecteren en te voorkomen dat de malware wordt geïnstalleerd of uitgevoerd in workloads.

Alle downloads scannen: indien geselecteerd, worden alle gedownloade bestanden en bijlagen gescand.

Gedragscontrole inschakelen: indien geselecteerd, wordt gedragscontrole ingeschakeld.

Netwerkbestanden scannen: indien geselecteerd, worden netwerkbestanden gescand.

Volledige scan toestaan voor toegewezen netwerkstations: indien geselecteerd, worden toegewezen netwerkstations volledig gescand.

E-mailscans toestaan: indien geselecteerd, parseert de engine de postvak- en e-mailbestanden, al naargelang de indeling, om de teksten van e-mails en bijlagen te analyseren.

Zie https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings voor meer informatie over de realtime beschermingsinstellingen voor Microsoft Defender Antivirus

Geavanceerd

Geef de geavanceerde scaninstellingen op:

- **Archiefbestanden scannen**: gearchiveerde bestanden, zoals .zip- of .rar-bestanden, opnemen in de scan.
- **Verwisselbare stations scannen**: verwisselbare stations scannen tijdens volledige scans.
- **Een systeemherstelpunt maken**: als een belangrijk bestand of een registervermelding ten onrechte wordt verwijderd als 'positief', dan kunt u hiermee een herstelbewerking uitvoeren vanaf een herstelpunt.
- **In quarantaine geplaatste bestanden verwijderen na**: hiermee definieert u de periode waarna de in quarantaine geplaatste bestanden worden verwijderd.
- **Bestandsvoorbeelden automatisch verzenden wanneer verdere analyse nodig is:**
  - **Altijd vragen**: u wordt om bevestiging gevraagd voordat het bestand wordt verzonden.
  - **Veilige voorbeelden automatisch verzenden**: de meeste voorbeelden worden automatisch verzonden, behalve bestanden die mogelijk persoonlijke informatie bevatten. Voor dergelijke bestanden is extra bevestiging vereist.
  - **Alle voorbeelden automatisch verzenden**: alle monsters worden automatisch verzonden.

- **Windows Defender Antivirus GUI uitschakelen**: indien geselecteerd, is de WDA-gebruikersinterface niet beschikbaar voor een gebruiker. U kunt het WDA-beleid beheren via de Cyber Protect-console.
- **MAPS (Microsoft Active Protection Service)**: een online community die u helpt kiezen hoe u moet reageren op potentiële bedreigingen.
  - **Ik wil niet deelnemen aan MAPS**: er wordt geen informatie over de gedetecteerd software verzonden naar Microsoft.
  - **Basislidmaatschap**: er wordt basisinformatie over de gedetecteerde software verzonden naar Microsoft.
  - **Geavanceerd lidmaatschap**: er wordt meer gedetailleerde informatie over de gedetecteerde software verzonden naar Microsoft.

  Zie https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/ voor meer informatie

Zie https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings voor meer informatie over de geavanceerde instellingen voor Microsoft Defender Antivirus

Uitsluitingen

U kunt de volgende bestanden en mappen definiëren die moeten worden uitgesloten van scans:

- **Processen**: elk bestand waarvoor het gedefinieerde proces lees- of schrijftoegang heeft, wordt uitgesloten van scans. U moet een volledig pad definiëren naar het uitvoerbare bestand van het proces.
- **Bestanden en mappen**: de opgegeven bestanden en mappen worden uitgesloten van scans. U moet een volledig pad naar een map of bestand definiëren of de bestandsextensie definiëren.

Zie https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings voor meer informatie over de uitsluitingsinstellingen voor Microsoft Defender Antivirus

Firewallbeheer

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Met firewallbeheer kunt u eenvoudig firewallinstellingen configureren voor beschermde workloads.

Deze functionaliteit in Cyber Protect wordt geleverd via een ingebouwd Microsoft Defender Firewall-onderdeel van Microsoft Windows. Microsoft Defender Firewall blokkeert ongeautoriseerd netwerkverkeer van of naar uw workloads.

Firewallbeheer is van toepassing op de workloads waarop Microsoft Defender Firewall is geïnstalleerd.

Ondersteunde Windows-besturingssystemen

De volgende Windows-besturingssystemen worden ondersteund voor het firewallbeheer:

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server wordt niet ondersteund.

Firewallbeheer in- en uitschakelen

U kunt firewallbeheer inschakelen wanneer u een beschermingsschema maakt. U kunt een bestaand beschermingsschema wijzigen om firewallbeheer in of uit te schakelen.

Firewallbeheer in- of uitschakelen:

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Voer een van de volgende handelingen uit om het deelvenster voor het beschermingsschema te openen:
   - Als u een nieuw beschermingsschema wilt maken, selecteert u een machine om te beschermen en klikt u vervolgens op **Beschermen** en op **Schema maken**.
   - Als u een bestaand beschermingsschema wilt wijzigen, selecteert u een beschermde machine, klikt u op **Beschermen**, klikt u op de ellips (...) naast de naam van het beschermingsschema en klikt u vervolgens op **Bewerken**.
3. Ga in het deelvenster voor het beschermingsschema naar het gebied **Firewallbeheer** en schakel de optie **Firewallbeheer** in of uit.
4. Voer een van de volgende handelingen uit om uw wijzigingen door te voeren:
   - Als u een beschermingsschema maakt, klikt u op **Maken**.
   - Als u een beschermingsschema bewerkt, klikt u op **Opslaan**.

De **status van Microsoft Defender Firewall** in het gebied **Firewallbeheer** van het deelvenster Beschermingsschema wordt weergegeven als **Aan** of **Uit**, afhankelijk van of u firewallbeheer hebt in- of uitgeschakeld.

Indien gewenst, kunt u het deelvenster voor het beschermingsschema ook openen vanaf het tabblad Beheer. Deze mogelijkheid is echter niet beschikbaar in alle edities van de Cyber Protection-service.

Quarantaine

Quarantaine is een speciale geïsoleerde map op de harde schijf van een machine waar de verdachte bestanden die zijn gedetecteerd door Antivirus- en antimalwarebeveiliging, worden geplaatst om verdere verspreiding van bedreigingen te voorkomen.

Met Quarantaine kunt u verdachte en potentieel gevaarlijke bestanden van alle machines bekijken en beslissen of ze moeten worden verwijderd of hersteld. De in quarantaine geplaatste bestanden worden automatisch verwijderd als de machine uit het systeem wordt verwijderd.

Hoe komen bestanden in de quarantainemap?

1. U configureert het beschermingsschema en definieert In quarantaine plaatsen als standaardactie voor geïnfecteerde bestanden.
2. Het systeem detecteert schadelijke bestanden tijdens geplande scans of scans bij toegang en plaatst deze in de beveiligde map Quarantaine.
3. De quarantainelijst op machines wordt automatisch bijgewerkt.
4. Bestanden worden automatisch opgeschoond uit de quarantainemap na de tijdsperiode die is gedefinieerd in de instelling **In quarantaine geplaatste bestanden verwijderen na** in het beschermingsschema.

In quarantaine geplaatste bestanden beheren

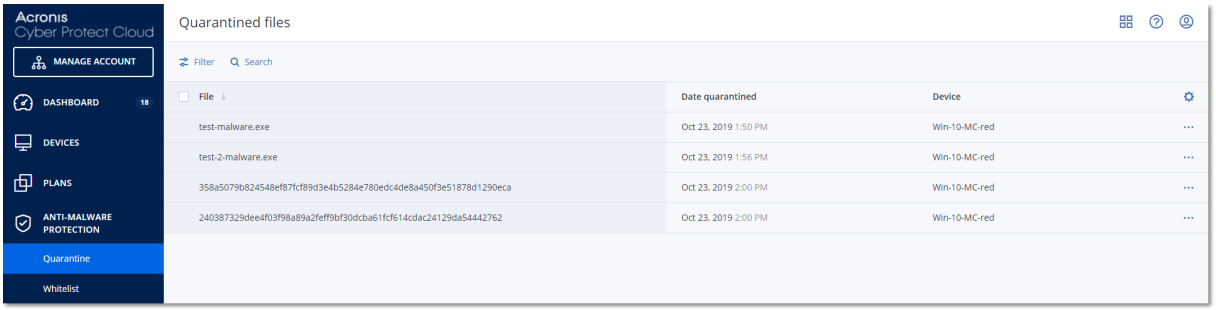
Als u de in quarantaine geplaatste bestanden wilt beheren, gaat u naar **Antimalwarebeveiliging** > **Quarantaine**. U ziet een lijst met de in quarantaine geplaatste bestanden op alle machines.

Naam	Beschrijving
Bestand	De bestandsnaam.
In quarantaine geplaatst op	De datum en tijd waarop het bestand in quarantaine is geplaatst.
Apparaat	Het apparaat waarop het geïnfecteerde bestand is gevonden.
Naam van bedreiging	De naam van de bedreiging.
Beschermingsschema	Het beschermingsschema dat is toegepast om het verdachte bestand in quarantaine te plaatsen.

U kunt twee acties uitvoeren voor in quarantaine geplaatste bestanden:

- **Verwijderen**: een in quarantaine geplaatst bestand definitief verwijderen van alle machines. U kunt alle bestanden met dezelfde bestandshash verwijderen. U kunt alle bestanden met dezelfde bestandshash herstellen. Groepeer de bestanden op hash, selecteer de nodige bestanden en verwijder ze vervolgens.

- **Terugzetten**: Zet een in quarantaine geplaatst bestand zonder wijzigingen terug naar de oorspronkelijke locatie. Als er op dat moment een bestand met dezelfde naam op de oorspronkelijke locatie is, wordt dat bestand overschreven door het teruggezette bestand. Let op: Het teruggezette bestand wordt toegevoegd aan de acceptatielijst en overgeslagen tijdens verdere antimalwarescans.



Quarantainelocatie op machines

De standaardlocatie voor in quarantaine geplaatste bestanden is:

- Voor een Windows-machine: `%programdata%\Acronis\NGMP\quarantine`
- Voor een Mac-machine: `/Library/Application Support/Acronis/NGMP/quarantine`
- Voor een Linux-machine: `/var/lib/Acronis/NGMP/quarantine`

De quarantaineopslag valt onder de zelfverdedigingsbescherming van de serviceprovider.

Aangepaste selfservicemap op aanvraag

U kunt aangepaste mappen selecteren voor de workload en ze rechtstreeks scannen vanuit het contextmenu.

Scan openen met de optie Cyber Protect in het contextmenu

In het geval van workloads waarvoor Antivirus- en antimalware is ingeschakeld in het beschermingsschema, klikt u met de rechtermuisknop op de bestanden/mappen die u wilt scannen.

Opmerking
Deze optie is alleen beschikbaar voor beheerders van de workload.

Witte lijst van het bedrijf

Een antivirusoplossing kan legitieme bedrijfsspecifieke toepassingen mogelijk aanmerken als verdacht. Deze foutpositieve detecties kunnen worden voorkomen door de vertrouwde toepassingen handmatig toe te voegen aan een witte lijst, maar dit is een tijdrovende procedure.

Opmerking
De witte lijst van bedrijven heeft geen invloed op antimalwarescans van back-ups.

Met Cyber Protection kan dit proces worden geautomatiseerd: back-ups worden gescand door de module Antivirus- en antimalwarebeveiliging en de gescande gegevens worden geanalyseerd. Vervolgens worden de betreffende toepassingen op de witte lijst geplaatst om te voorkomen dat ze ten onrechte worden aangemerkt als positief. De verdere scanprestaties van antimalware worden ook verbeterd door de witte lijst van het hele bedrijf.

De witte lijst wordt voor elke klant gemaakt en is alleen gebaseerd op de gegevens van deze klant.

De witte lijst kan worden in- en uitgeschakeld. Wanneer de lijst is uitgeschakeld, worden de aan de lijst toegevoegde bestanden tijdelijk verborgen.

Opmerking
Alleen accounts met een beheerdersrol (bijvoorbeeld Cyber Protection-beheerder, bedrijfbeheerder, partnerbeheerder die optreedt namens een bedrijfbeheerder, eenheidbeheerder) kunnen de witte lijst configureren en beheren. Deze functionaliteit is niet beschikbaar voor een alleen-lezen beheerdersaccount of een gebruikersaccount.

Automatisch toevoegen aan de witte lijst

1. Voer een cloudscan van back-ups uit voor ten minste twee machines. U kunt dit doen door gebruik te maken van de schema's voor back-upscans.
2. Activeer de schakelaar **Witte lijst automatisch genereren** in de instellingen voor de witte lijst.

Handmatig toevoegen aan de witte lijst

U kunt bestanden handmatig toevoegen aan de witte lijst, zelfs wanneer de schakelaar **Witte lijst automatisch genereren** is gedeactiveerd.

1. Ga in de Cyber Protect-console naar **Antimalware beveiliging** > **Witte lijst**.
2. Klik op **Bestand toevoegen**.
3. Geef het pad naar het bestand op en klik vervolgens op **Toevoegen**.

In quarantaine geplaatste bestanden toevoegen aan de witte lijst

U kunt bestanden die in quarantaine zijn geplaatst, toevoegen aan de witte lijst.

1. Ga in de Cyber Protect-console naar **Antimalware beveiliging** > **Quarantaine**.
2. Selecteer een bestand dat in quarantaine is geplaatst en klik vervolgens op **Toevoegen aan witte lijst**.

Instellingen voor witte lijst

Wanneer u de schakelaar **Witte lijst automatisch genereren** activeert, moet u een van de volgende niveaus van heuristische bescherming opgeven:

- **Laag**
  Bedrijfstoepassingen worden pas na lange tijd en veel controles toegevoegd aan de witte lijst.

Dergelijke toepassingen zijn meer vertrouwd. Deze benadering vergroot echter de kans dat fout-positieve items worden gedetecteerd. De criteria om een bestand als schoon en vertrouwd te beschouwen, zijn hoog.

- **Standaard**
  Bedrijfstoepassingen worden aan de witte lijst toegevoegd met het aanbevolen beveiligingsniveau om het aantal ten onrechte als positief aangemerkte detecties te verminderen. De criteria om een bestand als schoon en vertrouwd te beschouwen, zijn gemiddeld.
- **Hoog**
  Bedrijfstoepassingen worden sneller toegevoegd aan de witte lijst om het aantal ten onrechte als positief aangemerkte detecties te verminderen. Hiermee wordt echter niet gegarandeerd dat de software schoon is, want deze kan later nog worden herkend als verdacht of malware. De criteria om een bestand als schoon en vertrouwd te beschouwen, zijn laag.

Details bekijken over items op de witte lijst

U kunt op een item in de witte lijst klikken om er meer informatie over te bekijken en het online te analyseren.

Als u niet zeker bent over een item dat u hebt toegevoegd, kunt u dit controleren met de VirusTotal-analyse. Wanneer u op **Controleren met VirusTotal** klikt, analyseert de site verdachte bestanden en URL's om typen malware te detecteren met behulp van de bestandshash van het item dat u hebt toegevoegd. U kunt de hash bekijken in de string **Bestandshash (MD5)**.

De waarde **Machines** vertegenwoordigt het aantal machines waar een dergelijke hash is gevonden tijdens de back-upscan. Deze waarde wordt alleen ingevuld als een item afkomstig is van Back-upscan of Quarantaine. Dit veld blijft leeg als het bestand handmatig aan de witte lijst is toegevoegd.

Antimalwarescan van back-ups

U kunt een antimalwarescan van back-ups gebruiken om te controleren of uw back-ups vrij zijn van malware en te voorkomen dat geïnfecteerde bestanden worden hersteld. Antimalwarescans worden uitgevoerd door een cloudagent in het Cyber Protection-datacenter. Er worden geen lokale computerresources gebruikt.

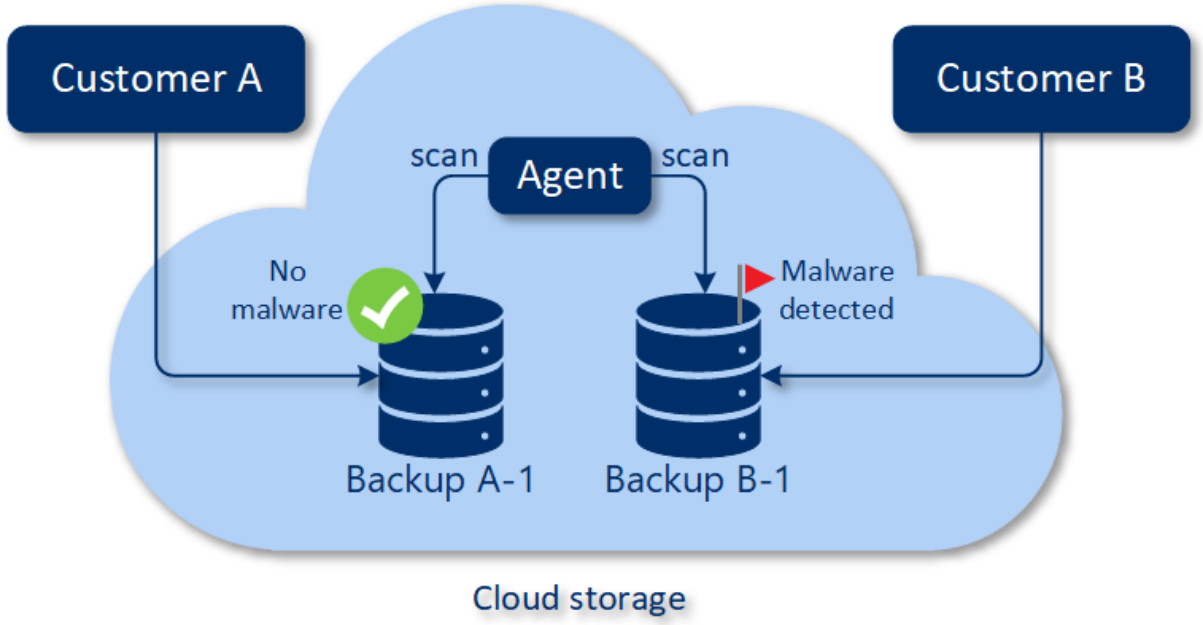
Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Als u een antimalwarescan wilt uitvoeren, moet u een schema voor back-upscans configureren. Zie "Schema's voor back-upscans" (p. 241) voor meer informatie over hoe u dit kunt doen.

In elk schema voor back-upscans wordt een scantaak voor de cloudagent gemaakt en toegevoegd aan een wachtrij, één per datacenter. Scantaken worden verwerkt volgens de volgorde in de wachtrij. De scantijd hangt ook af van de grootte van de back-up. Daarom is er een vertraging tussen het maken van een schema voor back-upscans en het voltooien van de scan.

De back-ups die u hebt geselecteerd om te scannen, kunnen een van de volgende statussen hebben:

- Niet gescand
- Geen malware
- Malware gedetecteerd



U kunt de resultaten van een back-upscan controleren in de widget **Back-upscangegevens (bedreigingen)**. U vindt deze in de Cyber Protect-console, op het tabblad **Monitoring** > **Overzicht**.

Beperkingen

- Antimalwarescan wordt alleen ondersteund voor back-ups van het type **Volledige machine** of **Schijven/volumes** voor de volgende workloads:
  - Windows-machines waarop een beveiligingsagent is geïnstalleerd.
  - Virtuele Windows-machines waarvan een back-up wordt gemaakt op hypervisorniveau (back-up zonder agent) door Agent voor Hyper-V en Agent voor VMware (Windows).

  Antimalwarescan wordt niet ondersteund voor back-ups die zijn gemaakt door virtuele toepassingen, zoals Agent voor VMware (Virtual appliance), Agent for Virtuozzo, Agent for Scale Computing HC3.
- Alleen volumes met het NTFS-bestandssysteem en GPT- of MBR-partities worden gescand.
- Alleen de standaardcloudopslag wordt ondersteund als back-uplocatie. Lokale opslag en cloudopslag die eigendom is van partners, worden niet ondersteund.
- Wanneer u back-ups selecteert om te scannen, kunt u back-upsets selecteren die een CDP-back-up (Continuous data protection) bevatten. Maar alleen de back-ups die geen CDP-back-ups zijn, worden gescand in deze back-upsets. Raadpleeg "Continue gegevensbescherming (CDP)" (p. 435)

voor meer informatie over CDP-back-ups.

- Wanneer u veilig herstel van een volledige machine uitvoert, kunt u een back-upset selecteren die een CDP-back-up bevat. Bij deze herstelbewerking worden de gegevens in de CDP-back-up echter niet gebruikt. Als u de CDP-gegevens wilt herstellen, voert u een aanvullende herstelbewerking voor **Bestanden/mappen** uit.

Werken met de functies van Advanced Protection

Cyber Protect bevat standaard functies tegen de meeste cyberbeveiligingsrisico's. U kunt deze functies gebruiken zonder extra kosten. Daarnaast kunt u geavanceerde functies inschakelen om de bescherming van uw workloads te verbeteren.

- Als er een functie van Advanced Protection beschikbaar is voor u, wordt deze in het beschermingsschema weergegeven met het pictogram voor geavanceerde functies:  .
- Als een functie van geavanceerde bescherming niet beschikbaar is voor u, vraagt u uw beheerder om het vereiste geavanceerde beschermingspakket in te schakelen.
- Als de beheerder u toestemming heeft gegeven om extra beveiligingspakketten te kopen, kunt u ervoor kiezen om de geavanceerde functies in te schakelen. Er wordt een bericht weergegeven en u wordt omgeleid naar een scherm met de mededeling dat er extra facturering van toepassing is.

Opmerking
Als ten minste één functie is ingeschakeld, moet u het bijbehorende Advanced Protection-pakket kopen.

Opmerking
Als alle geavanceerde functies in uw beschermingsschema zijn uitgeschakeld, wordt het bijbehorende Advanced Protection-pakket uitgeschakeld.

Advanced Protection-pakket	Geavanceerde beschermingsfuncties
Advanced Backup	Beschermt uw workloads continu en waarborgt dat zelfs lastminutewijzigingen van uw werk niet verloren gaan. Functies zijn onder andere: • Herstel met één klik • Continue gegevensbescherming • Back-upondersteuning voor Microsoft SQL Server-clusters en Microsoft Exchange-clusters – AlwaysOn-beschikbaarheidsgroepen (AAG) en databasebeschikbaarheidsgroepen (DAG) • Back-upondersteuning voor MariaDB, MySQL, Oracle DB en SAP HANA • Overzicht van gegevensbescherming en compliancerapporten • Gegevensverwerking buiten de host • Back-upfrequentie voor Microsoft 365- en Google Workspace-workloads • Bewerkingen op afstand met opstartmedia • Directe back-up naar Microsoft Azure, Amazon S3 en openbare Wasabi-cloudopslag
Advanced Security + EDR	Beschermt uw workloads continu tegen alle malwarebedreigingen. Functies zijn onder andere:

	• Incidenten beheren op een gecentraliseerde pagina voor incidenten • De reikwijdte en impact van incidenten visualiseren • Aanbevelingen en stappen voor herstel • De bedreigingsfeeds raadplegen om openbaar gemaakte aanvallen op uw workloads te bekijken • Beveiligingsgebeurtenissen bewaren gedurende 180 dagen • Antivirus- en antimalwarebeveiliging met lokale detectie op basis van handtekeningen (met realtime bescherming) • Preventie tegen aanvallen • URL-filtering • Beheer van eindpuntfirewall • Forensische back-up, scannen van back-ups op malware, veilig herstel, acceptatielijst van bedrijf • Schema's voor slimme bescherming (integratie met CPOC-waarschuwingen) • Gecentraliseerde back-upscans voor malware • Extern wissen • Microsoft Defender Antivirus • Microsoft Security Essentials
Advanced Management	Hiermee kunt u beveiligingsproblemen patchen voor de beschermde workloads. Functies zijn onder andere: • Patchbeheer • Schijfintegriteit • Software-inventaris • Foutveilig patchen • Cyber Scripting • Hulp op afstand • Bestandsoverdracht en bestanden delen • Een sessie selecteren om verbinding mee te maken • Workloads bekijken in multiweergave • Verbindingsmodi: Besturen, Alleen bekijken en Verbergen (Gordijn) • Verbinding via de Quick Assist-toepassing • Protocollen voor externe verbindingen: NEAR en Schermdeling van Apple • Sessieopname voor NEAR-verbindingen • Overdracht van momentopname • Rapport Sessiegeschiedenis • 24 controles • Controle op basis van drempelwaarden • Controle op basis van anomalieën
Advanced Data Loss Prevention	Voorkomt het lekken van gevoelige informatie uit de beschermde workloads. Functies zijn on der andere: • Op inhoud gebaseerde preventie van gegevensverlies uit workloads via

	randapparatuur en netwerkcommunicatie • Vooraf ingestelde automatische detectie van persoonsgegevens (PII), beschermde gezondheidsinformatie (PHI), gegevens onder de Informatiebeveiligingsstandaard voor betaalkaartbedrijven (PCI DSS) en documenten in de categorie 'Gemarkeerd als vertrouwelijk' • Automatisch beleid voor preventie van gegevensverlies opstellen, met optionele hulp voor eindgebruikers • Adaptieve handhaving van preventie van gegevensverlies met automatische, op leren gebaseerde beleidsaanpassing • Gecentraliseerde controlelogboekregistratie, waarschuwingen en meldingen voor eindgebruikers, alles vanuit de cloud

Advanced Data Loss Prevention

De Advanced Data Loss Prevention-module maakt gebruik van het beleid voor gegevensstromen om de inhoud en context van gegevensoverdrachten voor beveiligde workloads te analyseren en om te voorkomen dat gevoelige gegevens worden gelekt via randapparatuur of netwerkoverdrachten binnen en buiten het bedrijfsnetwerk.

De functies van Advanced Data Loss Prevention kunnen in elk beschermingsschema voor een klanttenant worden opgenomen als de Protection-service en het Advanced Data Loss Prevention-pakket voor deze klant zijn ingeschakeld.

Voordat u de module Advanced Data Loss Prevention gaat gebruiken, moet u controleren of u de basisconcepten en de logica van het beheer van Advanced DLP-beheer, zoals beschreven in de Basishandleiding, hebt gelezen en begrepen.

U kunt ook het document Technische specificaties bekijken.

Beleid en beleidsregels voor gegevensstromen maken

Het basisprincipe van preventie van gegevensverlies houdt in dat gebruikers van een bedrijfs-IT-systeem alleen gevoelige gegevens mogen verwerken voor zover dat nodig is om hun taken uit te voeren. Alle andere overdrachten van gevoelige gegevens – die niet relevant zijn voor de bedrijfsprocessen – moeten worden geblokkeerd. Het is dus essentieel om een onderscheid te maken tussen bedrijfsgerelateerde en 'rogue' gegevensoverdrachten of gegevensstromen.

Het beleid voor gegevensstromen bevat regels om te bepalen welke gegevensstromen zijn toegestaan en welke niet zijn toegestaan. Met deze regels wordt de ongeoorloofde overdracht van gevoelige informatie voorkomen wanneer de module Preventie van gegevensverlies is ingeschakeld in een beschermingsschema en wordt uitgevoerd in de afdwingingsmodus.

Elke gevoeligheidscategorie in het beleid bevat één standaardregel, gemarkeerd met een sterretje (*) en één of meer expliciete (niet-standaard) regels die de gegevensstromen voor specifieke gebruikers of groepen definiëren. Lees meer over de typen beleidsregels in de Basishandleiding.

Het beleid voor gegevensstromen wordt doorgaans automatisch gemaakt wanneer Advanced Data Loss Prevention wordt uitgevoerd in de observatiemodus. De tijd die nodig is voor het maken van een representatief beleid voor gegevensstromen, bedraagt ongeveer een maand, maar dit kan variëren, afhankelijk van de bedrijfsprocessen in uw organisatie. Het beleid voor gegevensstromen kan ook handmatig worden gemaakt, geconfigureerd of bewerkt door een bedrijfbeheerder of eenheidbeheerder.

Beleid voor gegevensstromen automatisch genereren

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Navigeer naar **Beheer** > **Beschermingsschema's**.
3. Klik op **Schema maken**.
4. Vouw het gedeelte **Preventie van gegevensverlies** uit en klik op de rij **Modus**.
5. Selecteer in het dialoogvenster Modus de optie **Observatiemodus**, en selecteer hoe de gegevensoverdrachten moeten worden verwerkt:

Optie	Beschrijving
Alles toestaan	Alle overdrachten van gevoelige gegevens vanuit gebruikersworkloads worden behandeld als noodzakelijk voor het bedrijfsproces en als veilig. Voor elke gedetecteerde gegevensstroom die niet overeenkomt met een reeds gedefinieerde regel in het beleid, wordt een nieuwe regel gemaakt.
Alles motiveren	Alle overdrachten van gevoelige gegevens vanuit gebruikersworkloads worden behandeld als noodzakelijk voor het bedrijfsproces, maar als riskant. Daarom moet de gebruiker een eenmalige zakelijke motivering geven voor elke onderschepte overdracht van gevoelige gegevens naar een ontvanger of bestemming (zowel binnen als buiten de organisatie) die niet overeenkomt met een eerder gemaakte regel voor gegevensstromen. Wanneer de motivering wordt ingediend, wordt een nieuwe regel voor gegevensstromen gemaakt in het beleid voor gegevensstromen.
Gemengd	De logica 'Alles toestaan' wordt toegepast voor alle interne gegevensstromen van gevoelige gegevens, en de logica 'Alles motiveren' voor alle externe gegevensstromen. **Opmerking** Raadpleeg Automatische doeldetectie voor meer informatie over interne en externe gegevens

6. Sla het beschermingsschema op en pas het toe op de workloads waarvan u gegevens wilt verzamelen om daarmee het beleid te maken.

Opmerking
Gegevenslekken worden niet voorkomen in de observatiemodus.

Beleid voor gegevensstromen handmatig configureren

1. Navigeer in de Cyber Protect-console naar **Bescherming** > **Beleid voor gegevensstromen**.
2. Klik op **Nieuwe regel voor gegevensstromen**.
   Het deelvenster Nieuwe regel voor gegevensstromen wordt uitgevouwen aan de rechterkant.
3. Selecteer een gevoeligheidscategorie, voeg een afzender en een ontvanger toe, en definieer de machtiging voor gegevensoverdracht voor de geselecteerde categorie, afzender en ontvanger.

Optie	Beschrijving
Toestaan	Sta toe dat deze afzender gegevens van deze gevoeligheidscategorie overdraagt aan deze ontvanger.
Uitzondering	Sta niet toe dat deze afzender gegevens van deze gevoeligheidscategorie overdraagt aan deze ontvanger, maar sta wel toe dat de afzender een uitzondering op de regel indient voor een specifieke overdracht. Blokkeer pogingen van deze afzender om gegevens van deze gevoeligheidscategorie over te dragen aan deze ontvanger, en vraag de afzender een uitzondering in te dienen om deze overdracht toe te laten. Wanneer de uitzondering is ingediend, mag de gegevensoverdracht doorgaan. **Belangrijk** Alle volgende gegevensoverdrachten tussen deze afzender en ontvanger voor deze gevoeligheidscategorie worden toegestaan gedurende vijf minuten nadat de uitzondering is ingediend.
Weigeren	Sta niet toe dat deze afzender gegevens van deze gevoeligheidscategorie overdraagt aan deze ontvanger, en sta niet toe dat de afzender een uitzondering op de regel aanvraagt.

4. (Optioneel) Selecteer een actie die moet worden uitgevoerd wanneer de regel wordt geactiveerd.

Actie	Beschrijving
Schrijven in logboek	Sla een gebeurtenisrecord op in het auditlogboek wanneer de regel wordt geactiveerd. Wij raden aan deze actie te selecteren voor regels met de machtiging **Uitzondering**.
Een waarschuwing genereren	Genereer een waarschuwing op het tabblad Cyber Protect **Waarschuwingen** wanneer de regel wordt geactiveerd. Als meldingen zijn ingeschakeld voor de beheerder, wordt er ook een e-mailbericht met de melding verzonden.
De eindgebruiker waarschuwen wanneer een gegevensoverdracht wordt geweigerd	Stel de gebruiker in real time op de hoogte met een waarschuwing op het scherm wanneer de regel wordt geactiveerd.

5. Klik op **Opslaan**.
6. Herhaal de stappen 2 tot 5 om meerdere regels van verschillende gevoeligheidscategorieën en opties te maken en controleer of de resulterende regels overeenkomen met de opties die u hebt geselecteerd.

Structuur van het beleid voor gegevensstromen

In de weergave **Beleid voor gegevensstromen** worden de beleidsregels gegroepeerd op categorie van de gevoelige gegevens die hiermee worden beheerd. De gevoeligheidscategorie-id wordt rechts boven de groep van beleidsregels weergegeven.

- Gevoelig
  - Beschermde gezondheidsinformatie (PHI)
  - Persoonsgegevens (PII)
  - Informatiebeveiligingsstandaard voor betaalkaartbedrijven (PCI DSS),
  - Gemarkeerd als Vertrouwelijk
- Niet-gevoelig

Zie de Basishandleiding voor meer informatie over het concept en de functies van het beleid voor gegevensstromen.

Structuur van de regels

Elke beleidsregel bestaat uit de volgende elementen.

- **Gevoeligheidscategorie**
  - **Beschermde gezondheidsinformatie (PHI)**
  - **Persoonsgegevens (PII)**
  - **Gegevensbeveiligingsnorm van de betaalkaartindustrie (PCI DSS)**
  - **Gemarkeerd als Vertrouwelijk**

    Zie "Definities van gevoelige gegevens" (p. 931)
- **Afzender**: geeft de initiator aan van een gegevensoverdracht die wordt beheerd met deze regel. De afzender kan een enkele gebruiker, een lijst met gebruikers of een gebruikersgroep zijn.
  - **Elke interne**: een gebruikersgroep die alle interne gebruikers van de organisatie omvat.
  - **Contact/Van organisatie**: een Windows-account in de organisatie, dat wordt herkend door Advanced Data Loss Prevention, plus alle andere accounts (waaronder accounts gebruikt door communicatietoepassingen van derden) die eerder door een bepaald Windows-account zijn gebruikt.
  - **Contact/Aangepaste identiteit**: identificatie van een interne gebruiker die is opgegeven in een van de volgende indelingen: e-mail, Skype-ID, ICQ-id, IRC-id, e-mailadres van Jabber, e-mailadres van Mail.ru-agent, Viber-telefoonnummer, e-mailadres van Zoom.
    De volgende jokertekens kunnen worden gebruikt om een groep contacten op te geven:
    - *****: een willekeurig aantal symbolen
    - **?**: een willekeurig symbool
- **Ontvanger**: geeft de bestemming aan van een gegevensoverdracht die wordt beheerd met deze regel. De ontvanger kan een enkele gebruiker, een lijst met gebruikers, een gebruikersgroep of

andere typen bestemmingen zijn zoals hieronder aangegeven.
  - **Elke**: elke van de door Advanced DLP ondersteunde typen ontvangers.
  - **Contact/Elk contact**: elk intern of extern contact.
  - **Contact/Elk intern contact**: elk contact van een interne gebruiker (zie "Automatische doeldetectie" (p. 930)).
  - **Contact/Elk extern contact**: elk contact van een externe persoon of externe entiteit.
  - **Contact/Van organisatie**: hetzelfde principe als beschreven in het veld Afzender.
  - **Contact/Aangepaste identiteit**: hetzelfde principe als beschreven in het veld Afzender.
  - **Services voor bestanden delen**: de id van een beheerde service voor het delen van bestanden.
  - **Sociaal netwerk**: de id van een beheerd sociaal netwerk.
  - **Host/Elke host**: elke computer die door Advanced DLP als intern of extern wordt herkend.
  - **Host/Elke interne host**: elke computer die door Advanced DLP als intern wordt herkend.
  - **Host/Elke externe host**: elke computer die door Advanced DLP als extern wordt herkend.
  - **Host/Specifieke host**: een computer-id opgegeven als hostnaam (bijvoorbeeld FQDN) of als IP-adres (IPv4 of IPv6).
  - **Apparaat/Elk apparaat**: elk randapparaat dat is verbonden met de workload.
  - **Apparaat/Extern apparaat**: een verwisselbare opslag of omgeleid toegewezen station dat is verbonden met de workload.
  - **Apparaat/Versleuteld verwisselbaar**: een verwisselbaar opslagapparaat dat is versleuteld met BitLocker To Go.
  - **Apparaat/Omgeleid klembord**: een omgeleid klembord dat is verbonden met de workload.
  - **Printers**: elke lokale printer of netwerkprinter die is verbonden met de workload.
- **Machtiging**: een besturingselement van preventief beheer dat wordt afgedwongen voor een gegevensoverdracht die wordt beheerd met deze regel. Een meer gedetailleerde beschrijving vindt u in het onderwerp Machtigingen in beleidsregels voor gegevensstromen.
- **Actie**: een niet-preventieve actie die wordt uitgevoerd wanneer deze regel wordt geactiveerd. Standaard is dit veld ingesteld op 'Geen actie'. U kunt kiezen uit de volgende opties:
  - **Schrijven in logboek**: sla een gebeurtenisrecord op in het auditlogboek wanneer de regel wordt geactiveerd.
  - **De eindgebruiker waarschuwen wanneer een gegevensoverdracht wordt geweigerd**: gebruikers krijgen op het scherm een waarschuwing in real time wanneer ze de regel activeren.
  - **Een waarschuwing genereren**: de beheerder krijgt een waarschuwing wanneer de regel wordt geactiveerd.

Waarschuwing!
Wanneer **Geen actie** is geselecteerd en de regel wordt geactiveerd:

- er wordt geen gebeurtenisrecord toegevoegd aan het auditlogboek;
- er wordt geen waarschuwing verzonden naar de beheerder gestuurd;
- er wordt geen melding op het scherm getoond voor de eindgebruiker.

Waardoor wordt een beleidsregel geactiveerd?

Een gegevensoverdracht komt overeen met een beleidsregel voor gegevensstromen als aan alle volgende voorwaarden wordt voldaan:

- Alle afzenders van deze gegevensoverdracht worden vermeld of behoren tot een gebruikersgroep die in het veld **Afzender** van de regel is opgegeven.
- Alle ontvangers van deze gegevensoverdracht worden vermeld of behoren tot een gebruikersgroep die in het veld **Ontvanger** van de regel is opgegeven.
- De gegevens die worden overgedragen, komen overeen met de **Gevoeligheidscategorie** van de regel.

De machtigingen in beleidsregels voor gegevensstromen aanpassen

Advanced Data Loss Prevention ondersteunt drie typen machtigingen in beleidsregels voor gegevensstromen. De machtigingen worden afzonderlijk geconfigureerd in elke regel van het beleid.

Toestaan (toegankelijk)	Gegevensoverdrachten die overeenkomen met de in de regel gedefinieerde combinatie van gevoeligheidscategorie, afzender en ontvanger, zijn toegestaan.
Uitzondering (beperkend)	Gegevensoverdrachten die overeenkomen met de in de regel gedefinieerde combinatie van gevoeligheidscategorie, afzender en ontvanger, zijn niet toegestaan, maar de afzender kan een uitzondering op de regel indienen om een specifieke overdracht toe te laten. **Belangrijk** Alle volgende gegevensoverdrachten tussen deze afzender en ontvanger voor deze gevoeligheidscategorie worden toegestaan gedurende vijf minuten nadat de uitzondering is ingediend.
Weigeren (beperkend)	Gegevensoverdrachten die overeenkomen met de in de regel gedefinieerde combinatie van gevoeligheidscategorie, afzender en ontvanger, zijn niet toegestaan en de afzender kan geen uitzondering indienen.

Daarnaast kan er een prioriteitsvlag worden toegewezen aan de machtigingen **Toestaan** en **Uitzondering** om de flexibiliteit van het beleidsbeheer te vergroten. Met deze instelling kunt u de machtigingen overschrijven die voor specifieke groepen zijn ingesteld in andere regels voor gegevensstromen in het beleid. U kunt hiervan gebruikmaken als u een regel voor gegevensstromen

voor een groep alleen wilt toepassen op sommige van de groepsleden. In dat geval moet u een regel voor gegevensstromen maken voor specifieke gebruikers die u wilt uitsluiten van de groepsregels, en vervolgens instellen dat hun machtigingen prioriteit hebben boven de beperkingen voor gegevensstromen die zijn geconfigureerd in de regels voor de groep waartoe deze gebruikers behoren. Zie "Beleidsregels voor gegevensstromen combineren" (p. 922) voor informatie over de prioriteiten van machtigingen bij het combineren van regels.

Belangrijk
Belangrijk: Als u het beleid voor een bedrijf of eenheid wilt overschakelen van de observatiemodus naar de afdwingingsmodus, moet u de standaardregels voor elke categorie gevoelige gegevens overschakelen van 'toegankelijk' naar 'beperkt'. Standaardregels zijn gemarkeerd met een sterretje (*) in de weergave **Beleid voor gegevensstromen**. Lees meer over de typen beleidsregels in de Basishandleiding.

Machtigingen bewerken in de beleidsregels

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Navigeer naar **Bescherming** > **Beleid voor gegevensstromen**.
3. Selecteer de beleidsregel die u wilt bewerken en klik op **Bewerken** boven de lijst met regels.
   Het venster **Regel voor gegevensstromen bewerken** wordt geopend.
4. Selecteer in het gedeelte **Machtiging** de optie **Toestaan**, **Uitzondering** of **Weigeren**.
5. (Optioneel) Als u de machtiging **Toestaan** of **Uitzondering** voor deze regel prioriteit wilt toekennen boven de machtigingen in andere regels, schakelt u het selectievakje **Met prioriteit** in.
   U hoeft dit selectievakje niet te gebruiken om een regel voor gegevensstromen prioriteit te geven boven de standaardregel Elke > Andere, omdat deze regel standaard de laagste prioriteit heeft in het beleid.
   Zie "Beleidsregels voor gegevensstromen combineren" (p. 922) voor informatie over de prioriteiten van machtigingen bij het combineren van regels.
6. (Optioneel) Selecteer een actie die moet worden uitgevoerd wanneer de regel wordt geactiveerd.
7. Sla de wijzigingen van de beleidsregel op.

Beleidsregels voor gegevensstromen combineren

Wanneer een gegevensoverdracht overeenkomt met meer dan één regel, worden de geconfigureerde machtigingen en acties voor alle regels gecombineerd en als volgt toegepast.

Machtigingen

Als een gegevensoverdracht overeenkomt met meer dan één regel en deze regels verschillende machtigingen hebben voor dezelfde gegevenscategorie, dan wordt de regel met de machtiging met de hoogste prioriteit toegepast, volgens de onderstaande lijst met machtigingsprioriteiten (in aflopende volgorde):

1. Uitzondering met de vlag **Met prioriteit**
2. Toestaan met de vlag **Met prioriteit**
3. Weigeren
4. Uitzondering
5. Toestaan

Als een gegevensoverdracht overeenkomt met meer dan één regel en deze regels verschillende machtigingen hebben voor verschillende gegevenscategorieën, wordt de volgende logica toegepast voor het bepalen van de toe te passen regel:

1. De meest restrictieve regelmachtiging wordt gedefinieerd voor elk van de gevoeligheidscategorieën waarmee de gegevensoverdracht overeenkomt.
2. De meest restrictieve regelmachtiging, zoals gedefinieerd in punt 1, wordt afgedwongen.

Voorbeeld

Een bestandsoverdracht komt overeen met drie regels in verschillende gevoeligheidscategorieën, als volgt:

Gevoeligheidscategorie	Machtiging
PII	Toestaan – Met prioriteit
PHI	Uitzondering – Met prioriteit
PCI	Weigeren

De machtiging die wordt toegepast, is Weigeren.

Acties

Als een gegevensoverdracht overeenkomt met meer dan één regel en er voor deze regels verschillende opties zijn geconfigureerd in het veld **Actie**, dan worden alle geconfigureerde acties in alle geactiveerde regels uitgevoerd.

Evaluatie en beheer van het beleid

Voordat het automatisch gemaakte basisbeleid voor gegevensstromen wordt afgedwongen, moet het door de klant worden geëvalueerd, gevalideerd en goedgekeurd, omdat de klant alle details van de bedrijfsprocessen kent en dus kan beoordelen of deze consistent zijn meegenomen in het basisbeleid. Ook kan de klant onnauwkeurigheden vaststellen, die vervolgens door de partnerbeheerder worden verholpen.

Tijdens de beleidsevaluatie presenteert de partnerbeheerder het basisbeleid voor gegevensstromen aan de klant. De klant evalueert elke gegevensstroom in het beleid en bevestigt dat deze in overeenstemming is met de bedrijfsprocessen (validatie). Voor de validatie zijn geen technische vaardigheden vereist, omdat de weergave van beleidsregels in de Cyber Protect-console intuïtief

duidelijk is: op elke regel wordt beschreven wie de afzender en wie de ontvanger is van een gegevensstroom van gevoelige gegevens.

De partnerbeheerder past het basisbeleid handmatig aan conform de instructies van de klant door beleidsregels voor gegevensstromen te bewerken, te verwijderen en toe te voegen. Na goedkeuring door de klant wordt het geëvalueerde beleid afgedwongen voor beschermde workloads door het beschermingsschema voor deze workloads in te stellen op de afdwingingsmodus.

Voordat u een geëvalueerd beleid afdwingt, moet u de machtiging **Toestaan** in alle automatisch gemaakte standaardbeleidsregels voor categorieën gevoelige gegevens instellen op **Weigeren** of **Uitzondering**. De machtiging **Weigeren** kan niet worden overschreven door gebruikers. De machtiging **Uitzondering** blokkeert een overdracht die overeenkomt met de regel, maar laat wel toe dat gebruikers de blokkade opheffen in een noodsituatie door een bedrijfsgerelateerde uitzondering in te dienen.

Beleid voor gegevensstromen vernieuwen

Wanneer het bedrijfsproces van het bedrijf of een eenheid aanzienlijk wordt gewijzigd, moeten de DLP-beleidsregels worden vernieuwd om ze af te stemmen op de wijzigingen in de gegevensstromen van gevoelige gegevens van het bijgewerkte bedrijfsproces. Een vernieuwing van het beleid is ook vereist als de functie van een werknemer wordt gewijzigd. In dat geval moet het deel van het eenheidbeleid dat de workload van de werknemer beschermt, ook worden vernieuwd.

Met de workflow voor het beheer van Advanced DLP-beleid kunnen beheerders de vernieuwing van beleid automatiseren voor het hele bedrijf, een eenheid, een gebruiker of een deel van de gebruikers in een eenheid.

Het beleid voor een bedrijf of eenheid vernieuwen

Alle opties van de observatiemodus kunnen worden gebruikt om het beleid te vernieuwen, ongeacht of het gaat om het beleid van een bedrijf, eenheid, een deel van een eenheid of een of meer gebruikers in de eenheid.

Het beleid voor een bedrijf of eenheid vernieuwen

Voor vernieuwing moeten de volgende stappen worden uitgevoerd door een bedrijfbeheerder of een partner die de workloads van het bedrijf beheert.

1. Verwijder alle niet-standaard regels in het afgedwongen beleid.
2. Start de vernieuwing: stel het beschermingsschema met Advanced DLP dat van toepassing is op het bedrijf of de eenheid, in op een van de opties van de observatiemodus (kies de optie die optimaal is voor dit specifieke bedrijf of deze eenheid) en pas het plan vervolgens toe op alle workloads in het bedrijf of de eenheid.
3. Wanneer de vernieuwingsperiode afloopt, neemt u het nieuwe bedrijf- of eenheidbeleid door met de klant en past u het zo nodig aan om instemming van de klant te krijgen.

4. Stel het beschermingsschema dat van toepassing is op de workloads van het bedrijf of eenheid, in op een toepasselijke optie van de afdwingingsmodus. Kies een optie die de klant optimaal vindt om gegevenslekken vanuit de workloads van de eenheid te voorkomen.

Het beleid vernieuwen voor één of meer gebruikers in het bedrijf of de eenheid

Beleidsregels op gebruikersniveau kunnen worden vernieuwd via elke optie van de observatiemodus en via de adaptieve afdwingingsmodus.

De observatiemodus gebruiken voor het vernieuwen van het beleid voor een gebruiker

Bij het gebruik van de observatiemodus voor het vernieuwen van het beleid voor een gebruiker of een deel van de gebruikers in het bedrijf (of de eenheid) is het volgende van toepassing: het beleid voor gegevensstromen dat voor het hele bedrijf (of de hele eenheid) wordt afgedwongen, wordt niet afgedwongen voor de gegevensoverdrachten van de gebruiker tijdens de vernieuwingsperiode. Daardoor kunnen tijdens de vernieuwing nieuwe individuele regels voor de gebruiker worden gemaakt die mogelijk in strijd zijn of juist overeenstemmen met bestaande groepsregels in het afgedwongen beleid voor het bedrijf (of de eenheid). Wanneer de vernieuwing is voltooid en het beleid opnieuw wordt afgedwongen voor de gegevensoverdrachten van de gebruiker, moet worden bepaald of deze nieuwe individuele regels die voor de gebruiker zijn gemaakt, al dan niet worden toegepast op de gegevensoverdrachten van de gebruiker. Dit hangt af van de prioriteit van die regels ten opzichte van andere regels in het beleid waarmee deze gegevensoverdrachten overeenkomen.

Het beleid voor een gebruiker vernieuwen via de observatiemodus

Voor vernieuwing moeten de volgende stappen worden uitgevoerd door een bedrijfbeheerder of een partner die de workloads van het bedrijf beheert.

1. Verwijder alle niet-standaard regels in het afgedwongen beleid voor het bedrijf (of de eenheid) als de gebruiker de enige afzender is in die regels.
2. Verwijder de gebruiker uit de lijst met afzenders voor alle niet-standaard regels voor gegevensstromen in het afgedwongen beleid.
3. Maak een nieuw beschermingsschema met Advanced DLP in de observatiemodus en pas het toe op de workload van de gebruiker om de vernieuwingsperiode (observatie) te starten.
   De duur van de vernieuwingsperiode hangt af van de tijd die de gebruiker nodig heeft om alle of 90-95% van de normale bedrijfsactiviteiten uit te voeren waarbij gevoelige gegevens van de workloads worden overgebracht.
4. Wanneer de vernieuwingsperiode afloopt, controleert u de nieuwe regels die aan het afgedwongen beleid zijn toegevoegd voor deze gebruiker. Pas ze zo nodig aan en laat ze goedkeuren door de klant.
5. Stel het beschermingsschema dat van toepassing is op de workload van de gebruiker, in op de modus **Strikte afdwinging** of **Adaptieve afdwinging**. Kies de optie die de klant optimaal vindt om gegevenslekken vanuit de workload van de gebruiker te voorkomen.
   U kunt er ook voor kiezen om het beschermingsschema dat van toepassing is voor het bedrijf (of de eenheid), opnieuw toe te passen op de workload van de gebruiker.

De adaptieve afdwingingsmodus gebruiken voor het vernieuwen van het beleid voor een gebruiker

U kunt het beleid voor een enkele gebruiker of een deel van alle gebruikers in het bedrijf (of de eenheid) vernieuwen via de adaptieve afdwingingsmodus van een beschermingsschema waarbij Advanced DLP wordt toegepast op de workload van de gebruiker.

Opmerking
Bij deze methode voor het vernieuwen van het beleid is het volgende van toepassing: de beleidsregels voor een bedrijf (of eenheid) die worden afgedwongen voor afzendergroepen met lidmaatschap van gebruikers (dat wil zeggen Elke interne), worden ook afgedwongen voor gegevensoverdrachten van deze gebruiker tijdens de vernieuwing. Hierdoor worden er tijdens de vernieuwing geen nieuwe individuele regels voor de gebruiker gemaakt die mogelijk in strijd zijn of juist overeenstemmen met deze reeds bestaande beleidsregels voor afzendergroepen. Welke van deze twee methoden het meest effectief is voor het vernieuwen van het beleid voor de gebruikers van een bepaalde klant hangt af van de specifieke IT-beveiligingseisen

Het beleid voor een gebruiker vernieuwen via de adaptieve afdwingingsmodus

Voor vernieuwing moeten de volgende stappen worden uitgevoerd door een bedrijfbeheerder of een partner die de workloads van het bedrijf beheert.

1. Verwijder alle niet-standaard regels in het afgedwongen beleid voor het bedrijf (of de eenheid) als de gebruiker de enige afzender is in die regel.
2. Verwijder de gebruiker uit de lijst met afzenders voor alle niet-standaard regels voor gegevensstromen in het afgedwongen beleid.
3. Stel de machtiging voor alle standaardregels in het afgedwongen beleid voor het bedrijf (of de eenheid) in op **Uitzondering** en selecteer de actie **Schrijven in logboek** in het veld **Actie**.
4. Als het beschermingsschema dat momenteel van toepassing is op de workload van de gebruiker, is ingesteld op de modus **Strikte afdwinging**, maakt u een nieuw beschermingsschema met Advanced DLP en past u dit toe op de workload van de gebruiker in de modus **Adaptieve afdwinging** om de vernieuwingsperiode te starten.
   De duur van de vernieuwingsperiode hangt af van de tijd die de gebruiker nodig heeft om alle of 90-95% van de normale bedrijfsactiviteiten uit te voeren waarbij gevoelige gegevens van de workloads worden overgebracht.
5. Wanneer de vernieuwingsperiode afloopt, controleert u de nieuwe regels die aan het afgedwongen beleid zijn toegevoegd voor deze gebruiker. Pas ze zo nodig aan en laat ze goedkeuren door de klant.
6. Stel het beschermingsschema dat van toepassing is op de workload van de gebruiker, in op de modus **Strikte afdwinging** of gebruik de huidige modus **Adaptieve afdwinging**. Kies de optie die de klant optimaal vindt om gegevenslekken vanuit de workload van de gebruiker te voorkomen.
   U kunt er ook voor kiezen om het beschermingsschema dat van toepassing is voor het bedrijf (of de eenheid), opnieuw toe te passen op de workload van de gebruiker.

Advanced Data Loss Prevention inschakelen in beschermingsschema's

De functies van Advanced Data Loss Prevention kunnen in elk beschermingsschema voor een klanttenant worden opgenomen als de Protection-service en het Advanced Data Loss Prevention-pakket voor deze klant zijn ingeschakeld.

Advanced DLP is de geavanceerde module van de groep functies voor gegevensverliespreventie. De functies van Advanced DLP en Apparaatbeheer kunnen onafhankelijk of samen worden gebruikt (in een enkel beschermingsplan, of in twee plannen die dezelfde workload beschermen). Als ze samen worden gebruikt, worden de mogelijkheden van de functies als volgt gecoördineerd.

- Gebruikerstoegang tot de lokale kanalen waar Advanced DLP de inhoud van overgedragen gegevens inspecteert, wordt niet meer beheerd door Apparaatbeheer. Apparaatbeheer blijft wel de volgende apparaattypen beheren als deze zijn geconfigureerd voor alleen-lezen of geweigerde toegang:
  - Verwisselbaar
  - Versleuteld verwisselbaar
  - Toegewezen station

  Voorbeeld: Als u zowel Apparaatbeheer als Advanced DLP hebt ingeschakeld in een enkel beschermingsplan of in twee plannen die dezelfde workload beschermen, en u hebt Alleen-lezen toegang geconfigureerd voor USB-apparaten in Apparaatbeheer, dan wordt Alleen-lezen toegang toegepast op alle USB-apparaten, behalve voor de apparaten op de acceptatielijst, ongeacht de toegangsinstellingen in de Advanced DLP-module. Als de standaardinstelling Toegang inschakelen is geconfigureerd in Apparaatbeheer, wordt de toegangsinstelling van Advanced DLP toegepast.
- Gebruikerstoegang tot de volgende lokale kanalen en randapparatuur in de acceptatielijst wordt afgedwongen door Apparaatbeheer:
  - Optische stations
  - Diskettestations
  - Via MTP verbonden mobiele apparaten
  - Bluetooth-adapters
  - Windows-klembord
  - Schermopnamen
  - USB-apparaten en -apparaattypen (behalve Verwisselbare opslag en Versleuteld)

Een beschermingsschema maken met Advanced DLP

1. Navigeer naar **Beheer** > **Beschermingsschema's**.
2. Klik op **Schema maken**.

3. Vouw het gedeelte **Preventie van gegevensverlies** uit en klik op de rij **Modus**.
   Het dialoogvenster **Modus** wordt geopend.
   - Als u een beleid voor gegevensstromen wilt maken of vernieuwen, selecteert u **Observatiemodus** en vervolgens selecteert u hoe de gegevensoverdracht moet worden verwerkt:

Optie	Beschrijving
Alles toestaan	Alle overdrachten van gevoelige gegevens vanuit gebruikersworkloads worden behandeld als noodzakelijk voor het bedrijfsproces en als veilig. Voor elke gedetecteerde gegevensstroom die niet overeenkomt met een reeds gedefinieerde regel in het beleid, wordt een nieuwe regel gemaakt.
Alles motiveren	Alle overdrachten van gevoelige gegevens vanuit gebruikersworkloads worden behandeld als noodzakelijk voor het bedrijfsproces, maar als riskant. Daarom moet de gebruiker een eenmalige zakelijke motivering geven voor elke onderschepte overdracht van gevoelige gegevens naar een ontvanger of bestemming (zowel binnen als buiten de organisatie) die niet overeenkomt met een eerder gemaakte regel voor gegevensstromen. Wanneer de motivering wordt ingediend, wordt een nieuwe regel voor gegevensstromen gemaakt in het beleid voor gegevensstromen.
Gemengd	De logica 'Alles toestaan' wordt toegepast voor alle interne overdrachten van gevoelige gegevens, en de logica 'Alles motiveren' voor alle externe overdrachten van gevoelige gegevens. Zie "Automatische doeldetectie" (p. 930) voor de definitie van interne bestemmingen

Waarschuwing!
- Selecteer **Observatiemodus** alleen als u nog geen beleid voor gegevensstromen hebt gemaakt of als u het beleid vernieuwt. Zie "Beleid voor gegevensstromen vernieuwen" (p. 924) voordat u het beleid vernieuwt.
- Gegevenslekken worden niet voorkomen in de observatiemodus. Zie Observatiemodus in de Basishandleiding.

   - Als u het bestaande beleid voor gegevensstromen wilt afdwingen, selecteert u **Afdwingingsmodus** en selecteert u vervolgens hoe strikt u de beleidsregels voor gegevensstromen wilt afdwingen:

Optie	Beschrijving
Strikte afdwinging	Het beleid voor gegevensstromen wordt afgedwongen zoals het is en wordt niet uitgebreid met nieuwe toegankelijke beleidsregels wanneer niet eerder waargenomen gegevensstromen van gevoelige gegevens worden gedetecteerd. Zie Strikte afdwinging in de Basishandleiding.
Adaptieve afdwinging (afdwinging	Het afgedwongen beleid wordt automatisch aangepast aan de bedrijfsactiviteiten die niet zijn uitgevoerd tijdens de observatieperiode of aan wijzigingen in de bedrijfsprocessen. Met deze modus kan het afgedwongen beleid voor

Optie	Beschrijving
met machine learning)	gegevensstromen worden uitgebreid doordat er wordt geleerd van de nieuw gedetecteerde gegevensstromen in de workloads. Zie Adaptieve afdwinging in de Basishandleiding.

Belangrijk
Belangrijk: Als u het beleid voor een bedrijf of eenheid wilt overschakelen van de observatiemodus naar de afdwingingsmodus, moet u de standaardregels voor elke categorie gevoelige gegevens overschakelen van 'toegankelijk' naar 'beperkt'. Standaardregels zijn gemarkeerd met een sterretje (*) in de weergave **Beleid voor gegevensstromen**. Lees meer over de typen beleidsregels in de Basishandleiding.

4. Klik op **Gereed** om het dialoogvenster Modus te sluiten.
5. (Optioneel) Klik op **Geavanceerde instellingen** om optische tekenherkenning, acceptatielijsten en nog andere beschermingsopties te configureren.
   Zie "Geavanceerde instellingen" (p. 929) voor informatie over beschikbare opties.
6. Sla het beschermingsschema op en pas het toe op de workloads die u wilt beschermen.

Geavanceerde instellingen

U kunt de geavanceerde instellingen in beschermingsschema's met Advanced Data Loss Prevention gebruiken om de inspectie van gegevensinhoud nauwkeuriger in te stellen in de kanalen die worden beheerd met Advanced Data Loss Prevention. Daarnaast kunt u bepaalde elementen uitsluiten van het preventief beheer, bijvoorbeeld gegevensoverdrachten naar typen randapparatuur in de acceptatielijst, bepaalde categorieën netwerkcommunicatie, doelhosts en gegevensoverdrachten die worden geïnitieerd door toepassingen in de acceptatielijst. U kunt de volgende geavanceerde instellingen configureren:

- **Optische tekenherkenning**
  Met deze instelling wordt OCR (optische tekenherkenning) in- of uitgeschakeld. Met OCR kan tekst in 31 talen worden geëxtraheerd uit grafische bestanden en afbeeldingen in documenten, berichten, scans, schermopnamen en andere objecten, zodat de tekstinhoud verder kan worden geïnspecteerd.
- **Overdracht van met wachtwoord beveiligde gegevens**
  De inhoud van met wachtwoord beveiligde archieven en documenten kan niet worden geïnspecteerd. Met deze instelling kan de beheerder in Advanced DLP selecteren of uitgaande overdrachten van met een wachtwoord beveiligde gegevens moeten worden toegestaan of geblokkeerd.
- **Gegevensoverdracht voorkomen in het geval van fouten**
  Soms kan de analyse van de inhoud die wordt verzonden, niet worden uitgevoerd of er kan er een andere beheerfout optreden bij bewerkingen van de DLP-agent. Als deze optie is ingeschakeld, wordt de overdracht geblokkeerd. Als de optie is uitgeschakeld, wordt de overdracht toegestaan ondanks de fout.

- **Acceptatielijst voor apparaattypen en netwerkcommunicatie**
  Gegevensoverdrachten naar de in deze lijst aangevinkte typen randapparatuur en netwerkcommunicatie zijn toegestaan, ongeacht de gevoeligheid van de gegevens en het afgedwongen beleid voor gegevensstromen.

  Waarschuwing!
  Deze optie wordt gebruikt wanneer zich problemen voordoen met een specifiek apparaattype of protocol. Schakel dit alleen in op advies van iemand van het ondersteuningsteam.

- **Acceptatielijst voor externe hosts**
  Gegevensoverdrachten naar de in deze lijst opgegeven doelhosts zijn toegestaan, ongeacht de gevoeligheid van de gegevens en het afgedwongen beleid voor gegevensstromen.
- **Acceptatielijst voor toepassingen**
  Gegevensoverdrachten die worden uitgevoerd door in deze lijst opgegeven toepassingen, zijn toegestaan, ongeacht de gevoeligheid van de gegevens en het afgedwongen beleid voor gegevensstromen.

De indicator **Beveiligingsniveau** van de geavanceerde instellingen die wordt weergegeven in de weergave **Beschermingsschema maken** en in de weergave 'Details' van een beschermingsschema, heeft de volgende logica van niveau-indicatie:

- **Standaard** geeft aan dat geen enkele geavanceerde instelling is ingeschakeld.
- **Matig** geeft aan dat één of meer instellingen zijn ingeschakeld, maar dat de combinatie van **OCR**, **Overdracht van met wachtwoord beveiligde gegevens** en **Gegevensoverdracht voorkomen in het geval van fouten** niet is geactiveerd.
- **Strikt**: betekent dat ten minste de combinatie van de instellingen **OCR**, **Overdracht van met wachtwoord beveiligde gegevens** en **Gegevensoverdracht voorkomen in het geval van fouten** is geactiveerd.

Automatische doeldetectie

Als de observatiemodus Gemengd is ingeschakeld, worden door Advanced Data Loss Prevention verschillende regels toegepast, afhankelijk van de bestemming van de gedetecteerde gegevensoverdracht: intern of extern. De logica om te bepalen of een bestemming als intern wordt beschouwd, wordt hieronder beschreven. Alle andere bestemmingen worden als extern beschouwd.

Bij elke onderschepte gegevensoverdracht wordt door Advanced Data Loss Prevention automatisch gedetecteerd of de HTTP-, FTP- of SMB-doelserver intern is. Hiertoe wordt een DNS-aanvraag uitgevoerd en wordt de FQDN-naam van de machine waarop de Data Loss Prevention-agent wordt uitgevoerd, vergeleken met die van de externe server. Als de DNS-aanvraag mislukt, wordt ook gecontroleerd of de beschermde workload en de externe server zich in hetzelfde netwerk bevinden. Servers die dezelfde domeinnaam hebben (of zich in hetzelfde subnetwerk bevinden) als de machine waarop de Data Loss Prevention agent wordt uitgevoerd, worden als intern beschouwd.

Bij e-mailcommunicatie geldt dat alle e-mails die vanaf een bedrijfsmailadres worden verzonden via de bedrijfsmailserver, door Advanced Data Loss Prevention worden behandeld als interne overdrachten indien het e-mailadres van de ontvanger zich op hetzelfde domein bevindt als het e-mailadres van de afzender en de ontvangende mailserver dezelfde naam heeft.

Niet-zakelijke e-mails worden behandeld als externe communicatie, tenzij het account van de ontvanger bekend is. Bekende e-mailadressen worden bijgewerkt wanneer Data Loss Prevention de gebruikersactiviteit op het netwerk controleert en de database aan de back-end bijwerkt met gegevens voor e-mailadressen die zijn gekoppeld aan de gebruiker.

Communicatie via chats wordt behandeld als externe communicatie, tenzij het account van de ontvanger bekend is. Bekende accounts worden bijgewerkt wanneer Data Loss Prevention de gebruikersactiviteit op het netwerk controleert en de database aan de back-end bijwerkt met gegevens voor accounts die zijn gekoppeld aan de gebruiker.

Definities van gevoelige gegevens

In dit onderwerp wordt de logica beschreven waarmee gevoelige gegevens worden geïdentificeerd tijdens inhoudsanalyse.

Identieke overeenkomsten worden geteld als één overeenkomst voor alle groepen van de beschreven logische expressies. Dit is bedoeld om het aantal fout-positieven te verminderen.

Belangrijk
De logische expressies die worden gebruikt voor identificatie van de inhoud, worden alleen ter informatie gegeven en geven geen volledige beschrijving van alle details van de oplossing.

Beschermde gezondheidsinformatie (PHI)

Ondersteunde talen

- VS, VK, Engels (internationaal)
- Fins
- Italiaans
- Frans
- Pools
- Russisch
- Hongaars
- Noors
- Spaans

Gegevens beschouwd als beschermde gezondheidsinformatie (PHI)

De volgende gegevens worden beschouwd als beschermde gezondheidsinformatie.

- Voor- en achternamen
- Adres (straat, plaats, provincie, gemeente, postcode en de overeenkomstige geocodes)
- Telefoonnummers
- E-mailadressen
- Burgerservicenummers
- Ziekenfondsnummers
- Bankrekeningnummers
- URL's
- IP-adresnummers
- ICD-10-CM-codes
- ICD-10-PCS-and-GEMs
- HIPAA
- Andere zorgnummers
- Creditcardnummers

Logische expressie gebruikt voor inhoudsdetectie

De logische expressie bestaat uit de volgende tekenreeksen die worden gekoppeld met de logische operator OR. De operator OR wordt gebruikt om verschillende gegevensgroepen in de bovenstaande lijst te koppelen als de logische operator AND niet expliciet is opgegeven. De getallen tussen haakjes geven het aantal gedetecteerde gevallen aan waarvoor een positief resultaat wordt geretourneerd bij de detectie.

- **Burgerservicenummers** (5)
- (Voor- en achternamen (3) OR Adres (3) OR Telefoonnummers (3) OR E-mailadres (3) OR Bankrekeningnummers (3) OR Creditcardnummers (3)) AND (Burgerservicenummers (3) OR Ziekenfondsnummers (3) * OR ICD-10-CM-codes (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR * Andere zorgnummers (3))

Persoonsgegevens (PII)

Ondersteunde talen

- VS, VK, Engels (internationaal)
- Bulgaars
- Chinees
- Tsjechisch
- Deens
- Nederlands

- Fins
- Frans
- Duits
- Hongaars
- Indonesisch
- Italiaans
- Koreaans
- Maleis
- Noors
- Pools
- Portugees (Brazilië)
- Portugees (Portugal)
- Roemeens
- Russisch
- Servisch
- Singapore
- Spaans
- Zweeds
- Taiwan
- Turks
- Thais
- Japans

Gegevens beschouwd als persoonsgegevens (PII)

- Voor- en achternamen
- Adres (straat, stad, provincie, postcode)
- Bankrekeningnummers
- Persoonlijke en belastingnummers
- Paspoortnummers
- Burgerservicenummers
- Telefoonnummers
- Kentekens
- Rijbewijsnummers
- Identificatienummers en serienummers

- IP-adres
- E-mailadressen
- Creditcardnummers

Logische expressie gebruikt voor inhoudsdetectie

Logische expressie voor alle ondersteunde talen behalve Japans

De logische expressie bestaat uit de volgende tekenreeksen, gekoppeld met de logische operator OR of AND. De getallen tussen haakjes geven het aantal gedetecteerde gevallen aan waarvoor een positief resultaat wordt geretourneerd bij de detectie.

- Persoonlijke en belastingnummers (5)
- Voor- en achternamen (3) AND **(**Creditcardnummer (3) OR Burgerservicenummer (3) OR Bankrekeningnummer (3) OR Persoonlijke en belastingnummers (3) OR Rijbewijsnummers (3) OR Paspoortnummers (3) OR Burgerservicenummers (3) OR IP-adressen (3) OR Kentekens (3) OR Identificatienummers en serienummers**)**
- Telefoonnummers (3) AND **(**Creditcardnummer (3) OR Burgerservicenummer (3) OR Bankrekeningnummer (3) OR Adres (3) OR Persoonlijke en belastingnummers (3) OR Rijbewijsnummers (3) OR Paspoortnummers (3) OR Burgerservicenummers (3) OR Kentekens (3) OR Identificatienummers en serienummers (3)**)**
- **(**Voor- en achternamen (30) OR Adres (30)**)** AND **(**E-mailadressen (30) OR Telefoonnummers (30) OR IP-adressen (30)**)**
- E-mailadressen (3) AND **(**Creditcardnummer (3) OR Burgerservicenummer (3) OR Bankrekeningnummer (3) OR Persoonlijke en belastingnummers (3) OR Rijbewijsnummers (3) OR Paspoortnummers (3) OR Burgerservicenummers (3) OR Kentekens (3) OR Identificatienummers en serienummers (3)**)**
- E-mailadres (30) AND **(**Adres (30) OR Telefoonnummers (30)**)**
- Voor- en achternamen (30) AND Adres (30)
- Telefoonnummers (30) AND Adres (30)
- Voor- en achternamen (3) AND Bankrekeningnummers (3)
- Telefoonnummers (3) AND **(**Creditcardnummer (3) OR Bankrekeningnummer (3) OR Burgerservicenummers (3) OR Persoonlijke en belastingnummers (3) OR Rijbewijsnummers (3) OR Paspoortnummers (3)**)**

Logische expressie voor Japans

Opmerking
Alleen unieke overeenkomsten worden geteld bij inhoudsdetectie.

De logische expressie bestaat uit de volgende tekenreeksen, gekoppeld met de logische operator OR. De operator OR wordt gebruikt om verschillende groepen te koppelen als de logische operator AND niet expliciet is opgegeven.

- Burgerservicenummers (5)
- Voor- en achternamen (3) AND **(**Creditcardnummer (3) OR Bankrekeningnummer (3) OR Rijbewijsnummers (3) OR Paspoortnummers (3) OR Burgerservicenummers (3)**)**
- Voor- en achternamen (30) AND **(**E-mailadressen (30) OR Telefoonnummers (30) OR IP-adressen (30) OR Adres (30)**)**
- Adres (3) AND **(**Creditcardnummer (3) OR Bankrekeningnummer (3) OR Rijbewijsnummers (3) OR Paspoortnummers (3) OR Burgerservicenummers (3)**)**
- E-mailadres (3) AND **(**Creditcardnummer (3) OR Bankrekeningnummer (3) OR Burgerservicenummers (3) OR Rijbewijsnummers (3)**)**
- Adres (5) AND **(**E-mailadres (5) OR Voor- en achternamen (5) OR Telefoonnummers (5) OR IP-adressen (5)**)**
- Voor- en achternamen (3) AND Bankrekeningnummers (3)
- Telefoonnummers (3) AND **(**Creditcardnummer (3) OR Bankrekeningnummer (3) OR Adres (3) OR Burgerservicenummers (3) OR Rijbewijsnummers (3)**)**

Gegevensbeveiligingsnorm van de betaalkaartindustrie (PCI DSS)

Ondersteunde talen

Voor deze gevoeligheidsgroep wordt slechts één taal gebruikt. De PCI DSS-gegevens zijn voor alle landen in het Engels.

Gegevens die worden beschouwd als PCI DSS

- Gegevens van de kaarthouder
  - Primair rekeningnummer (PAN)
  - Naam van de kaarthouder
  - Verloopdatum
  - Servicecode
- Gevoelige verificatiegegevens
  - Volledige traceringsgegevens (gegevens op magneetstrip of equivalent op een chip)
  - CAV2/CVC2/CVV2/CID
  - Pincodes/Pincodeblokken

Logische expressie gebruikt voor inhoudsdetectie

De logische expressie bestaat uit de volgende tekenreeksen, gekoppeld met de logische operator OR. De getallen tussen haakjes geven het aantal gedetecteerde gevallen aan waarvoor een positief resultaat wordt geretourneerd bij de detectie.

- Creditcardnummer (5)
- Kredietkaartnummer (3) AND (Amerikaanse naam (Ex) (3) OR Amerikaanse naam (3) OR PCI DSS-trefwoorden (3) OR Datum (maand/jaar) (3))
- Creditcard-dump (5)

Gemarkeerd als Vertrouwelijk

Gegevens die als vertrouwelijk zijn gemarkeerd, worden gedetecteerd via de trefwoordengroep.

De voorwaarde voor Overeenkomst is gebaseerd op gewicht, en elk woord heeft het gewicht == 1. De inhoudsdetectie wordt beschouwd als positief bij een overeenkomst als het gewicht > 3.

Ondersteunde talen

- Nederlands
- Bulgaars
- Chinees (Vereenvoudigd)
- Chinees (Traditioneel)
- Tsjechisch
- Deens
- Nederlands
- Fins
- Frans
- Duits
- Hongaars
- Indonesisch
- Italiaans
- Japans
- Koreaans
- Maleis
- Noors
- Pools
- Portugees (Brazilië)
- Portugees (Portugal)
- Russisch
- Servisch
- Spaans

- Zweeds
- Turks

Trefwoordgroepen

De trefwoordgroep voor elke taal bevat de landspecifieke equivalenten van de volgende trefwoorden die worden gebruikt voor het Engels (niet hoofdlettergevoelig).

- vertrouwelijk
- interne distributie
- niet voor distributie
- niet distribueren
- niet voor algemeen gebruik
- niet voor externe distributie
- alleen voor intern gebruik
- documentatie voor hooggekwalificeerde personen
- privé
- informatie voor bevoegden
- alleen voor intern gebruik
- alleen voor officieel gebruik

Gebeurtenissen in Preventie van gegevensverlies

Gebeurtenissen in de DLP-gebeurtenisviewer worden als volgt gegenereerd in Advanced Data Loss Prevention.

- In de observatiemodus worden er gebeurtenissen gegenereerd voor alle gemotiveerde gegevensoverdrachten.
- In de afdwingingsmodus worden gebeurtenissen gegenereerd op basis van de actie **Schrijven in logboek** die is geconfigureerd voor elke beleidsregel die wordt geactiveerd.

De gebeurtenissen voor een regel bekijken in het beleid voor gegevensstromen

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Navigeer naar **Bescherming** > **Beleid voor gegevensstromen**.
3. Zoek de regel waarvan u de gebeurtenissen wilt bekijken en klik op de ellips aan het einde van de lijn met de regel.
4. Selecteer **Gebeurtenissen bekijken**.

Details van een gebeurtenis bekijken in de DLP-gebeurtenisviewer:

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Navigeer naar **Bescherming** > **DLP-gebeurtenissen**.
3. Klik op een gebeurtenis in de lijst om meer details te bekijken.
   Het deelvenster Details van gebeurtenis wordt uitgevouwen aan de rechterkant.
4. Scrol omlaag en omhoog in het deelvenster Details van gebeurtenis om de beschikbare informatie te bekijken.
   Welke details in het deelvenster worden weergegeven, hangt af van het type regel en de regelinstellingen waardoor de gebeurtenis is geactiveerd.

Gebeurtenissen filteren in de lijst met DLP-gebeurtenissen

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Navigeer naar **Bescherming** > **DLP-gebeurtenissen**.
3. Klik linksboven op **Filter**.
4. Selecteer gevoeligheidscategorie, workload, actietype, gebruiker en kanaal in de vervolgkeuzemenu's.
   U kunt meer dan één item in de vervolgkeuzemenu's selecteren. Bij het filteren wordt de logische operator OR gebruikt tussen items in hetzelfde menu, en de logische operator AND tussen items uit verschillende menu's.
   Als u bijvoorbeeld de gevoeligheidscategorieën **PHI** en **PII** selecteert, worden alle gebeurtenissen geretourneerd die PHI of PII, of beide, bevatten. Als u gevoeligheidscategorie **PHI** en actie **Schrijftoegang** selecteert, worden in het gefilterde resultaat alleen gebeurtenissen weergegeven die met beide categorieën overeenkomen.
5. Klik op **Toepassen**.
6. Als u alle gebeurtenissen opnieuw wilt bekijken, klikt u op **Filter**, op **Terugzetten naar standaardwaarden** en ten slotte op **Toepassen**.

Gebeurtenissen zoeken in de lijst met DLP-gebeurtenissen

1. Herhaal stap 1-2 van de procedure hierboven.
2. Kies in de vervolgkeuzelijst rechts van Filter een categorie waarin u wilt zoeken: **Afzender**, **Bestemming**, **Proces**, **Onderwerp van bericht** of **Reden**.
3. Voer in het tekstvak de gewenste woorden in en bevestig door op Enter te drukken.
   Alleen gebeurtenissen die overeenkomen met de door u ingevoerde woorden, worden weergegeven in de lijst.
4. Als u de lijst met gebeurtenissen opnieuw wilt instellen, klikt u op het **X**-teken in het tekstvak Zoeken en drukt u op Enter.

De lijst met gebeurtenissen voor specifieke regels bekijken in het beleid voor gegevensstromen

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Navigeer naar **Bescherming** > **Beleid voor gegevensstromen**.

3. Schakel het selectievakje in voor de naam van de gewenste beleidsregel.
   U kunt indien nodig meerdere beleidsregels selecteren.
4. Klik op **Gebeurtenissen bekijken**.
   U ziet de weergave **Bescherming** > **DLP-gebeurtenissen**. In de lijst worden de gebeurtenissen weergegeven die betrekking hebben op de door u geselecteerde beleidsregels.

Widgets van Advanced Data Loss Prevention op het dashboard Overzicht

Het dashboard **Overzicht** bevat enkele aanpasbare widgets die een overzicht bieden van de bewerkingen voor de Cyber Protection-service, met inbegrip van Advanced Data Loss Prevention. Op het dashboard **Overzicht**, onder **Controle**, vindt u de volgende widgets voor Advanced Data Loss Prevention.

- **Overdrachten van gevoelige gegevens**: geeft het totale aantal overdrachten van gevoelige gegevens naar interne en externe ontvangers weer. Het diagram is onderverdeeld volgens het type machtiging: toegestaan, gemotiveerd of geblokkeerd. U kunt deze widget aanpassen door het gewenste tijdbereik te selecteren (1 dag, 7 dagen, 30 dagen, of deze maand).
- **Categorieën van uitgaand verkeer van gevoelige gegevens**: geeft het totale aantal overdrachten van gevoelige gegevens naar externe ontvangers weer. Het diagram is onderverdeeld in diverse categorieën gevoelige gegevens: Beschermde gezondheidsinformatie (PHI), persoonsgegevens (PII), gegevens onder de Informatiebeveiligingsstandaard voor betaalkaartbedrijven (PCI DSS) en Gemarkeerd als vertrouwelijk (vertrouwelijk).
- **Top afzenders van uitgaand verkeer van gevoelige gegevens**: geeft het totale aantal overdrachten van gevoelige gegevens weer vanuit de organisatie naar externe ontvangers, plus een lijst van de top vijf gebruikers met het grootste aantal overdrachten (samen met deze aantallen). Deze statistiek omvat zowel toegestane als gemotiveerde overdrachten. U kunt deze widget aanpassen door het gewenste tijdbereik te selecteren (1 dag, 7 dagen, 30 dagen, of deze maand).
- **Top afzenders van geblokkeerde overdrachten van gevoelige gegevens**: geeft het totale aantal geblokkeerde overdrachten van gevoelige gegevens weer, plus een lijst van de top vijf gebruikers met het grootste aantal pogingen tot overdracht (samen met deze aantallen). U kunt deze widget aanpassen door het gewenste tijdbereik te selecteren (1 dag, 7 dagen, 30 dagen, of deze maand).
- **Recente DLP-gebeurtenissen**: geeft details van recente gebeurtenissen van Preventie van gegevensverlies weer voor het geselecteerde tijdbereik. U kunt deze widget aanpassen met de volgende opties:
  - **Bereik (datum van bericht)**: (1 dag, 7 dagen, 30 dagen of deze maand).
  - Naam van de **workload**
  - **Status van de bewerking** (toegestaan, gemotiveerd of geblokkeerd)
  - **Gevoeligheid** (PHI, PII, Vertrouwelijk, PCI DSS)

- **Type bestemming** (extern, intern)
- **Groep** (workload, gebruiker, kanaal, type bestemming)

De widgets worden elke vijf minuten bijgewerkt. De widgets hebben klikbare elementen waarmee u problemen kunt onderzoeken en oplossen. U kunt de huidige status van het dashboard downloaden of in PDF- en/of XLSX-indeling via e-mail verzenden.

Aangepaste gevoeligheidscategorieën

Organisaties die hun intellectuele eigendom en specifieke vertrouwelijke gegevens van de organisatie willen beschermen, kunnen aangepaste categorieën voor gevoelige gegevens gebruiken als aanvulling op de ingebouwde Advanced DLP-catalogus van inhoudsdefinities voor naleving van de regelgeving.

Aangepaste gevoeligheidscategorieën maken:

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Navigeer naar **Bescherming** > **Preventie van gegevensverlies** > **Gegevensclassificaties**.
3. Selecteer **Gevoeligheidscategorie**.
4. U ziet een lijst met gevoeligheden, zowel ingebouwde (zoals beschermde gezondheidsinformatie of persoonlijk identificeerbare informatie) als aangepaste gevoeligheden.
5. Klik op **Gevoeligheid maken** in de rechterbovenhoek van het venster.
6. Geef de naam op in het volgende venster.
7. Nieuwe aangepaste gevoeligheden zijn standaard altijd uitgeschakeld. U kunt ze inschakelen zodra u alle bijbehorende parameters hebt geconfigureerd.
8. Nadat u een nieuwe gevoeligheid hebt gemaakt, moet u de inhoudsdetectoren hiervoor instellen. Klik op een pijl om de inhoud van uw nieuwe gevoeligheid uit te vouwen en selecteer **Inhoudsdetector toevoegen**.
9. In het volgende venster kunt u een van de bestaande inhoudsdetectoren gebruiken (door op het vinkje naast de betreffende naam te klikken en vervolgens op **Toevoegen** in de rechterbenedenhoek te klikken) of een nieuwe definiëren.
10. Als u geen nieuwe gevoeligheid wilt maken, kunt u een bestaande (ingebouwde of bestaande aangepaste gevoeligheid) hergebruiken door deze te klonen en de bijbehorende parameters aan te passen.
    - Als u een bestaande gevoeligheid wilt klonen, klikt u op een vinkje naast de betreffende naam en selecteert u vervolgens **Klonen** in het vervolgkeuzemenu Actie (aangegeven als ellips) in de linkerbovenhoek. U kunt meerdere items tegelijk selecteren als u meer dan een gevoeligheid wilt klonen.
    - In het volgende venster kunt u selecteren welke parameters van de bestaande gevoeligheid u wilt behouden door op de vinkjes naast de betreffende parameter te klikken.

Opmerking
Als u ingebouwde gevoeligheden binnen één tenant kopieert, wordt er een nieuwe gevoeligheid met dezelfde detectoren gemaakt (ze krijgen d se status Aangepast zodra ze zijn gekopieerd)

Een nieuwe inhoudsdetector maken:

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Navigeer naar **Bescherming** > **Preventie van gegevensverlies** > **Gegevensclassificaties**.
3. Selecteer **Inhoudsdetectoren**.
4. U ziet een lijst met inhoudsdetectoren, zowel ingebouwde als aangepaste.
5. Klik op **Inhoudsdetector maken** in de rechterbovenhoek van het venster.
6. Er wordt een vervolgkeuzemenu geopend waarin u het type detector kunt selecteren dat u wilt maken. Op dit moment is alleen de inhoudsdetector voor **bestandstype** beschikbaar, maar er komen er meer bij in toekomstige updates.
7. In het volgende venster kunt u de inhoudsdetector configureren.

Type inhoudsdetector	Beschrijving
Inhoudsdetector voor bestandstype	a. Er zijn twee lijsten: **Ondersteunde bestandstypen** en **Geselecteerde bestandstypen**. Door op een 'plus'-pictogram rechts van het ondersteunde bestandstype te klikken, verplaatst u het naar de lijst Geselecteerde bestandstypen. Als u meerdere ondersteunde bestandstypen wilt selecteren, kunt u op de vinkjes naast de betreffende namen klikken en vervolgens de knop **Geselecteerde toevoegen** in de rechterbovenhoek gebruiken. b. Als u een bestandstype wilt verwijderen uit de lijst Geselecteerde bestandstypen, klikt u op het prullenbakpictogram rechts van de betreffende naam. U kunt ook meerdere bestandstypen tegelijk verwijderen met behulp van vinkjes en de knop **Selectie verwijderen**.
Nieuwe inhoudsdetector voor trefwoorden	a. Wanneer u een nieuwe inhoudsdetector voor trefwoorden maakt, moet u trefwoorden uit een bestand importeren. Wanneer deze zijn geïmporteerd, kunt u nieuwe trefwoorden samenvoegen met de lijst met bestaande trefwoorden of de bestaande trefwoorden vervangen door de geïmporteerde trefwoorden. b. U moet ook bepalen of u wilt dat de inhoudsdetector overeenkomt met alle trefwoorden uit de lijst, een bepaald trefwoord uit de lijst of een aangepast aantal trefwoorden.

8. Als u geen nieuwe inhoudsdetector wilt maken, kunt u een bestaande (ingebouwde of aangepaste) hergebruiken door deze te klonen en de bijbehorende parameters aan te passen.
   - Als u een bestaande inhoudsdetector wilt klonen, klikt u op een vinkje naast de naam en selecteert u vervolgens **Klonen** in het vervolgkeuzemenu Actie (aangegeven als ellips) in de

linkerbovenhoek. U kunt meerdere items tegelijk selecteren als u meer dan een inhoudsdetector wilt klonen.

Opmerking
Als u een ingebouwde inhoudsdetector kopieert, krijgt deze de status Aangepast.

Organisatiekaart

Opmerking
Deze functionaliteit is alleen toegankelijk voor gebruikers met de rol van bedrijfbeheerder.

De organisatiekaart is een database die gegevens bevat voor gebruikers en al hun accounts die worden gebruikt voor gegevensoverdracht via chat, e-mail, of enig ander middel, en die is onderschept door Advanced DLP.

De organisatiekaart biedt middelen om gebruikersgroepen te maken en beheren in Advanced DLP, en om gebruikers en de aan gebruikers gekoppelde accounts in Advanced DLP te beheren. Gebruikersgroepen kunnen vervolgens worden gebruikt voor op groepen gebaseerd beleidsbeheer in DLP.

De organisatiekaart vinden

- Navigeer in de Cyber Protect Cloud-console naar **Bescherming** > **Preventie van gegevensverlies** > **Organisatiekaart**.

Hoe werkt dit?

Opmerking
Gegevens worden in de organisatiekaart ingevuld wanneer de observatiemodus van de Advanced DLP-module actief is.

Voor elke gegevensoverdracht die door de DLP-agent wordt onderschept, worden de volgende kenmerken verzameld in de backend.

Kenmerk	Beschrijving	Label in de UI
Organisatie-eenheid	Een handmatig gemaakte groep. De organisatie-eenheid kan een of meer geneste organisatie-eenheden bevatten.	Groepsnaam, zoals gedefinieerd
Beveiliging-id	Een unieke identificatie van de beveiliging.	Op de pagina met gebruikersgegevens > **SID**
	Een gebruiksvriendelijke weergavenaam afgeleid van de accountnamen voor de gebruiker. Deze naam is niet altijd beschikbaar in de organisatiekaart.	**Naam**

Kenmerk	Beschrijving	Label in de UI
Pc\Gebruikersnaam	De naam van de gebruiker van het eindpunt (workload). Een gebruikersnaam kan slechts aan één organisatie-eenheid worden toegewezen.	**Gebruikersnaam**
Apparaat (workload)	De naam van het eindpunt (workload).	**Workload**
Account	Accounts die door een gebruiker zijn gebruikt voor communicatie via chat en e-mail, en die is onderschept door de DLP-agent. Als de agent bijvoorbeeld detecteert dat de gebruikersnaam 'Pc\Jan' het adres jan@gmail.com gebruikt om een e-mail te sturen: dit account is gekoppeld aan de gebruikersnaam Pc\Jan.	**Accounts**

In de organisatiekaart kunt u accounts, gebruikers en groepen bekijken en zoeken, en groepen maken, bewerken en verwijderen.

Specifieke accounts zoeken

Als onderdeel van een onderzoek naar een incident kan het voorkomen dat gebruikers met de rol van beheerder soms de eigenaar van een specifiek account moeten vinden als dat account betrokken was bij een mogelijk datalek.

1. Navigeer in de Cyber Protect Cloud-console naar **Bescherming** > **Preventie van gegevensverlies** > **Organisatiekaart**.
2. Begin met typen of plak het account in het tekstvak **Zoeken** boven de lijst met gebruikers.
   De lijst wordt gefilterd terwijl u typt.

Een specifieke gebruikersnaam zoeken

1. Navigeer in de Cyber Protect Cloud-console naar **Bescherming** > **Preventie van gegevensverlies** > **Organisatiekaart**.
2. Als u wilt zoeken in een specifieke groep, klikt u op de groepsnaam in de lijst.
3. Begin met typen of plak een gebruikersnaam in het tekstvak **Zoeken** boven de lijst met gebruikers.
   De lijst wordt gefilterd terwijl u typt.

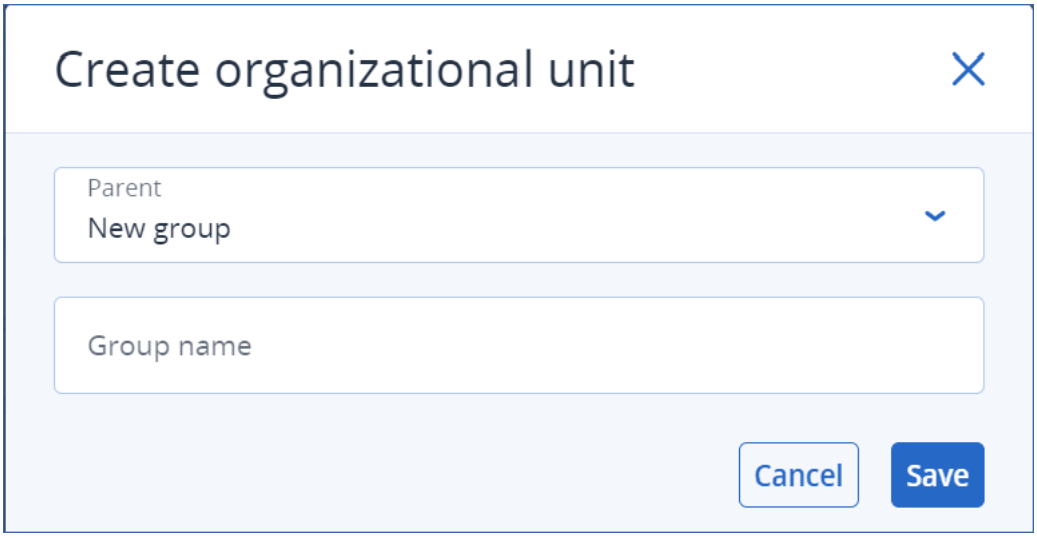
De accounts bekijken die worden gebruikt door een specifieke gebruikersnaam

1. Zoek de gebruiker in de lijst met gebruikers.
2. Klik op de drie puntjes aan het einde van de rij met gebruikers en selecteer **Weergeven**.
3. Open het dialoogvenster met gebruikersgegevens en zoek de sectie **Gekoppelde accounts**.
4. In het tekstvak Beschrijving kunt u opmerkingen toevoegen.

Een gebruikersgroep maken

1. Navigeer in de Cyber Protect Cloud-console naar **Bescherming** > **Preventie van gegevensverlies** > **Organisatiekaart**.

2. Ga naar de sectie linksonder in de groepenlijst en klik op **Groep maken**.
   Het dialoogvenster voor het maken van een organisatie-eenheid wordt geopend.



3. Open het vervolgkeuzemenu Bovenliggend en selecteer de context voor de nieuwe groep.

   Opmerking
   U kunt het bovenliggende item later niet wijzigen. De groep blijft genest in deze context.

4. Voer een groepsnaam in en klik op **Opslaan**.

Een gebruiker toevoegen aan een groep

1. Navigeer in de Cyber Protect Cloud-console naar **Bescherming** > **Preventie van gegevensverlies** > **Organisatiekaart**.
2. Ga naar de lijst met gebruikers, zoek de gebruiker die u wilt toevoegen en schakel het selectievakje in aan het begin van de rij met gebruikers.
   De knoppen **Geselecteerde verplaatsen** en **Geselecteerde verwijderen** worden weergegeven boven de lijst met gebruikers.
3. Klik op **Geselecteerde verplaatsen**.
   Het dialoogvenster Gebruiker verplaatsen wordt geopend.
4. Selecteer een nieuw bovenliggend item voor de geselecteerde gebruiker en klik op **Opslaan**.

Opmerking
Een gebruiker kan slechts tot één groep behoren.

Een account verwijderen dat is gekoppeld aan een gebruiker

1. Zoek de gebruiker in de lijst met gebruikers.
2. Klik op de drie puntjes aan het einde van de rij met gebruikers en selecteer **Weergeven**.
3. Open het dialoogvenster met gebruikersgegevens en zoek de sectie **Gekoppelde accounts**.

4. Zoek het account dat u wilt verwijderen en klik op de drie puntjes ernaast.
5. Open de vervolgkeuzelijst en selecteer **Verwijderen**.

Naam van een gebruikersgroep wijzigen

1. Navigeer in de Cyber Protect Cloud-console naar **Bescherming** > **Preventie van gegevensverlies** > **Organisatiekaart**.
2. Klik op de drie puntjes naast de naam van de groep en klik op **Hernoemen**.

Een gebruikersgroep verwijderen:

1. Navigeer in de Cyber Protect Cloud-console naar **Bescherming** > **Preventie van gegevensverlies** > **Organisatiekaart**.
2. Klik op de drie puntjes naast de naam van de groep en klik op **Verwijderen**.
   Alle gebruikers van de groep zijn verplaatst naar de bovenliggende entiteit.

Bekende problemen en beperkingen

- [DEVLOCK-4028] Er is geen besturingselement voor de groepschats in de Zoom-desktopagent.
- [DEVLOCK-4016] Beschrijvende naam en afzender-ID worden niet vastgelegd voor GMX Web Mail en Web.de Mail wanneer een concept wordt gemaakt.
- [DEVLOCK-4447] Er is geen Motivering-dialoogvenster voor naver.com WebMail wanneer een concept wordt gemaakt.
- [DEVLOCK-1033] DeviceLockDriver: mogelijke foutcontrole DRIVER_POWER_STATE_FAILURE veroorzaakt door een impasse tijdens de verwerking van IRP_MN_QUERY_DEVICE_RELATIONS.

Eindpuntdetectie en -respons (EDR)

Opmerking
Deze functionaliteit maakt deel uit van het Advanced Security + EDR-beschermingspakket (en dit pakket is een onderdeel van de Cyber Protection-service). Let op: wanneer u EDR-functionaliteit toevoegt aan een beschermingsschema, worden er mogelijk extra kosten in rekening gebracht.

Met Eindpuntdetectie en -respons (EDR) worden verdachte activiteiten voor de workload gedetecteerd, waaronder onopgemerkte aanvallen. In EDR worden er vervolgens incidenten gegenereerd, met een stapsgewijs overzicht van elke aanval, zodat u begrijpt hoe een aanval heeft plaatsgevonden en hoe u kunt voorkomen dat dit opnieuw gebeurt. Dankzij gemakkelijk te begrijpen interpretaties van elke fase van de aanval kunnen aanvallen binnen enkele minuten worden onderzocht.

Waarom u Eindpuntdetectie en -respons (EDR) nodig hebt

In de huidige uitdijende wereld van cyberdreigingen en kwaadaardige aanvallen is preventie niet langer voldoende om volledige bescherming te waarborgen. Er zijn altijd aanvallen die de preventielagen kunnen doorbreken en het netwerk binnendringen. Conventionele oplossingen

kunnen niet zien wanneer dit gebeurt, waardoor aanvallers dagen, weken of maanden vrij spel hebben in uw omgeving.

Bestaande EDR-oplossingen helpen deze 'stille inbreuken' te voorkomen door aanvallers snel te vinden en te verwijderen. Hiervoor is echter doorgaans een hoog niveau van beveiligingsexpertise vereist of u moet beroep doen op dure Security Operation Center (SOC)-analisten. De analyse van incidenten kan bovendien veel tijd kosten.

Met de functionaliteit van Acronis Advanced Security + EDR worden deze beperkingen verholpen. Onopgemerkte aanvallen worden gedetecteerd en u krijgt inzicht in de manier waarop een aanval heeft plaatsgevonden en hoe u kunt voorkomen dat dit opnieuw gebeurt. Bovendien bent u zo minder tijd kwijt aan het onderzoek naar de aanvallen.

Dit is waarom u EDR nodig hebt:

- **Volledige zichtbaarheid**: Begrijp wat er is gebeurd en hoe het is gebeurd, zelfs in het geval van onopgemerkte aanvallen. De voortgang van elke aanval wordt ook stap voor stap visueel in kaart gebracht (van het eerste punt van binnenkomst tot het bekijken van de gegevens die het doelwit waren en/of die zijn geëxfiltreerd), zodat u snel de reikwijdte en impact van een incident kunt begrijpen. Zie "Incidenten in de cyber kill chain onderzoeken" (p. 973) voor meer informatie.
- **Kortere onderzoekstijd**: Verkort de onderzoekstijd van incidenten, van uren tot slechts enkele minuten. EDR beschrijft elke stap van de aanval in duidelijke, gemakkelijk te begrijpen menselijke taal, waardoor er minder behoefte is aan dure experts of extra personeel. Zie "Incidenten onderzoeken" (p. 972) voor meer informatie
- **Controle op bekende bedreigingen voor uw workloads**: U kunt uw workloads automatisch laten onderzoeken op bedreigingen van malware, beveiligingsproblemen en andere typen globale gebeurtenissen die van invloed kunnen zijn op uw gegevensbescherming. Deze bedreigingen worden Incidents of Compromise (IOC's of inbreukincidenten) genoemd en zijn gebaseerd op bedreigingsgegevens ontvangen van het Cyber Protection Operations Center (CPOC). Zie "Controleren op inbreukindicatoren (IOC's) in openbaar bekende aanvallen op uw workloads" (p. 985) voor meer informatie.
- **Snellere reactie op incidenten**: U hebt zicht op alle activiteiten na de inbreuk, met een uitsplitsing van elke stap in de kill chain, zodat u diverse acties kunt uitvoeren om elk aanvalspunt te herstellen. U kunt onder andere onderzoek uitvoeren met externe besturing en forensische back-up (deze functie is niet beschikbaar in de versie Vroege toegang), workloads in quarantaine plaatsen en malwareprocessen beëindigen. U kunt bedrijfsactiviteiten ook herstellen met behulp van Cyber Disaster Recovery Cloud. Zie "Incidenten verhelpen" (p. 989) voor meer informatie.
- **Betrouwbare rapportage over uw beveiligingsstatus**: Als EDR is ingeschakeld, kunt u een groot deel van de onzekerheid en angst voor de impact van cyberaanvallen op uw bedrijf wegnemen. Daarnaast wordt informatie over incidenten gedurende 180 dagen bewaard, zodat deze kan worden gebruikt voor audits.

Functies

Eindpuntdetectie en -respons (EDR) biedt de volgende functies:

- Waarschuwingsmeldingen ontvangen wanneer er een schending plaatsvindt
- Uw incidenten beheren op de pagina voor incidenten
- Eenvoudig te begrijpen visualisatie van de verhaallijn van de aanval
- Aanbevelingen en stappen voor herstel
- De bedreigingsfeeds raadplegen om openbaar gemaakte aanvallen op uw workloads te bekijken
- Snel overzicht krijgen in het dashboard
- Beveiligingsgebeurtenissen bewaren gedurende 180 dagen

Waarschuwingsmeldingen ontvangen wanneer er een schending plaatsvindt

EDR biedt waarschuwingsmeldingen wanneer er zich een incident voordoet. Deze waarschuwingen worden gemarkeerd in het hoofdmenu van de Cyber Protect-console. U kunt een waarschuwing vervolgens onderzoeken door te klikken op de knop **Incident onderzoeken**. U wordt dan omgeleid naar het scherm voor het onderzoeken van incidenten (ook bekend als de cyber kill chain).

Zie "Incidenten bekijken" (p. 951) voor meer informatie.

Uw incidenten beheren op de pagina voor incidenten

Met EDR kunt u al uw incidenten beheren op de pagina Incidenten (toegankelijk via het menu Bescherming in de Cyber Protect-console). Op de pagina Incidenten, die kan worden gefilterd op basis van uw vereisten, kunt u snel en eenvoudig de huidige status van uw incidenten nagaan, inclusief de ernst, de getroffen workload en het positiviteitsniveau. U kunt ook rechtstreeks naar de cyber kill chain navigeren om de verhaallijn van de aanval per knooppunt te bekijken.

Zie "Incidenten bekijken" (p. 951) voor meer informatie over de pagina Incidenten.

Eenvoudig te begrijpen visualisatie van de verhaallijn van de aanval

EDR biedt een visuele weergave van een aanval in een gemakkelijk leesbare indeling. Zo kunnen ook medewerkers die niet zijn gespecialiseerd in beveiliging, inzicht krijgen in de doelen en ernst van elke aanval. U hoeft geen Security Operation Center (SOC)-service te hebben of beveiligingsexperts in te huren, want EDR beschrijft precies hoe een aanval plaatsvond, met informatie over:

- Hoe de aanvaller kon binnendringen
- Hoe de aanvaller de eigen sporen heeft verborgen
- Wat voor schade er is aangericht
- Hoe de aanvaller werd verspreid

Zie "Incidenten in de cyber kill chain onderzoeken" (p. 973) voor meer informatie.

Aanbevelingen en stappen voor herstel

EDR biedt duidelijke en eenvoudig te implementeren aanbevelingen voor het oplossen van aanvallen op een workload. Als u een aanval snel wilt oplossen, klikt u op de knop **Het hele**

incident verhelpen. Bekijk en volg de aanbevolen stappen om het incident te verhelpen. Met deze aanbevolen stappen kunt u de door een aanval getroffen bewerkingen snel hervatten. Als u echter meer gedetailleerde stappen voor herstel wilt uitvoeren, kunt u naar elk knooppunt navigeren en daar de relevante actie uitvoeren.

Zie "Incidenten verhelpen" (p. 989) voor meer informatie.

De bedreigingsfeeds raadplegen om openbaar gemaakte aanvallen op uw workloads te bekijken

EDR biedt de mogelijkheid om bestaande, bekende aanvallen in bedreigingsfeeds voor uw workloads te bekijken. Deze bedreigingsfeeds worden automatisch gegenereerd op basis van bedreigingsgegevens die zijn ontvangen van het Cyber Protection Operations Center (CPOC). Met EDR kunt u nagaan of een bedreiging al dan niet uw workload beïnvloedt, en vervolgens de nodige stappen ondernemen om de bedreiging ongedaan te maken.

Zie "Controleren op inbreukindicatoren (IOC's) in openbaar bekende aanvallen op uw workloads" (p. 985) voor meer informatie.

Snel overzicht krijgen in het dashboard

EDR biedt een reeks statistieken in het dashboard van de Cyber Protect-console. U kunt de volgende gegevens bekijken:

- De huidige status van bedreigingen, met nadruk op incidenten die moeten worden onderzocht.
- De voortgang van aanvallen naar ernstgraad, met aanwijzingen voor mogelijke aanvalscampagnes.
- De efficiëntiegraad voor het afhandelen van incidenten.
- De meest specifiek op uw klanten gerichte aanvalstactieken.
- De netwerkstatus van de workload: of deze geïsoleerd of verbonden is.

Beveiligingsgebeurtenissen bewaren gedurende 180 dagen

EDR verzamelt gebeurtenissen van workloads en toepassingen en slaat deze op gedurende 180 dagen. Gebeurtenissen die ouder zijn dan de periode van 180 dagen, worden verwijderd (verwijdering van gebeurtenissen is gebaseerd op leeftijd en niet op basis van opslagruimte). Let op: zelfs wanneer EDR is uitgeschakeld, blijven alle eerder verzamelde gebeurtenissen voor een workload behouden, zodat ze beschikbaar zijn voor onderzoek naar incidenten.

Softwarevereisten

Eindpuntdetectie en -respons (EDR) ondersteunt de volgende besturingssystemen:

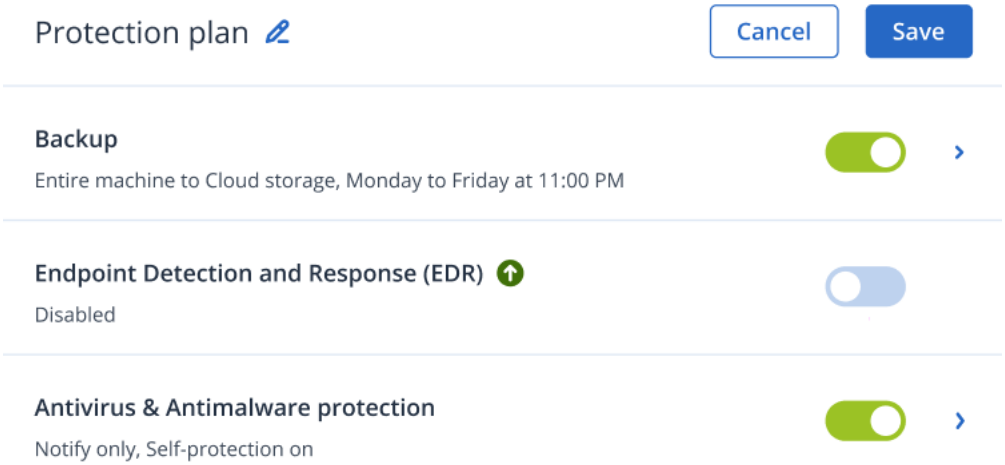
- Microsoft Windows 7 Service Pack 1 en later
- Microsoft Windows Server 2008 R2 en later

Functionaliteit van Eindpuntdetectie en -respons (EDR) inschakelen

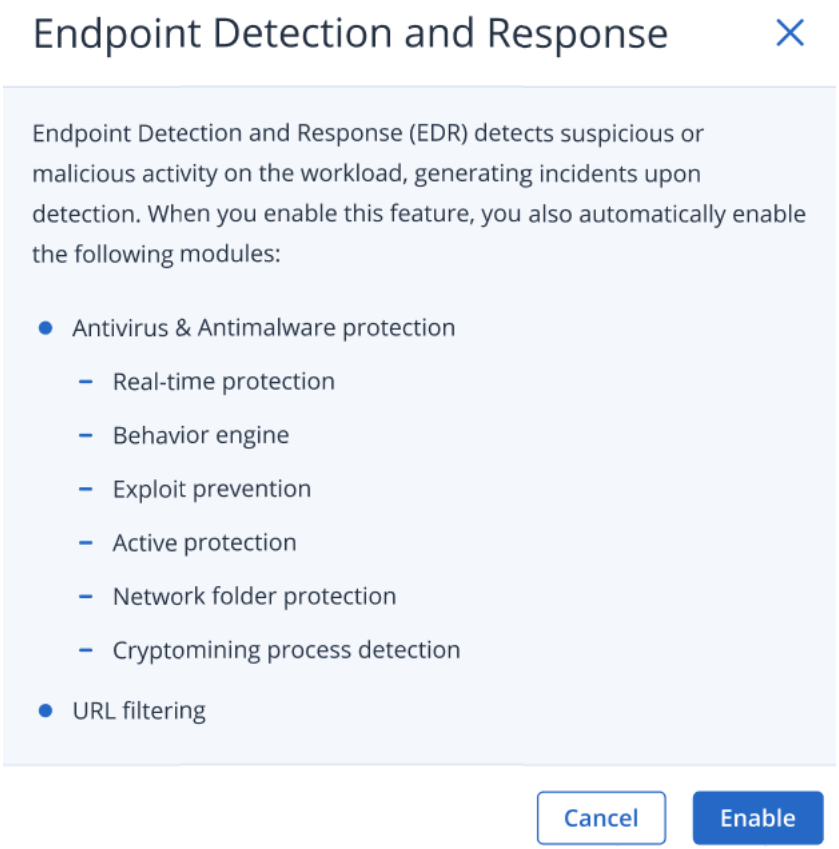
U kunt EDR inschakelen in elk beschermingsschema.

EDR inschakelen:

1. Ga in de Cyber Protect-console naar **Beheer > Beschermingsschema's**.
2. Selecteer het gewenste beschermingsschema in de weergegeven lijst en klik in de rechterzijbalk op **Bewerken**.
   U kunt indien gewenst ook een nieuw beschermingsschema maken en doorgaan naar de volgende stap. Zie "Beschermingsschema's en -modules" (p. 216) voor meer informatie over het werken met beschermingsschema's.
3. Ga naar de zijbalk van het beschermingsschema en schakel de module **Eindpuntdetectie en -respons** in door op de schakelaar naast de naam van de module te klikken.



4. Klik in het weergegeven dialoogvenster op **Inschakelen**. Let op: wanneer EDR is ingeschakeld, zijn andere beschermingsmodules ook ingeschakeld, zoals weergegeven in het dialoogvenster.



Opmerking
Als een van de modules **Active Protection**, **Gedragengine**, **Preventie tegen aanvallen** of **URL-filtering** is **uitgeschakeld**, wordt **Eindpuntdetectie en -respons (EDR)** ook **uitgeschakeld**.

5. Het pictogram van het **Advanced Security + EDR**-pakket, zoals hieronder weergegeven, wordt toegevoegd aan de lijst met beschermingspakketten die vereist zijn voor de implementatie van het beschermingsschema, afhankelijk van de aanvullende pakketten die u selecteert.

Eindpuntdetectie en -respons (EDR) gebruiken

Met EDR kunt u onopgemerkte aanvallen detecteren en krijgt u inzicht in de manier waarop een aanval heeft plaatsgevonden en hoe u kunt voorkomen dat dit opnieuw gebeurt. Dankzij gemakkelijk te begrijpen interpretaties van elke fase van de aanval kunnen aanvallen binnen enkele minuten worden onderzocht.

De onderstaande tabel bevat de algemene workflow van EDR. In eerste instantie bekijkt en prioriteert u nieuwe incidenten. U kunt deze dan verder onderzoeken in de cyber kill chain en vervolgens de relevante herstelacties ondernemen.

Stap	EDR gebruiken
STAP 1: Incidenten bekijken	In de lijst met incidenten van EDR: • Krijg inzicht in de beveiligingsstatus van een organisatie: hoeveel incidenten moeten worden onderzocht? • Ga na wat de meest kritieke incidenten zijn en prioriteer het onderzoek op basis van de ernstgraad. • Ontdek welke incidenten nieuw of doorlopend zijn.
STAP 2: Incidenten onderzoeken	In de cyber kill chain van EDR: • Krijg inzicht in de doelen van de aanvaller en bekijk de gebruikte aanvalstechnieken. • Controleer hoe waarschijnlijk het is dat een incident een echte kwaadaardige aanval is. • Controleer of een bedreigingsfeed al dan niet van invloed is op uw workload. • Bekijk welke responsacties al zijn toegepast op een incident.
STAP 3: Incidenten verhelpen	In de relevante gedeelten over herstel in EDR: • Verhelp snel en eenvoudig een volledig incident door globale responsacties toe te passen. • Verhelp individuele aanvalspunten binnen een incident. • Pas acties toe om te voorkomen dat de aanval (of toekomstige aanvallen) zich verspreiden of workloads beïnvloeden die nog niet het doelwit zijn van de aanvaller.

Incidenten bekijken

Eindpuntdetectie en -respons (EDR) biedt een lijst met incidenten, met zowel preventie (of malware) als verdachte detecties voor een workload. De lijst met incidenten biedt u een snel overzicht van eventuele aanvallen of bedreigingen die van invloed zijn op uw workloads, inclusief bedreigingen die nog niet zijn verholpen.

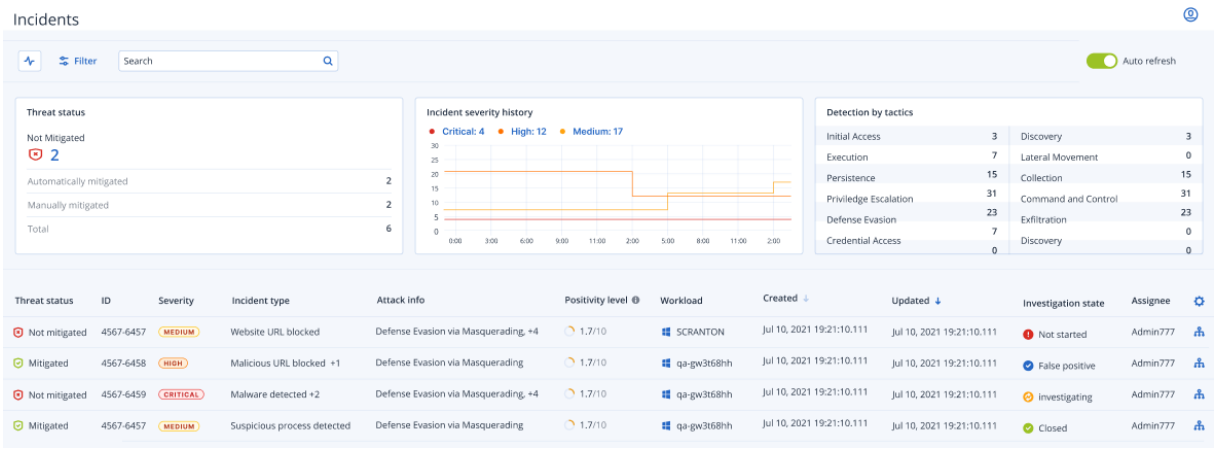
Met behulp van de incidentenlijst kunt u snel het volgende bepalen:

- De beveiligingsstatus van een organisatie: hoeveel incidenten moeten worden onderzocht?
- Wat zijn de meest kritieke incidenten en wat zijn de prioriteiten voor onderzoek op basis van de ernstgraad?
- Welke incidenten zijn nieuw en welke zijn doorlopend?

Opmerking
Wanneer u bent aangemeld als partnerbeheerder, kunt u alle EDR-incidenten bekijken op een enkel scherm waarop incidenten van al uw klanten samen worden weergegeven, zodat u niet elke afzonderlijke incidentweergave van de klant hoeft te openen. Een extra kolom **Klanten** wordt weergegeven, met de klantnaam waartoe elk incident behoort. De widgets op het dashboard **Overzicht** bevatten geaggregeerde metrische gegevens over alle klanten.

De lijst met incidenten, zoals hieronder weergegeven, is toegankelijk via het menu **Bescherming** in de Cyber Protect-console. Zie "Bekijken welke incidenten nog niet worden verholpen" (p. 954) voor meer informatie over het bekijken van de incidenten in de lijst met incidenten en zie Wat zijn incidenten? voor meer informatie over wanneer er een incident wordt gemaakt.

Opmerking
Als Managed Detection and Response (MDR) is ingeschakeld voor uw workloads, wordt een extra kolom **MDR-ticket** weergegeven. Deze kolom toont het ticketnummer dat door de MDR-leverancier is opgegeven.



Opmerking
De Cyber Protect-console moet zijn geopend om incidentmeldingen te kunnen ontvangen.

Wat zijn incidenten?

Incidenten, of beveiligingsincidenten, kunnen worden gezien als *containers* van ten minste één preventief of verdacht detectiepunt (of een combinatie ervan) en omvatten alle gerelateerde gebeurtenissen en detecties van een enkele aanval. Deze beveiligingsincidenten kunnen ook aanvullende goedaardige gebeurtenissen omvatten die meer context geven over de gebeurtenis.

Hierdoor kunt u aanvalsgebeurtenissen samen in één incident bekijken en inzicht krijgen in de logische stappen die de aanvaller heeft uitgevoerd. Daarnaast hebt u zo minder tijd nodig voor het onderzoek naar een aanval.

Wanneer EDR is ingeschakeld in het beschermingsschema, worden er beveiligingsincidenten gemaakt in de volgende gevallen:

- **Er is iets gestopt door een preventielaag:** Deze incidenten worden automatisch gesloten door het systeem, afhankelijk van de instellingen van het beschermingsschema. U kunt echter wel onderzoeken wat de malware precies deed voordat deze werd gestopt. Ransomware wordt bijvoorbeeld gestopt wanneer het begint bestanden te versleutelen, maar mogelijk zijn er voordien al referenties gestolen of is er een service geïnstalleerd.
- **Er is verdachte activiteit gedetecteerd door EDR:** Dit zijn detecties die moeten worden onderzocht en verholpen. Door de visueel verbeterde cyber kill chain te bekijken (zie "Incidenten

in de cyber kill chain onderzoeken" (p. 973) voor meer informatie) kunt u gemakkelijk de betreffende herstelacties toepassen.

Prioriteren welke incidenten onmiddellijke aandacht vereisen

De lijst met incidenten van de Cyber Protect-console is op elk moment toegankelijk via het menu **Bescherming** in de Cyber Protect-console. De lijst met incidenten biedt u een snel overzicht van eventuele aanvallen of bedreigingen, zodat u prioriteit kunt geven aan incidenten die aandacht vereisen.

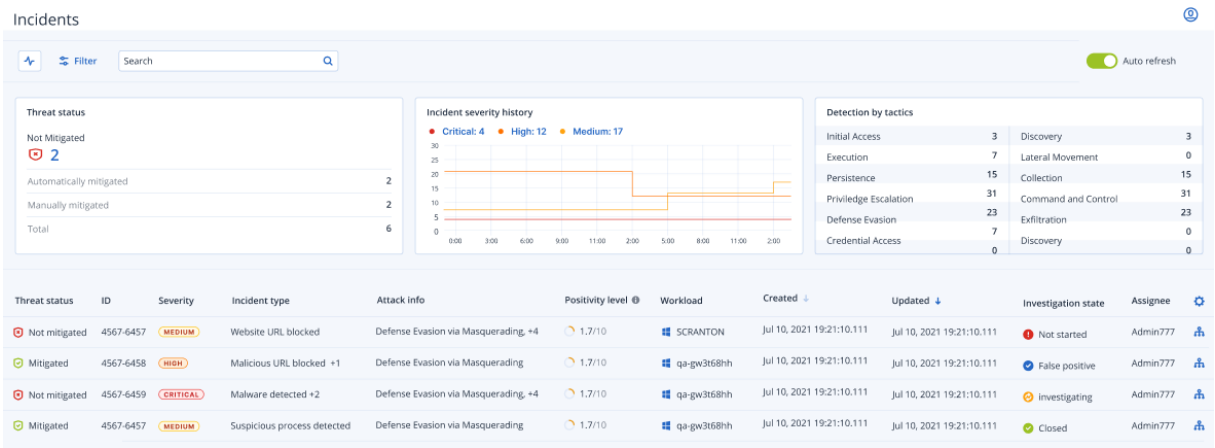
Belangrijk
Als u wilt waarborgen dat uw workloads veilig blijven, moet u *altijd* de incidenten analyseren en prioriteren die actueel zijn of nog niet zijn verholpen.

Analyseren welke beveiligingsincidenten onmiddellijke aandacht nodig hebben

Met de incidentenlijst kunt u analyseren en prioriteren welke van de vermelde incidenten uw aandacht vereisen. U kunt:

- Bekijken welke incidenten momenteel nog niet zijn verholpen: Gebruik de lijst met incidenten om snel te zien of er momenteel aanvallen gaande zijn. Alle incidenten die nog niet zijn verholpen, zoals aangegeven in de kolom **Bedreigingsstatus**, moeten onmiddellijk worden onderzocht (de lijst met incidenten wordt standaard gefilterd om deze incidenten weer te geven).
- Inzicht krijgen in de reikwijdte en impact van incidenten: U kunt filteren op nieuw begonnen of actuele aanvallen om inzicht te krijgen in de ernst van de gefilterde incidenten en de impact op uw bedrijf.

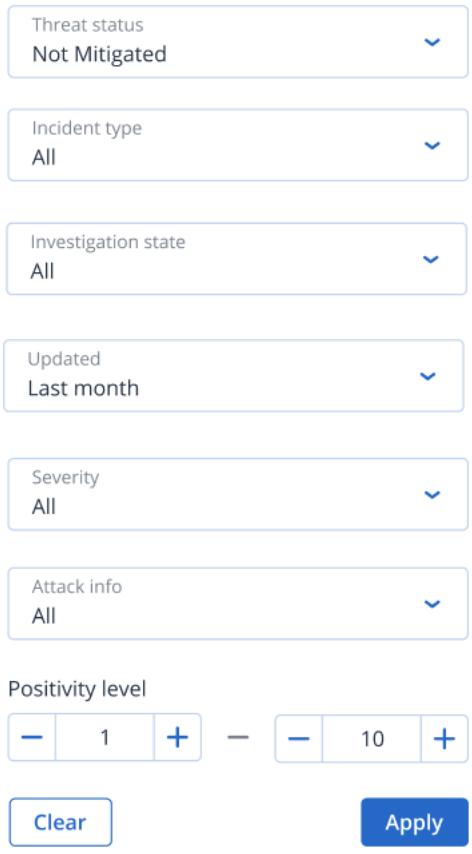
Wanneer u een nauwkeurige lijst van de belangrijkste incidenten hebt, kunt u de details van de incidenten analyseren om meer inzicht te krijgen in specifieke incidenten en de technieken die door aanvallers worden gebruikt om hun doelen te bereiken. Zie "Details van incident analyseren" (p. 957) voor meer informatie.



Opmerking
De lijst met incidenten wordt standaard gesorteerd op de kolom **Bijgewerkt**. Deze kolom bevat de datum en tijd waarop het incident voor het laatst is bijgewerkt met nieuwe detecties die zijn geregistreerd voor het incident. Let op: elk bestaand incident kan op elk moment worden bijgewerkt, zelfs als het incident eerder is gesloten. U kunt de lijst ook filteren om nieuw begonnen of actuele aanvallen weer te geven volgens uw vereisten, zoals beschreven in de onderstaande procedure.

De lijst met incidenten filteren

1. Klik bovenaan de lijst met incidenten op **Filteren** om de weergegeven lijst met incidenten te filteren. Als u bijvoorbeeld een begin- en einddatum selecteert in het veld **Gemaakt**, bevatten de lijst met incidenten en de widgets alleen de incidenten die tijdens de gedefinieerde periode zijn gemaakt.



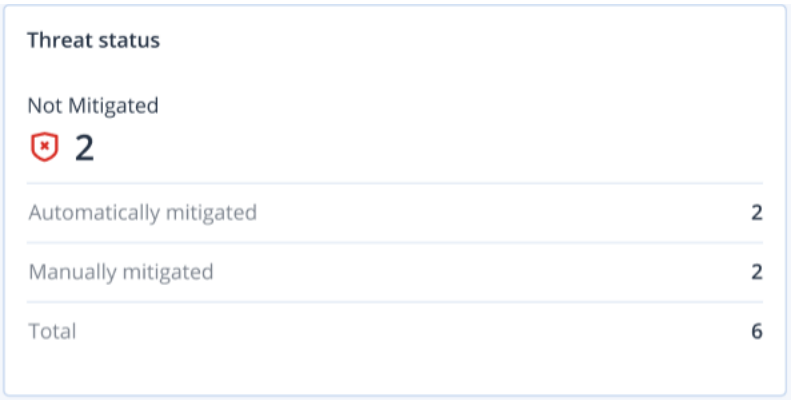
2. Wanneer u klaar bent, klikt u op **Toepassen**.

Bekijken welke incidenten nog niet worden verholpen

U kunt de huidige bedreigingsstatus voor incidenten bekijken in de kolom **Bedreigingsstatus**, die aangeeft of het incident de status **Beperkt** of **Niet beperkt** heeft. De bedreigingsstatus wordt automatisch bepaald door EDR. Elk incident dat nog niet wordt verholpen, moet zo snel mogelijk worden onderzocht.

Vervolgens kunt u de weergegeven lijst met incidenten verder verfijnen door filters toe te passen. Als u de lijst bijvoorbeeld wilt filteren op bedreigingsstatus *en* een bepaalde ernstgraad, selecteert u de betreffende filteropties. Wanneer u de incidenten hebt gefilterd die voor u van belang zijn, kunt u deze onderzoeken, zoals beschreven in "Incidenten onderzoeken" (p. 972).

U kunt ook de widget **Bedreigingsstatus** gebruiken, zoals hieronder weergegeven, voor een snel overzicht van de huidige bedreigingsstatus. Let op: de gegevens die in deze widget worden weergegeven, komen overeen met de filters die u hebt toegepast. Zie "De lijst met incidenten filteren" (p. 954).



Inzicht krijgen in de reikwijdte en impact van incidenten

U krijgt snel inzicht in de reikwijdte en impact van incidenten door de kolommen **Ernstgraad**, **Info over aanval** en **Positiviteitsniveau** te bekijken. Zoals hierboven vermeld, kunt u, nadat u hebt vastgesteld welke incidenten nog actueel zijn, de volgende aanvullende kolommen filteren:

- De kolom **Ernstgraad**: bekijken welke incidenten het meest kritiek zijn. De ernstgraad van een incident kan **Kritiek**, **Hoog** of **Matig** zijn.
  - **Kritiek**: Er is een ernstig risico van kwaadaardige cyberactiviteit met het risico dat kritieke hosts in uw omgeving worden gecompromitteerd.
  - **Hoog**: Er is een hoog risico van kwaadaardige cyberactiviteit met het risico dat uw omgeving ernstige schade ondervindt.
  - **Medium**: Er is een verhoogd risico van kwaadaardige cyberactiviteit.

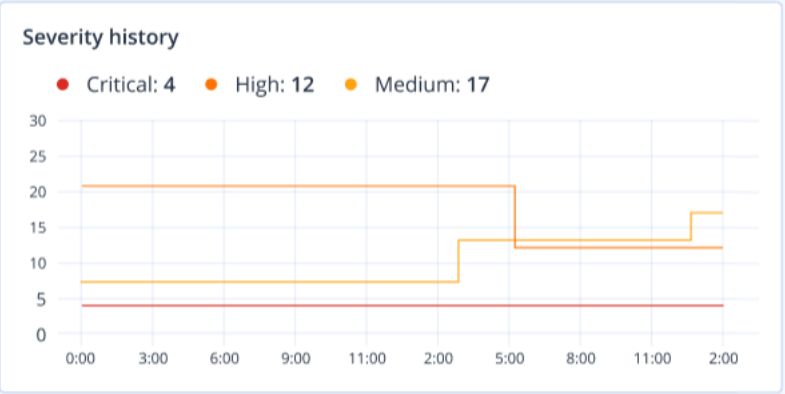
    Opmerking
    Bij het bepalen van de ernstgraad houdt het EDR-algoritme rekening met het type workload en de reikwijdte van elke stap van de aanval. Een incident dat stappen bevat met betrekking tot diefstal van referenties, wordt bijvoorbeeld ingesteld op **Kritiek**.

- Ga naar de kolom **Type incident** om te zien waarom een incident is gegenereerd. Het type incident kan een of meer van de volgende typen zijn:
  - **Ransomware gedetecteerd**
  - **Malware gedetecteerd**
  - **Verdacht proces gedetecteerd**

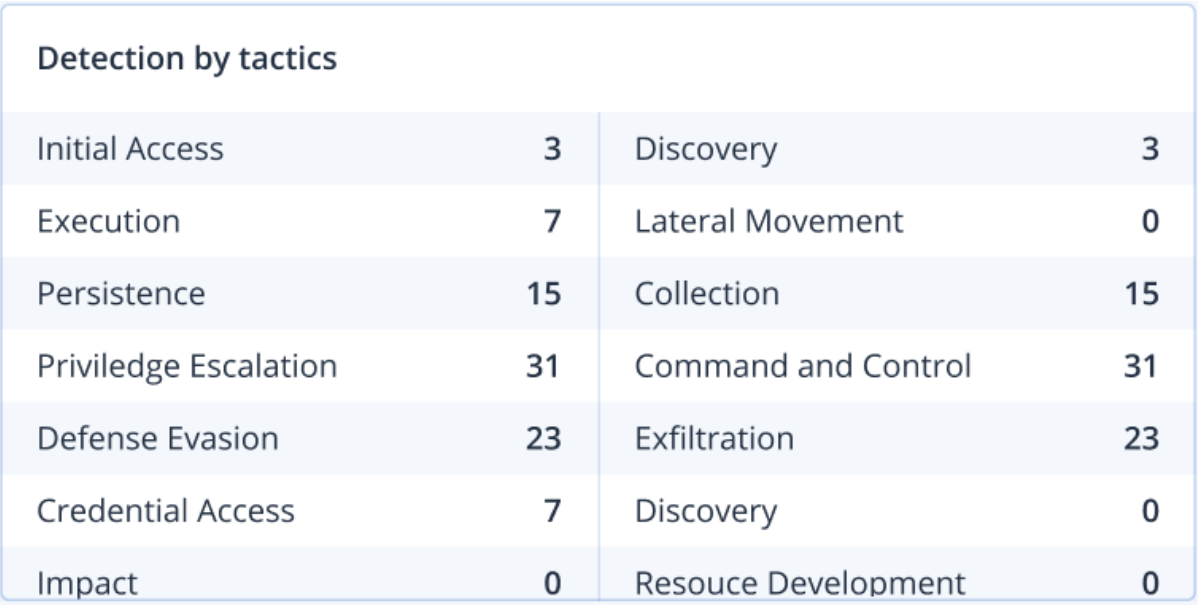
    - **Schadelijk proces gedetecteerd**
    - **Verdachte URL geblokkeerd**
    - **Schadelijke URL geblokkeerd**
- De kolom **Info over aanval**: bepalen welke aanvalstechnieken worden gebruikt en inzicht krijgen in eventuele gemeenschappelijke thema's of patronen in de aanvallen.
- De kolom **Positiviteitsniveau**: bevestigen hoe waarschijnlijk het is dat een incident daadwerkelijk een kwaadaardige aanval is aan de hand van een score tussen 1 en 10 (hoe hoger de score, hoe groter de kans dat de aanval een daadwerkelijk een kwaadaardige aanval is).

Nadat u de incidenten hebt gevonden die onmiddellijke aandacht vereisen, kunt u deze onderzoeken, zoals beschreven in "Incidenten onderzoeken" (p. 972)

U kunt ook de widgets **Geschiedenis van de ernst** en **Detectie door tactieken** gebruiken voor een snel overzicht van de ernstgraad en aanvalstechnieken.



De widget **Detectie door tactieken** geeft de verschillende gebruikte aanvalstechnieken weer, met waarden in groen of rood die de toename of afname aangeven in de eerder opgegeven periode. Deze widget biedt een geaggregeerd overzicht van alle doelstellingen in de gefilterde incidenten, waardoor u snel een overzicht krijgt van de impact op uw klanten.

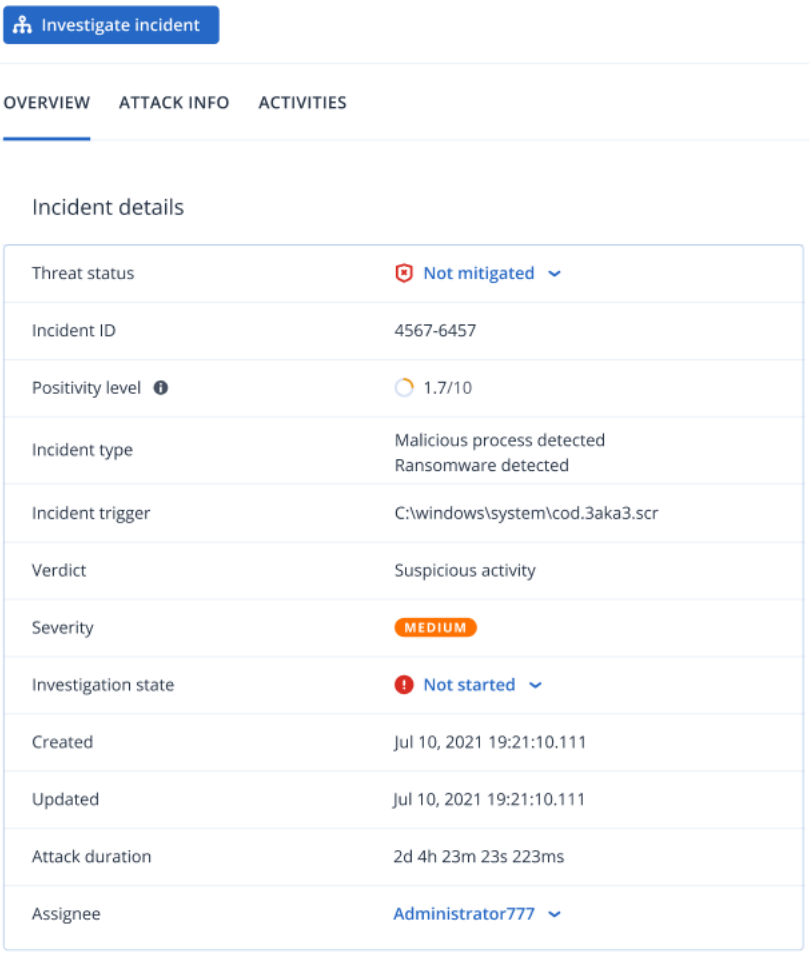


Details van incident analyseren

Tijdens de beoordelingsfase van het incident kunt u ook de details analyseren van elk incident in de lijst met incidenten van Eindpuntdetectie en -respons (EDR). Met deze details kunt u inzoomen op het hele incident en begrijpen hoe en waarom het heeft plaatsgevonden. Daarnaast kunt u een incident toewijzen aan specifieke gebruikers voor onderzoek en u kunt de onderzoeksstatus instellen.

Details van incident analyseren:

1. Ga in de Cyber Protect-console naar **Bescherming > Incidenten**. De lijst met incidenten wordt weergegeven.
2. Klik op het incident dat u wilt bekijken. De details van het geselecteerde incident worden weergegeven.
3. Op het weergegeven tabblad **Overzicht** kunt u de details van het incident en de workload bekijken, inclusief de huidige bedreigingsstatus en ernstgraad. U kunt ook de **onderzoeksstatus** definiëren (kies uit **Wordt onderzocht**, **Niet gestart** (de standaardstatus), **Fout-positief** of **Gesloten**) en een gebruiker selecteren aan wie u het incident wilt toewijzen (selecteer de betreffende gebruiker in de vervolgkeuzelijst **Toegewezen persoon**).



4. Klik op het tabblad **Info over aanval** om de details van de aanval en de bij de aanval gebruikte technieken te bekijken. Klik op de link naast elke vermelde aanvalstechniek en lees meer informatie over de techniek op MITRE.org.
5. Klik op het tabblad **Activiteiten** om alle acties te bekijken die in de cyber kill chain zijn ondernomen om een incident te verhelpen. Zie "Incidenten in de cyber kill chain onderzoeken" (p. 973) voor meer informatie.
   Als er bijvoorbeeld een patch is uitgevoerd voor de workload, kunt u zien wie de patch heeft geïnitieerd, hoeveel tijd nodig was voor de implementatie en welke fouten er zijn opgetreden tijdens de implementatie van de patch.
6. Klik op **Incident onderzoeken** om toegang te krijgen tot de cyber kill chain waar u het incident per knooppunt kunt onderzoeken. Zie "Incidenten in de cyber kill chain onderzoeken" (p. 973) voor meer informatie.

Zoeken naar inbreukindicatoren (IoC) en verdachte activiteiten

Opmerking
Deze functie maakt deel uit van het Early Access Program. Sommige functionaliteiten en beschrijvingen zijn mogelijk niet volledig.

Als u bedreigingen wilt detecteren en beperken voordat ze uitgroeien tot incidenten met een hoge impact, kunt u gebruikmaken van de functie **Gebeurtenissen zoeken**. Met deze zoekfunctie kunt u IoC's en verdachte activiteiten opsporen in alle workloads die zijn ingeschakeld met Eindpuntdetectie en -respons (EDR).

Gebruik de functie **Gebeurtenissen zoeken** voor het volgende:

- Aangepaste zoekopdrachten uitvoeren voor gebeurtenisgegevens die zijn verzameld uit alle workloads om te zoeken naar hashes. U kunt ook maatstaven ophalen om bepaalde vragen te beantwoorden (bijvoorbeeld: workloads met een ongebruikelijk hoog aantal processen weergeven).
- Zoekopdrachten filteren met behulp van kenmerken die door EDR-eindpunten worden geleverd en gegevens uit andere integraties, zoals activiteiten van het besturingssysteem, gebruikersactiviteiten en netwerkactiviteiten.

De functie **Gebeurtenissen zoeken** is toegankelijk vanuit het menu **Bescherming** in de Cyber Protect-console.

Opmerking
De standaard-retentieperiode voor zoekresultaten van EDR-gebeurtenissen is zeven dagen.

Gebeurtenissen zoeken

Opmerking
Deze functie maakt deel uit van het Early Access Program. Sommige functionaliteiten en beschrijvingen zijn mogelijk niet volledig.

U kunt zoeken naar Eindpuntdetectie en -respons (EDR)-gebeurtenissen in alle workloads die worden beschermd door EDR.

Let op: wanneer u de Cyber Protect-console gebruikt op het niveau van de partnertenant **(Alle klanten)**, kunt u zoeken naar gebeurtenissen van al uw beheerde klanten. Als u werkt op het niveau van de klanttenant, kunt u zoeken naar gebeurtenissen die specifiek zijn voor de geselecteerde klant.

Gebeurtenissen zoeken:

1. Ga in de Cyber Protect-console naar **Bescherming** > **Gebeurtenissen zoeken**.
2. Voer uw zoekopdracht in met behulp van Acronis XDR Query Language (XQL) en definieer een datumbereik.

   Let op: XQL maakt gebruik van AutoAanvullen om u te helpen bij het schrijven van een zoekopdracht. Voor meer informatie over de syntaxis en beschikbare opties voor zoekopdrachten: zie "Syntaxis" (p. 960).
3. Klik op het pijlpictogram rechts van het invoerveld om de zoekopdracht uit te voeren.

   Let op: u kunt ook gebruikmaken van de volgende toetsenbordcombinaties:
   - Druk op **Enter** om de cursor naar de volgende regel te verplaatsen. Het teken "|" wordt aan het begin van de nieuwe regel toegevoegd (dit is handig is bij het schrijven van zoekopdrachten met meereder fasen).
   - Druk op **Shift+Enter** om de cursor naar de volgende regel te verplaatsen.
   - Druk op **Ctrl+Enter** om de zoekopdracht uit te voeren.
4. Verfijn indien nodig uw zoekopdracht. U kunt bijvoorbeeld selecteren of u specifieke velden of gebeurtenissen wilt weergeven die een bepaalde bestandsnaam bevatten.

Acronis XDR Query Language (XQL)

Opmerking
Deze functie maakt deel uit van het Early Access Program. Sommige functionaliteiten en beschrijvingen zijn mogelijk niet volledig.

Gebruik XQL om te zoeken naar Eindpuntdetectie en -respons (EDR)-gebeurtenissen en bekijk vervolgens de details van de gebeurtenissen die u zoekt. Dit gedeelte bevat de verschillende elementen van XQL die u moet kennen bij het zoeken naar EDR-gebeurtenissen:

- Syntaxis (inclusief voorbeelden van zoekopdrachten)
- Gebeurtenistypen en velden

Voor meer informatie over het gebruik van de functie **Gebeurtenissen zoeken**: zie "Zoeken naar inbreukindicatoren (IoC) en verdachte activiteiten" (p. 958).

Syntaxis

Bewerking	Voorbeeld
Gegevensbron selecteren Selecteert de gegevensbron voor de betreffende zoekopdracht. Deze operator moet de eerste operator in de zoekopdracht zijn.	`eventType`

Gegevens filteren
 	
Filtert gegevens op basis van voorwaarden, en moet beginnen met sleutelwoord `where` .
 	
Let op de volgende filteropties:
• Tekenreeksen kunnen worden ingesloten in enkele of dubbele aanhalingstekens.
• Logische operatoren zoals `AND` en `OR` kunnen worden gebruikt om de filters te combineren.
`key = value AND key < value OR key = value`
• Haakjes kunnen worden toegevoegd rond operators:
`(key = value) AND (key < value OR key = value)`
• Gebruik `CONTAINS` voor gedeeltelijke tekenreeksovereenkomsten:
`key CONTAINS 'value'`
• Gebruik `ICONTAINS` voor gedeeltelijke tekenreeksovereenkomsten die niet hoofdlettergevoelig zijn:
`key ICONTAINS 'value'`
• Gebruik `IN` voor lidmaatschapscontrole:
`key IN ('value1', 'value2')`
• Gebruik regex-overeenkomsten volgens de RE2- standaard:
`key MATCHES 'regex string'`
	`eventType | where field == 'value'`
	
	`eventType | where field != 'value'`
	
	`eventType | where field > 'value'`
	
	`eventType | where field < 'value'`
	
	`eventType | where field >= 'value'`
	
	`eventType | where field <= 'value'`
	
	`eventType | where field CONTAINS 'substring'`
	
	`eventType | where field NOT CONTAINS 'substring'`
	
	`eventType | where field ICONTAINS 'substring'`
	
	`eventType | where field NOT ICONTAINS 'substring'`
	
	`eventType | where field IN ('value1', 'value2')`
	
	`eventType | where field NOT IN ('value1', 'value2')`
	
	`eventType | where field MATCHES 'value1*'`
	
	`eventType | where field NOT MATCHES 'value1*'`

Velden kiezen Geeft aan welke velden moeten worden geselecteerd en geretourneerd voor een zoekopdracht.	`eventType | columns field1, field2, field3 ...`

Sorteren
 	
Sorteert de resultaten van de zoekopdracht. Waarde kan oplopend of aflopend zijn. Als er geen volgorde is opgegeven, wordt de standaardvolgorde (oplopend) gebruikt.
	`eventType | order field1, field2, field3 ...`
	
	`eventType | order field asc`
	
	`eventType | order field desc`

Bewerking	Voorbeeld
Limiet Beperkt het resultaat van de zoekopdracht.	`eventType | limit 10` `eventType | limit 1000 | group [field1, field2] | limit 10`

Groepsbewerking
Voert een `group operation` uit voor de gegevens.
(Optioneel) U kunt aggregatiefuncties opgeven die moeten worden uitgevoerd voor de geaggregeerde velden, of alleen aggregatiefuncties opgeven zonder `group operation` uit te voeren voor specifieke velden.
	`eventType | group [field]`
	`eventType | group [field1, field2, field3, ...]`
	`eventType | group with [max (field1), min(field2), avg(field3)]`
	`eventType | group [field1, field2, field3, ...] with [max(field1), min (field2), avg(field3)]`
	`eventType | group [field1, field2, field3, ...] with [max(field1) as max_field, min(field2), avg(field3) as avg_field]`

Aggregatie
Aggregeert de resultaten van de zoekopdracht om een bewerking uit te voeren.
Deze functies kunnen alleen samen met `group operation` worden gebruikt (zie hierboven).
	`min(field)`
	`max(field)`
	`avg(field)`
	`count()`
	`count(field)`
	`countdistinct(field)`

Voorbeeldzoekopdrachten

Dit gedeelte bevat enkele voorbeeldzoekopdrachten die laten zien hoe u XQL-syntaxisregels kunt toepassen op uw zoekopdracht.

- Velden selecteren in het gebeurtenistype `WinProcCreate`:

```
WinProcCreate | fields host_name, parent_start, parent_gpid, parent_pid, parent_
user, proc_name
```

- Filteren met voorwaarden, voordat de resultaten worden gegroepeerd op `proc_name` en vervolgens de aggregatiefuncties `min()` toepassen op `parent_pid`:

```
WinProcCreate | where host_name == 'BNi-Kub' AND parent_pid != -1 AND proc_name
CONTAINS '1' AND host_name IN ('Computer1') | group [proc_name] with [min(parent_
pid)]
```

- Gegevens selecteren met filters en vervolgens het aantal geretourneerde rijen tellen en ordenen:

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [count() as new_count] |
order new_count
```

- Gegevens selecteren met regex-filters:

```
WinProcCreate | where host_name match 'BNi.*'
```

- Gegevens selecteren met complexe filters en de resultaten beperken:

```
WinProcCreate | where (host_name contains 'BNi-Kub') OR (host_name in
('Computer1', 'Computer2')) | limit 10
```

- Gegevens selecteren met filters en vervolgens het unieke aantal geretourneerde rijen tellen:

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [countdistinct(*)]
```

- Gegevens selecteren met filters, sorteren op een veld en het aantal geretourneerde rijen beperken:

```
WinProcCreate | where host_name == 'BNi-Kub' | order host_name | limit 10
```

Gebeurtenistypen en velden

Dit gedeelte bevat:

- Gebeurtenisvelden

Gebeurtenistypen

Naam	Beschrijving	Type
WinProcCreate Voor meer informatie over de beschikbare velden: zie WinProcCreate.	Windows-gebeurtenissen bij het maken van processen	Gebeurtenissen
WinProcTerminate Voor meer informatie over de beschikbare velden: zie WinProcTerminate.	Windows-gebeurtenissen bij het beëindigen van processen	Gebeurtenissen
WinNetAccess Voor meer informatie over de beschikbare velden: zie WinNetAccess.	Windows-gebeurtenissen bij netwerktoegang	Gebeurtenissen
WinRegAccess Voor meer informatie over de beschikbare velden: zie WinRegAccess.	Windows-gebeurtenissen bij registertoegang	Gebeurtenissen
WinScriptExec Voor meer informatie over de beschikbare velden: zie WinScriptExec.	Windows-gebeurtenissen bij scriptuitvoering (inclusief PowerShell, VBS, enz.)	Gebeurtenissen
WinFileAccess Voor meer informatie over de beschikbare velden: zie WinFileAccess.	Windows-gebeurtenissen bij bestandstoegang (lezen/schrijven)	Gebeurtenissen
WinLogin Voor meer informatie over de beschikbare velden: zie WinLogin.	Windows-gebeurtenissen bij gebruikersaanmelding	Gebeurtenissen
WinLogout Voor meer informatie over de beschikbare velden: zie WinLogout.	Windows-gebeurtenissen bij gebruikersafmelding	Gebeurtenissen
WinAgentDetection Voor meer informatie over de beschikbare velden: zie WinAgentDetection.	Windows-gebeurtenissen bij detectie	Detecties

Voorbeeldgegevenstypen

Gegevenstype	Voorbeeld	Beschrijving
Tekenreeks	`WinProcCreate | where host_name == 'BNi-Kub'` `WinProcCreate | where host_name == "BNi-Kub"`	Tekenreeksen moeten worden omgeven door enkele aanhalingstekens of dubbele aanhalingstekens.
UUID	`WinProcCreate | where agent_id == '61f0c404-5cb3-11e7-907b-a6006ad3dba0'` `WinProcCreate | where agent_id == "61f0c404-5cb3-11e7-907b-a6006ad3dba0"`	UUID's zijn tekenreekswaarden en moeten worden omgeven door enkele aanhalingstekens of dubbele aanhalingstekens. UUID-waarden moeten de volgende indeling hebben: 8-4-4-4-12.
DateTime	`WinProcCreate | where event_time < '2022-11-01'` `WinProcCreate | where event_time < "2022-11-01"`	DateTime is een tekenreekswaarde en moet worden omgeven door enkele aanhalingstekens of dubbele aanhalingstekens. DateTime moet de volgende indeling hebben: JJJJ-MM-DD.

Bool	`WinLogin | where is_admin == 1`
	`WinLogin | where is_admin == 0`
	`WinLogin | where is_admin == true`
	`WinLogin | where is_admin == false`
		Booleaanse waarden kunnen worden weergegeven als `1`, `0`, `true` of `false`.

Geheel getal	`WinLogin | where proc_pid > 25`	Een geheel getal.

Gebeurtenisvelden

Gebeurtenistype	Veld (Gegevenstype)
WinProcCreate	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID)

Gebeurtenistype	Veld (Gegevenstype)
	• parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_prod (String) • proc_prod_desc (String) • proc_sha1 (String) • proc_sha256 (String) • proc_signatures (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinProcTerminate	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String)

Gebeurtenistype	Veld (Gegevenstype)
	• proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • term_args (String) • term_gpid (UUID) • term_integrity_level (String) • term_md5 (String) • term_name (String) • term_oname (String) • term_path (String) • term_pid (Int) • term_sha1 (String) • term_sha256 (String) • term_start (DateTime) • term_upn (String) • term_user (String) • term_user_domain (String) • timestamp (DateTime)
WinNetAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • net_dst_ip (String) • net_dst_port (Int) • net_host (String) • net_http_method (String) • net_http_url (String) • net_protocol (String) • net_src_ip (String) • net_src_port (Int)

Gebeurtenistype	Veld (Gegevenstype)
	• owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinRegAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String)

Gebeurtenistype	Veld (Gegevenstype)
	• parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • reg_key (String) • reg_operation (String) • reg_original_key (String) • reg_original_value_data (String) • reg_value_data (String) • reg_value_name (String) • reg_value_type (String) • resource_id (UUID) • timestamp (DateTime)
WinScriptExec	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String)

Gebeurtenistype	Veld (Gegevenstype)
	• parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • script_data (String) • script_fragment (Bool) • script_size (Int) • script_type (String) • timestamp (DateTime)
WinFileAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • file_md5 (String) • file_name (String) • file_op (String)

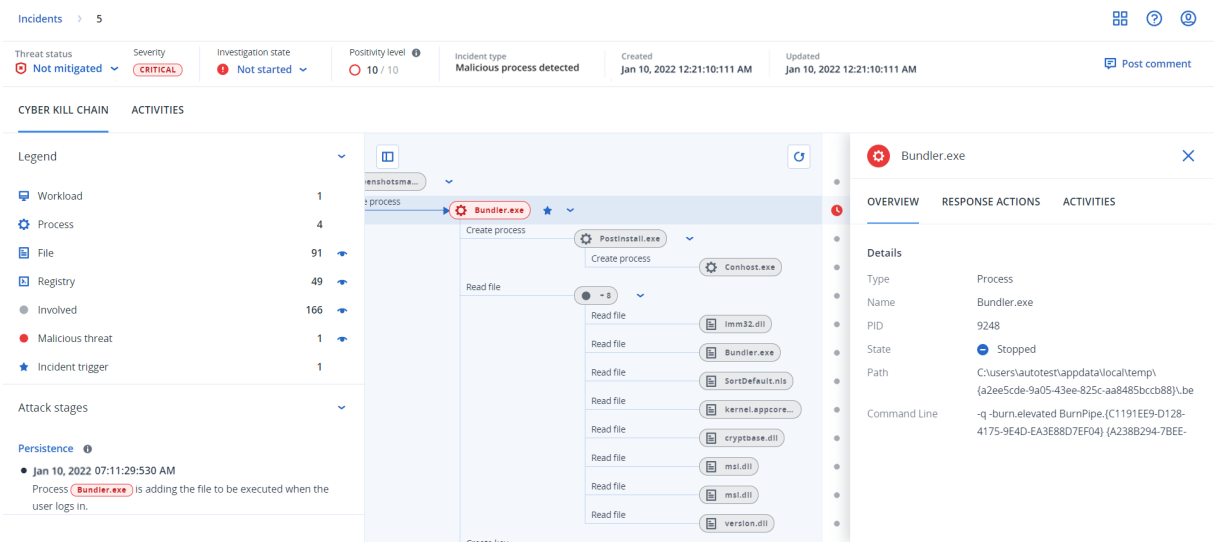
Gebeurtenistype	Veld (Gegevenstype)
	• file_path (String) • file_sha1 (String) • file_sha256 (String) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinLogin	• agent_id (UUID) • customer (String) • domain (String) • event_time (DateTime)

Gebeurtenistype	Veld (Gegevenstype)
	• host_name (String) • id (UUID) • is_admin (Bool) • login_time (DateTime) • name (String) • owner (String) • resource_id (UUID) • security_id (String) • timestamp (DateTime) • type (String)
WinLogout	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • logout_time (DateTime) • resource_id (UUID) • security_id (String) • timestamp (DateTime)
WinAgentDetection	• agent_id (UUID) • customer (String) • detection_type (String) • event_time (DateTime) • file_md5 (String) • file_name (String) • file_path (String) • file_sha1 (String) • file_sha256 (String) • host_name (String) • id (UUID) • mitre_stid (Int) • mitre_tactics (Array(Int)) • mitre_tid (Int) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String)

Gebeurtenistype	Veld (Gegevenstype)
	• parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • severity (String) • threat_name (String) • timestamp (DateTime) • url (String) • url_blocked (Bool) • url_cat (Array(String)) • url_list (String) • url_md5 (String)

Incidenten onderzoeken

Met Eindpuntdetectie en -respons (EDR) kunt u een volledig incident onderzoeken, inclusief alle aanvalsfasen en objecten (processen, registers, geplande taken en domeinen) die door een aanval zijn getroffen. Deze objecten worden vertegenwoordigd door knooppunten in de gemakkelijk te begrijpen cyber kill chain, zoals hieronder weergegeven. Gebruik de cyber kill chain om snel te begrijpen wat er precies is gebeurd en wanneer het is gebeurd.



Elke stap van een aanval wordt bekeken in de cyber kill chain, die een gedetailleerde interpretatie biedt van de manier waarop het incident plaatsvond en de reden ervan. De cyber kill chain maakt gebruik van eenvoudig te begrijpen zinnen en grafieken die helpen bij de uitleg van elke stap van de aanval, zodat u zo min mogelijk tijd kwijt bent met het onderzoek.

U krijgt snel inzicht in de reikwijdte en impact van een incident, doordat de voortgang van de aanval is gekoppeld aan het MITRE-framework. Hierdoor kunt u analyseren wat er tijdens elke stap van een aanval is gebeurd, zoals:

- Het eerste punt van binnenkomst
- Hoe de aanval werd uitgevoerd
- Eventuele escalaties van bevoegdheden
- Technieken om detectie te vermijden
- Zijdelingse verplaatsingen naar andere workloads
- Diefstal van referenties
- Pogingen van exfiltratie

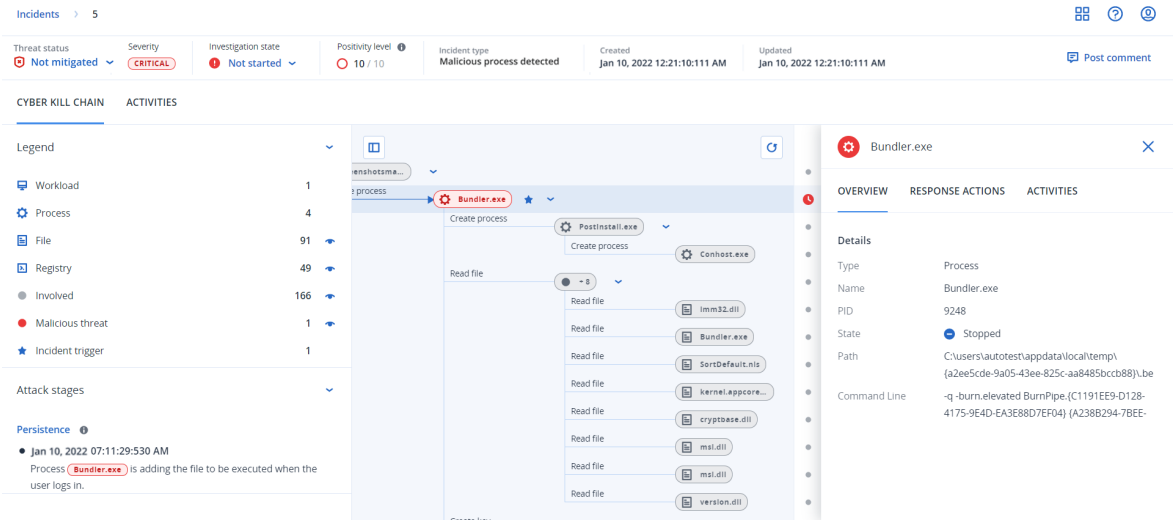
Opmerking
Elk object (proces, register, geplande taak of domein) dat door de aanval wordt getroffen, wordt vertegenwoordigd door een knooppunt in de cyber kill chain.

Incidenten in de cyber kill chain onderzoeken

U kunt elke stap van een aanval onderzoeken in de cyber kill chain. Volg de gemakkelijk te begrijpen zinnen en grafieken van de cyber kill chain om inzicht te krijgen in elke stap van de aanval. Op die manier bespaart u ook op de tijd die nodig is voor het onderzoek.

Een onderzoek starten in de cyber kill chain

1. Ga in de Cyber Protect-console naar **Bescherming > Incidenten**.
2. Klik in de weergegeven lijst met incidenten op in de uiterst rechtse kolom van het incident dat u wilt onderzoeken. De cyber kill chain voor het geselecteerde incident wordt weergegeven.



3. Bekijk een samenvatting van het incident in de statusbalk van de bedreiging bovenaan de pagina. De statusbalk van de bedreiging bevat de volgende informatie:
   - Huidige bedreigingsstatus: De bedreigingsstatus wordt automatisch door het systeem bepaald. Elk incident met de status **Niet verholpen** moet zo snel mogelijk worden onderzocht.

     Belangrijk
     Een incident wordt ingesteld op **Verholpen** wanneer herstel vanaf back-up is voltooid of wanneer alle detecties zijn verholpen door de betreffende items te stoppen, in quarantaine te plaatsen of terug te draaien.

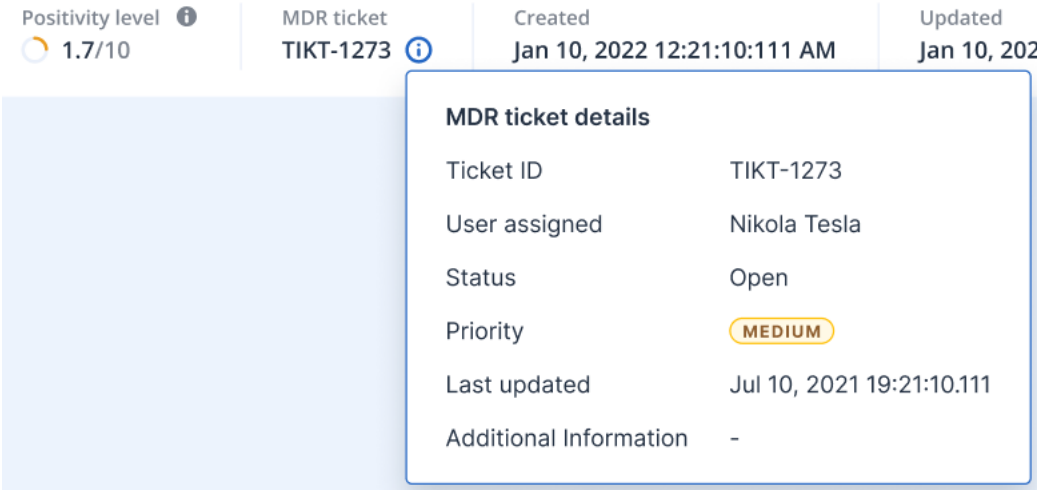
     Een incident wordt ingesteld op **Niet verholpen** wanneer herstel vanaf back-up niet kon worden voltooid of wanneer ten minste één detectie niet is verholpen door het betreffende item te stoppen, in quarantaine te plaatsen of terug te draaien.

     U kunt de bedreigingsstatus ook handmatig instellen op **Verholpen** of **Niet verholpen**. Wanneer u een van beide statussen selecteert, wordt u gevraagd een opmerking in te voeren. Deze opmerking wordt opgeslagen als onderdeel van de onderzoeksactiviteiten en kan worden bekeken op het tabblad **Activiteiten**. Denk eraan dat EDR de bedreigingsstatus nog steeds kan terugzetten naar **Verholpen** of **Niet verholpen** als er nieuwe detecties voor het incident zijn of als er responsacties met goed gevolg zijn uitgevoerd.

   - Ernst van incident: **Kritiek**, **Hoog** of **Matig**. Zie "Incidenten bekijken" (p. 951) voor meer informatie.
   - Huidige onderzoeksstatus: Een van de opties **Wordt onderzocht**, **Niet gestart** (de standaardstatus), **Fout-positief** of **Gesloten**. U moet de status wijzigen wanneer u het

incident gaat onderzoeken, zodat andere collega's op de hoogte zijn van eventuele wijzigingen in het incident.

- Positiviteitsniveau: Geeft aan hoe waarschijnlijk het is dat een incident een echte kwaadaardige aanval is, met een score van 1 tot 10. Zie "Incidenten bekijken" (p. 951) voor meer informatie.
- Type incident: bijvoorbeeld **Ransomware gedetecteerd**, **Malware gedetecteerd**, **Verdacht proces gedetecteerd**, **Schadelijk proces gedetecteerd**, **Verdachte URL geblokkeerd** en **Schadelijke URL geblokkeerd** of een combinatie hiervan.
- Als Managed Detection and Response (MDR) is ingeschakeld voor de workload, wordt een veld **MDR-ticket** weergegeven. U kunt de details van het MDR-ticket voor het incident bekijken en zien welke MDR-beveiligingsanalist is toegewezen aan het incident.



- Wanneer het incident is gemaakt en bijgewerkt: Datum en tijd waarop het incident is gedetecteerd, of wanneer het incident voor het laatst is bijgewerkt met nieuwe detecties die zijn geregistreerd voor het incident.

4. Klik op het tabblad **Legenda** om de verschillende knooppunten van de kill chain-grafiek te bekijken en om te definiëren welke knooppunten u wilt bekijken. Zie "De cyber kill chain-weergave begrijpen en aanpassen" (p. 976) voor meer informatie.
5. Onderzoek en verhelp het incident door de volgende stappen uit te voeren. Let op: dit is de gebruikelijke workflow is voor het onderzoek naar en verhelpen van een incident, maar dit kan per incident en al naargelang uw eigen vereisten verschillen.
   a. Onderzoek elke fase van de aanval op het tabblad **Aanvalsfasen**. Zie "Navigeren in aanvalsfasen" (p. 978) voor meer informatie.
   b. Klik op **Het hele incident verhelpen** om herstelacties toe te passen. Zie "Een heel incident verhelpen" (p. 989) voor meer informatie.

      U kunt ook afzonderlijke knooppunten in de cyber kill chain verhelpen, zoals beschreven in "Responsacties voor afzonderlijke knooppunten in de cyber kill chain" (p. 994).
   c. Tabblad **Activiteiten**: bekijk de ondernomen acties om het incident te verhelpen. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

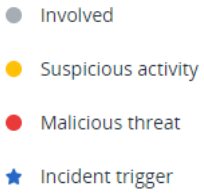
De cyber kill chain-weergave begrijpen en aanpassen

Ga naar de legenda om inzicht te krijgen in de knooppunten die worden beïnvloed in de cyber kill chain. De legenda toont alle knooppunten die betrokken zijn bij een incident, zodat u kunt begrijpen hoe de verschillende knooppunten zijn beïnvloed door de aanvaller. U kunt ook de knooppunten definiëren die u wilt verbergen of weergeven in de cyber kill chain.

Toegang tot de legenda:

1. Klik op het pijlpictogram rechts van het gedeelte Legenda.
   Het gedeelte Legenda wordt uitgevouwen, zoals hieronder weergegeven.

2. Er worden vier hoofdkleuren gebruikt in de legenda, zodat u snel kunt begrijpen wat er met elk knooppunt in de cyber kill chain is gebeurd, zoals hieronder weergegeven. Deze knooppunten met kleurcodes worden ook weergegeven in de aanvalsfasen, zoals beschreven in "Navigeren in aanvalsfasen" (p. 978).



Knooppunten in de cyber kill chain verbergen of weergeven

1. Vouw het gedeelte Legenda uit en controleer of wordt weergegeven naast de knooppunten die u wilt weergeven in de cyber kill chain. Als het weergegeven pictogram is, klikt u op het

pictogram om het te wijzigen in .

2. Klik op om een knooppunt in de cyber kill chain te verbergen. Het pictogram verandert in en het knooppunt wordt niet meer weergegeven in de cyber kill chain.

De aanvalsfasen van een incident onderzoeken

De aanvalsfasen van een incident bieden gemakkelijk te begrijpen interpretaties van elk incident.

U krijgt voor elke aanvalsfase een overzicht van wat er precies is gebeurd en welke objecten (ook wel *knooppunten* in de cyber kill chain genoemd) het doelwit waren. Als een gedownload bestand zich bijvoorbeeld voordeed als iets anders, wordt dit vermeld bij de aanvalsfase, met links naar het betreffende knooppunt in de cyber kill chain die u kunt onderzoeken, en naar de betreffende MITRE ATT&CK-techniek.

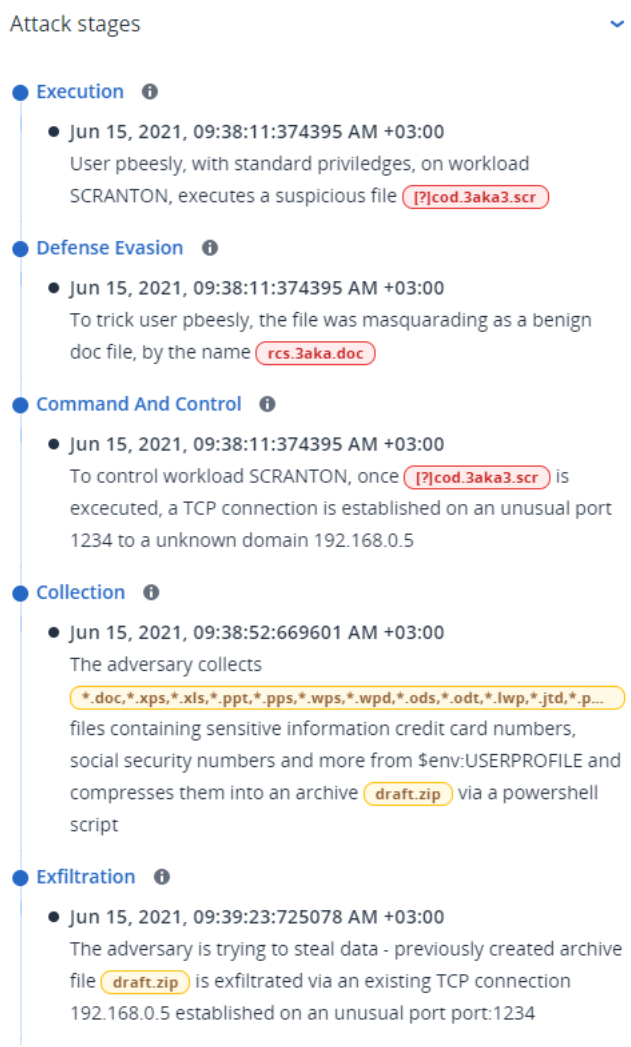
Elke aanvalsfase geeft u de nodige informatie om drie cruciale vragen te beantwoorden:

- Wat was het doel van de aanvaller?
- Hoe heeft de aanvaller dit doel bereikt?
- Welke knooppunten waren het doelwit?

Nog belangrijker is dat de geboden interpretatie u veel tijd bespaart bij het onderzoek naar een incident, omdat u niet langer elke beveiligingsgebeurtenis hoeft te bekijken via een tijdlijn of grafiekknooppunt om daarmee te proberen een interpretatie van de aanval te genereren.

De aanvalsfasen bevatten ook informatie over gecompromitteerde bestanden die gevoelige informatie bevatten, zoals creditcardnummers en burgerservicenummers, zoals weergegeven in de fase **Verzameling** in het onderstaande voorbeeld.

Zie "Welke informatie is opgenomen in een aanvalsfase?" (p. 978) voor meer informatie.



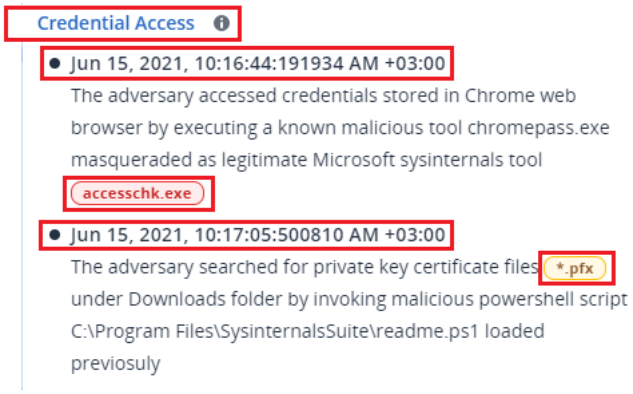
Navigeren in aanvalsfasen

Aanvalsfasen worden in chronologische volgorde weergegeven. Scrol naar beneden om de volledige lijst met aanvalsfasen voor het incident te zien.

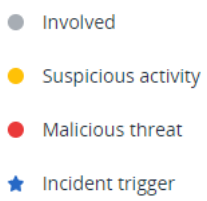
Als u een specifieke aanvalsfase verder wilt onderzoeken, klikt u ergens in de aanvalsfase om naar het betreffende knooppunt in de cyber kill chain-grafiek te navigeren. Zie "Afzonderlijke knooppunten onderzoeken in de cyber kill chain" (p. 980) voor meer informatie over de navigatie in de cyber kill chain-grafiek en specifieke knooppunten.

Welke informatie is opgenomen in een aanvalsfase?

Elke aanvalsfase biedt een gemakkelijk te begrijpen interpretatie van de aanval, in gemakkelijk leesbare menselijke taal. Deze interpretatie is opgebouwd uit een aantal elementen, zoals hieronder weergegeven en beschreven in de volgende tabel.



Element van aanvalsfase	Beschrijving
Header	Beschrijft wat de aanvaller probeerde te doen, en het doel (in het bovenstaande voorbeeld **Toegang tot Referenties**), met een link naar een bekende MITRE ATT&CK-techniek. Klik op de link naar de MITRE ATT&CK-website voor meer informatie. **Opmerking** Als een aanvalsfase geen bekende MITRE ATT&CK-techniek is, bevat de koptekst geen link. Dit is relevant voor generieke technieken zoals bestanden die in een willekeurige map worden gedetecteerd.
Tijdstempel	Het tijdstip van de aanvalsfase.
Techniek	Hoe de aanvaller technisch heeft geprobeerd het doel te bereiken en welke objecten (registervermeldingen, bestanden of geplande taken) zijn getroffen. In de tekstbeschrijving van de aanvalstechniek zijn links met kleurcodes opgenomen naar elk getroffen knooppunt in de cyber kill chain (zie bovenstaand voorbeeld). Door deze links met kleurcodes kunt u snel naar het getroffen knooppunt navigeren om te onderzoeken wat er precies is gebeurd. De kleuren die in een aanvalsfase worden gebruikt, geven het volgende aan:

Element van aanvalsfase	Beschrijving
	 In de bovenstaande legende zien we dat de aanvalsfase van het voorbeeld (om toegang te krijgen tot referenties) een link bevat naar een malwareknooppunt accesschk.exe en een verdacht bestandsknooppunt *.pfx (klik op de links om naar het betreffende knooppunt in de cyber kill chain te gaan). Zie "Afzonderlijke knooppunten onderzoeken in de cyber kill chain" (p. 980) voor meer informatie over de navigatie naar deze knooppunten en de mogelijke acties. Let op: de aanvalsfasen bevatten ook links naar bestandsknooppunten die informatie bevatten over gecompromitteerde bestanden met gevoelige informatie, zoals beschermde gezondheidsinformatie (PHI), creditcardnummers en burgerservicenummers.

Opmerking
Elke aanvalsfase is een enkele detectiegebeurtenis. De inhoud die in elke fase wordt vermeld (header, tijdstempel, techniek) wordt gegenereerd volgens specifieke parameters in de detectiegebeurtenis. De parameters zijn gebaseerd op aanvalsfasesjablonen die zijn opgeslagen in Eindpuntdetectie en -respons (EDR).

Afzonderlijke knooppunten onderzoeken in de cyber kill chain

U kunt de aanvalsfasen bekijken en vervolgens navigeren naar elk van de aanvalsknooppunten in de cyber kill chain. Zo kunt u inzoomen op specifieke knooppunten in de cyber kill chain en elk knooppunt naar behoefte onderzoeken en herstellen.

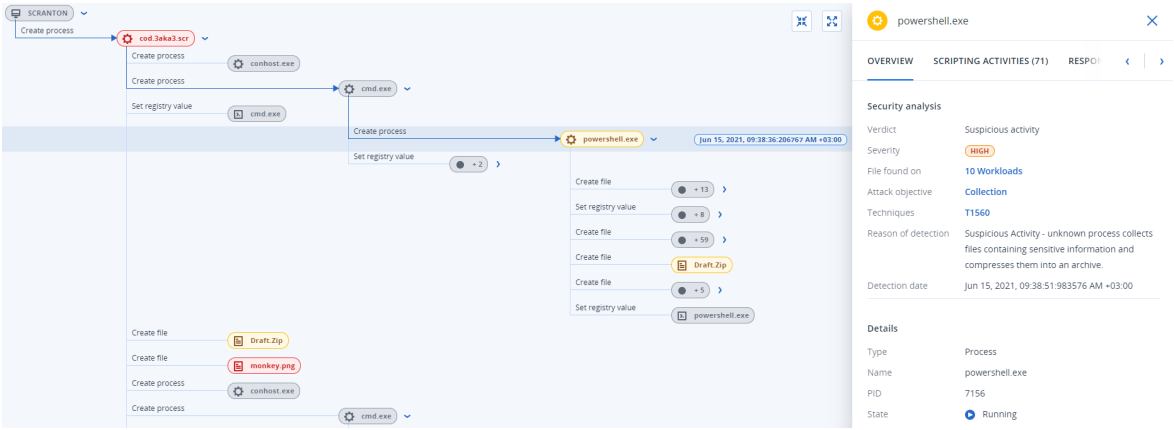
U kunt bijvoorbeeld bepalen hoe waarschijnlijk het is dat een incident een echte schadelijke aanval is. Op basis van uw onderzoek kunt u ook een aantal responsacties toepassen op het knooppunt, bijvoorbeeld door een workload te isoleren of een verdacht bestand in quarantaine te plaatsen.

Afzonderlijke knooppunten onderzoeken in de cyber kill chain:

1. Ga in de Cyber Protect-console naar **Bescherming > Incidenten**.
2. Klik in de weergegeven lijst met incidenten op  in de uiterst rechtse kolom van het incident dat u wilt onderzoeken. De cyber kill chain voor het geselecteerde incident wordt weergegeven.
3. Navigeer naar het betreffende knooppunt en klik erop om de zijbalk voor het knooppunt weer te geven.

   Opmerking
   Klik op het knooppunt om het uit te vouwen en de bijbehorende knooppunten weer te geven.

   Als u bijvoorbeeld klikt op het **powershell.exe**-knooppunt in het onderstaande voorbeeld, wordt de zijbalk voor het knooppunt geopend. U kunt ook op het pijlpictogram naast het knooppunt klikken om de bijbehorende knooppunten te bekijken, inclusief bestanden en registerwaarden, die mogelijk worden beïnvloed door het **powershell.exe**-knooppunt. U kunt vervolgens op deze bijbehorende knooppunten klikken voor verder onderzoek.



4. Onderzoek de informatie op de tabbladen van de zijbalk:
   - **Overzicht**: Bevat drie hoofdgedeelten die een beveiligingsoverzicht geven van het aangevallen knooppunt.
     - **Beveiligingsanalyse**: Biedt een analyse van het aangevallen knooppunt, inclusief het EDR-oordeel over de bedreiging (zoals verdachte activiteit), het doel van de aanval volgens MITRE-aanvalstechnieken (klik op de link om naar de MITRE-website te gaan), de reden voor detectie, en het aantal workloads dat mogelijk door de aanval is beïnvloed (klik op de link **n workloads** om de getroffen workloads te bekijken).

       Opmerking
       De link **n workloads** geeft aan dat het specifieke schadelijke of verdachte object ook is *gevonden* in andere workloads. Dat wil niet zeggen dat er een aanval plaatsvindt op deze andere workloads, maar dat er een inbreukindicator is voor deze andere workloads. De aanval is mogelijk al gebeurd (en heeft een ander incident veroorzaakt), of de aanvaller bereidt zich voor om deze andere workloads te raken met behulp van een specifieke 'toolkit'.

- **Details**: Bevat details over het knooppunt, inclusief het type, de naam en de huidige status, het pad naar het knooppunt en eventuele bestandshashes en digitale handtekeningen (zoals MD5 en serienummers van certificaten).

- **Scripting-activiteiten**: Bevat details van alle scripts die tijdens de aanval zijn aangeroepen of geladen. Klik op  om het script naar uw klembord te kopiëren voor verder onderzoek.

  Opmerking
  Het tabblad **Scripting-activiteiten** wordt alleen weergegeven voor procesknooppunten die opdrachten of scripts uitvoeren (zoals cmd- of PowerShell-opdrachten).

- **Responsacties**: Bevat een aantal gedeelten met aanvullende onderzoeks-, herstel- en preventieve acties, afhankelijk van het type knooppunt.
  Voor workloadknooppunten kunt u bijvoorbeeld een aantal responsacties definiëren, zoals forensische back-up en herstel vanaf back-up. In het geval van schadelijke of verdachte knooppunten kunt u het knooppunt ook stoppen of in quarantaine plaatsen, de door de aanval aangebrachte wijzigingen ongedaan maken en het knooppunt toevoegen aan een acceptatielijst of blokkeringslijst van een beschermingsschema.
  Zie "Responsacties voor afzonderlijke knooppunten in de cyber kill chain" (p. 994) voor meer informatie over het toepassen van responsacties voor specifieke knooppunten.
- **Activiteiten**: Geeft in chronologische volgorde de acties weer die op het incident zijn toegepast. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Inzicht in de ondernomen acties om een incident te verhelpen

Nadat u een incident hebt bekeken en hebt onderzocht hoe de aanval plaatsvond, kunt u responsacties toepassen. Nadat u responsacties hebt toegepast, kunt u deze acties op diverse plekken bekijken om meer inzicht te krijgen in de stappen die zijn ondernomen om het incident te verhelpen.

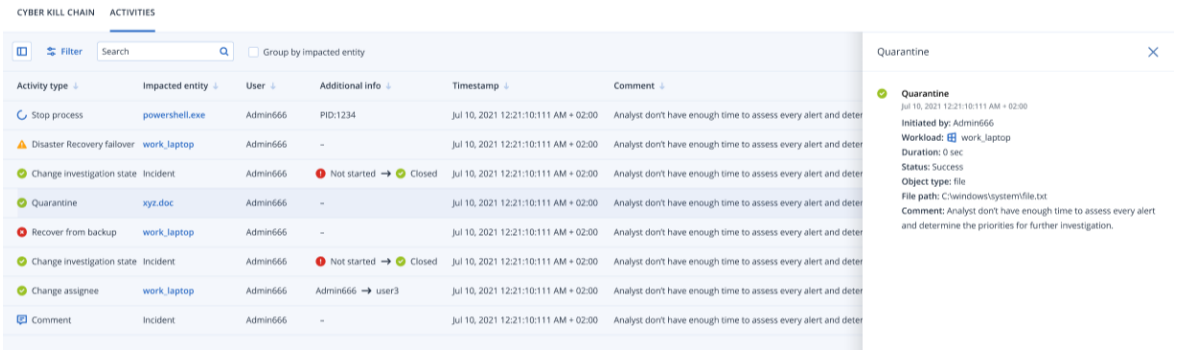
Opmerking
Voor incidenten die zijn gemaakt door preventielagen, worden automatisch de acties toegepast die zijn geconfigureerd in het beschermingsschema. Voor detectiepunten moet u de betreffende responsacties definiëren om in te spelen op elk aanvalsscenario.

Als u inzicht wilt krijgen in de ondernomen responsacties, kunt u alle responsacties bekijken die zijn toegepast op een volledig incident, of de acties bekijken die zijn toegepast op een specifiek knooppunt in de cyber kill chain van het incident.

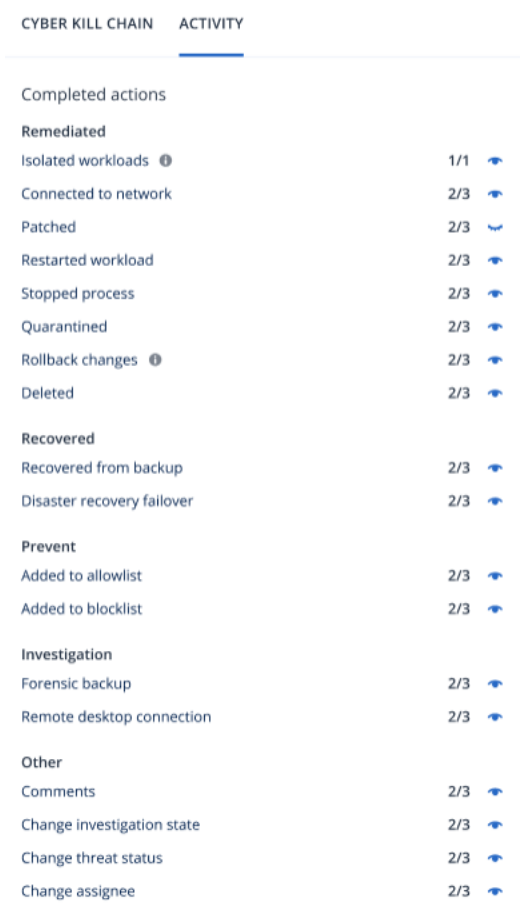
Alle responsacties bekijken die zijn toegepast op een incident

1. Ga in de Cyber Protect-console naar **Bescherming > Incidenten**.
2. Klik in de weergegeven lijst met incidenten op  in de uiterst rechtse kolom van het incident dat u wilt onderzoeken. De cyber kill chain voor het geselecteerde incident wordt weergegeven.

3. Klik op het tabblad **Activiteiten**.
   De lijst met responsacties die al op het incident zijn toegepast, wordt weergegeven.

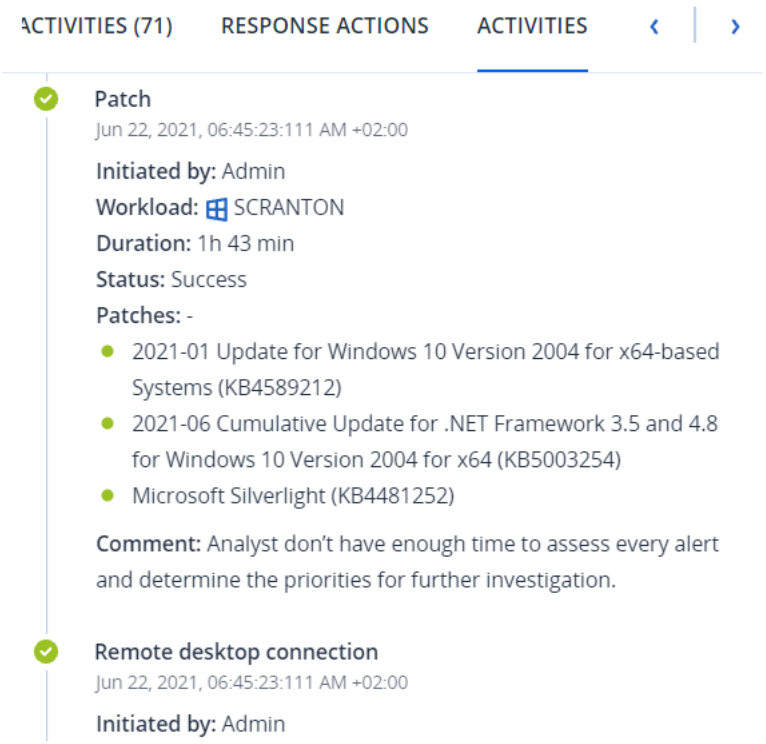


4. U kunt diverse acties uitvoeren in de weergegeven lijst:
   - Klik op een rij met het type activiteit om meer informatie weer te geven over de geselecteerde activiteit. De informatie wordt weergegeven in een zijbalk, zoals weergegeven in stap 3, en bevat details over wie de actie heeft geïnitieerd, de status, het bestandspad en eventuele opmerkingen die zijn toegevoegd door de initiatiefnemer.
   - Gebruik het **zoek** vak om een specifieke actie te zoeken.
   - Klik op **Filter** om filters toe te passen op de lijst.
   - Schakel het selectievakje **Groeperen op betroffen entiteit** in om de betreffende acties te groeperen op entiteit.
   - Klik op om de lijst met voltooide acties weer te geven of te verbergen.
     Controleer of wordt weergegeven naast de acties die u wilt weergeven. Als u een actie uit de weergegeven lijst wilt verbergen, klikt u opnieuw om deze te wijzigen in .



Responsacties bekijken die zijn toegepast op een specifiek knooppunt:

1. Klik in de cyber kill chain op een knooppunt om de zijbalk voor dat knooppunt te bekijken.
2. Klik op het tabblad **Activiteiten**.



3. Als u volledig inzicht wilt krijgen in de acties die zijn toegepast en de reden hiervan, moet u mogelijk door de toegepaste responsacties voor het knooppunt bladeren. Voor acties voor verbinding met een extern bureaublad kunt u bijvoorbeeld bekijken wie de actie heeft gestart en wanneer, hoe lang de actie heeft geduurd en wat de algemene status is (voltooid, mislukt of voltooid met fouten).

Controleren op inbreukindicatoren (IOC's) in openbaar bekende aanvallen op uw workloads

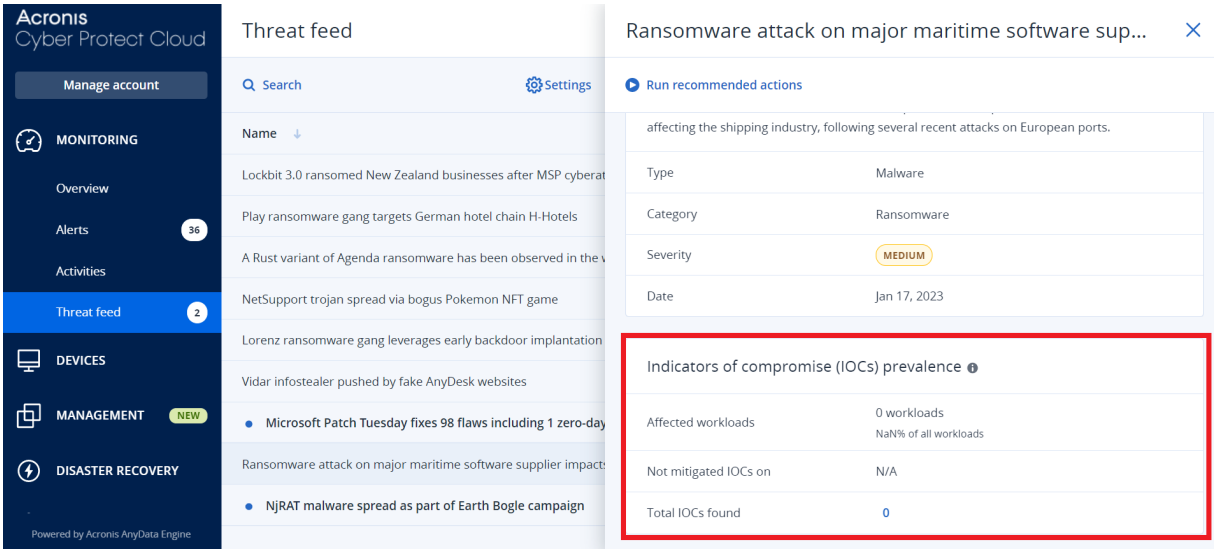
Eindpuntdetectie en -respons (EDR) biedt de mogelijkheid om bestaande, bekende aanvallen tegen uw workloads te bekijken in bedreigingsfeeds. Deze bedreigingsfeeds worden automatisch gegenereerd op basis van bedreigingsgegevens die zijn ontvangen van het Cyber Protection Operations Center (CPOC). Met EDR kunt u nagaan of een bedreiging al dan niet uw workload beïnvloedt, en vervolgens de nodige stappen ondernemen om de bedreiging ongedaan te maken.

U hebt toegang tot bedreigingsfeeds via het menu **Controle** in de Cyber Protect-console. Zie "Bedreigingsfeed" (p. 291) voor meer informatie.

Klik op een bedreigingsfeed om specifieke bedreigingsdetails te bekijken en te bevestigen of deze van invloed zijn op uw workload. U kunt het aantal gedetecteerde IOC's en de getroffen workloads bekijken en inzoomen op workloads met IOC's die nog niet zijn verholpen.

Opmerking

Als EDR niet is ingeschakeld voor het beschermingsschema, wordt deze aanvullende functionaliteit voor bedreigingsfeeds, niet weergegeven (zie hieronder).



Instellingen voor bedreigingsfeed definiëren

U kunt diverse instellingen voor bedreigingsfeeds definiëren om bekende bedreigingen automatisch te vinden en te verhelpen.

Instellingen voor bedreigingsfeed definiëren:

1. Ga in de Cyber Protect-console naar **Controle > Bedreigingsfeed**.
2. Klik op de weergegeven pagina Bedreigingsfeed op **Instellingen**.

3. Selecteer een van de volgende opties in het weergegeven dialoogvenster:

Optie	Beschrijving
Inbreukindicatoren (IOC's) zoeken	Klik op de schakelaar om automatisch zoeken naar IOC's voor uw workloads in te schakelen. Wanneer deze optie is ingeschakeld, worden ook de opties **Actie bij detectie** en **Waarschuwing genereren** weergegeven.
Actie bij detectie	Selecteer in de vervolgkeuzelijst de actie die moet worden ondernomen voor de relevante bestanden wanneer een bedreiging wordt ontdekt voor een workload: • **Geen actie** • **Quarantaine** • **Verwijderen** • **Workloads isoleren**
Waarschuwing genereren	Schakel het selectievakje in om een waarschuwing te genereren als er een IOC wordt gevonden in een workload. De waarschuwing wordt weergegeven op de pagina Waarschuwingen.

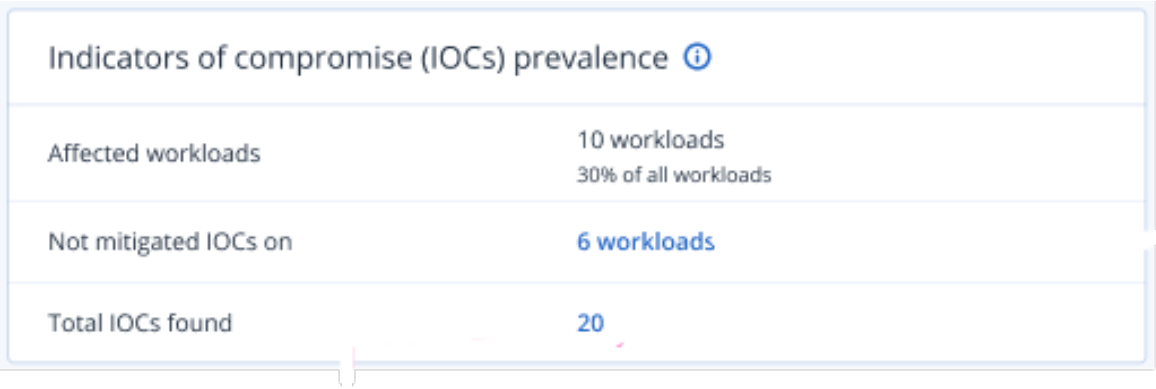
4. Klik op **Toepassen**.

IOC's voor getroffen workloads bekijken en verhelpen

Wanneer Eindpuntdetectie en -respons (EDR) is ingeschakeld in een beschermingsschema, kunt u alle bekende bedreigingen bekijken die van invloed zijn op workloads in het beschermingsschema. U kunt ook alle resterende inbreukindicatoren (IOC's) verhelpen die nog niet automatisch zijn verholpen. Zie "Instellingen voor bedreigingsfeed definiëren" (p. 986) voor informatie over hoe u IOC's automatisch kunt verhelpen.

De getroffen workloads bekijken en verhelpen

1. Ga in de Cyber Protect-console naar **Controle > Bedreigingsfeed**.
2. Klik op een bedreiging om de details weer te geven.
3. Klik in het gedeelte **Prevalentie van inbreukindicatoren (IOC's)** op de link ***n* workloads** om de workloads met niet-verholpen IOC's te bekijken.



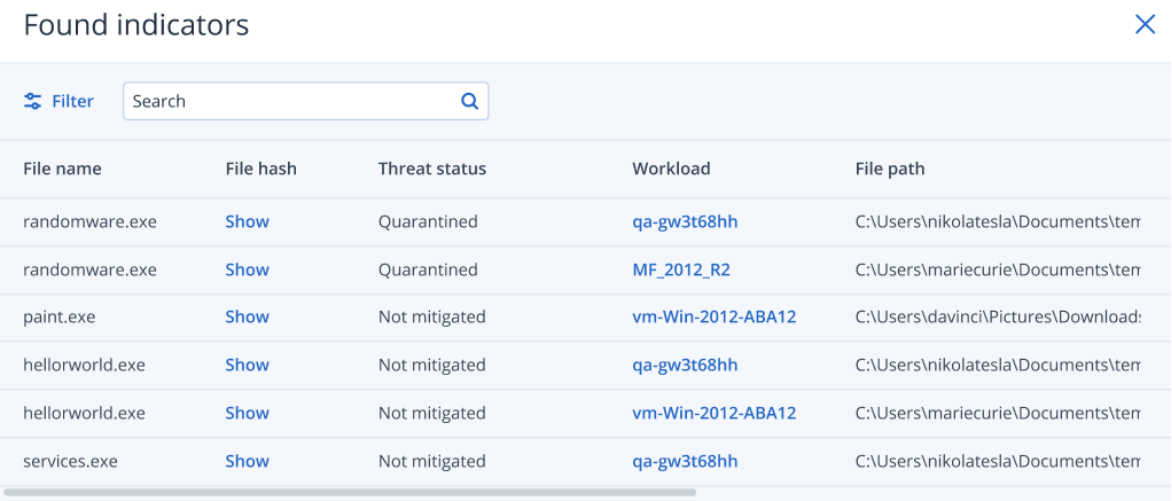
4. Klik op de weergegeven pagina Workloads op de betreffende workload en bekijk de details. U kunt specifieke functionaliteit uitvoeren voor de workload, bijvoorbeeld aanvullende URL's definiëren om te filteren (zie "URL-filtering" (p. 893)) en schadelijke processen blokkeren (zie het gedeelte Uitsluitingen in "Instellingen voor Antivirus- en antimalwarebeveiliging" (p. 868)).
Als een bedreigingsfeed bijvoorbeeld aangeeft dat er een IOC is voor een workload, moet u eerst de IOC vinden en analyseren, zoals beschreven in "Gedetecteerde IOC's bekijken en analyseren" (p. 988). Ga vervolgens naar het beschermingsschema voor de workload en definieer aanvullende bescherming, zoals schadelijke bestandshashes of processen blokkeren.

Gedetecteerde IOC's bekijken en analyseren

U kunt niet alleen workloads bekijken die worden beïnvloed door bekende bedreigingen, maar u kunt ook specifieke inbreukindicatoren (IOC's) bekijken en analyseren. Hierdoor kunt u de afzonderlijke workloads bekijken die worden beïnvloed door een IOC, en de IOC verhelpen.

IOC's bekijken en analyseren

1. Ga in de Cyber Protect-console naar **Controle > Bedreigingsfeed**.
2. Klik op een bedreiging om de details weer te geven.
3. Klik in het gedeelte **Prevalentie van inbreukindicatoren (IOC's)** op de link **n Totaal aantal gevonden IOC's**.
De pagina Gevonden indicatoren wordt weergegeven.



4. (Optioneel) Gebruik de optie **Filter** om de lijst met IOC's te filteren op basis van hun status. U kunt ook de optie **Zoeken** gebruiken om specifieke IOC's te zoeken.
5. Klik op de link in de kolom **Workload** om de workload te bekijken die wordt beïnvloed door een IOC. U kunt vervolgens diverse acties uitvoeren voor de workload, zoals patchbeheer uitvoeren of een beschermingsschema wijzigen.
6. (Optioneel) Klik in de kolom **Bestandshash** op **Weergeven** om de bestandshashes weer te geven die zijn gevonden voor een specifieke IOC. Klik in het weergegeven dialoogvenster op om de bestandshash van de IOC te kopiëren naar een teksteditor.

Incidenten verhelpen

Met Eindpuntdetectie en -respons (EDR) kunt u hele incidenten of de afzonderlijke aanvalspunten van een incident verhelpen.

Als u kiest voor het hele incident verhelpen, kunt u aangeven met welke actie(s) u het incident globaal wilt verhelpen. Als u het incident meer in detail moet beheren, kunt u desgewenst kiezen voor afzonderlijke aanvalspunten verhelpen. U kunt bijvoorbeeld het netwerk van een workload isoleren om zijdelingse verplaatsing of Command and control (C&C)-activiteiten te stoppen. Hoewel de workload geïsoleerd is, blijven alle technologieën van Acronis Cyber Protect dan toch functioneel, zodat u een onderzoek kunt starten.

EDR waarborgt effectief herstel via de volgende opties:

- Verhelpen: de bedreiging wordt gestopt.
- Herstellen: de services zijn onmiddellijk weer online.
- Voorkomen: de gebruikte technieken bij een aanval worden voorkomen voor toekomstige aanvallen.

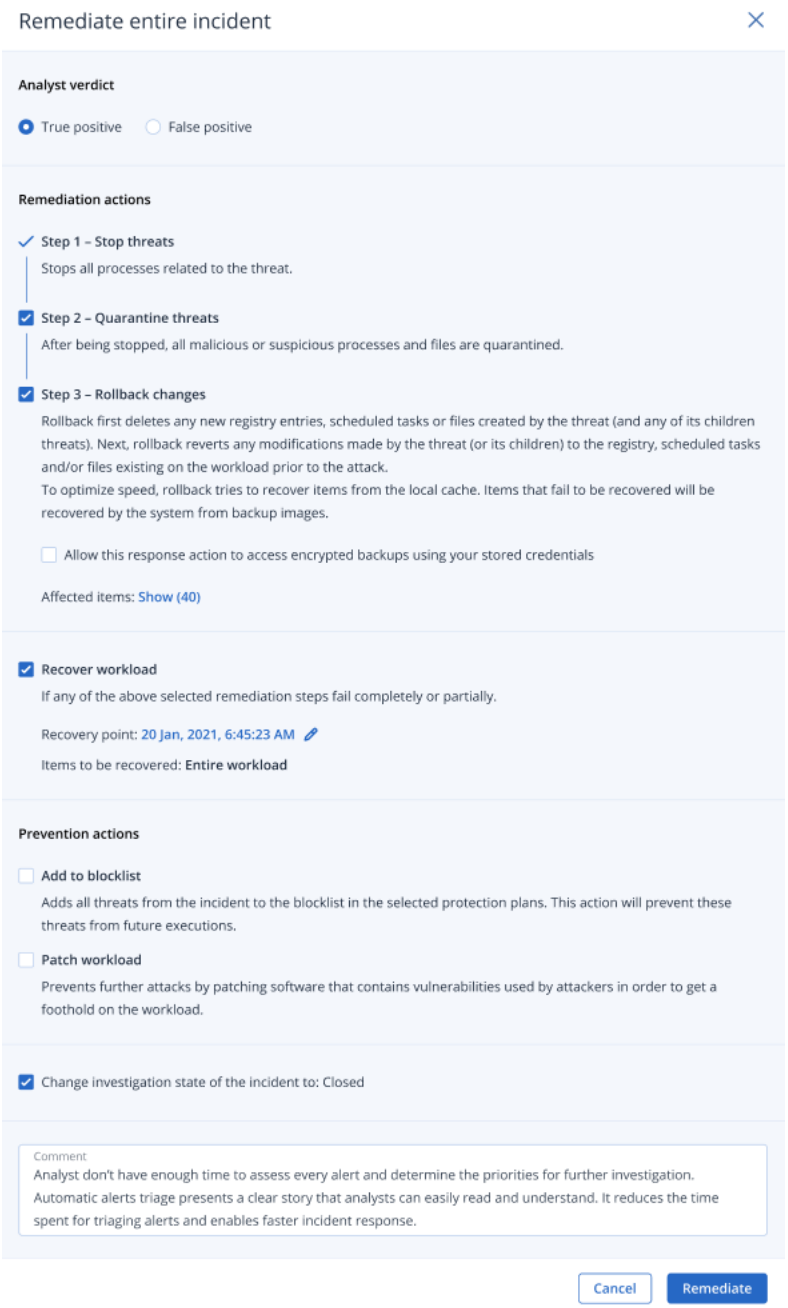
Een heel incident verhelpen

Als u kiest voor het verhelpen van een heel incident, kunt u snel en gemakkelijk aangeven met welke actie(s) u het incident globaal wilt verhelpen. Eindpuntdetectie en -respons (EDR) biedt stapsgewijze begeleiding voor het hele proces om een incident te verhelpen.

Als u uw netwerk en het incident meer in detail moet beheren, raadpleegt u "Responsacties voor afzonderlijke knooppunten in de cyber kill chain" (p. 994).

Een heel incident verhelpen:

1. Ga in de Cyber Protect-console naar **Beveiliging > Incidenten**.
2. Klik in de weergegeven lijst met incidenten op in de uiterst rechtse kolom van het incident dat u wilt onderzoeken. De cyber kill chain voor het geselecteerde incident wordt weergegeven.
3. Klik op **Het hele incident verhelpen**. Het dialoogvenster Het hele incident verhelpen wordt weergegeven.



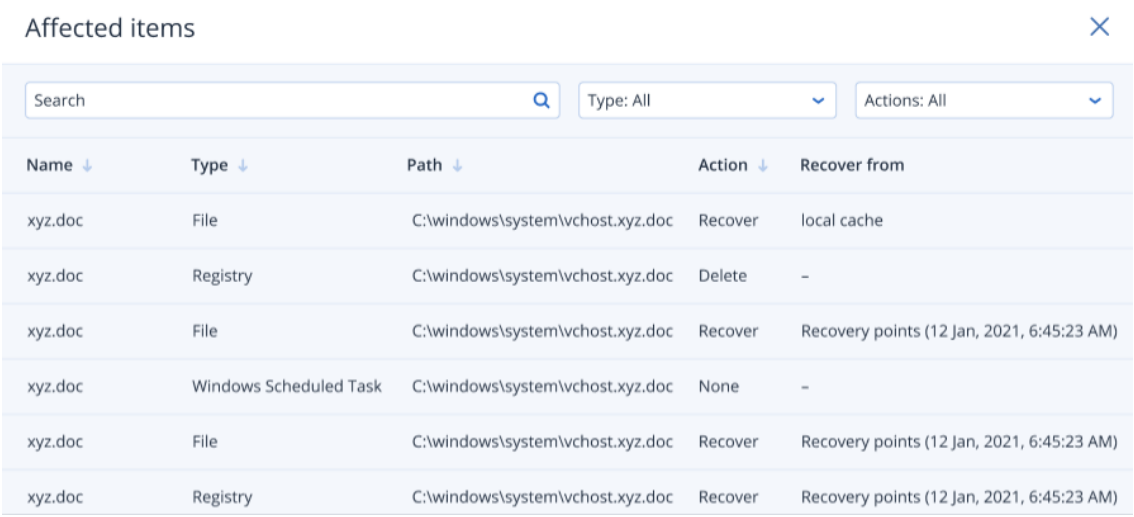
4. Ga naar het gedeelte **Oordeel van analist** en selecteer, op basis van uw onderzoek naar het incident, een van de volgende opties:
   - **Terecht-positief**: Selecteer deze optie of u zeker weet dat de aanval een echte aanval is. Wanneer u deze optie hebt geselecteerd, voegt u herstel- en preventieve acties toe, zoals beschreven in de volgende stappen.
   - **Fout-positief**: Selecteer deze optie of u zeker weet dat de aanval geen echte aanval is. In deze modus kunt u definiëren hoe u wilt voorkomen dat dit opnieuw gebeurt, bijvoorbeeld door het incident toe te voegen aan de acceptatielijst van een beschermingsschema.

Opmerking
Nadat u **Fout-positief** hebt geselecteerd, kunt u alleen preventieve acties definiëren. Zie "Een fout-positief incident verhelpen" (p. 993) voor meer informatie.

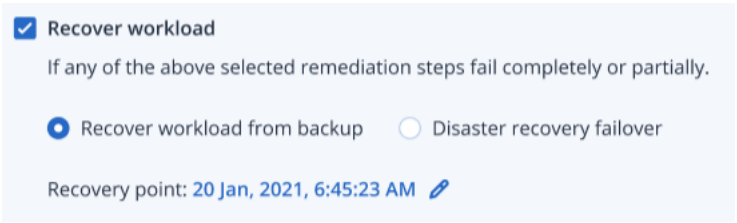
5. Voer in het gedeelte **Herstelacties** de volgende stappen voor herstel uit. Deze moeten in de juiste volgorde worden uitgevoerd: u kunt stap 2 bijvoorbeeld niet selecteren voordat stap 1 is voltooid.
   a. **Stap 1 - Bedreigingen stoppen**: Schakel het selectievakje in om alle processen te stoppen die zijn gerelateerd aan de bedreiging.
   b. **Stap 2 - Bedreigingen in quarantaine plaatsen**: Wanneer de bedreiging is gestopt, schakelt u het selectievakje in om alle schadelijke en verdachte processen en bestanden in quarantaine te plaatsen.
   c. **Stap 3 - Wijzigingen terugdraaien**: Nadat de bedreigingen in quarantaine zijn geplaatst, schakelt u het selectievakje in om alle nieuwe registervermeldingen, geplande taken of door de bedreiging (en onderliggende bedreigingen) gemaakte bestanden te verwijderen. Vervolgens worden alle wijzigingen die door de bedreiging (of bijbehorende onderliggende bedreigingen) zijn aangebracht in het register, de geplande taken en/of bestanden van de workload, teruggedraaid naar de situatie van vóór de aanval. Bij het terugdraaien worden items hersteld uit de lokale cache, zodat de bewerking sneller verloopt. Items die hiermee niet kunnen worden hersteld, worden automatisch hersteld vanaf back-upimages.

   Opmerking
   Tijdens het terugdraaien worden alleen items in de lokale cache hersteld. In toekomstige releases wordt het ook mogelijk om back-uparchieven terug te draaien.

   Als de toegang tot de relevante back-ups is versleuteld, kunt u gebruikmaken van het selectievakje **Deze responsactie toestaan om toegang te krijgen tot versleutelde back-ups via opgeslagen referenties**. EDR heeft toegang tot de opgeslagen gebruikersreferenties om de versleutelde archieven te ontsleutelen en naar de relevante bestanden te zoeken.
   U kunt ook op **Betroffen items** klikken om alle items (bestanden, register of geplande taken) te bekijken die worden beïnvloed door het terugdraaien, samen met de toegepaste acties (**Verwijderen**, **Herstellen** of **Geen**), en om te zien of de items worden hersteld vanuit de lokale cache of vanuit back-upimages.



d. **Workload herstellen**: Als een van de hierboven geselecteerde stappen geheel of gedeeltelijk mislukt, schakelt u het selectievakje voor het herstel van een workload in.



Selecteer een van de volgende herstelopties:

- **Workload herstellen vanaf back-up**: Hiermee kunt u een workload herstellen vanuit een specifiek herstelpunt. Klik op het pictogram voor het bewerken van een herstelpunt om een keuze te maken in een lijst met herstelback-ups.
- **Failover voor Disaster Recovery**: Hiermee kunt u noodherstel uitvoeren (als u deze functionaliteit hebt ingeschakeld in uw beschermingsschema). We raden u aan deze optie te gebruiken voor kritieke workloads, zoals AD-servers of databaseservers. Zie "Noodherstel implementeren" (p. 775) voor meer informatie.

6. Ga naar het gedeelte **Preventieve acties** en selecteer de betreffende stappen voor herstel:
   - **Toevoegen aan blokkeringslijst**: Schakel het selectievakje in en selecteer de betreffende beschermingsschema's in de weergegeven lijst met beschermingsschema's. Met deze preventieve actie wordt de uitvoering van alle detecties van het incident geblokkeerd voor de geselecteerde beschermingsschema's.
   - **Workload patchen**: Schakel het selectievakje in om kwetsbare software te patchen en te voorkomen dat aanvallers toegang krijgen tot de workload. U kunt vervolgens de actie selecteren die moet worden uitgevoerd wanneer de patch is voltooid (**Niet opnieuw opstarten**, **Opnieuw opstarten** of **Alleen opnieuw opstarten indien nodig**), afhankelijk van of de gebruiker is aangemeld of niet.
     U kunt ook het selectievakje **Niet opnieuw opstarten terwijl de back-up wordt uitgevoerd** inschakelen als u niet wilt dat de workload opnieuw wordt opgestart terwijl er een back-up wordt gemaakt.

7. Schakel het selectievakje **De onderzoeksstatus van het incident wijzigen in: Gesloten** in. Indien deze optie niet is geselecteerd, blijft de vorige onderzoeksstatus behouden.
8. Klik op **Herstellen**. De door u geselecteerde herstelacties worden stap voor stap uitgevoerd, waarbij de voortgang van elke stap wordt weergegeven in het dialoogvenster Het hele incident verhelpen.
   Vervolgens ziet u de knop **Ga naar activiteiten**. Klik op **Ga naar activiteiten** om alle responsacties te bekijken die zijn toegepast voor het incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

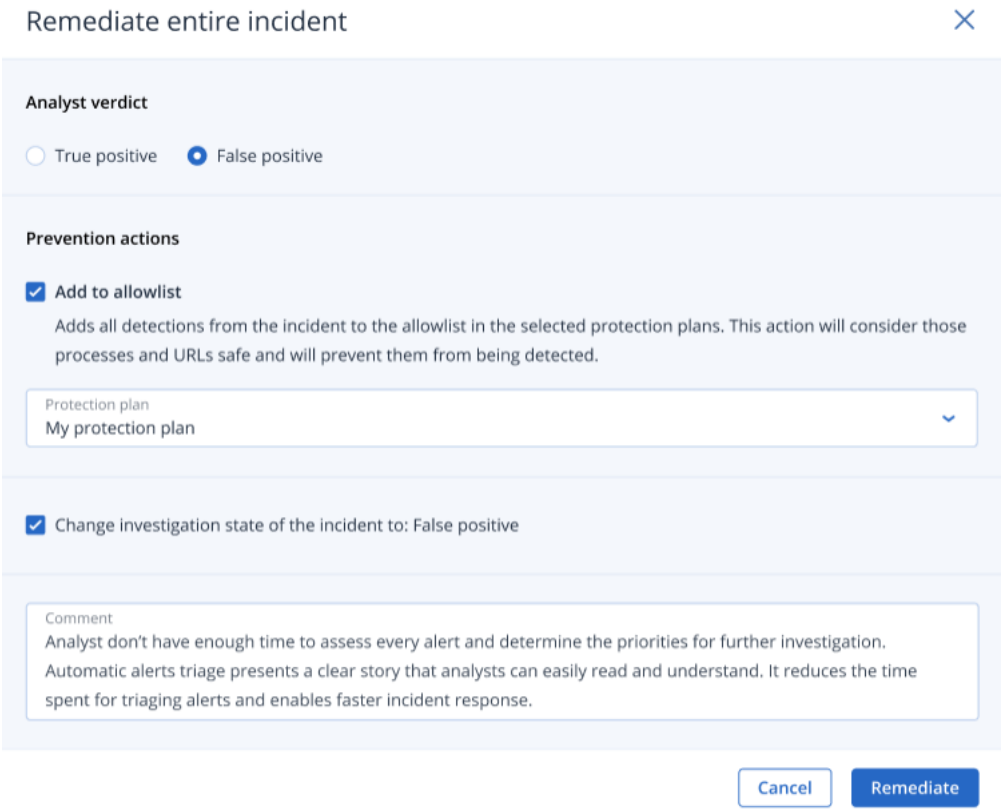
Een fout-positief incident verhelpen

Als u zeker weet dat een aanval geen echte aanval is (dat wil zeggen een fout-positieve aanval is), kunt u definiëren hoe u wilt voorkomen dat het incident zich opnieuw voordoet. U kunt het incident bijvoorbeeld toevoegen aan een acceptatielijst van een beschermingsschema.

Een fout-positief incident verhelpen:

1. Klik in de cyber kill chain voor het geselecteerde incident op **Het hele incident verhelpen**. Het dialoogvenster Het hele incident verhelpen wordt weergegeven.

2. Ga naar het gedeelte **Oordeel van analist** en selecteer **Fout-positief**.



3. Schakel in het gedeelte **Preventieve acties** het selectievakje **Toevoegen aan acceptatielijst** in.
   Ga naar de weergegeven lijst met beschermingsschema's en selecteer de betreffende beschermingsschema's.
   Door deze preventieve actie worden alle detecties van het incident niet opgenomen voor de geselecteerde beschermingsschema's.
4. Schakel het selectievakje **De onderzoeksstatus van het incident wijzigen in: Fout-positief** in.
5. Klik op **Herstellen**.
   Vervolgens ziet u de knop **Ga naar activiteiten**. Klik op **Ga naar activiteiten** om de responsacties te bekijken die zijn toegepast voor het incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Responsacties voor afzonderlijke knooppunten in de cyber kill chain

Als u het incident meer in detail moet beheren, kunt u verschillende responsacties toepassen voor afzonderlijke knooppunten in de cyber kill chain. Met deze responsacties kunt u elk knooppunt snel en eenvoudig herstellen.

Opmerking
Zie "Een heel incident verhelpen" (p. 989) voor het toepassen van globale responsacties voor een heel incident.

Responsacties zijn onderverdeeld in de volgende categorieën, maar niet alle categorieën zijn van toepassing op alle knooppunten:

- **Herstellen**: Met de acties van deze categorie kunt u onmiddellijk op de aanval reageren, bijvoorbeeld door acties zoals netwerkisolatie beheren voor een workload, en bestanden, processen en registerwaarden verwijderen en in quarantaine plaatsen.
- **Onderzoeken**: Met de acties van deze categorie (alleen van toepassing op workloads) kunt u een forensische back-up of een externe desktopverbinding uitvoeren voor een diepgaander onderzoek.
- **Onderzoeken**: Met de acties van deze categorie (alleen van toepassing op workloads) kunt u een verbinding met extern bureaublad uitvoeren voor een diepgaander onderzoek.
- **Herstel**: Met de acties van deze categorie (alleen van toepassing op workloads) kunt u reageren op intensieve aanvallen door een herstel uit te voeren vanaf een back-up of via een failover voor Disaster Recovery.
- **Voorkomen**: Met de acties van deze categorie kunt u toekomstige bedreigingen of vals-positieven voorkomen door ze toe te voegen aan een acceptatielijst of blokkeringslijst van een beschermingsschema.

Opmerking
Als een incident is gesloten, kunt u geen responsactie toepassen op een knooppunt. Als u een gesloten incident toch wilt heropenen, kunt u de status van het onderzoek wijzigen en weer instellen op **Onderzoeken**. Wanneer het onderzoek dan weer is geopend, kunt u responsacties toepassen.

De volgende tabel bevat een beschrijving van elk van de typen knooppunten in de cyber kill chain, de toepasselijke categorieën voor elk knooppunt en de mogelijke responsacties.

Knooppunt	Categorie	Responsacties
Workload	Herstellen	• Netwerkisolatie beheren • Workload opnieuw opstarten
	Onderzoeken	• Forensische back-up • Verbinding met extern bureaublad
	Onderzoeken	• Verbinding met extern bureaublad
	Herstel	• Herstel vanaf back-up • Failover voor Disaster

Knooppunt	Categorie	Responsacties
		Recovery
	Voorkomen	• Patch
Proces	Herstellen	• Proces stoppen • Quarantaine
	Voorkomen	• Toevoegen aan acceptatielijst • Toevoegen aan blokkeringslijst
Bestand	Herstellen	• Verwijderen • Quarantaine
	Voorkomen	• Toevoegen aan acceptatielijst • Toevoegen aan blokkeringslijst
Register	Herstellen	• Verwijderen
Netwerk	Voorkomen	• Toevoegen aan acceptatielijst • Toevoegen aan blokkeringslijst

Responsacties definiëren voor een getroffen workload

Als onderdeel van uw reactie op een aanval kunt u de volgende acties toepassen voor getroffen workloads:

- **Netwerkisolatie beheren**: Hiermee kunt u de netwerkisolatie van een workload beheren om zijdelingse verplaatsing of Command and control (C&C)-activiteiten te stoppen. Zie "De netwerkisolatie van een workload beheren" (p. 997) voor meer informatie.
- **Patch**: Hiermee kunt u een workload patchen om misbruik van beveiligingsproblemen te voorkomen bij toekomstige potentiële aanvallen. Zie "Een workload patchen" (p. 1001) voor meer informatie.
- **Workload opnieuw opstarten**: Hiermee kunt u een workload onmiddellijk opnieuw opstarten of de workload opnieuw opstarten volgens een vooraf gedefinieerde time-outperiode. Zie "Een workload opnieuw opstarten" (p. 1002) voor meer informatie.
- **Forensische back-up**: Hiermee kunt u op aanvraag een forensische back-up maken voor audit- of verdere onderzoeksdoeleinden. Zie "Een forensische back-up op aanvraag uitvoeren voor een workload" (p. 1003) voor meer informatie.

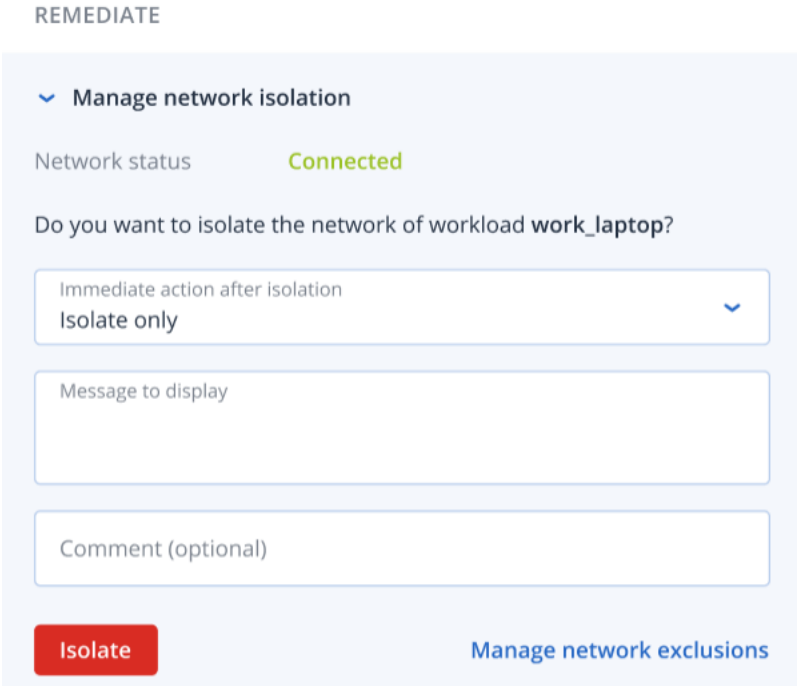
- **Verbinding met extern bureaublad**: Hiermee hebt u op afstand toegang tot de workload die wordt onderzocht. Zie "Externe verbinding met een workload" (p. 1004) voor meer informatie.
- **Herstellen vanaf back-up**: Hiermee kunt u uw volledige machine herstellen vanaf een back-up of specifieke bestanden of mappen. Zie "Herstel vanaf back-up" (p. 1005) voor meer informatie.
- **Failover voor Disaster Recovery**: Hiermee kunt u "Noodherstel implementeren" (p. 775) uitvoeren. Let op: u moet een abonnement op Advanced Disaster Recovery hebben voor uw workload. Zie "Failover voor Disaster Recovery" (p. 1006) voor meer informatie.

De netwerkisolatie van een workload beheren

Met EDR kunt u de netwerkisolatie van een workload beheren om zijdelingse verplaatsing of Command and control (C&C)-activiteiten te stoppen. U munt kiezen uit diverse opties voor isolatie, afhankelijk van uw vereisten. Let op: alle technologieën van Acronis Cyber Protect zijn functioneel, zelfs als een workload is geïsoleerd, zodat u een volledig onderzoek kunt uitvoeren.

Een workload isoleren van het netwerk:

1. Klik in de cyber kill chain op het workloadknooppunt dat u wilt herstellen.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.
3. Klik in het gedeelte **Herstellen** op **Netwerkisolatie beheren**.



Opmerking
De waarde van **Netwerkstatus** geeft aan of de workload momenteel is verbonden of niet. Als de waarde **Geïsoleerd** is, kunt u de geïsoleerde workload opnieuw verbinden met het netwerk, zoals beschreven in de onderstaande procedure. Als de workload offline is, kunt u de workload toch nog isoleren. Wanneer de workload weer online gaat, krijgt deze automatisch de status **Geïsoleerd**.

4. In de vervolgkeuzelijst **Onmiddellijke actie na isolatie** selecteert u een van de volgende opties:
   - **Alleen isoleren**
   - **Workload isoleren en back-up maken**
   - **Workload isoleren en back-up maken met forensische gegevens**
   - **Workload isoleren en uitschakelen**

   Zie "Back-up en herstel van workloads en bestanden beheren" (p. 422) voor meer informatie over het definiëren van een locatie voor back-ups van de workload en mogelijke versleutelingsopties.
5. [Optioneel] Voeg in het veld **Bericht om weer te geven** een bericht toe dat wordt weergegeven voor eindgebruikers wanneer ze toegang krijgen tot de geïsoleerde workload. U kunt gebruikers bijvoorbeeld laten weten dat de workload nu geïsoleerd is en dat netwerktoegang naar en uit de workload momenteel niet beschikbaar is. Let op: dit bericht wordt ook weergegeven als een tray monitor-melding en het blijft zichtbaar totdat de gebruiker het bericht sluit.
6. [Optioneel] Voeg een opmerking toe in het veld **Opmerking**. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
7. Klik op **Netwerkuitsluitingen beheren** om poorten, URL's, hostnamen en IP-adressen toe te voegen die toegang hebben tot de workload tijdens de isolatie. Zie Netwerkuitsluitingen beheren voor meer informatie.
8. Klik op **Isoleren**.
   De workload is geïsoleerd. Deze actie kan ook worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

   Opmerking
   De workload wordt ook weergegeven als **Geïsoleerd** in het menu **Workloads** in de Cyber Protect-console. U kunt enkele of meerdere workloads ook isoleren via het menu **Workloads > Workloads met agents**. Selecteer de relevante workload(s) en selecteer **Netwerkisolatie beheren** in de rechterzijbalk. In het weergegeven dialoogvenster kunt u netwerkuitsluitingen beheren. Klik op **Isoleren** of **Alles isoleren** om de geselecteerde workload(s) te isoleren.

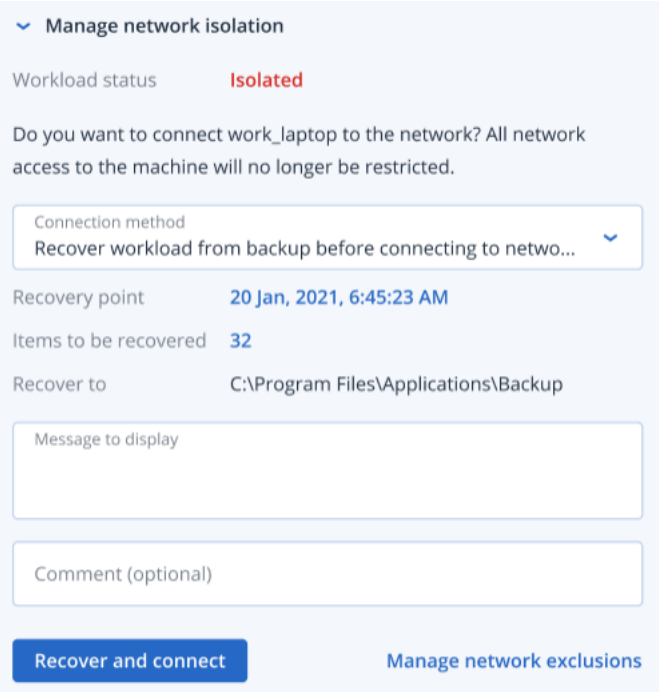
Een geïsoleerde workload opnieuw verbinden met het netwerk:

1. Klik in de cyber kill chain op het workloadknooppunt dat u opnieuw wilt verbinden.

   Opmerking
   Als de geïsoleerde workload momenteel offline is, kunt u deze toch nog opnieuw verbinden met het netwerk. Wanneer de workload weer online gaat, krijgt deze automatisch de status **Verbonden**.

2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.

3. Klik in het gedeelte **Herstellen** op **Netwerkisolatie beheren**.
4. Selecteer een van de volgende opties:
   - **Onmiddellijk verbinding maken met netwerk**: De workload wordt opnieuw verbonden met het netwerk.
   - **Workload herstellen vanaf back-up voordat verbinding wordt gemaakt met het netwerk**: Selecteer een herstelpunt van waaruit u de workload wilt herstellen:
     a. Klik in het veld **Herstelpunt** op **Selecteren**.
     b. Ga naar de weergegeven zijbalk en selecteer het betreffende herstelpunt.
     c. Klik op **Herstellen > Volledige workload** om alle bestanden en mappen voor de workload te herstellen.
     Of
     Klik op **Herstellen > Bestanden/mappen** om specifieke bestanden en mappen voor de workload te herstellen. U wordt vervolgens gevraagd om de relevante bestanden of mappen te selecteren. Wanneer u deze hebt geselecteerd, kunt u de lijst met items bekijken door op de betreffende waarde te klikken in het veld **Items om te herstellen**.



Opmerking
Als het door u geselecteerde herstelpunt is versleuteld, wordt u om het wachtwoord gevraagd.

5. [Optioneel] Schakel het selectievakje **De workload indien nodig automatisch opnieuw opstarten** in. Deze optie is alleen relevant als u in stap 4 **Herstellen > Volledige workload** hebt geselecteerd.
6. [Optioneel] Voeg in het veld **Bericht om weer te geven** een bericht toe dat wordt weergegeven voor eindgebruikers wanneer ze toegang krijgen tot de verbonden workload. U kunt gebruikers

bijvoorbeeld laten weten dat er een back-up is hersteld voor de workload en dat netwerktoegang naar en uit de workload is hervat.

7. [Optioneel] Voeg een opmerking toe in het veld **Opmerking**. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
8. Klik op **Verbinden** als u **Onmiddellijk verbinding maken met netwerk** hebt geselecteerd in stap 4.
   Of
   Klik op **Herstellen en verbinden** als u **Workload herstellen vanaf back-up voordat verbinding wordt gemaakt met het netwerk** hebt geselecteerd in stap 4.
   De workload wordt opnieuw verbonden met het netwerk en er zijn geen beperkingen meer voor toegang tot het netwerk.

Opmerking
U kunt enkele of meerdere geïsoleerde workloads ook verbinden via het menu **Workloads > Workloads met agents** in de Cyber Protect-console. Selecteer de betreffende workload(s) en selecteer **Netwerkisolatie beheren** in de rechterzijbalk. Klik in het weergegeven dialoogvenster op **Verbinden** of **Alles verbinden** om de geselecteerde workload(s) weer te verbinden met het netwerk.

Netwerkuitsluitingen beheren

Opmerking
Zelfs als alle technologieën van Acronis Cyber Protect werken wanneer de workload geïsoleerd is, kunnen er scenario's zijn waarin u extra netwerkverbindingen tot stand moet brengen (u moet bijvoorbeeld een bestand van de workload uploaden naar een gedeelde map). In deze scenario's kunt u een netwerkuitsluiting toevoegen, maar u moet wel eventuele bedreigingen verwijderen voordat u de uitsluiting toevoegt.

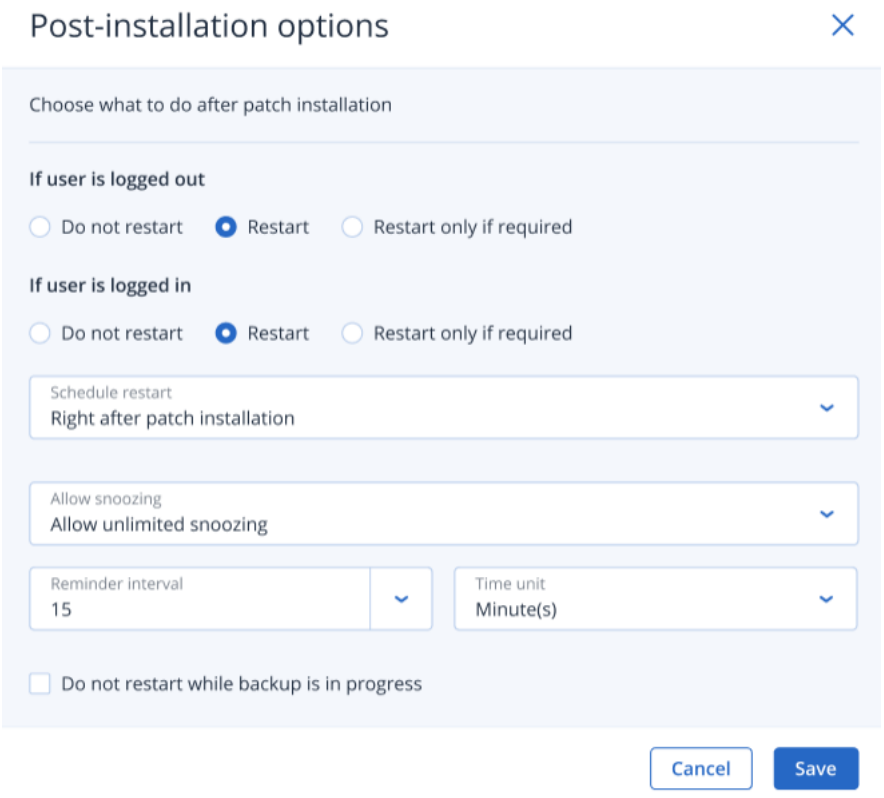
1. Klik in het gedeelte **Herstellen** van het tabblad **Responsacties** op **Netwerkuitsluitingen beheren**.
2. Voeg in de zijbalk Netwerkuitsluitingen de betreffende uitsluitingen toe. Doe het volgende voor elk van de beschikbare opties (poorten, URL-adres en hostnaam/IP-adres):
   a. Klik op **Toevoegen** en voer vervolgens de relevante poort(en), URL-adressen of hostnaam/IP-adressen in.
   b. Selecteer in de vervolgkeuzelijst **Verkeersrichting** een van de opties: **Binnenkomende en uitgaande verbindingen**, **Alleen binnenkomende verbindingen** of **Alleen uitgaande verbindingen**.
   c. Klik op **Toevoegen**.
3. Klik op **Opslaan**.

Een workload patchen

EDR detecteert automatisch of er een patch nodig is voor een workload, zodat u de workload kunt patchen om misbruik van beveiligingsproblemen te voorkomen bij toekomstige potentiële aanvallen. Let op: deze functie is alleen beschikbaar is als de partner een abonnement op Advanced Management heeft voor de workload.

Een workload patchen:

1. Klik in de cyber kill chain op het workloadknooppunt dat u wilt patchen.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.
3. Klik in het gedeelte **Herstellen** op **Patchen**.
4. Klik in het veld **Patches om te installeren** op **Selecteren**. Selecteer in het weergegeven dialoogvenster de betreffende patches en klik vervolgens op **Selecteren**.
5. Klik in het veld **Opties na de installatie** op de weergegeven link. Het dialoogvenster Opties na de installatie wordt weergegeven.



6. Selecteer de actie die moet worden uitgevoerd nadat de patch is geïnstalleerd:
   - **Als de gebruiker is afgemeld**: Selecteer een van de opties **Niet opnieuw opstarten**, **Opnieuw opstarten** of **Alleen opnieuw opstarten indien nodig**.
   - **Als de gebruiker is aangemeld**: Selecteer een van de opties **Niet opnieuw opstarten**, **Opnieuw opstarten** of **Alleen opnieuw opstarten indien nodig**.
     Wanneer u **Opnieuw opstarten** selecteert, kunt u ook het volgende definiëren:

- Opnieuw opstarten plannen.
- Slaapstand toestaan, inclusief de gedefinieerde intervallen tussen twee slaapstanden.

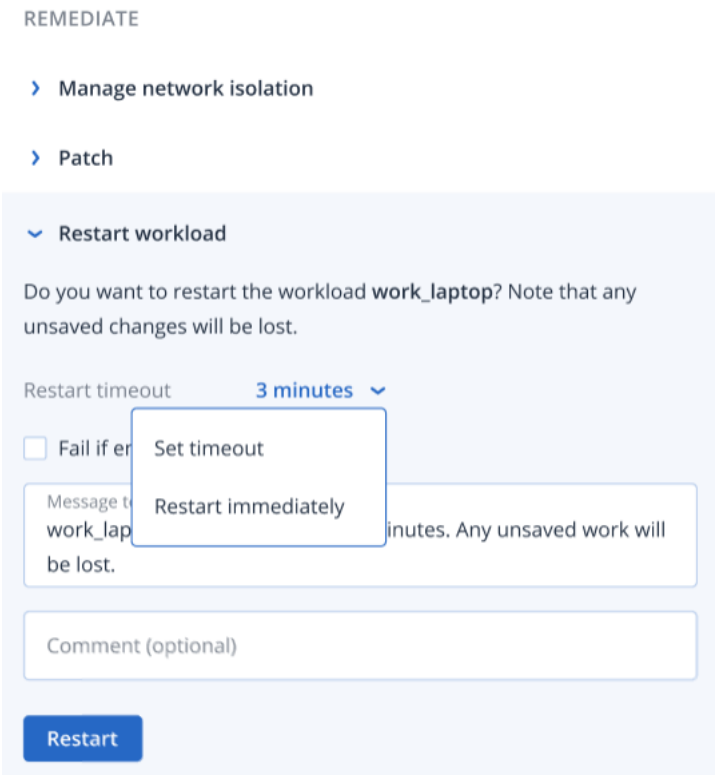
7. [Optioneel] Schakel het selectievakje **Niet opnieuw opstarten terwijl de back-up wordt uitgevoerd** in als u niet wilt dat de workload opnieuw wordt opgestart terwijl er een back-up wordt gemaakt.
8. Klik op **Opslaan**.
9. Klik op het tabblad **Responsacties** op **Patchen**.
   De geselecteerde patch wordt uitgevoerd. Deze actie kan ook worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Een workload opnieuw opstarten

Als onderdeel van uw reactie op een aanval kunt u EDR gebruiken om een workload onmiddellijk opnieuw op te starten of de workload opnieuw op te starten volgens een vooraf gedefinieerde time-outperiode.

Een workload opnieuw opstarten:

1. Klik in de cyber kill chain op het workloadknooppunt waarvoor u een schema voor opnieuw opstarten wilt instellen.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.
3. Klik in het gedeelte **Herstellen** op **Workload opnieuw opstarten**.



4. Klik in het veld **Time-out voor opnieuw opstarten** op de weergegeven link en selecteer een van de volgende opties:

- **Time-out instellen**: Stel in het dialoogvenster Time-out voor opnieuw opstarten de periode voor het opnieuw opstarten van de workload in en klik vervolgens op **Opslaan**.
- **Onmiddellijk opnieuw opstarten**: Selecteer deze optie als u de workload meteen opnieuw wilt opstarten.

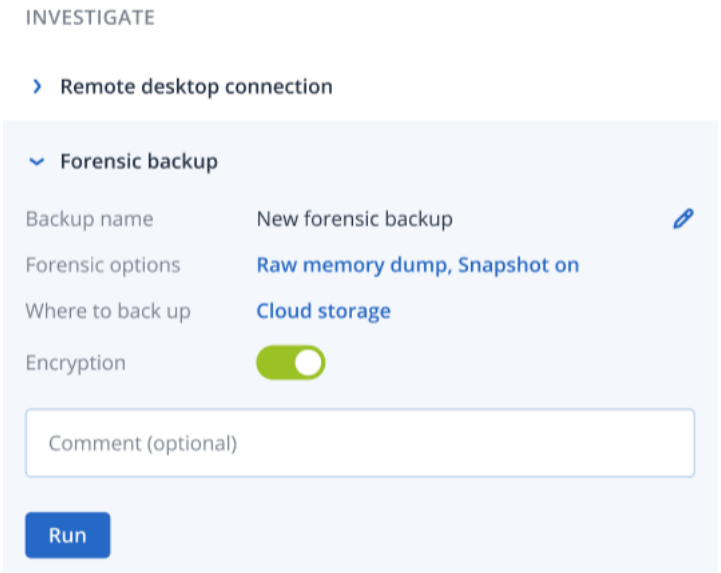
5. [Optioneel] Schakel het selectievakje **Mislukt als eindgebruiker is aangemeld** in om te voorkomen dat de workload opnieuw wordt opgestart als de gebruiker is aangemeld.
6. Voeg in het veld **Bericht om weer te geven** een bericht toe dat wordt weergegeven voor gebruikers wanneer ze toegang krijgen tot de geïsoleerde workload.
7. [Optioneel] Voeg een opmerking toe in het veld **Opmerking**. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
8. Klik op **Opnieuw opstarten**.
   U hebt nu ingesteld dat de workload opnieuw wordt opgestart volgens het gedefinieerde schema. Deze actie kan ook worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Een forensische back-up op aanvraag uitvoeren voor een workload

Bij uw onderzoek naar een aanval kunt u EDR gebruiken om op aanvraag een forensische back-up uit te voeren voor audit- of verdere onderzoeksdoeleinden. Let op: deze functie is alleen beschikbaar is als de partner een abonnement op Advanced Backup heeft voor de workload.

Een forensische back-up uitvoeren

1. Klik in de cyber kill chain op het workloadknooppunt waarvoor u een forensische back-up wilt uitvoeren.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.
3. Klik in het gedeelte **Onderzoeken** op **Forensische back-up**.



4. [Optioneel] Klik in het veld **Naam van back-up** op het bewerkingspictogram om de naam van de back-up te bewerken.
5. Klik in het veld **Forensische opties** op de weergegeven link. In het dialoogvenster Forensische opties dat wordt weergegeven, selecteert u een van de volgende opties:
   - **Onbewerkte geheugendump verzamelen**
   - **Kernelgeheugendump verzamelen**

   U kunt ook het selectievakje **Momentopname van actieve processen** inschakelen om informatie toe te voegen over de processen die worden uitgevoerd op het moment dat de back-up wordt gestart. Deze informatie wordt opgeslagen in een back-upimage.

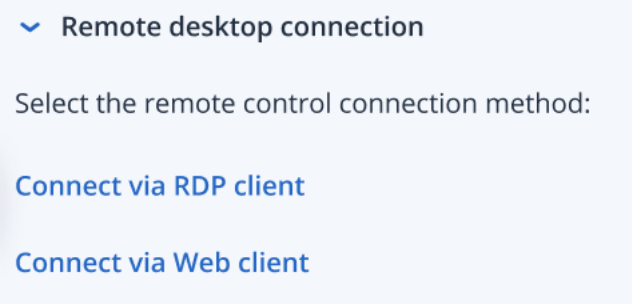
   Klik op **Opslaan** om het dialoogvenster Forensische opties te sluiten.
6. Klik in het veld **Waar back-up maken** op de weergegeven link om een locatie voor de back-up te definiëren.
7. [Optioneel] Klik op de optie **Versleuteling** om versleuteling in te schakelen. Voer in het weergegeven dialoogvenster het wachtwoord voor de versleutelde back-up in en selecteer het gewenste versleutelingsalgoritme.
8. [Optioneel] Voeg een opmerking toe in het veld **Opmerking**. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
9. Klik op **Uitvoeren**.
   De forensische back-up wordt gestart. Deze actie kan ook worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Externe verbinding met een workload

Bij uw onderzoek naar een aanval kunt u EDR gebruiken om op afstand toegang te krijgen tot de workload die u onderzoekt.

Op afstand verbinding maken met een workload:

1. Klik in de cyber kill chain op het workloadknooppunt waarmee u op afstand verbinding wilt maken.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.
3. Klik in het gedeelte **Onderzoeken** op **Verbinding met extern bureaublad**.



4. Selecteer een van de volgende methoden voor externe verbinding:
   - **Verbinding maken via RDP-client**: Bij deze methode wordt u gevraagd om de client voor Verbinding met extern bureaublad te downloaden en te installeren. Vervolgens kunt u op afstand verbinding maken met een workload vanaf de Cyber Protect-console.
   - **Verbinding maken via webclient**: Bij deze methode hoeft u geen RDP-client te installeren voor uw workload. U wordt omgeleid naar het aanmeldingsscherm waar u de referenties voor de externe machine moet invoeren.

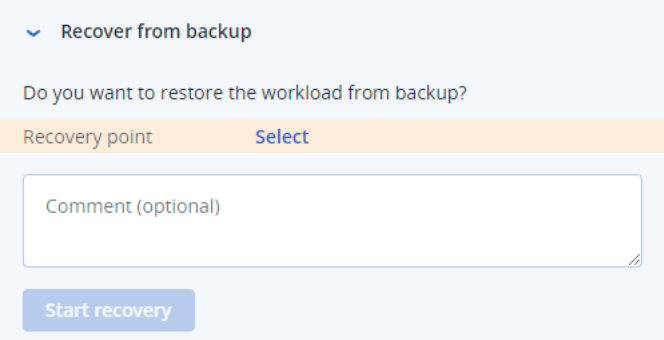
   Wanneer de externe verbinding is gestart, kan deze actie worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Herstel vanaf back-up

Als onderdeel van uw reactie op een aanval kunt u EDR gebruiken om uw volledige machine of specifieke bestanden of mappen te herstellen vanaf een back-up.

Uw workload herstellen vanaf back-up

1. Klik in de cyber kill chain op het workloadknooppunt dat u wilt herstellen.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.
3. Klik in het gedeelte **Herstel** op **Herstellen vanaf back-up**.



4. Klik in het veld **Herstelpunt** op **Selecteren** en voer de volgende stappen uit:
   a. Ga naar de weergegeven zijbalk en selecteer het betreffende herstelpunt.
   b. Klik op **Herstellen > Volledige workload** om alle bestanden en mappen voor de workload te herstellen.
      Of
      Klik op **Herstellen > Bestanden/mappen** om specifieke bestanden en mappen voor de workload te herstellen. U wordt vervolgens gevraagd om de relevante bestanden of mappen te selecteren. Wanneer u deze hebt geselecteerd, kunt u de voor herstel geselecteerde items bekijken door op de betreffende waarde te klikken in het veld **Items om te herstellen**.

      Opmerking
      Als het door u geselecteerde herstelpunt is versleuteld, wordt u om het wachtwoord gevraagd.

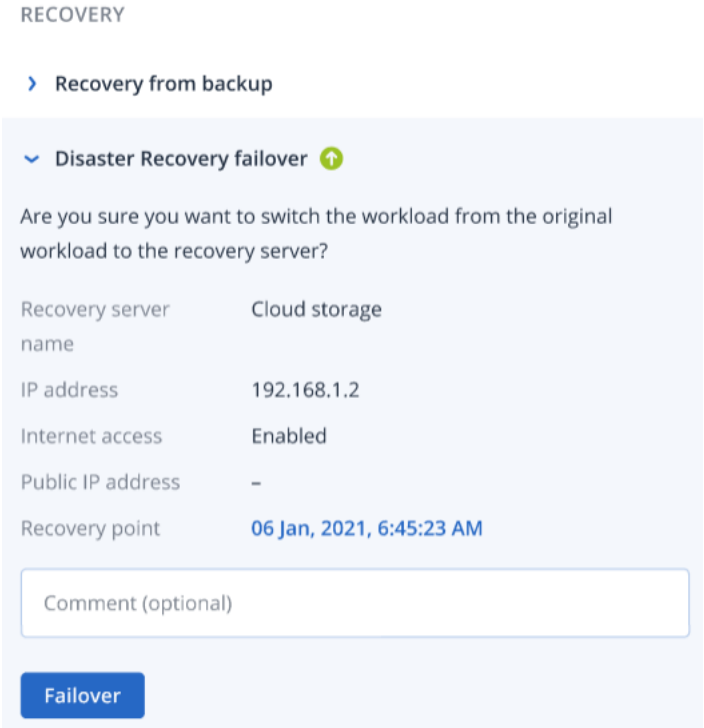
5. [Optioneel] Schakel het selectievakje **De workload automatisch opnieuw opstarten** in. Deze optie is alleen relevant als u in stap 4 **Herstellen > Volledige workload** hebt geselecteerd.
6. [Optioneel] Voeg een opmerking toe in het veld **Opmerking**. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
7. Klik op **Herstel starten**.
   Het proces om de workload te herstellen begint. De voortgang van deze actie kan worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Failover voor Disaster Recovery

Als onderdeel van uw reactie op een aanval kunt u EDR gebruiken om "Noodherstel implementeren" (p. 775) uit te voeren. Hierdoor wordt de workload verplaatst naar de herstelserver. Let op: u moet een abonnement op Advanced Disaster Recovery hebben voor uw workload.

Failover voor Disaster Recovery uitvoeren:

1. Klik in de cyber kill chain op het workloadknooppunt dat u wilt herstellen.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.
3. Klik in het gedeelte **Herstel** op **Failover voor Disaster Recovery**.



4. Ga naar het veld het **Herstelpunt** en voer de volgende stappen uit:
   a. Klik op de huidige herstelpuntdatum om een herstelpunt te selecteren.
   b. Ga naar de weergegeven zijbalk en selecteer het betreffende herstelpunt.

Opmerking
Als u een abonnement op Advanced Disaster Recovery hebt, kunt u de betreffende herstelserver (de offline VM) selecteren die is gemaakt in Disaster Recovery. Als u geen abonnement hebt, wordt u gevraagd om Disaster Recovery te configureren.

5. [Optioneel] Voeg een opmerking toe in het veld **Opmerking**. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
6. Klik op **Failover**.
   De workload wordt verplaatst naar de herstelserver. Deze actie kan worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Responsacties definiëren voor een verdacht proces

Als onderdeel van uw reactie op een aanval kunt u de volgende acties toepassen in het geval van verdachte processen:

- Een proces stoppen (zie hieronder)
- Een proces in quarantaine plaatsen (zie hieronder)
- De door een proces gemaakte wijzigingen terugdraaien (zie hieronder)
- Het proces toevoegen aan een acceptatielijst of blokkeringslijst van een beschermingsschema (zie "Een proces, bestand of netwerk toevoegen of verwijderen in de blokkeringslijst of acceptatielijst van het beschermingsschema" (p. 1013))

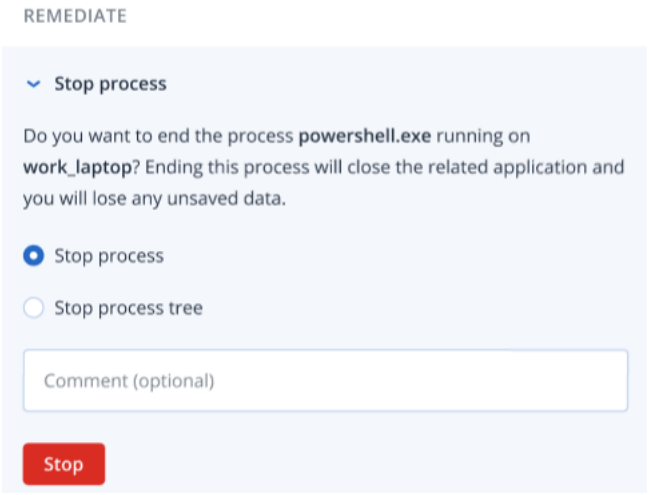
Een verdacht proces stoppen:

1. Klik in de cyber kill chain op het procesknooppunt dat u wilt herstellen.

   Opmerking
   Kritieke Windows-processen of niet-actieve processen kunnen niet worden gestopt en worden uitgeschakeld in de cyber kill chain.

2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.

3. Klik in het gedeelte **Herstellen** op **Proces stoppen**.



4. Selecteer een van de volgende opties:
   - **Proces stoppen** (stopt het specifieke proces)
   - **Processtructuur stoppen** (stopt het specifieke proces en alle onderliggende processen)
5. [Optioneel] Voeg een opmerking toe. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
6. Klik op **Stoppen**. Het proces wordt gestopt.

   Opmerking
   De betreffende toepassing wordt gesloten en niet-opgeslagen gegevens gaan verloren.

   Deze actie kan ook worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

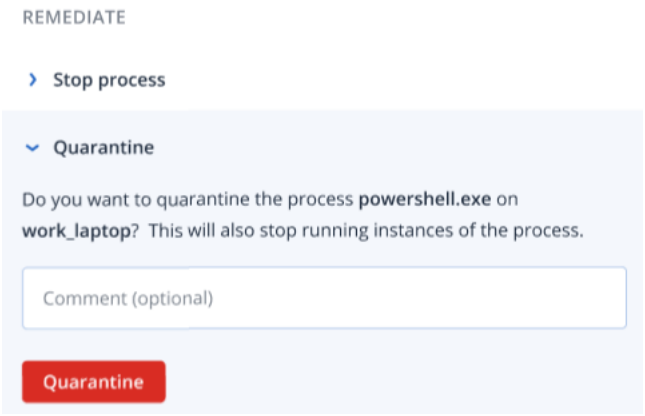
Een verdacht proces in quarantaine plaatsen:

1. Klik in de cyber kill chain op het procesknooppunt dat u in quarantaine wilt plaatsen.

   Opmerking
   Kritieke Windows-processen kunnen niet in quarantaine worden geplaatst en worden uitgeschakeld in de cyber kill chain.

2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.

3. Klik in het gedeelte **Herstellen** op **Quarantaine**.



4. [Optioneel] Voeg een opmerking toe. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
5. Klik op **Quarantaine**. Het proces wordt gestopt en vervolgens in quarantaine geplaatst.

Opmerking
Het proces wordt toegevoegd aan en beheerd in het gedeelte Quarantaine onder Antimalwarebeveiliging.

Deze actie kan ook worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

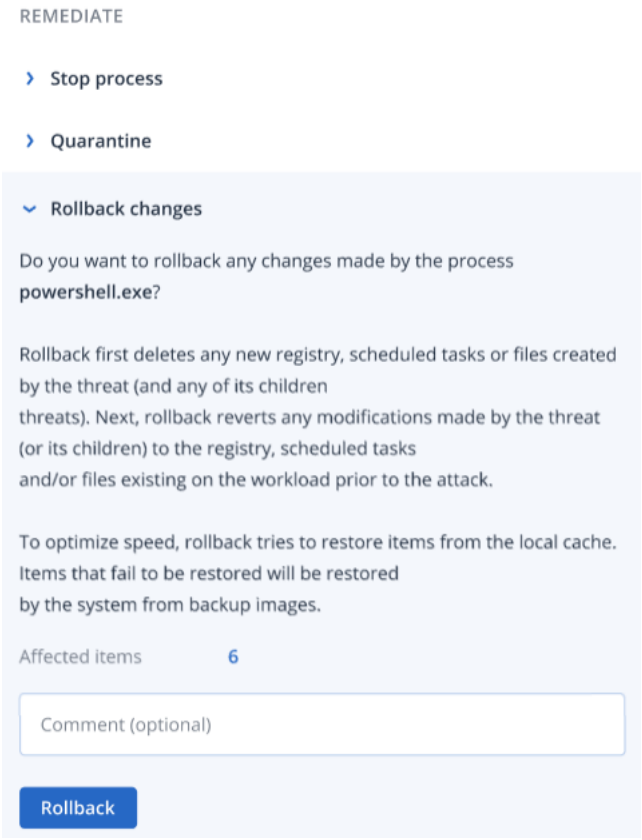
Wijzigingen terugdraaien:

1. Klik in de cyber kill chain op het procesknooppunt waarvoor u wijzigingen wilt terugdraaien.

Opmerking
Deze actie is alleen beschikbaar voor detectieknooppunten (weergegeven als rode of gele knooppunten).

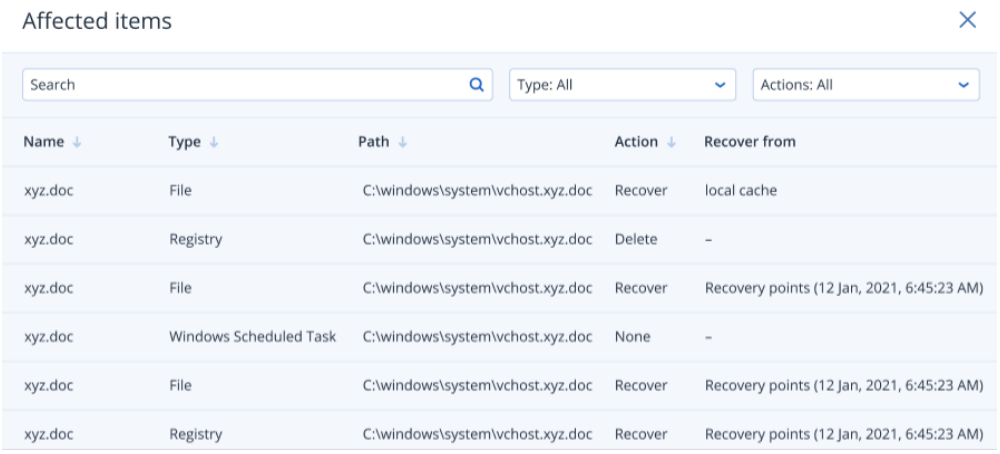
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.

3. Klik in het gedeelte **Herstellen** op **Wijzigingen terugdraaien**.



Opmerking
Tijdens het terugdraaien worden alleen items in de lokale cache hersteld. In toekomstige releases wordt het ook mogelijk om back-uparchieven terug te draaien.

4. Klik op de link **Betroffen items** om de items te bekijken die worden beïnvloed door de teruggedraaide wijzigingen. Het weergegeven dialoogvenster toont alle items (bestanden, register, geplande taken) die worden teruggedraaid en welke actie hiervoor is gebruikt (**Verwijderen**, **Herstellen** of **Geen**). Daarnaast kunt u zien of de herstelde items worden hersteld vanuit de lokale cache of vanuit back-upherstelpunten.



5. [Optioneel] Voeg een opmerking toe. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
6. Klik op **Terugdraaien**. Met de functionaliteit voor terugdraaien worden alle dor het proces gemaakte wijzigingen van registers, bestanden of geplande taken ongedaan gemaakt. Dit gebeurt als volgt:
   a. Alle nieuwe vermeldingen (register, geplande taken, bestanden) die door de bedreiging (en bijbehorende onderliggende bedreigingen) zijn gemaakt, worden verwijderd.
   b. Alle wijzigingen die door de bedreiging (en bijbehorende onderliggende bedreigingen) zijn aangebracht in het register, de geplande taken en/of bestanden van de workload, worden teruggedraaid naar de situatie van vóór de aanval.
   c. Bij het terugdraaien wordt geprobeerd items te herstellen uit de lokale cache. Items die niet kunnen worden hersteld, worden door EDR automatisch hersteld vanaf schone back-upimages.

   De terugdraaiactie kan ook worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

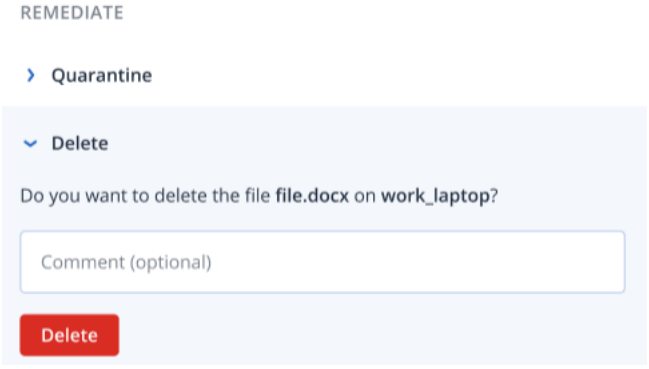
Responsacties voor een verdacht bestand definiëren

Als onderdeel van uw reactie op een aanval kunt u de volgende acties toepassen in het geval van verdachte bestanden:

- Een bestand verwijderen (zie hieronder)
- Een bestand in quarantaine plaatsen (zie hieronder)
- Het bestand toevoegen aan een acceptatielijst of blokkeringslijst van een beschermingsschema (zie "Een proces, bestand of netwerk toevoegen of verwijderen in de blokkeringslijst of acceptatielijst van het beschermingsschema" (p. 1013))

Een verdacht bestand verwijderen:

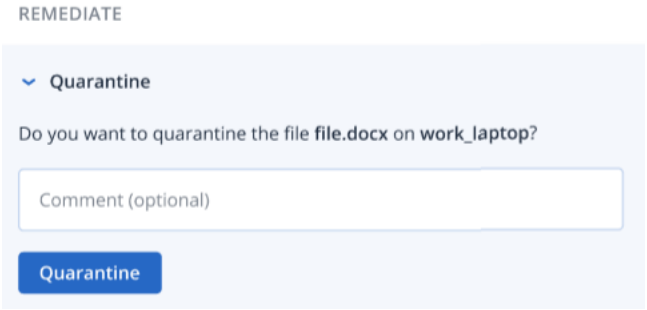
1. Klik in de cyber kill chain op het bestandsknooppunt dat u wilt herstellen.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.
3. Klik in het gedeelte **Herstellen** op **Verwijderen**.



4. [Optioneel] Voeg een opmerking toe. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
5. Klik op **Verwijderen**.
   Het bestand wordt verwijderd. Deze actie kan ook worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Een verdacht bestand in quarantaine plaatsen:

1. Klik in de cyber kill chain op het bestandsknooppunt dat u wilt herstellen.
2. Ga in de weergegeven zijbalk naar **Responsacties**.
3. Klik in het gedeelte **Herstellen** op **Quarantaine**.



4. [Optioneel] Voeg een opmerking toe. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
5. Klik op **Quarantaine**.
   Het bestand wordt in quarantaine geplaatst. Deze actie kan ook worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Responsacties definiëren voor een verdachte registervermelding

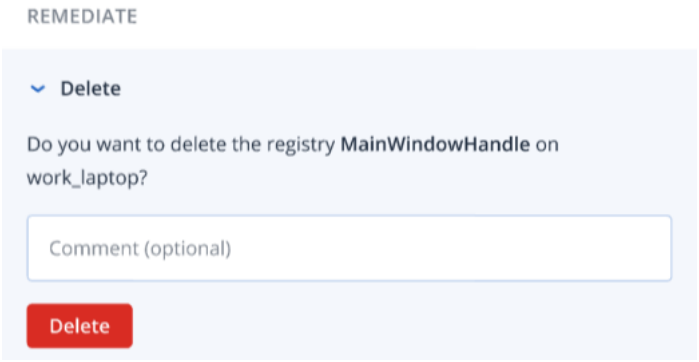
Als onderdeel van uw reactie op een aanval kunt u de volgende verdachte registervermeldingen verwijderen.

Deze optie is beschikbaar voor registerknooppunten in de cyber kill chain.

Een verdachte registervermelding verwijderen:

1. Klik in de cyber kill chain op het knooppunt dat u wilt herstellen.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.

3. Klik in het gedeelte **Herstellen** op **Verwijderen**.



4. [Optioneel] Voeg een opmerking toe. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
5. Klik op **Verwijderen**.
   De registervermelding wordt verwijderd. Deze actie kan ook worden bekeken op het tabblad **Activiteiten** van zowel het afzonderlijke knooppunt als het hele incident. Zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982) voor meer informatie.

Een proces, bestand of netwerk toevoegen of verwijderen in de blokkeringslijst of acceptatielijst van het beschermingsschema

Als onderdeel van uw preventieve reactie op een aanval kunt u een knooppunt toevoegen aan de acceptatielijst of blokkeringslijst van uw beschermingsschema.

U kunt een knooppunt aan een acceptatielijst toevoegen als u het knooppunt als veilig beschouwt en toekomstige detecties ervan wilt voorkomen. Voeg een knooppunt toe aan een blokkeringslijst als u wilt voorkomen dat het knooppunt in de toekomst actief wordt.

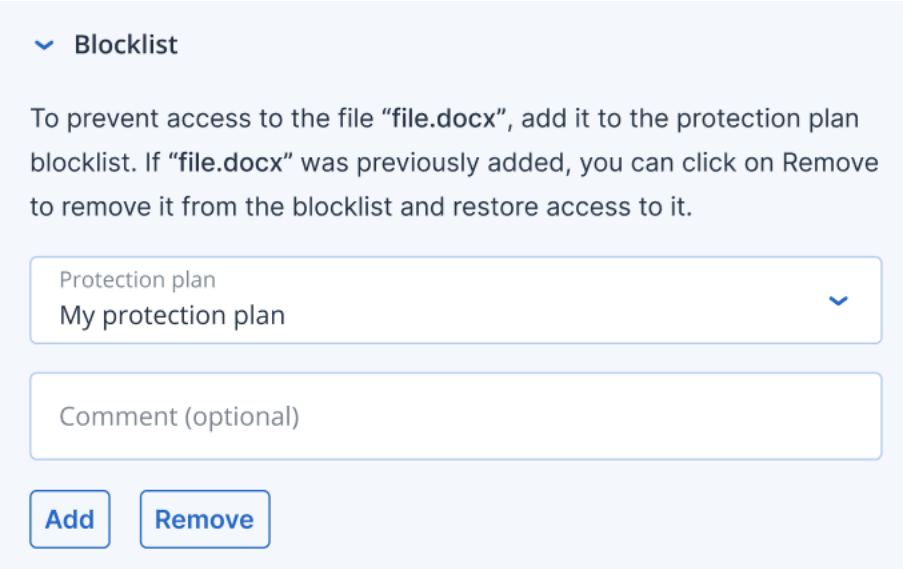
U kunt een knooppunt ook verwijderen uit de acceptatielijst of blokkeringslijst om toekomstige toegang tot het knooppunt toe te staan of te voorkomen.

Deze optie is beschikbaar voor de volgende knooppunten in de cyber kill chain:

- Proces
- Bestand
- Netwerk

Een proces, bestand of netwerk toevoegen of verwijderen in de blokkeringslijst van het beschermingsschema

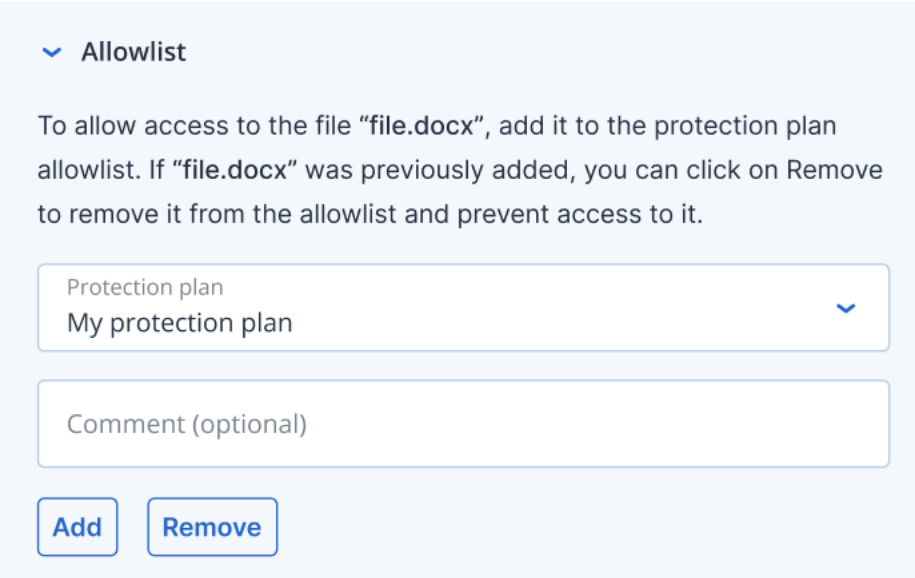
1. Klik in de cyber kill chain op het proces, het bestand of het netwerkknooppunt dat u wilt herstellen.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.
3. Klik in het gedeelte **Voorkomen** op het pijlpictogram naast **Blokkeringslijst**.



4. Selecteer de relevante beschermingsschema's waarop u deze actie wilt toepassen.
5. [Optioneel] Voeg een opmerking toe. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
6. Klik op **Toevoegen**.
   De actie is geïmplementeerd zodat het proces, bestand of netwerk in de toekomst niet meer wordt gestart.
   Als u een proces, bestand of netwerk dat eerder aan de blokkeringslijst is toegevoegd, toch nog wilt verwijderen uit de blokkeringslijst, klikt u op **Verwijderen** om toekomstige toegang tot het knooppunt mogelijk te maken.
   U kunt de acties van toevoegen of verwijderen ook bekijken in de tabbladen **Activiteiten** voor zowel het afzonderlijke knooppunt als het hele incident. Voor meer informatie: zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982).

Een proces, bestand of netwerk toevoegen of verwijderen in de acceptatielijst van het beschermingsschema

1. Klik in de cyber kill chain op het proces, het bestand of het netwerkknooppunt dat u wilt herstellen.
2. Klik in de weergegeven zijbalk op het tabblad **Responsacties**.
3. Klik in de sectie **Voorkomen** op het pijlpictogram naast **Acceptatielijst**.



4. Selecteer de relevante beschermingsschema's waarop u deze actie wilt toepassen.
5. [Optioneel] Voeg een opmerking toe. Deze opmerking is zichtbaar op het tabblad **Activiteiten** (voor een enkel knooppunt of voor het hele incident) en kan u (of uw collega's) eraan herinneren waarom u de actie hebt ondernomen wanneer u het incident opnieuw bekijkt.
6. Klik op **Toevoegen**.
   De actie is geïmplementeerd zodat het proces, bestand of netwerk in de toekomst niet meer wordt gedetecteerd.
   Als u een proces, bestand of netwerk dat eerder aan de acceptatielijst is toegevoegd, toch nog wilt verwijderen uit de acceptatielijst, klikt u op **Verwijderen** om toekomstige toegang tot het knooppunt te voorkomen.
   U kunt de acties van toevoegen of verwijderen ook bekijken in de tabbladen **Activiteiten** voor zowel het afzonderlijke knooppunt als het hele incident. Voor meer informatie: zie "Inzicht in de ondernomen acties om een incident te verhelpen" (p. 982).

Controlemodus inschakelen voor Eindpuntdetectie en -respons (EDR)

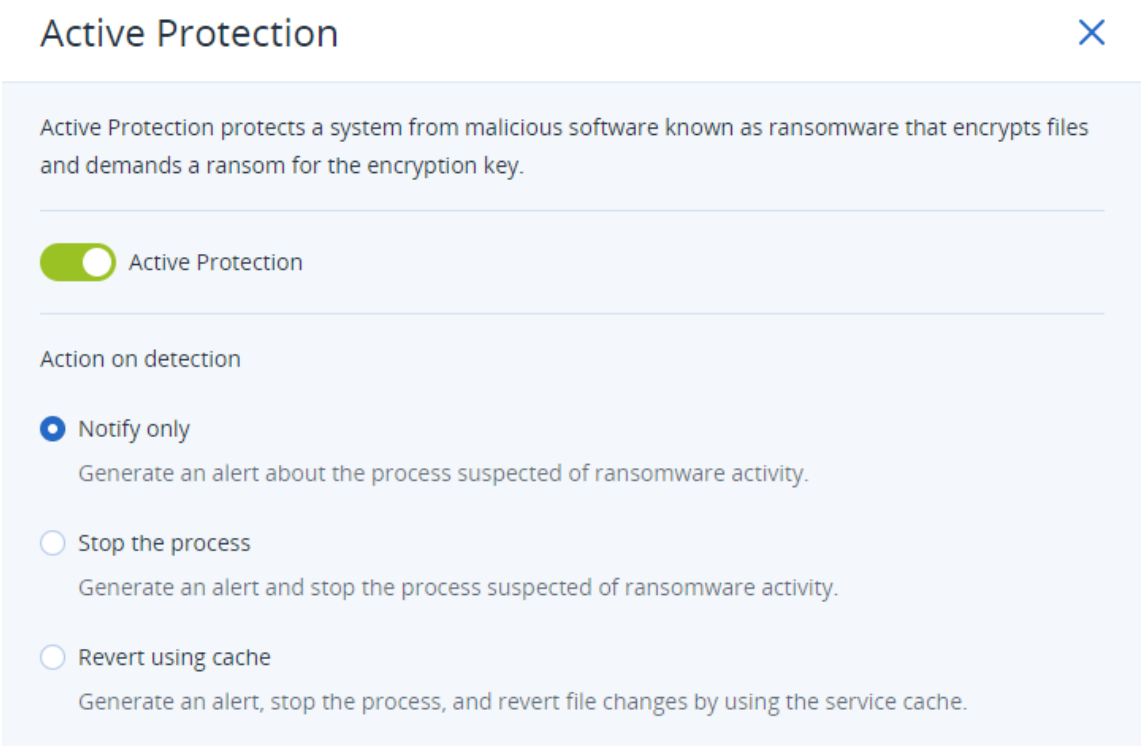
Via de controlemodus in Cyber Protection kunt u EDR gebruiken in een productieomgeving. Op die manier kunt u controleren op eventuele fout-positieven en noodzakelijke uitsluitingen maken voordat u EDR volledig implementeert.

In de controlemodus wordt er niets geblokkeerd of gestopt. Er worden incidenten gegenereerd, maar geen respons geïnitieerd.

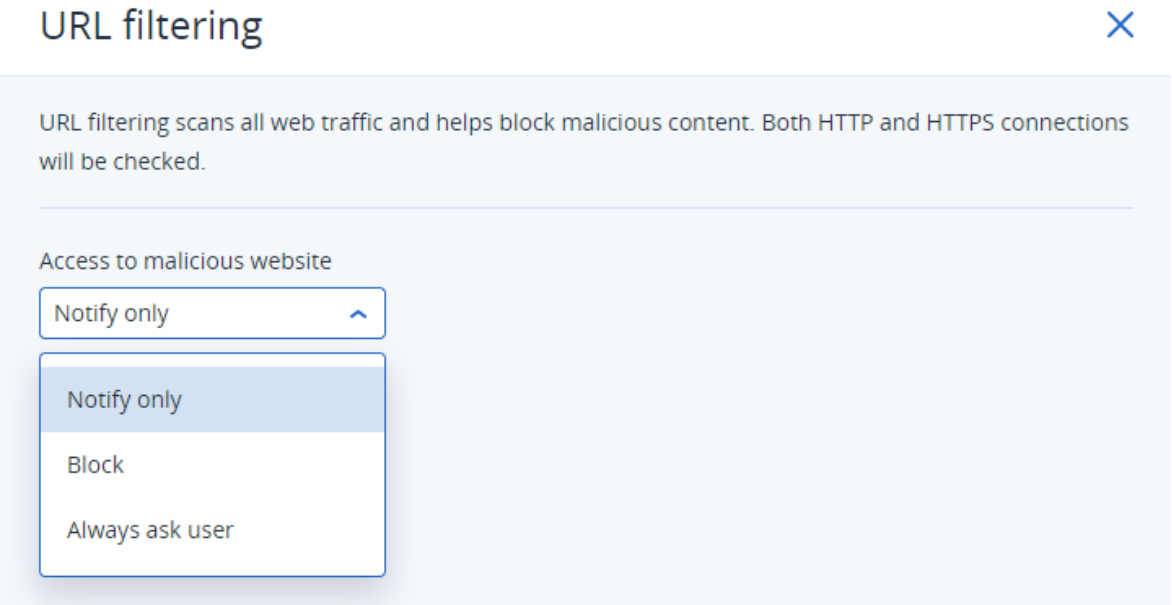
De controlemodus voor EDR inschakelen

1. Controleer of EDR is ingeschakeld in het betreffende beschermingsplan. Voor meer informatie: zie "Functionaliteit van Eindpuntdetectie en -respons (EDR) inschakelen" (p. 949).

2. Vouw de module **Antivirus- en antimalwarebeveiliging** uit en definieer het volgende:
   - Klik op **Actieve Protection**, ga naar de sectie **Actie bij detectie**, selecteer **Alleen melden** en klik op **Gereed**. Voor meer informatie: zie "Active Protection" (p. 869).



   - Klik op **Gedragenegine**, ga naar de sectie **Actie bij detectie**, selecteer **Alleen melden** en klik op **Gereed**. Voor meer informatie: zie "Gedragengine" (p. 874).
   - Klik op **Preventie tegen aanvallen**, ga naar de sectie **Actie bij detectie**, selecteer **Alleen melden** en klik op **Gereed**. Voor meer informatie: zie "Preventie tegen aanvallen" (p. 875).
   - Klik op **Realtime bescherming**, ga naar de sectie **Actie bij detectie**, selecteer **Alleen melden** en klik op **Gereed**. Voor meer informatie: zie "Realtime bescherming" (p. 877).
   - Klik op **Scan plannen**, ga naar de sectie **Actie bij detectie**, selecteer **Alleen melden** en klik op **Gereed**. Voor meer informatie: zie "Scan plannen" (p. 878).
3. Vouw de **URL-filtering**-module uit, open de vervolgkeuzelijst **Toegang tot schadelijke website**, selecteer **Alleen melden** en klik op **Gereed**. Voor meer informatie: zie "URL-filtering" (p. 893).



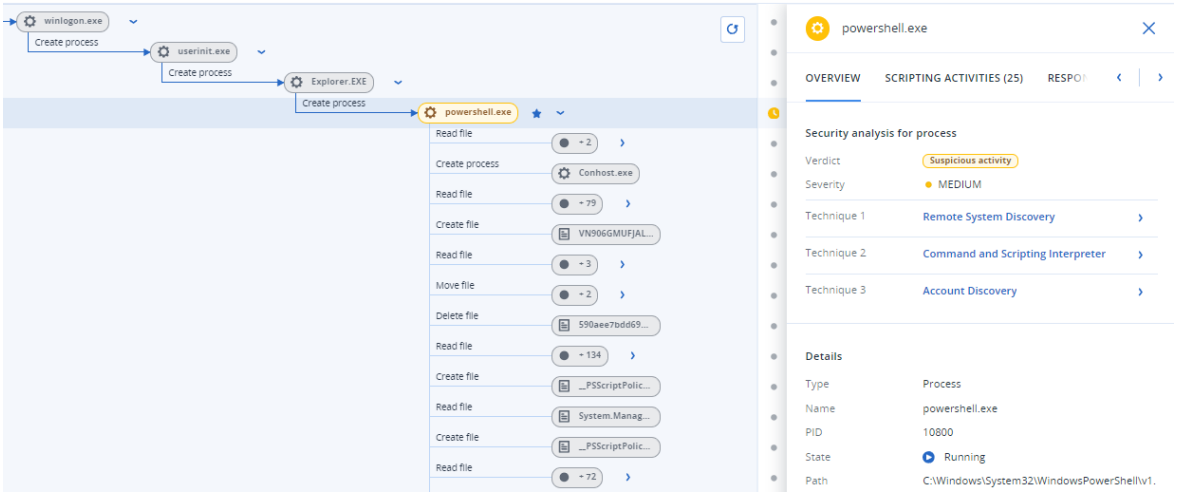
Testen of Endpoint Detection and Response (EDR) correct werkt

Als u wilt controleren of EDR is geïmplementeerd en werkt, kunt u een aantal opdrachten uitvoeren om EDR-detecties te activeren.

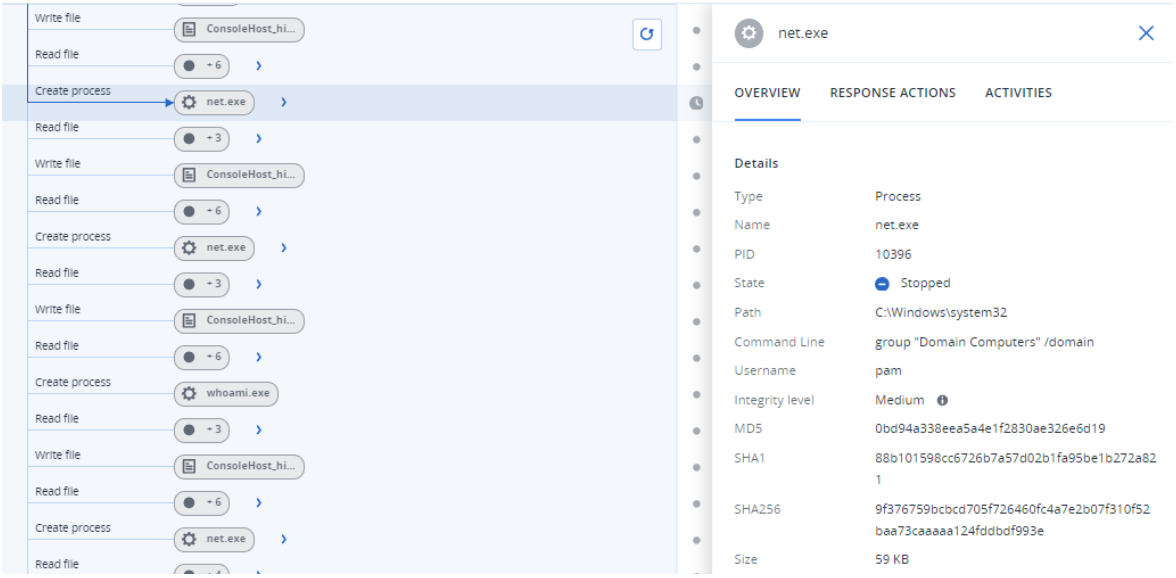
Opmerking
Wanneer EDR is geïmplementeerd, worden incidenten onmiddellijk weergegeven als er verdachte activiteiten plaatsvinden. Met onderstaande stappen kunt u controleren of EDR werkt als er gedurende enkele dagen geen nieuwe incidenten zijn gemeld.

Testen of EDR is geïmplementeerd en correct werkt:

1. Meld u aan bij het relevante Active Directory-gebruikersaccount dat is toegevoegd aan het domein.
2. Voer de volgende twee opdrachten uit in Windows PowerShell:
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. Ga in de Cyber Protect-console naar **Bescherming > Incidenten** om het gegenereerde incident te bekijken.
   U kunt ook op het gegenereerde incident met type ernstgraad **Matig** klikken om het weer te geven in de EDR-cyber kill chain en om de PowerShell-opdrachten te bevestigen die u in de vorige stap hebt uitgevoerd (zie onderstaand voorbeeld).



4. Voer de volgende opdrachten uit in Windows PowerShell:
   - `c:\>whoami`
   - `c:\>net localgroup`
   - `c:\>net localgroup administrators`
   - `c:\>powershell -command start-process cmd -verb runas`
   - `c:\WINDOWS\system32>net user administrator /active:yes`
   - `c:\>powershell -command Get-Hotfix`
5. Ga naar de EDR-cyber kill chain en klik op de uitvoerbare knooppunten (bijvoorbeeld **net.exe** of **whoami.exe**) om de exacte PowerShell-opdrachten weer te geven die op de opdrachtregel worden uitgevoerd. Deze opdrachten worden weergegeven in het gedeelte **Details** van het tabblad **Overzicht** in het onderstaande voorbeeld.



6. Nadat u hebt bevestigd dat er een EDR-incident is gegenereerd, stelt u de **Bedreigingsstatus** voor het incident handmatig in op **Verholpen** en de **Onderzoeksstatus** op **Gesloten**. Zie "Incidenten in de cyber kill chain onderzoeken" (p. 973) voor meer informatie. U kunt ook een opmerking bij het incident invoeren om aan te geven dat het een testincident betreft.

Beveiligingsproblemen evalueren en patches beheren

Evaluatie van beveiligingsproblemen is een proces voor het identificeren, kwantificeren en prioriteren van gevonden beveiligingsproblemen in het systeem. In de module Evaluatie van beveiligingsproblemen kunt u uw machines scannen op beveiligingsproblemen en controleren of de besturingssystemen en geïnstalleerde toepassingen up-to-date zijn en correct werken.

Evaluatie van beveiligingsproblemen wordt ondersteund voor machines met de volgende besturingssystemen:

- Windows. Zie "Ondersteunde producten van Microsoft en derden" (p. 1020) voor meer informatie.
- macOS. Zie "Ondersteunde producten van Apple en derden" (p. 1021) voor meer informatie.
- Linux-machines (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Zie "Ondersteunde Linux-producten" (p. 1022) voor meer informatie.

Gebruik de functionaliteit **Patchbeheer** om patches (updates) te beheren voor toepassingen en besturingssystemen die op uw machines zijn geïnstalleerd en om uw systemen up-to-date houden. In de module voor patchbeheer kunt u de update-installaties op uw machines automatisch of handmatig goedkeuren.

Patchbeheer wordt ondersteund voor machines met Windows-besturingssystemen. Zie "Ondersteunde producten van Microsoft en derden" (p. 1020) voor meer informatie.

Evaluatie van beveiligingsproblemen

Het proces van de evaluatie van beveiligingsproblemen bestaat doorgaans uit de volgende stappen:

1. U gaat als volgt te werk: maak een beschermingsschema terwijl de module Evaluatie van beveiligingsproblemen is ingeschakeld, geef de Instellingen voor evaluatie van beveiligingsproblemen op en wijs het schema toe aan machines.
2. Het systeem verzendt, volgens schema of op aanvraag, een opdracht om de scan voor evaluatie van beveiligingsproblemen uit te voeren naar de beveiligingsagenten die op machines zijn geïnstalleerd.
3. De agenten krijgen de opdracht, beginnen de machines te scannen op beveiligingsproblemen en genereren de scanactiviteit.
4. Nadat de scan voor evaluatie van beveiligingsproblemen is voltooid, genereren de agenten de resultaten en sturen deze naar de controleservice.
5. De controleservice verwerkt de gegevens van de agenten en toont de resultaten in de widgets voor evaluatie van beveiligingsproblemen en een lijst met gevonden beveiligingsproblemen.
6. Wanneer u een lijst met gevonden beveiligingsproblemen krijgt, kunt u deze verwerken en besluiten welke van de gevonden beveiligingsproblemen moet worden opgelost.

U kunt de resultaten van de evaluatie van beveiligingsproblemen controleren in **Controle** > **Overzicht** > widgets **Beveiligingsproblemen/Bestaande beveiligingsproblemen**.

Ondersteunde producten van Microsoft en derden

De volgende Microsoft-producten en producten van derden voor Windows-besturingssystemen worden ondersteund voor evaluatie van beveiligingsproblemen en patchbeheer:

Ondersteunde Microsoft-producten

Windows OS

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server OS

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office en gerelateerde onderdelen

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Windows OS-gerelateerde onderdelen

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studio en toepassingen
- Onderdelen van het besturingssysteem

Servertoepassingen

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019

Ondersteunde producten van derden voor Windows OS

Wereldwijd wordt er steeds vaker op afstand gewerkt en daarom zijn samenwerkings- en communicatieprogramma's en VPN-clients nu onmisbaar om altijd up-to-date te zijn en op de hoogte te blijven van mogelijke beveiligingsproblemen. De Cyber Protection-service biedt ondersteuning voor de evaluatie van beveiligingsproblemen en het patchbeheer voor dergelijke toepassingen.

Samenwerkings- en communicatieprogramma's, VPN-clients

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

Zie Lijst met producten van derden die worden ondersteund door patchbeheer (62853) voor meer informatie over de ondersteunde producten van derden voor Windows OS.

Ondersteunde producten van Apple en derden

De volgende Apple-producten en producten van derden voor macOS worden ondersteund voor evaluatie van beveiligingsproblemen:

Ondersteunde Apple-producten

macOS

- macOS 10.13.x en later

Ingebouwde macOS-toepassingen

- Safari, iTunes, enzovoort.

Ondersteunde producten van derden voor macOS

- Microsoft Office (Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC media player

Ondersteunde Linux-producten

De volgende Linux-distributies en -versies worden ondersteund voor evaluatie van beveiligingsproblemen:

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

Instellingen voor evaluatie van beveiligingsproblemen

Raadpleeg 'Een beschermingsschema maken' voor meer informatie over het maken van een beschermingsschema met de module Evaluatie van beveiligingsproblemen. Een scan voor evaluatie van beveiligingsproblemen kan volgens schema of op aanvraag worden uitgevoerd (met de actie **Nu uitvoeren** in een beschermingsschema).

U kunt de volgende instellingen opgeven in de module Evaluatie van beveiligingsproblemen.

Wat wilt u scannen?

Definieer welke softwareproducten u wilt scannen op beveiligingsproblemen:

- Windows-machines:
  - **Microsoft-producten**
  - **Windows-producten van derden** (zie Lijst met producten van derden die worden ondersteund door patchbeheer (62853)) voor meer informatie over de ondersteunde producten van derden voor Windows OS
- macOS-machines:
  - **Apple-producten**
  - **Producten van derden voor macOS**
- Linux-machines:
  - **Linux-pakketten scannen**

Planning

Definieer het schema op basis waarvan de scan voor evaluatie van beveiligingsproblemen wordt uitgevoerd op de geselecteerde machines:

Veld	Beschrijving
De taakuitvoering plannen met de volgende gebeurtenissen	Met deze instelling definieert u wanneer de taak wordt uitgevoerd. De volgende waarden zijn beschikbaar: • **Schema op tijd**: dit is de standaardinstelling. De taak wordt uitgevoerd volgens de opgegeven tijd. • **Wanneer de gebruiker zich aanmeldt bij het systeem**: standaard wordt de taak geactiveerd wanneer een gebruiker zich aanmeldt. U kunt deze instelling ook wijzigen, zodat alleen een specifiek gebruikersaccount de taak kan activeren. • **Wanneer de gebruiker zich afmeldt bij het systeem**: standaard wordt de taak geactiveerd wanneer een gebruiker zich afmeldt. U kunt deze instelling ook wijzigen, zodat alleen een specifiek gebruikersaccount de taak kan activeren. **Opmerking** De taak wordt niet uitgevoerd bij het afsluiten van het systeem. Afsluiten en afmelden zijn verschillende gebeurtenissen in de planningsconfiguratie. • **Wanneer het systeem wordt opgestart**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt gestart. • **Wanneer het systeem wordt afgesloten**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt afgesloten.
Type schema	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd.

Veld	Beschrijving
	De volgende waarden zijn beschikbaar: • **Maandelijks**: selecteer de maanden en de weken of dagen van de maand wanneer de taak zal worden uitgevoerd. • **Dagelijks**: dit is de standaardinstelling. Selecteer de dagen van de week waarop de taak wordt uitgevoerd. • **Elk uur**: selecteer de dagen van de week, het aantal herhalingen en het tijdinterval waarin de taak wordt uitgevoerd.
Starten om	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd. Selecteer het exacte tijdstip waarop de taak wordt uitgevoerd.
Uitvoeren binnen een datumbereik	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd. Stel een bereik in waarin het geconfigureerde schema van kracht is.
Geef een gebruikersaccount op waarvoor een taak wordt geïnitieerd zodra het account wordt aangemeld bij het besturingssysteem	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Wanneer de gebruiker zich aanmeldt bij het systeem** hebt geselecteerd. De volgende waarden zijn beschikbaar: • **Elke gebruiker**: gebruik deze optie als u wilt dat de taak wordt geactiveerd wanneer een willekeurige gebruiker zich aanmeldt. • **De volgende gebruiker**: gebruik deze optie als u wilt dat de taak alleen wordt geactiveerd wanneer een specifiek gebruikersaccount zich aanmeldt.
Geef een gebruikersaccount op waarvoor een taak wordt geïnitieerd zodra het account wordt afgemeld bij het besturingssysteem	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Wanneer de gebruiker zich afmeldt bij het systeem** hebt geselecteerd. De volgende waarden zijn beschikbaar: • **Elke gebruiker**: gebruik deze optie als u wilt dat de taak wordt geactiveerd wanneer een willekeurige gebruiker zich afmeldt. • **De volgende gebruiker**: gebruik deze optie als u wilt dat de taak alleen wordt geactiveerd wanneer een specifiek gebruikersaccount zich afmeldt.
Startvoorwaarden	Hiermee definieert u alle voorwaarden waaraan tegelijkertijd moet worden voldaan om de taak uit te voeren. De startvoorwaarden voor antimalwarescans zijn vergelijkbaar met de startvoorwaarden voor de **module Back-up** die worden

Veld	Beschrijving
	beschreven in 'Startvoorwaarden'. U kunt de volgende aanvullende startvoorwaarden definiëren: • **Starttijd van taak binnen een tijdvenster distribueren**: met deze optie kunt u het tijdsbestek instellen voor de taak om knelpunten in het netwerk te voorkomen. U kunt de vertraging opgeven in uren of minuten. Als de standaardstarttijd bijvoorbeeld 10:00 uur en de vertraging 60 minuten is, dan zal de taak beginnen tussen 10:00 uur en 11:00 uur. • **Als de machine is uitgeschakeld, gemiste taken uitvoeren wanneer de machine wordt opgestart** • **De slaap- of sluimerstand voorkomen tijdens het uitvoeren van taken**: deze optie is alleen van toepassing op machines met Windows. • **Voer de taak na de start uit, zelfs als niet aan de startvoorwaarden wordt voldaan**: geef aan na hoeveel tijd de taak wordt uitgevoerd, ongeacht de andere startvoorwaarden. **Opmerking** Startvoorwaarden worden niet ondersteund voor Linux.

Evaluatie van beveiligingsproblemen voor Windows-machines

U kunt Windows-machines en producten van derden voor Windows scannen op beveiligingsproblemen.

Evaluatie van beveiligingsproblemen configureren voor Windows-machines

1. Kies in de Cyber Protect-console de optie Een beschermingsschema maken en schakel de module **Evaluatie van beveiligingsproblemen** in.
2. Geef de instellingen voor evaluatie van beveiligingsproblemen op:
   - **Wat wilt u scannen**: selecteer **Microsoft-producten**, **producten van derden voor Windows** of beide.
   - **Planning**: definieer de planning voor de evaluatie van beveiligingsproblemen.

   Voor meer informatie over de opties voor **Planning** raadpleegt u "Instellingen voor evaluatie van beveiligingsproblemen" (p. 1022).
3. Wijs het schema toe aan de Windows-machines.

Na een scan voor evaluatie van beveiligingsproblemen kunt u een lijst met gevonden beveiligingsproblemen zien. U kunt de informatie verwerken en besluiten welke van de gevonden beveiligingsproblemen moeten worden opgelost.

Ga naar **Controle** > **Overzicht** > widgets **Beveiligingsproblemen/Bestaande beveiligingsproblemen** als u de resultaten van de evaluatie van beveiligingsproblemen wilt controleren.

Evaluatie van beveiligingsproblemen voor Linux-machines

U kunt Linux-machines scannen op beveiligingsproblemen op toepassingsniveau en op kernelniveau.

Evaluatie van beveiligingsproblemen configureren voor Linux-machines

1. Kies in de Cyber Protect-console de optie Een beschermingsschema maken en schakel de module **Evaluatie van beveiligingsproblemen** in.
2. Geef de instellingen voor evaluatie van beveiligingsproblemen op:
   - **Wat wilt u scannen**: selecteer **Linux-pakketten scannen**.
   - **Planning**: definieer de planning voor de evaluatie van beveiligingsproblemen.

   Voor meer informatie over de opties voor **Planning** raadpleegt u "Instellingen voor evaluatie van beveiligingsproblemen" (p. 1022).
3. Wijs het schema toe aan de Linux-machines.

Na een scan voor evaluatie van beveiligingsproblemen kunt u een lijst met gevonden beveiligingsproblemen zien. U kunt de informatie verwerken en besluiten welke van de gevonden beveiligingsproblemen moeten worden opgelost.

Ga naar **Controle** > **Overzicht** > widgets **Beveiligingsproblemen/Bestaande beveiligingsproblemen** als u de resultaten van de evaluatie van beveiligingsproblemen wilt controleren.

Evaluatie van beveiligingsproblemen voor macOS-apparaten

U kunt macOS-apparaten scannen op beveiligingsproblemen in het besturingssysteem en in toepassingen.

Evaluatie van beveiligingsproblemen configureren voor macOS-apparaten

1. Kies in de Cyber Protect-console de optie Een beschermingsschema maken en schakel de module **Evaluatie van beveiligingsproblemen** in.
2. Geef de instellingen voor evaluatie van beveiligingsproblemen op:
   - **Wat wilt u scannen**: selecteer **Apple-producten**, **producten van derden voor macOS** of beide.
   - **Planning**: definieer de planning voor de evaluatie van beveiligingsproblemen.

   Voor meer informatie over de opties voor **Planning** raadpleegt u "Instellingen voor evaluatie van beveiligingsproblemen" (p. 1022).
3. Wijs het schema toe aan de macOS-apparaten.

Na een scan voor evaluatie van beveiligingsproblemen kunt u een lijst met gevonden beveiligingsproblemen zien. U kunt de informatie verwerken en besluiten welke van de gevonden beveiligingsproblemen moeten worden opgelost.

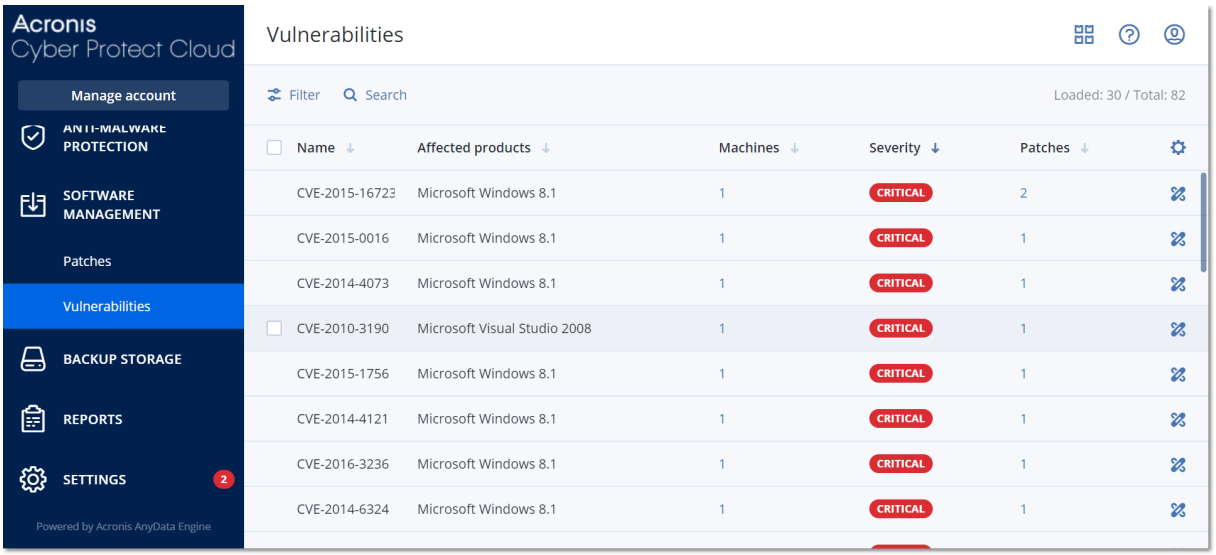
Ga naar **Controle** > **Overzicht** > widgets **Beveiligingsproblemen/Bestaande beveiligingsproblemen** als u de resultaten van de evaluatie van beveiligingsproblemen wilt controleren.

Gevonden beveiligingsproblemen beheren

Als de evaluatie van beveiligingsproblemen ten minste eenmaal is uitgevoerd en er enkele beveiligingsproblemen zijn gevonden, dan kunt u deze zien in **Softwarebeheer** > **Beveiligingsproblemen**. De lijst met beveiligingsproblemen geeft zowel beveiligingsproblemen weer waarvoor patches moeten worden geïnstalleerd als beveiligingsproblemen waarvoor geen patches worden voorgesteld. U kunt het filter gebruiken om alleen beveiligingsproblemen met patches weer te geven.

Naam	Beschrijving
Naam	De naam van het beveiligingsprobleem.
Betroffen producten	Softwareproducten waarvoor de beveiligingsproblemen zijn gevonden.
Machines	Het aantal betroffen machines.
Ernstgraad	De ernst van het gevonden beveiligingsprobleem. De volgende niveaus kunnen worden toegewezen volgens het Common Vulnerability Scoring System (CVSS): • **Kritiek**: 9 – 10 CVSS • **Hoog**: 7 – 9 CVSS • **Medium**: 3 – 7 CVSS • **Laag**: 0 – 3 CVSS • **Geen**
Patches	Het aantal geschikte patches.
Gepubliceerd	De datum en tijd waarop het beveiligingsprobleem is gepubliceerd in Common Vulnerabilities and Exposures (CVE).
Gedetecteerd	De eerste datum waarop een bestaand beveiligingsprobleem is gedetecteerd op machines.

U kunt de beschrijving van het gevonden beveiligingsprobleem vinden door op de naam in de lijst te klikken.



Het herstelproces voor het beveiligingsprobleem starten

1. Ga in de Cyber Protect-console naar **Softwarebeheer** > **Beveiligingsproblemen**.
2. Selecteer het beveiligingsprobleem in de lijst en klik vervolgens op **Patches installeren**. De wizard voor het herstellen van beveiligingsproblemen wordt geopend.
3. Selecteer de patches die op de geselecteerde machines moeten worden geïnstalleerd en klik vervolgens op **Volgende**.
4. Selecteer de machines waarop u de patches wilt installeren.
5. Selecteer de opties voor opnieuw opstarten.
   a. Selecteer of u wilt dat de machine opnieuw wordt opgestart nadat de patches zijn geïnstalleerd.

Optie	Beschrijving
Nee	De machines worden niet automatisch opnieuw opgestart nadat de patches zijn geïnstalleerd.
Indien nodig	De machines worden alleen opnieuw opgestart als dit nodig is voor het toepassen van de patches.
Ja	De machines worden automatisch opnieuw opgestart nadat de patches zijn geïnstalleerd. U kunt ook een vertraging opgeven voor het opnieuw opstarten.

   b. [Optioneel] Als u het opnieuw opstarten van de machine wilt uitstellen wanneer er een back-up van de machine wordt gemaakt, selecteert u **Niet opnieuw opstarten totdat de back-up is voltooid**.
6. Klik op **Patches installeren**.

Hierdoor worden de geselecteerde patches op de geselecteerde machines geïnstalleerd.

Patchbeheer

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Zie Lijst met producten van derden die worden ondersteund door patchbeheer (62853) voor meer informatie over de ondersteunde producten van derden voor Windows OS.

Gebruik de functie voor patchbeheer voor het volgende:

- updates installeren op OS- en toepassingsniveau
- patches handmatig of automatisch goedkeuren
- patches op aanvraag of volgens schema installeren
- precies definiëren welke patches moeten worden geïnstalleerd op basis van verschillende criteria: ernst, categorie en goedkeuringsstatus
- een back-up maken voordat een update wordt uitgevoerd, om te voorkomen dat updates mislukken
- de actie voor opnieuw opstarten na installatie van de patch definiëren

Opmerking
Als u met Windows-updates wilt werken en de functie voor patchbeheer wilt gebruiken, moeten Windows-updates zijn ingeschakeld voor de workload.

Cyber Protection maakt gebruikt van peer-to-peer-technologie om het verkeer voor de netwerkbandbreedte te minimaliseren. U kunt een of meer speciale agenten kiezen die updates van internet downloaden en deze distribueren onder andere agenten in het netwerk. Alle agenten delen ook updates met elkaar als peer-to-peer-agenten.

De workflow voor patchbeheer

De workflow voor patchbeheer omvat de volgende stappen: een beschermingsschema configureren en toepassen, een scan voor evaluatie van beveiligingsproblemen uitvoeren, patchinstellingen configureren, patches goedkeuren en ten slotte de goedgekeurde patches installeren. De exacte stappen van de workflow zijn als volgt.

1. Configureer een beschermingsschema waarvoor zowel de module **Evaluatie van beveiligingsproblemen** als de module **Patchbeheer** is ingeschakeld.
2. Configureer de instellingen voor evaluatie van beveiligingsproblemen. Zie "Instellingen voor evaluatie van beveiligingsproblemen" (p. 1022) voor meer informatie over deze instellingen.
3. Configureer de instellingen voor patchbeheer. Zie "Instellingen voor patchbeheer in het beschermingsschema" (p. 1030) voor meer informatie over deze instellingen
4. Pas het beschermingsschema toe op een of meerdere machines.

5. Wacht tot een scan van de evaluatie van beveiligingsprobleem is voltooid. De scan start automatisch volgens het schema dat is geconfigureerd in het beschermingsschema. U kunt de scan ook handmatig op aanvraag starten door te klikken op het pictogram **Nu uitvoeren** in de module **Evaluatie van beveiligingsproblemen** in het beschermingsschema.
6. Keur de patches goed. U kunt instellingen definiëren voor automatische patchgoedkeuring, waaronder een automatische installatie van de patches op testmachines. Zie "Automatische patchgoedkeuring" (p. 1038) voor meer informatie. U kunt patches ook handmatig goedkeuren door de goedkeuringsstatus in te stellen op **Goedgekeurd**. Zie "Patches handmatig goedkeuren" (p. 1043) voor meer informatie.
7. Installeer de patches. De goedgekeurde patches kunnen automatisch worden geïnstalleerd, volgens het schema dat is geconfigureerd in het beschermingsschema. U kunt de patches ook handmatig op aanvraag installeren. Zie "Patches op aanvraag installeren" (p. 1043) voor meer informatie.

U kunt de resultaten van de patchinstallatie controleren in de widget **Controle** > **Overzicht** > **Patchinstallatiegeschiedenis**.

Instellingen voor patchbeheer in het beschermingsschema

In de module **Patchbeheer** van het beschermingsschema kunt u de volgende instellingen voor patchbeheer configureren:

- Welke updates u wilt installeren voor Microsoft en voor producten van derden voor Windows OS.
- Wanneer u de automatische installatie van patches wilt uitvoeren.
- Of u een back-up wilt maken voordat een update wordt uitgevoerd.

Voor meer informatie over het maken van een beschermingsschema en het inschakelen van de module **Patchbeheer** raadpleegt u "Een beschermingsschema maken" (p. 217).

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

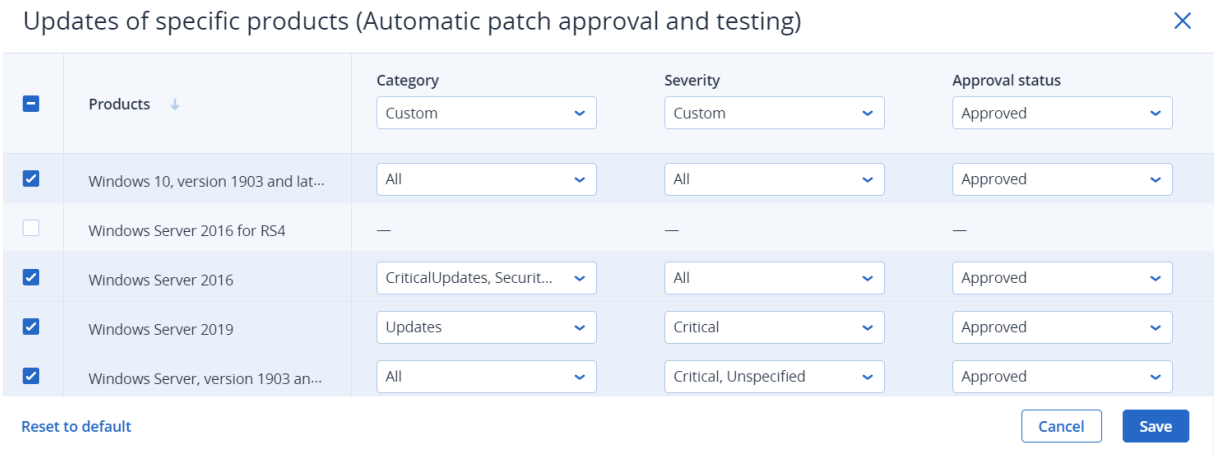
Microsoft-producten

Als u de Microsoft-updates wilt installeren op de geselecteerde machines, schakelt u de optie **Microsoft-producten bijwerken** in.

Selecteer de installatieoptie:

Optie	Beschrijving
Alle updates	Hiermee worden alle goedgekeurde updates geïnstalleerd.
Alleen beveiligings- en kritieke updates	Hiermee worden alle goedgekeurde beveiligings- en kritieke updates geïnstalleerd.

Optie	Beschrijving
Updates van specifieke producten (Automatische patchgoedkeuring en testen)	Hiermee worden aangepaste instellingen voor verschillende producten gedefinieerd. Als u specifieke producten wilt bijwerken, kunt u voor elk product definiëren welke updates moeten worden geïnstalleerd per categorie, ernst of goedkeuringsstatus. Als u automatische goedkeuring van testen en het testen van de patches wilt configureren, selecteert u deze optie.



Voor Microsoft-producten maakt de distributie van patches gebruik van de Windows API-service. Patches en updates worden niet intern of op distributieagents gedownload of opgeslagen. In plaats daarvan worden ze gedownload van Microsoft CDN. Zelfs als de Updater-rol is toegewezen, kan de agent dus geen patches downloaden en distribueren.

Windows-producten van derden

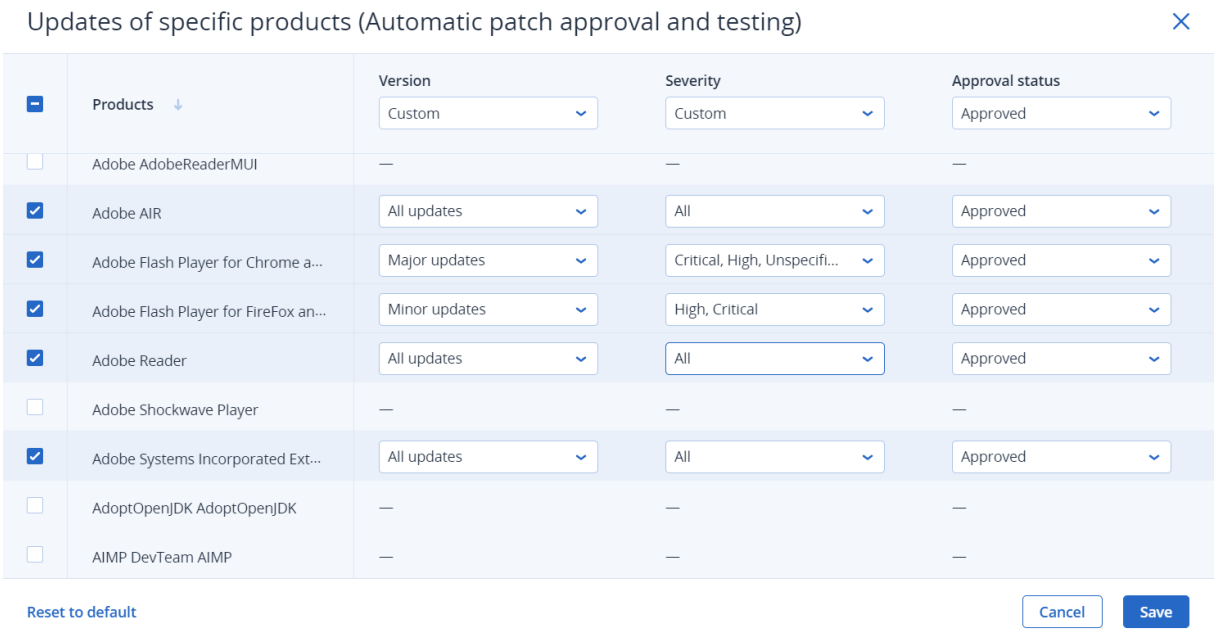
Als u updates van derden voor Windows OS wilt installeren op de geselecteerde machines, schakelt u de optie **Windows-producten van derden** in.

Selecteer de installatieopties:

Optie	Beschrijving
Alle updates	Hiermee worden alle goedgekeurde updates geïnstalleerd. *
Alleen belangrijke update	Hiermee worden alle goedgekeurde belangrijke updates geïnstalleerd.
Alleen kleine updates	Hiermee worden goedgekeurde kleine updates geïnstalleerd.
Updates van specifieke producten (Automatische	Hiermee worden aangepaste instellingen voor verschillende producten gedefinieerd.

Optie	Beschrijving
patchgoedkeuring en testen)	Als u specifieke producten wilt bijwerken, kunt u voor elk product definiëren welke updates moeten worden geïnstalleerd per categorie, ernst of goedkeuringsstatus. Als u automatische goedkeuring van testen en het testen van de patches wilt configureren, selecteert u deze optie.
Alleen de nieuwste versies installeren voor toepassingen met gedetecteerde beveiligingsproblemen	Schakel dit selectievakje in als u de nieuwste updates alleen wilt installeren voor toepassingen met gedetecteerde beveiligingsproblemen. *

* Voor deze optie is Cyber Protect-agent versie 23.11.36772 of later vereist.



Voor Windows-producten van derden worden patches rechtstreeks vanuit een interne Acronis-database naar de beheerde workloads gedistribueerd. Als de Updater-rol is toegewezen aan een agent, wordt deze agent gebruikt om patches te downloaden en te distribueren.

Planning

Definieer het schema en de voorwaarden op basis waarvan de updates worden geïnstalleerd op de geselecteerde machines.

Veld	Beschrijving
De taakuitvoering plannen met de volgende	Met deze instelling wordt gedefinieerd wanneer de taak wordt uitgevoerd. De volgende waarden zijn beschikbaar:

Veld	Beschrijving
gebeurtenissen	• **Schema op tijd**: dit is de standaardinstelling. De taak wordt uitgevoerd volgens de opgegeven tijd. • **Wanneer de gebruiker zich aanmeldt bij het systeem**: standaard wordt de taak gestart wanneer een gebruiker zich aanmeldt. U kunt deze instelling ook wijzigen, zodat alleen een specifiek gebruikersaccount de taak kan activeren. • **Wanneer de gebruiker zich afmeldt bij het systeem**: standaard wordt de taak gestart wanneer een gebruiker zich afmeldt. U kunt deze instelling ook wijzigen, zodat alleen een specifiek gebruikersaccount de taak kan activeren. **Opmerking** De taak wordt niet uitgevoerd bij het afsluiten van het systeem. Afsluiten en afmelden zijn verschillende gebeurtenissen in de planningsconfiguratie. • **Wanneer het systeem wordt opgestart**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt gestart. • **Wanneer het systeem wordt afgesloten**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt afgesloten.
Type schema	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd. De volgende waarden zijn beschikbaar: • **Maandelijks**: selecteer de maanden en de weken of dagen van de maand wanneer de taak zal worden uitgevoerd. • **Dagelijks**: dit is de standaardinstelling. Selecteer de dagen van de week waarop de taak wordt uitgevoerd. • **Elk uur**: selecteer de dagen van de week, het aantal herhalingen en het tijdinterval waarin de taak wordt uitgevoerd.
Starten om	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd Selecteer het exacte tijdstip waarop de taak wordt uitgevoerd.
Het tijdvenster voor onderhoud van patches configureren	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd. Selecteer deze instelling als u wilt dat de patchinstallatie alleen wordt uitgevoerd tijdens het tijdinterval dat u opgeeft. Als installatie van de patch niet is voltooid op de eindtijd die is gedefinieerd in het tijdvenster voor onderhoud voor patches,

Veld	Beschrijving
	wordt de installatie automatisch gestopt.
Uitvoeren binnen een datumbereik	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Schema op tijd** hebt geselecteerd. Stel een bereik in waarin het geconfigureerde schema van kracht is.
Geef een gebruikersaccount op waarvoor een taak wordt geïnitieerd zodra het account wordt aangemeld bij het besturingssysteem	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Wanneer de gebruiker zich aanmeldt bij het systeem** hebt geselecteerd. De volgende waarden zijn beschikbaar: • **Elke gebruiker**: gebruik deze optie als u wilt dat de taak wordt geactiveerd wanneer een willekeurige gebruiker zich aanmeldt. • **De volgende gebruiker**: gebruik deze optie als u wilt dat de taak alleen wordt geactiveerd wanneer een specifiek gebruikersaccount zich aanmeldt.
Geef een gebruikersaccount op waarvoor een taak wordt geïnitieerd zodra het account wordt afgemeld bij het besturingssysteem	Dit veld wordt weergegeven als u in **De taakuitvoering plannen met de volgende gebeurtenissen** de optie **Wanneer de gebruiker zich afmeldt bij het systeem** hebt geselecteerd. De volgende waarden zijn beschikbaar: • **Elke gebruiker**: gebruik deze optie als u wilt dat de taak wordt geactiveerd wanneer een willekeurige gebruiker zich afmeldt. • **De volgende gebruiker**: gebruik deze optie als u wilt dat de taak alleen wordt geactiveerd wanneer een specifiek gebruikersaccount zich afmeldt.
Startvoorwaarden	Hiermee definieert u alle voorwaarden waaraan tegelijkertijd moet worden voldaan om de taak uit te voeren. De startvoorwaarden voor antimalwarescans zijn vergelijkbaar met de startvoorwaarden voor de **module Back-up** die worden beschreven in 'Startvoorwaarden'. U kunt de volgende aanvullende startvoorwaarden definiëren: • **Starttijd van taak binnen een tijdvenster distribueren**: met deze optie kunt u het tijdsbestek instellen voor de taak om knelpunten in het netwerk te voorkomen. U kunt de vertraging opgeven in uren of minuten. Als de standaardstarttijd bijvoorbeeld 10:00 uur en de vertraging 60 minuten is, dan zal de taak beginnen tussen 10:00 uur en 11:00 uur. • **Als de machine is uitgeschakeld, gemiste taken uitvoeren wanneer de machine wordt opgestart**

Veld	Beschrijving
	• **De slaap- of sluimerstand voorkomen tijdens het uitvoeren van taken**: deze optie is alleen van toepassing op machines met Windows. • **Voer de taak na de start uit, zelfs als niet aan de startvoorwaarden wordt voldaan**: geef aan na hoeveel tijd de taak wordt uitgevoerd, ongeacht de andere startvoorwaarden. **Opmerking** Startvoorwaarden worden niet ondersteund voor Linux.
Opnieuw opstarten na update	Bepaal of de machine automatisch opnieuw moet worden opgestart nadat de installatie van de updates is voltooid. De volgende waarden zijn beschikbaar: • **Nooit**: er wordt nooit opnieuw opgestart na de updates. • **Indien nodig**: er wordt alleen opnieuw opgestart als dit is vereist voor het toepassen van de updates. • **Altijd**: er wordt altijd opnieuw opgestart na de updates. U kunt een vertraging opgeven voor het opnieuw opstarten.
Start niet opnieuw op tot de back-up is voltooid	Als u deze optie selecteert en er een back-upproces wordt uitgevoerd, wordt de machine pas opnieuw opgestart nadat de back-up is voltooid.

Back-up vóór update

Back-up uitvoeren voordat u software-updates installeert: het systeem maakt een incrementele back-up van de machine voordat hierop updates worden geïnstalleerd. Als er nog geen back-ups zijn gemaakt, wordt er een volledige back-up van de machine gemaakt. Hiermee kunt u voorkomen dat de installatie van updates mislukt en u terug moet keren naar de vorige status. De optie **Back-up vóór update** werkt alleen als op de betreffende machines zowel de module voor patchbeheer als de back-upmodule is ingeschakeld in een beschermingsschema, en de items waarvan u een back-up wilt maken, moeten ofwel een volledige machine ofwel opstart- + systeemvolumes zijn. Als u niet-geschikte items selecteert voor een back-up, kunt u de optie **Back-up vóór update** niet inschakelen.

De lijst met beschikbare patches weergeven

Wanneer een scan voor evaluatie van beveiligingsproblemen is voltooid, kunt u informatie over de beschikbare patches bekijken in **Softwarebeheer** > **Patches**.

Als u details over een specifieke patch wilt bekijken, klikt u in de lijst met patches op de betreffende patch.

De volgende tabel bevat een beschrijving van de informatie voor de patch die u kunt bekijken op het scherm.

Veld	Beschrijving
Goedkeuringsstatus	De goedkeuringsstatus is voornamelijk nodig voor scenario's met automatische goedkeuringen. U kunt een van de volgende statussen voor een patch definiëren: • **Goedgekeurd**: de patch is op ten minste één machine geïnstalleerd en gevalideerd • **Afgewezen**: de patch is niet veilig en kan een machinesysteem beschadigen • **Goedkeuring in behandeling**: de status van de patch is onduidelijk en moet worden gevalideerd
Licentieovereenkomst	• Akkoord • Niet mee eens. Als u het niet eens bent met de licentieovereenkomst, wordt de patchstatus de waarde **Afgewezen** en wordt deze niet geïnstalleerd
Ernstgraad	De ernst van de patch: • **Kritiek** • **Hoog** • **Medium** • **Laag** • **Geen**
Leverancier	De verkoper van de patch
Betroffen product	Product waarvoor de patch van toepassing is
Geïnstalleerde versies	Productversies die al zijn geïnstalleerd
Versie	Versie van de patch
Categorie	De categorie waartoe de patch behoort: • **Kritieke update**: algemeen uitgebrachte oplossingen voor specifieke, kritieke problemen die niet zijn gerelateerd aan de beveiliging. • **Beveiligingsupdate**: algemeen uitgebrachte oplossingen voor specifieke producten in verband met beveiligingsproblemen. • **Definitie-update**: updates voor virussen of andere definitiebestanden. • **Update-rollup**: cumulatieve set van hotfixes, beveiligingsupdates, kritieke updates en updates, gebundeld voor eenvoudige implementatie. Een rollup is doorgaans bedoeld voor een specifiek gebied, zoals beveiliging, of een specifiek onderdeel, zoals Internet Information Services (IIS). • **Servicepakket**: cumulatieve sets van alle hotfixes, beveiligingsupdates, kritieke updates en updates die zijn gemaakt sinds de release van het product. Servicepakketten kunnen ook een beperkt aantal door de klant gevraagde ontwerpwijzigingen of functies bevatten. • **Tool**: hulpprogramma's of functies die helpen bij het uitvoeren van een

	taak of een reeks taken. • **Functiepakket**: releases met nieuwe functies, meestal gebundeld met de volgende release van producten. • **Update**: algemeen uitgebrachte oplossingen voor specifieke, niet-kritieke problemen die niet zijn gerelateerd aan de beveiliging. • **Toepassing**: patches voor een toepassing.
Releasedatum	De datum waarop de patch is uitgebracht
Laatst gerapporteerd	De datum van de laatste keer dat de patch is gemeld
Eerst geïnstalleerd	De datum van de eerste installatie van de patch op een machine
Microsoft KB	Als de patch is bedoeld voor een Microsoft-product, wordt de id van het KB-artikel weergegeven
Machines	Aantal betroffen machines
Beveiligingsproblemen	Het aantal beveiligingsproblemen. Als u hierop klikt, wordt u omgeleid naar de lijst met beveiligingsproblemen.
Grootte	De gemiddelde grootte van de patch
Taal	De taal die wordt ondersteund door de patch
Leverancierssite	De officiële site van de verkoper

Levensduur van de patch configureren in de lijst

U kunt de lijst met patches up-to-date houden door de levensduur van de patch te configureren in de lijst op het scherm **Patches**. Met deze instelling bepaalt u hoe lang de gedetecteerde beschikbare patch zichtbaar zal zijn in de lijst met patches. De patch wordt uit de lijst verwijderd nadat deze is geïnstalleerd op alle machines waarop de patch als ontbrekend is aangegeven, of nadat de levensduur in de lijst is verstreken.

De levensduur van de patch configureren in de lijst:

1. Ga in de Cyber Protect-console naar **Softwarebeheer** > **Patches**.
2. Klik op **Instellingen**.
3. Ga naar **Levensduur in lijst** en selecteer de gewenste optie.

Optie	Beschrijving
Permanent	De patch wordt altijd in de lijst vermeld.
7 dagen	De patch wordt zeven dagen na de eerste installatie verwijderd uit de lijst. Stel dat u twee machines hebt waarop patches moeten worden geïnstalleerd. Een ervan is online, de andere offline. U hebt de patch op de eerste machine geïnstalleerd. Na 7 dagen wordt de patch verwijderd uit de lijst met patches, zelfs als deze niet is geïnstalleerd op de tweede machine

Optie	Beschrijving
	omdat deze offline was.
30 dagen	De patch wordt 30 dagen na de eerste installatie verwijderd uit de lijst.

Automatische patchgoedkeuring

Met automatische patchgoedkeuring kunt u updates eenvoudiger installeren op machines. Met automatische patchgoedkeuring voorkomt u dat de installatie van patches wordt vertraagd omdat de patches handmatig moeten worden goedgekeurd. Belangrijke updates en oplossingen worden sneller geïnstalleerd, waardoor de betrouwbaarheid van uw systeem toeneemt.

U kunt automatische patchgoedkeuring gebruiken in testscenario's voor de automatische installatie van patches. Als de patches correct zijn geïnstalleerd op de testmachines, worden de patches automatisch ook geïnstalleerd op de productiemachines. Zie "Gebruiksvoorbeeld van Automatische patchgoedkeuring en testen" (p. 1039) voor meer informatie over dit scenario.

U kunt automatische patchgoedkeuring ook gebruiken in scenario's voor het automatisch installeren van patches in uw productieomgeving, waarbij u de testfase overslaat. Zie "Gebruiksvoorbeeld van automatische patchgoedkeuring zonder testen" (p. 1042) voor meer informatie over dit scenario.

Automatische patchgoedkeuring configureren

U kunt automatische patchgoedkeuring configureren om te voorkomen dat de installatie van patches wordt vertraagd omdat de patches handmatig moeten worden goedgekeurd.

Automatische patchgoedkeuring configureren

1. Ga in de Cyber Protect-console naar **Softwarebeheer** > **Patches**.
2. Klik op **Instellingen**.
3. Schakel **Automatische patchgoedkeuring** in.
4. Configureer de instellingen voor automatische patchgoedkeuring.

a. Selecteer de optie Automatische patchgoedkeuring.

Optie	Beschrijving
Automatische patchgoedkeuring en testen	De goedkeuringsstatus van de patch wordt gewijzigd in **Goedgekeurd** na het verstrijken van het geselecteerde aantal dagen na de installatie van de patch. We raden u aan deze instelling te gebruiken als u de patches eerst wilt testen: installeer ze op een testmachine, controleer of alles naar verwachting werkt en installeer de patches vervolgens in uw productieomgeving.
Automatische patchgoedkeuring zonder testen	De goedkeuringsstatus van de patch wordt gewijzigd in **Goedgekeurd** na het verstrijken van het geselecteerde aantal dagen na detectie van de patch.

b. Selecteer het aantal dagen dat moet verstrijken nadat aan de voorwaarde van de optie voor automatische patchgoedkeuring is voldaan. Na deze periode wordt de goedkeuringsstatus van de patches automatisch bijgewerkt van **Goedkeuring in behandeling** naar **Goedgekeurd**.

5. Selecteer **Automatisch de licentieovereenkomsten accepteren**.
6. Klik op **Toepassen**.

Gebruiksvoorbeeld van Automatische patchgoedkeuring en testen

Als u de nieuwe patches op een testmachine wilt testen voordat u ze op uw productiemachines installeert, kunt u twee beschermingsschema's configureren: een schema voor de installatie van patches voor testdoeleinden, en een schema voor de installatie van geteste patches op productiemachines. Zo waarborgt u dat de patches die u in uw productieomgeving installeert, veilig zijn en dat uw productiemachines na de patchinstallatie correct werken.

Het gebruiksvoorbeeld omvat de volgende fasen:

1. Configureer de instellingen voor automatische patchgoedkeuring. Selecteer de optie **Automatische patchgoedkeuring en testen**. Zie "Automatische patchgoedkeuring configureren" (p. 1038) voor meer informatie.
2. Configureer een beschermingsschema voor testdoeleinden (bijvoorbeeld 'Testpatch') terwijl de module **Patchbeheer** is ingeschakeld en pas het schema toe op de machines in de testomgeving. Geef de volgende voorwaarde voor de patchinstallatie op: de goedkeuringsstatus voor de patch moet **Goedkeuring in behandeling** zijn. Deze stap is nodig om de patches te valideren en te controleren of de machines goed werken na de patchinstallatie. Zie "Het beschermingsschema Testpatch configureren" (p. 1040) voor meer informatie.
3. Configureer een beschermingsschema voor de productieomgeving (bijvoorbeeld 'Productiepatch') terwijl de module **Patchbeheer** is ingeschakeld en pas het schema toe op de machines in de productieomgeving. Geef de volgende voorwaarde op voor de patchinstallatie: de patchstatus moet **Goedgekeurd** zijn. Zie "Het beschermingsschema Productiepatch configureren" (p. 1041) voor meer informatie.

4. Voer het schema Testpatch uit en controleer de resultaten. De goedkeuringsstatus **Goedkeuring in behandeling** van de machines zonder problemen kan ongewijzigd blijven, maar de goedkeuringsstatus van de machines die niet correct werken, moet u wijzigen in **Afgewezen**. Afhankelijk van het aantal dagen dat is ingesteld in de instelling **Automatische patchgoedkeuring**, wordt de status **Goedkeuring in behandeling** van de patches automatisch gewijzigd in **Goedgekeurd**. Hierdoor worden alleen de patches met de status **Goedgekeurd** geïnstalleerd op de productiemachines wanneer u het schema Productiepatch uitvoert. Zie "Het beschermingsschema Testpatch uitvoeren en onveilige patches afwijzen" (p. 1042) voor meer informatie.
5. Voer het beschermingsschema Productiepatch uit.

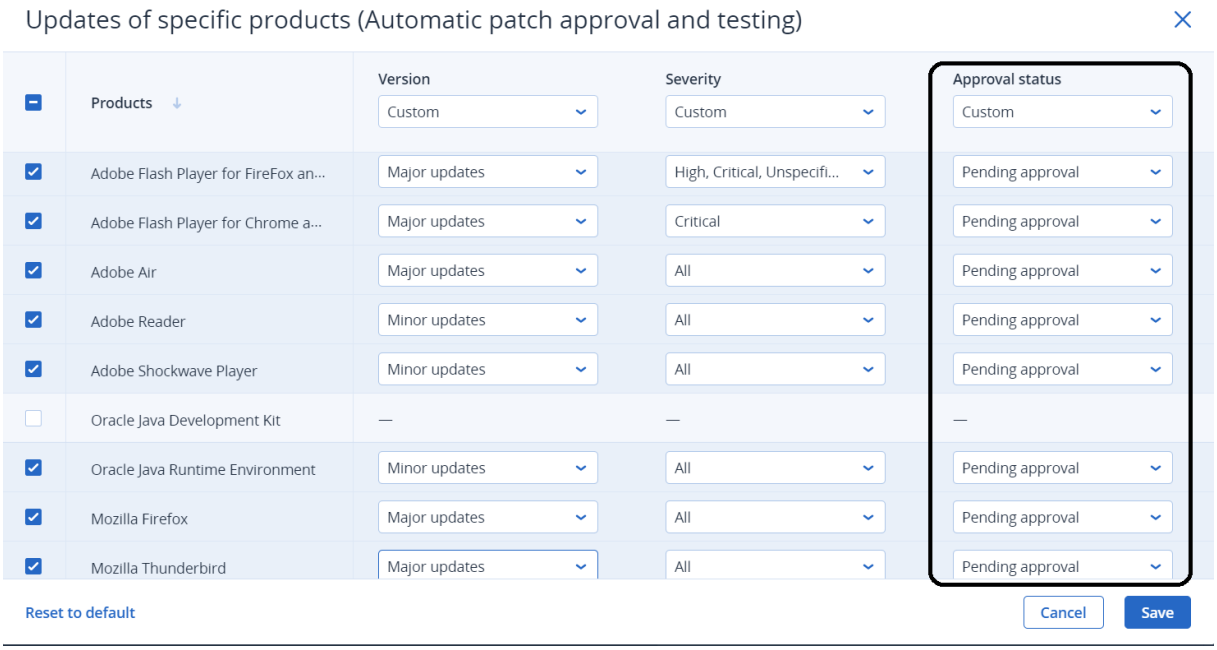
Het beschermingsschema Testpatch configureren

U kunt een beschermingsschema configureren met de patch-installatie-instellingen voor uw machines in de testomgeving.

Het beschermingsschema Testpatch configureren:

1. Ga in de Cyber Protect-console naar **Beheer** > **Beschermingsschema's**.
2. Klik op **Schema maken**.
3. Schakel de module **Patchbeheer** in.
4. Definieer welke updates u wilt installeren voor producten van Microsoft en derden, en geef het schema en back-up vóór update op. Zie "Instellingen voor patchbeheer in het beschermingsschema" (p. 1030) voor meer informatie over deze instellingen.

Belangrijk
Voor alle producten die u wilt bijwerken, selecteert u de goedkeuringsstatus **Goedkeuring in behandeling**. De agent installeert dan alleen patches met de status **Goedkeuring in behandeling** op de geselecteerde machines in de testomgeving.



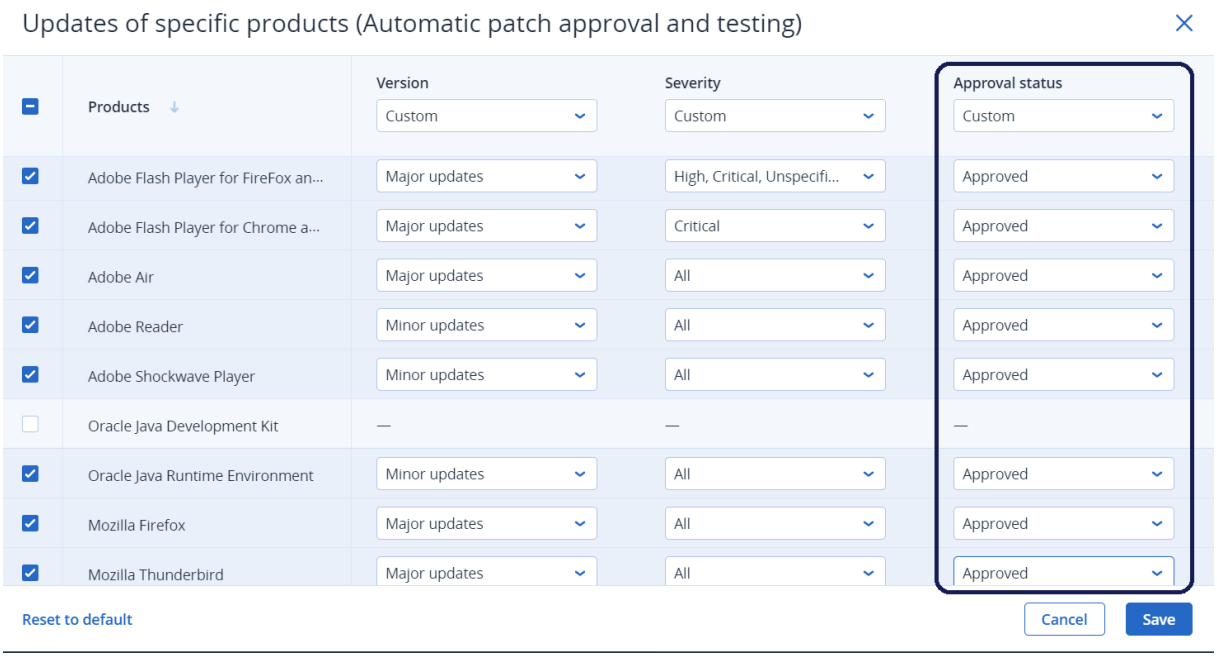
Het beschermingsschema Productiepatch configureren

U kunt een beschermingsschema configureren met de patch-installatie-instellingen voor uw machines in de productieomgeving.

Het beschermingsschema Productiepatch configureren:

1. Ga in de Cyber Protect-console naar **Beheer** > **Beschermingsschema's**.
2. Klik op **Schema maken**.
3. Schakel de module **Patchbeheer** in.
4. Definieer welke updates u wilt installeren voor producten van Microsoft en derden, en geef het schema en back-up vóór update op. Zie "Instellingen voor patchbeheer in het beschermingsschema" (p. 1030) voor meer informatie over deze instellingen.

Belangrijk
Voor alle producten die u wilt bijwerken, stelt u de **Goedkeuringsstatus** in op **Goedgekeurd**. De agent installeert dan alleen patches met de status **Goedgekeurd** op de geselecteerde machines in de productieomgeving.



Het beschermingsschema Testpatch uitvoeren en onveilige patches afwijzen

Nadat patches op de machines in uw testomgeving zijn geïnstalleerd, kunt u controleren of alles werkt zoals verwacht. De goedkeuringsstatus **Goedkeuring in behandeling** van de machines zonder problemen kan ongewijzigd blijven, maar de goedkeuringsstatus van de machines die niet correct werken, moet u wijzigen in **Afgewezen**.

Het beschermingsschema Testpatch uitvoeren en onveilige patches afwijzen:

1. Voer het beschermingsschema Testpatch uit (volgens schema of handmatig).
2. Afhankelijk van het resultaat kunt u zien welke van de geïnstalleerde patches veilig zijn.
3. Ga naar **Softwarebeheer** > **Patches** en stel de **Goedkeuringsstatus** in als **Afgewezen** voor de patches die niet veilig zijn.

Gebruiksvoorbeeld van automatische patchgoedkeuring zonder testen

Als u nieuwe patches zo snel mogelijk automatisch op uw productiemachines wilt installeren, zonder ze eerst op testmachines te installeren, kunt u slechts één beschermingsschema configureren.

Het gebruiksvoorbeeld omvat de volgende fasen:

1. Configureer de instellingen voor automatische patchgoedkeuring. Selecteer de optie **Automatische patchgoedkeuring zonder testen**. Zie "Automatische patchgoedkeuring configureren" (p. 1038) voor meer informatie.
2. Configureer een beschermingsschema voor de productieomgeving (bijvoorbeeld 'Productiepatch') terwijl de module **Patchbeheer** is ingeschakeld en pas het schema toe op de machines in de productieomgeving. Geef de volgende voorwaarde op voor de patchinstallatie:

de patchstatus moet **Goedgekeurd** zijn. Zie "Het beschermingsschema Productiepatch configureren" (p. 1041) voor meer informatie.

3. Voer het beschermingsschema Productiepatch uit.

Patches handmatig goedkeuren

U kunt een patch handmatig goedkeuren en de installatie ervan versnellen door de testfase over te slaan.

Vereisten

- Een beschermingsschema waarvoor de module **Patchbeheer** is ingeschakeld, wordt toegepast op ten minste één Windows-machine.
- Er zijn patches die nog niet zijn geïnstalleerd op de machine of machines waarop het beschermingsschema wordt toegepast.

Patches handmatig goedkeuren:

1. Ga in de Cyber Protect-console naar **Softwarebeheer** > **Patches**.
2. Selecteer de patches die u wilt installeren en accepteer de bijbehorende licentieovereenkomsten.
3. Stel de **Goedkeuringsstatus** van de patches in op **Goedgekeurd**.
   De goedkeuringsstatus van de patches is ingesteld op **Goedgekeurd**. De patches worden automatisch op de machines geïnstalleerd volgens het schema dat is gedefinieerd in het beschermingsschema. Als u de patches direct wilt installeren, volgt u de procedure zoals beschreven in "Patches op aanvraag installeren" (p. 1043).

Patches op aanvraag installeren

U kunt patches op aanvraag handmatig installeren wanneer u niet wilt wachten op de geplande installatietijd.

U kunt de handmatige installatie van de patches starten vanuit drie schermen: **Patches**, **Beveiligingsproblemen** en **Alle apparaten**.

Een patch handmatig installeren:

Vanuit Patches

1. Ga in de Cyber Protect-console naar **Softwarebeheer** > **Patches**.
2. Accepteer de licentieovereenkomsten voor de patches die u wilt installeren.
3. Open de wizard **Patches installeren**, selecteer de patches die u wilt installeren en klik vervolgens op **Installeren**.
4. Selecteer de machines waarop u de patches wilt installeren.
5. Selecteer de opties voor opnieuw opstarten.

a. Selecteer of u wilt dat de machine opnieuw wordt opgestart nadat de patches zijn geïnstalleerd.

Optie	Beschrijving
Nee	De machines worden niet automatisch opnieuw opgestart nadat de patches zijn geïnstalleerd.
Indien nodig	De machines worden alleen opnieuw opgestart als dit nodig is voor het toepassen van de patches.
Ja	De machines worden automatisch opnieuw opgestart nadat de patches zijn geïnstalleerd. U kunt ook een vertraging opgeven voor het opnieuw opstarten.

b. [Optioneel] Als u het opnieuw opstarten van de machine wilt uitstellen wanneer er een back-up van de machine wordt gemaakt, selecteert u **Niet opnieuw opstarten totdat de back-up is voltooid**.

6. Klik op **Patches installeren**.

Vanuit Beveiligingsproblemen

1. Ga in de Cyber Protect-console naar **Softwarebeheer** > **Beveiligingsproblemen**.
2. Voer het herstelproces uit, zoals beschreven in "Gevonden beveiligingsproblemen beheren" (p. 1027).

Vanuit Alle apparaten

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de machine waarop u de patches wilt installeren.
3. Klik op **Patch**.
4. Selecteer de patches die u wilt installeren en klik vervolgens op **Volgende**.
5. Selecteer de opties voor opnieuw opstarten.
   a. Selecteer of u wilt dat de machine opnieuw wordt opgestart nadat de patches zijn geïnstalleerd.

Optie	Beschrijving
Nee	De machines worden niet automatisch opnieuw opgestart nadat de patches zijn geïnstalleerd.
Indien nodig	De machines worden alleen opnieuw opgestart als dit nodig is voor het toepassen van de patches.
Ja	De machines worden automatisch opnieuw opgestart nadat de patches zijn geïnstalleerd. U kunt ook een vertraging opgeven voor het opnieuw opstarten.

b. [Optioneel] Als u het opnieuw opstarten van de machine wilt uitstellen wanneer er een back-up van de machine wordt gemaakt, selecteert u **Niet opnieuw opstarten totdat de back-up is voltooid**.

6. Klik op **Patches installeren**.

Uw software- en hardware-inventaris beheren

Software-inventaris

De functie voor software-inventarisatie is beschikbaar voor apparaten waarvoor het Advanced-pakket is ingeschakeld of die de (oudere) Cyber Protect-licentie hebben. Met deze functie kunt u alle softwaretoepassingen bekijken die op alle Windows- en macOS-apparaten zijn geïnstalleerd.

Als u de software-inventarisgegevens wilt verkrijgen, kunt u automatische of handmatige scans uitvoeren op de apparaten.

U kunt de gegevens van de software-inventaris gebruiken voor het volgende:

- bladeren in en vergelijken van de informatie over alle toepassingen die zijn geïnstalleerd op de apparaten van het bedrijf
- bepalen of een toepassing moet worden bijgewerkt
- bepalen of een ongebruikte toepassing moet worden verwijderd
- waarborgen dat diverse apparaten van het bedrijf dezelfde softwareversie hebben
- veranderingen van de softwarestatus tussen opeenvolgende scans bewaken.

De software-inventarisscans inschakelen

Wanneer software-inventarisscan is ingeschakeld op de apparaten, worden de softwaregegevens automatisch om de 12 uur verzameld.

De functie voor software-inventarisscan is standaard ingeschakeld voor alle apparaten met de vereiste licentie, maar u kunt de instelling indien nodig wijzigen.

Opmerking
Klanttenants kunnen de software-inventarisscans in- of uitschakelen. De tenants van de eenheid kunnen de instellingen van de software-inventarisscans bekijken, maar kunnen deze niet wijzigen.

De software-inventarisscans inschakelen

1. Ga in de Cyber Protect-console naar **Instellingen**.
2. Klik op **Bescherming**.
3. Klik op **Inventarisscan**.
4. Schakel de module **Software-inventarisscan** in door op de schakelaar naast de naam van de module te klikken.

De software-inventarisscans uitschakelen

1. Ga in de Cyber Protect-console naar **Instellingen**.
2. Klik op **Bescherming**.

3. Klik op **Inventarisscan**.
4. Schakel de module **Software-inventarisscan** uit door op de schakelaar naast de naam van de module te klikken.

Een software-inventarisscan handmatig uitvoeren

U kunt handmatig een software-inventarisscan uitvoeren vanaf het scherm **Software-inventaris** of vanaf het tabblad **Software** op het scherm **Inventaris**.

Vereisten

- Het apparaat maakt gebruik van het Windows- of macOS-besturingssysteem.
- Het apparaat heeft de vereiste (oudere) Cyber Protect-licentie of het Advanced Management-pakket is geactiveerd voor het apparaat.

Een software-inventarisscan uitvoeren vanaf het scherm Software-inventaris

1. Ga in de Cyber Protect-console naar **Softwarebeheer**.
2. Klik op **Software-inventaris**.
3. Selecteer in het vervolgkeuzeveld **Groeperen op:** de optie **Apparaten**.
4. Zoek het apparaat dat u wilt scannen en klik op **Nu scannen**.

Een software-inventarisscan uitvoeren vanaf het tabblad Software op het scherm Inventaris

1. Ga in de Cyber Protect-console naar **Apparaten**.
2. Klik op het apparaat dat u wilt scannen en klik op **Inventaris**.
3. Klik op het tabblad **Software** op **Nu scannen**.

Bladeren in de software-inventaris

U kunt de gegevens bekijken van alle softwaretoepassingen die beschikbaar zijn op alle apparaten van het bedrijf.

Vereisten

- De apparaten maken gebruik van het Windows- of macOS-besturingssysteem.
- De apparaten hebben de vereiste (oudere) Cyber Protect-licentie of het Advanced Management-pakket is geactiveerd voor de apparaten.
- Software-inventarisscan op de apparaten is voltooid.

Alle softwaretoepassingen bekijken die beschikbaar zijn op alle Windows- en macOS-apparaten van het bedrijf

1. Ga in de Cyber Protect-console naar **Softwarebeheer**.
2. Klik op **Software-inventaris**.

Standaard zijn de gegevens gegroepeerd per apparaat. De volgende tabel bevat een beschrijving van de gegevens die zichtbaar zijn op het scherm **Software-inventaris**.

Kolom	Beschrijving
Naam	Naam van de toepassing.
Versie	Versie van de toepassing.
Status	Status van de toepassing. • **Nieuw**. • **Bijgewerkt**. • **Verwijderd**. • **Geen wijziging**.
Leverancier	Leverancier van de toepassing.
Installatiedatum	Datum en tijd waarop de toepassing is geïnstalleerd.
Laatste uitvoering	Alleen voor macOS-apparaten. Datum en tijd waarop de toepassing voor het laatst actief was.
Locatie	Directory waar de toepassing is geïnstalleerd.
Gebruiker	Gebruiker die de toepassing heeft geïnstalleerd.
Systeemtype	Alleen voor Windows-apparaten. Type bit van de toepassing. • **X86** voor 32-bits toepassingen. • **X64** voor 64-bits toepassingen.

3. Als u de gegevens per toepassing wilt groeperen, selecteert u in het vervolgkeuzeveld **Groeperen op:** de optie **Applicaties**.
4. Als u de informatie op het scherm wilt verfijnen, gebruikt u een filter of een combinatie van filters.
   a. Klik op **Filteren**.
   b. Selecteer een filter of een combinatie van filters.

      De volgende tabel bevat een beschrijving van de filters op het scherm **Software-inventaris**.

Filter	Beschrijving
Apparaatnaam	Naam van het apparaat. Meervoudige selectie is mogelijk. Gebruik dit filter als u de software op specifieke apparaten wilt vergelijken.
Toepassing	Naam van de toepassing. Meervoudige selectie is mogelijk. Gebruik dit filter als u de gegevens voor een specifieke toepassing op specifieke apparaten of op alle apparaten wilt vergelijken.
Leverancier	Leverancier van de toepassing. Meervoudige selectie is

Filter	Beschrijving
	mogelijk. Gebruik dit filter als u alle toepassingen van een specifieke leverancier op specifieke apparaten of op alle apparaten wilt bekijken.
Status	Status van de toepassing. Meervoudige selectie is mogelijk. Gebruik dit filter als u alle toepassingen met de geselecteerde status op specifieke apparaten of op alle apparaten wilt bekijken.
Installatiedatum	Datum waarop de toepassing is geïnstalleerd. Gebruik dit filter als u alle toepassingen wilt bekijken die op een specifieke datum op specifieke apparaten of op alle apparaten zijn geïnstalleerd.
Datum van scan	Datum van de software-inventarisscan. Gebruik dit filter als u de informatie wilt bekijken over de software op specifieke apparaten of op alle apparaten die op die datum worden gescand.

c. Klik op **Toepassen**.

5. Als u door de hele software-inventarislijst wilt bladeren, gebruikt u de paginering linksonder in het scherm.

- Klik op het nummer van de pagina die u wilt openen.
- Selecteer in het vervolgkeuzeveld het paginanummer van de pagina die u wilt openen.

De software-inventaris van een bepaald apparaat bekijken

U kunt een lijst bekijken van alle softwaretoepassingen die op een bepaald apparaat zijn geïnstalleerd, samen met gedetailleerde informatie over de toepassingen, zoals status, versie, leverancier, installatiedatum, laatste uitvoering en locatie.

Vereisten

- Het apparaat maakt gebruik van het Windows- of macOS-besturingssysteem.
- Het apparaat heeft de vereiste (oudere) Cyber Protect-licentie of het Advanced Management-pakket is geactiveerd voor het apparaat.
- Software-inventarisscan op het apparaat is voltooid.

De software-inventaris van een bepaald apparaat bekijken vanaf het scherm Software-inventaris

1. Ga in de Cyber Protect-console naar **Softwarebeheer**.
2. Klik op **Software-inventaris**.
3. Selecteer in het vervolgkeuzeveld **Groeperen op:** de optie **Apparaten**.
4. Gebruik een van de volgende opties om het apparaat te zoeken dat u wilt inspecteren.

- Zoek het apparaat via **Filteren**:
  a. Klik op **Filteren**.
  b. Selecteer in het veld **Apparaatnaam** de naam van het apparaat dat u wilt weergeven.
  c. Klik op **Toepassen**.
- Zoek het apparaat via dynamisch **zoeken**:
  a. Klik op **Zoeken**.
  b. Typ de volledige naam van het apparaat of een deel van de naam van het apparaat.

De software-inventaris van een bepaald apparaat bekijken vanaf het scherm Apparaten

1. Ga in de Cyber Protect-console naar **Apparaten**.
2. Klik op het apparaat dat u wilt bekijken en klik op **Inventaris**.
3. Klik op het tabblad **Software**.

Hardware-inventaris

Met de functie voor hardware-inventaris kunt u alle hardwareonderdelen bekijken die beschikbaar zijn op:

- fysieke Windows- en macOS-apparaten met een licentie die de functie Hardware-inventaris ondersteunt.
- virtuele Windows- en macOS-machines die worden uitgevoerd op de volgende virtualisatieplatforms: VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo en Virtuozzo Hybrid Infrastructure. Zie "Ondersteunde virtualisatieplatforms" (p. 32) voor meer informatie over de ondersteunde versies van de virtualisatieplatforms.

Opmerking
De functie Hardware-inventaris voor virtuele machines wordt niet ondersteund in de verouderde Cyber Protect-edities.

De functie Hardware inventaris wordt alleen ondersteund voor apparaten waarop een beveiligingsagent is geïnstalleerd.

Als u de hardware-inventarisgegevens wilt verkrijgen, kunt u automatische of handmatige scans uitvoeren op de apparaten.

U kunt de gegevens van de hardware-inventaris gebruiken voor het volgende:

- alle hardwareassets van de organisatie verkennen
- bladeren door de hardware-inventaris van alle apparaten in uw organisatie
- de hardwareonderdelen op meerdere apparaten van het bedrijf vergelijken
- gedetailleerde informatie over een hardwareonderdeel bekijken.

De hardware-inventarisscans inschakelen

Wanneer hardware-inventarisscan is ingeschakeld op fysieke apparaten en virtuele machines, worden de hardwaregegevens automatisch om de 12 uur verzameld.

De functie voor hardware-inventarisscans is standaard ingeschakeld, maar u kunt de instelling indien nodig wijzigen.

Opmerking
Klanttenants kunnen de hardware-inventarisscans in- of uitschakelen. De tenants van de eenheid kunnen de instellingen van de hardware-inventarisscans bekijken, maar kunnen deze niet wijzigen.

De hardware-inventarisscans inschakelen

1. Ga in de Cyber Protect-console naar **Instellingen**.
2. Klik op **Bescherming**.
3. Klik op **Inventarisscan**.
4. Schakel de module **Hardware-inventarisscan** in door op de schakelaar naast de naam van de module te klikken.

De hardware-inventarisscans uitschakelen

1. Ga in de Cyber Protect-console naar **Instellingen**.
2. Klik op **Bescherming**.
3. Klik op **Inventarisscan**.
4. Schakel de module **Hardware-inventarisscan** uit door op de schakelaar naast de naam van de module te klikken.

Een hardware-inventarisscan handmatig uitvoeren

U kunt handmatig een hardware-inventarisscan uitvoeren voor een bepaald apparaat en de actuele gegevens van de hardwareonderdelen van het apparaat bekijken.

Opmerking
Het scannen van de hardware-inventaris van virtuele machines wordt alleen ondersteund wanneer de huidige datum en tijd van de virtuele machine overeenkomt met de huidige datum en tijd in UTC. Controleer of de virtuele machine de juiste tijdsinstellingen gebruikt: schakel de optie **Tijdsynchronisatie** van de virtuele machine uit, stel de huidige datum, tijd en tijdzone in en start **Acronis Agent Core Service** en **Acronis Managed Machine Service** vervolgens opnieuw op.

Vereisten

- (Voor alle apparaten) Het apparaat maakt gebruik van een Windows- of macOS-besturingssysteem.

- (Voor alle apparaten) De apparaten hebben een licentie die de functie Hardware-inventarisatie ondersteunt. Let op: de functie Hardware-inventarisatie voor virtuele machines wordt niet ondersteund in de (oudere) edities van Cyber Protect.
- (Voor alle apparaten) Een beveiligingsagent is geïnstalleerd op het apparaat.
- (Voor virtuele machines) De machine wordt uitgevoerd op een van de ondersteunde virtualisatieplatforms. Zie "Hardware-inventaris" (p. 1050) voor meer informatie.

Een hardware-inventarisscan uitvoeren voor een bepaald apparaat

1. Ga in de Cyber Protect-console naar **Apparaten**.
2. Klik op het apparaat dat u wilt scannen en klik op **Inventaris**.
3. Klik op het tabblad **Hardware** op **Nu scannen**.

Bladeren in de hardware-inventaris

U kunt de gegevens bekijken en doorzoeken voor alle hardwareonderdelen die beschikbaar zijn op alle apparaten van het bedrijf.

Vereisten

- (Voor alle apparaten) De apparaten maken gebruik van het Windows- of macOS-besturingssysteem.
- (Voor alle apparaten) De apparaten hebben een licentie die de functie Hardware-inventaris ondersteunt. Let op: De functie Hardware-inventaris voor virtuele machines wordt niet ondersteund in de verouderde Cyber Protect-edities.
- (Voor alle apparaten) Een beveiligingsagent is geïnstalleerd op het apparaat.
- (Voor alle apparaten) Hardware-inventarisscan op de apparaten is voltooid.
- (Voor virtuele machines) De machine wordt uitgevoerd op een van de ondersteunde virtualisatieplatforms. Zie "Hardware-inventaris" (p. 1050) voor meer informatie.

Alle hardwareonderdelen bekijken die beschikbaar zijn op de Windows- en macOS-apparaten van het bedrijf

1. Ga in de Cyber Protect-console naar **Apparaten**.
2. Selecteer in het vervolgkeuzeveld **Weergave:** de optie **Hardware**.

Opmerking
De weergave is een set kolommen waarmee wordt bepaald welke gegevens zichtbaar zijn op het scherm. De vooraf gedefinieerde weergaven zijn **Standard** en **Hardware**. U kunt aangepaste weergaven maken en opslaan met verschillende sets kolommen die meer aansluiten op uw behoeften.

De volgende tabel bevat een beschrijving van de gegevens die zichtbaar zijn in de weergave **Hardware**.

Kolom	Beschrijving
Naam	Naam van het apparaat.
Status van hardwarescan	Status van de hardware-scan. • **Voltooid**. • **Niet gestart**. • Status **Niet ondersteund**. wordt weergegeven voor workloads waarvoor de functionaliteit van de hardware-inventaris niet wordt ondersteund, d.w.z. virtuele machines, mobiele apparaten en Linux-apparaten. • **Update agent**. Weergegeven in het geval dat de verouderde versie van de agent is geïnstalleerd op het apparaat. Als u op deze actie klikt, wordt u omgeleid naar de pagina Instellingen > Agenten, waar de beheerder de agentupdate kan uitvoeren. • **Upgrade quota**. Door hierop te klikken opent u een dialoogvenster waarin de beheerder de huidige licentie kan omschakelen naar een van de andere beschikbare licenties voor tenants
Processor	Modellen van alle processoren van het apparaat.
Processorkernen	Aantal kernen van alle processoren van het apparaat.
Schijfopslag	Gebruikte opslag en totale opslag van alle schijven van het apparaat.
Geheugen	Totale RAM-capaciteit van het apparaat.
Datum van scan	De datum en tijd van de laatste hardware-inventarisscan.
Moederbord	Moederbord van het apparaat.
Serienummer van moederbord	Serienummer van het moederbord.
BIOS-versie	Versie van het BIOS van het systeem.
Organisatie	Organisatie waartoe het apparaat behoort.
Eigenaar	Eigenaar van het apparaat.
Domein	Domein van het apparaat.
Besturingssysteem	Besturingssysteem van het apparaat.
Build van besturingssysteem	Build van het besturingssysteem van het apparaat.

3. Als u kolommen in de tabel wilt toevoegen, klikt u op het pictogram voor kolomopties en selecteert u de kolommen die u zichtbaar wilt maken in de tabel.
4. Als u de informatie op het scherm wilt verfijnen, gebruikt u een of meer filters.
   a. Klik op **Zoeken**.
   b. Klik op de pijl en klik vervolgens op **Hardware**.
   c. Selecteer een filter of een combinatie van filters.
      De volgende tabel bevat een beschrijving van de **Hardware**filters.

Filter	Beschrijving
Processormodel	Meervoudige selectie is mogelijk. Gebruik dit filter als u de hardwaregegevens wilt bekijken van de apparaten met het opgegeven processormodel.
Processorkernen	Gebruik dit filter als u de hardwaregegevens wilt bekijken van de apparaten met het opgegeven aantal processorkernen.
Totale grootte van schijf	Gebruik dit filter als u de hardwaregegevens wilt bekijken van de apparaten met de opgegeven totale opslaggrootte.
Geheugencapaciteit	Gebruik dit filter als u de hardwaregegevens wilt bekijken van de apparaten met de opgegeven RAM-capaciteit.

   d. Klik op **Toepassen**.
5. Als u de gegevens in oplopende volgorde wilt sorteren, klikt u op de naam van een kolom.

De hardware van een bepaald apparaat bekijken

U kunt gedetailleerde informatie bekijken over het moederbord, de processors, het geheugen, de grafische specificaties, de opslagstations, het netwerk en het systeem van een specifiek apparaat.

Vereisten

- (Voor alle apparaten) Het apparaat maakt gebruik van het Windows- of macOS-besturingssysteem.
- (Voor alle apparaten) De apparaten hebben een licentie die de functie Hardware-inventaris ondersteunt. Let op: De functie Hardware-inventaris voor virtuele machines wordt niet ondersteund in de verouderde Cyber Protect-edities.
- (Voor alle apparaten) Een beveiligingsagent is geïnstalleerd op het apparaat.
- (Voor alle apparaten) Hardware-inventarisscan op het apparaat is voltooid.
- (Voor virtuele machines) De machine wordt uitgevoerd op een van de ondersteunde virtualisatieplatforms. Zie "Hardware-inventaris" (p. 1050) voor meer informatie.

De gedetailleerde informatie bekijken over de hardware van een specifiek apparaat

1. Ga in de Cyber Protect-console naar **Apparaten** > **Alle apparaten**.
2. Selecteer in het vervolgkeuzeveld **Weergave:** de optie **Hardware**.
3. Gebruik een van de hieronder beschreven methoden om het apparaat te zoeken dat u wilt inspecteren.
   - Zoek het apparaat via **Filteren**:
     a. Klik op **Filteren**.
     b. Selecteer een filterparameter of een combinatie van filterparameters om het apparaat te vinden.
     c. Klik op **Toepassen**.
   - Zoek het apparaat via **Zoeken**:
     a. Klik op **Zoeken**.
     b. Typ de volledige naam van het apparaat of een deel van de naam van het apparaat en klik op **Enter**.
4. Klik op de rij waar het apparaat wordt vermeld en klik op **Inventaris**.
5. Klik op het tabblad **Hardware**.
   De volgende hardwaregegevens zijn beschikbaar.

Hardwareonderdeel	Weergegeven informatie
Moederbord	Naam, fabrikant, model en serienummer van het moederbord van het apparaat.
Verwerkers	Fabrikant, model, maximale kloksnelheid en aantal kernen van elke processor van het apparaat.
Geheugen	Capaciteit, fabrikant en serienummer van het geheugen van het apparaat.
Grafische weergave	Fabrikant en model van de GPU's van het apparaat.
Opslagstations	Model, mediatype, beschikbare ruimte en grootte van de opslagstations van het apparaat.
Netwerk	Mac-adres, IP-adres en type van de netwerkadapters van het apparaat.
Systeem	Product-id, oorspronkelijke installatiedatum, systeemopstarttijd, systeemfabrikant, systeemmodel, BIOS-versie, opstartapparaat, landinstellingen en tijdzone van het systeem.

Verbinding maken met workloads voor een extern bureaublad of voor hulp op afstand

De functionaliteit voor extern bureaublad en hulp op afstand is een handige manier om verbinding te maken met workloads in uw organisatie als u externe besturing of hulp op afstand wilt gebruiken. Sinds december 2022 ondersteunt de functionaliteit de protocollen NEAR, RDP en Schermdeling van Apple. Zie "Protocollen voor externe verbindingen" (p. 1061) voor meer informatie.

U kunt de functionaliteit voor extern bureaublad gebruiken voor de volgende taken.

- Verbinding maken met externe Windows-, macOS- en Linux-workloads via NEAR in de modus Alleen bekijken.
- Verbinding maken met externe Windows-workloads via RDP.
- Verbinding maken met externe macOS-workloads via Schermdeling van Apple in de modus Alleen bekijken of Verbergen (Gordijn).
- Verbinding maken met beheerde workloads en ze extern besturen via externe cloudverbindingen.
- Verbinding maken met onbeheerde workloads en ze extern besturen via externe directe verbindingen.
- Verbinding maken met onbeheerde externe workloads via Acronis Quick Assist.
- Verbinding maken met externe workloads via verschillende verificatiemethoden: met referenties voor externe workloads, door toestemming te vragen voor bekijken of besturen, of via een toegangscode (voor Quick Assist).
- Meerdere monitors tegelijk bekijken in multiweergave.
- Externe sessies opnemen (wanneer verbonden via NEAR).
- Het sessiegeschiedenisrapport bekijken.

Zie "Ondersteunde functies van extern bureaublad en hulp op afstand" (p. 1058) voor meer informatie over de functies die deel uitmaken van het Standard- en Advanced Management-pakket.

U kunt de functionaliteit voor hulp op afstand gebruiken voor de volgende taken.

- Verbinding maken met externe Windows-, macOS- en Linux-workloads via NEAR in de modus Besturen.
- Verbinding maken met externe macOS-workloads via Schermdeling van Apple in de modus Besturen.
- Hulp op afstand bieden voor workloads via externe cloudverbindingen.
- Bestanden overdragen tussen de lokale en externe workloads.
- Basisbeheeracties uitvoeren voor de externe workload: opnieuw opstarten, afsluiten, in de slaapstand zetten, de prullenbak leegmaken en de externe gebruiker afmelden.
- De externe workload controleren door regelmatig momentopnamen van het bureaublad te maken.

Zie "Ondersteunde functies van extern bureaublad en hulp op afstand" (p. 1058) voor meer informatie over de functies die deel uitmaken van Standard Protection en Advanced Management.

Belangrijk
Als u de volledige functionaliteit van extern bureaublad en hulp op afstand wilt activeren voor een beheerde workload, moet u een schema voor extern beheer configureren en toepassen op de workload. U kunt slechts één schema voor extern beheer toepassen op een workload, maar afhankelijk van uw behoeften kunt u wel verschillende schema's voor extern beheer configureren en deze op verschillende workloads toepassen.

U kunt bijvoorbeeld een schema voor extern beheer maken waarvoor alleen het RDP-protocol is ingeschakeld en dit toepassen voor bepaalde workloads. Op die manier kunt u op afstand verbinding maken met deze workloads zonder de Advanced Management-licentie per workload te activeren en zonder extra kosten te betalen.

U kunt ook een ander schema voor extern beheer maken waarvoor de protocollen NEAR en Schermdeling van Apple zijn ingeschakeld. In dit geval wordt de Advanced Management-licentie per workload geactiveerd en worden er kosten in rekening gebracht voor elke workload waarvoor dit schema voor extern beheer wordt toegepast.

Zie "Schema's voor extern beheer" (p. 1065) voor meer informatie over schema's voor extern beheer en hoe u hiermee kunt werken.

Opmerking
Voor de functionaliteit van extern bureaublad en hulp op afstand is het volgende vereist:

- een eenmalige installatie van Connect Client voor de beherende workload (host). U krijgt automatisch een voorstel om de client te downloaden wanneer u voor het eerst probeert een actie op afstand uit te voeren (externe besturing of hulp op afstand) voor een doelworkload. U kunt Connect Client ook downloaden vanuit het venster **Downloads** in de Bescherming-console. Zie "De Connect Client-instellingen configureren" (p. 1098) voor meer informatie over de instellingen die u kunt configureren.
- installatie van Connect Agent voor de beheerde workloads. Connect Agent is een module die deel uitmaakt van de Bescherming-agent, vanaf versie 15.0.31266.
- voor externe macOS-workloads moeten de vereiste systeemmachtigingen worden toegekend aan Connect Agent. Zie "Beveiligingsagents installeren in macOS" (p. 86) voor meer informatie.
- uitvoering van de Acronis Quick Assist-toepassing voor de onbeheerde workloads. U kunt Acronis Quick Assist downloaden van de website.

Zie "Ondersteunde platforms" (p. 1060) voor meer informatie over de ondersteunde platforms voor elk onderdeel van extern bureaublad en hulp op afstand.

Ondersteunde functies van extern bureaublad en hulp op afstand

De volgende tabel bevat meer informatie over de wijzigingen die in december 2022 zijn geïntroduceerd voor de ondersteunde functies van extern bureaublad en hulp op afstand.

Functies	Standard Protection vóór december 2022	Advanced Management vóór december 2022	Standard Protection na december 2022	Advanced Management na december 2022
Verbinding met hulp op afstand via RDP voor Windows	Ja	Nee	Nee	Nee
Een externe verbinding delen met gebruikers	Nee	Ja	Nee	Nee
Externe verbindingen				
Acties op afstand	Nee	Nee	Ja	Ja
Een sessie selecteren om verbinding mee te maken voor Windows/macOS/Linux	Nee	Nee	Nee	Ja
Direct verbinden via RDP en Schermdeling van Apple	Nee	Nee	Nee	Ja
Besturing van meerdere vensters	Nee	Nee	Nee	Ja
Verbindingsmodi: Besturen/Alleen bekijken/Verbergen (Gordijn)	Nee	Nee	Nee	Ja
Algemene ondersteuning voor referenties voor externe verbindingen	Nee	Nee	Ja	Ja
Gelijktijdige verbindingen per technicus				
via RDP	Ja	Ja	Ja	Ja

Functies	Standard Protection vóór december 2022	Advanced Management vóór december 2022	Standard Protection na december 2022	Advanced Management na december 2022
via NEAR	Nee	Nee	Nee	Ja
Bestanden overdragen en delen				
van Windows naar Windows/macOS/Linux	Nee	Nee	Nee	Ja
van macOS naar Windows/macOS/Linux	Nee	Nee	Nee	Ja
van Linux naar Windows/macOS/Linux	Nee	Nee	Nee	Ja
Verbinding maken via de Quick Assist-toepassing				
van Windows naar Windows/macOS/Linux	Nee	Nee	Nee	Ja
van macOS naar Windows/macOS/Linux	Nee	Nee	Nee	Ja
van Linux naar Windows/macOS/Linux	Nee	Nee	Nee	Ja
Externe verbindingen via protocollen				
Externe verbinding via NEAR				
van Windows naar Windows/macOS/Linux	Nee	Nee	Nee	Ja
van macOS naar Windows/macOS/Linux	Nee	Nee	Nee	Ja
van Linux naar Windows/macOS/Linux	Nee	Nee	Nee	Ja
Externe verbinding via RDP (bureaubladclient)				
van Windows naar Windows	Ja	Ja	Ja	Ja
van macOS naar Windows	Ja	Ja	Ja	Ja
van Linux naar Windows	Nee	Nee	Ja	Ja
Externe verbinding via RDP (webclient)				

Functies	Standard Protection vóór december 2022	Advanced Management vóór december 2022	Standard Protection na december 2022	Advanced Management na december 2022
van Windows naar Windows	Ja	Ja	Ja	Ja
van macOS naar Windows	Ja	Ja	Ja	Ja
van Linux naar Windows	Nee	Nee	Ja	Ja
Externe verbinding via Schermdeling van Apple				
van Windows/macOS/Linux naar macOS	Nee	Nee	Nee	Ja
Sessiebeheer				
Sessieopname	Nee	Nee	Nee	Ja
Rapportage en controle				
Sessiegeschiedenis en sessies zoeken	Nee	Nee	Nee	Ja
Overdracht van momentopname	Nee	Nee	Nee	Ja

Ondersteunde platforms

De volgende tabel bevat een overzicht van de ondersteunde besturingssystemen per onderdeel van de functionaliteit voor extern bureaublad en hulp op afstand.

Onderdeel van extern bureaublad	Ondersteunde platforms
Connect Client	• Windows 7 of later • macOS 10.13 of later • Linux: openSUSE 8 Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20

Onderdeel van extern bureaublad	Ondersteunde platforms
	Manjaro 20
Connect Agent	• Windows 7 of later • Windows Server 2008 R2 of later • macOS 10.13 of later • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1
Acronis Quick Assist	• Windows 7 of later • Windows Server 2008 R2 of later • macOS 10.13 of later • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

Protocollen voor externe verbindingen

De functionaliteit voor extern bureaublad maakt gebruik van de volgende protocollen voor externe verbindingen.

NEAR

NEAR is een zeer veilig protocol dat is ontwikkeld door Acronis. Het heeft de volgende kenmerken.

- ### H.264

  NEAR biedt modi voor drie kwaliteiten: **Smooth**, **Balanced** en **Sharp**. In de modus **Smooth** gebruikt NEAR hardware H.264-codering voor macOS en Windows om de bureaubladafbeelding te coderen, en software-encoder als hardware-encoder niet beschikbaar is. Het beeldformaat is momenteel beperkt tot Full HD-resolutie (1920x1080).

- ### Adaptieve codec

  In de modi voor de kwaliteit **Balanced** en **Sharp** maakt NEAR gebruik van de adaptieve codec. Deze levert volledige beeldkwaliteit in 32 bits, in tegenstelling tot de 'video'-modus die wordt gebruikt door H.264.

  In de modus **Balanced** wordt de kwaliteit van de afbeelding automatisch aangepast aan uw huidige netwerkomstandigheden en blijft de huidige framesnelheid behouden.

  In de modus **Sharp** heeft de afbeelding volledige kwaliteit, maar mogelijk met een lagere framesnelheid als uw netwerk, processor of videokaart overbelast is.

  De adaptieve codec maakt gebruikt van OpenCL in Windows en macOS (indien beschikbaar in de grafische stuurprogramma's).

- ### Geluidsoverdracht

  NEAR kan het geluid van de externe computer opnemen en overdragen naar de host. Zie "Omleiding van extern geluid" (p. 1063) voor meer informatie over hoe u omleiding van extern geluid kunt inschakelen in Windows, macOS en Linux.

- ### Verschillende aanmeldingsopties

  U kunt de volgende methoden gebruiken om u aan te melden bij de externe workload.

  Toegangscode: de gebruiker die is aangemeld bij de externe workload, voert Quick Assist uit en verstrekt u de toegangscode. Met deze methode maakt u altijd verbinding met de sessie van de op dat moment aangemelde gebruiker.

  Workloadreferenties: meld u aan bij de externe workload met de beheerdersreferenties die zijn geregistreerd in de workload.

  Toestemming vragen om te bekijken of besturen: de gebruiker die is aangemeld bij de externe workload wordt gevraagd om de verbinding toe te staan of te weigeren.

- ### Beveiliging

  In NEAR zijn uw gegevens altijd in twee richtingen versleuteld met AES-versleuteling.

RDP

Remote Desktop Protocol (RDP) is een door Microsoft ontwikkeld eigen protocol waarmee verbinding kan worden gemaakt met de externe Windows-computer via een netwerkverbinding.

Schermdeling van Apple

Schermdeling van Apple is een VNC-client van Apple die deel uitmaakt van macOS versie 10.5 en later.

Omleiding van extern geluid

Connect Client ondersteunt audiostreaming via het NEAR-verbindingsprotocol. Zie "Protocollen voor externe verbindingen" (p. 1061) voor meer informatie over NEAR.

Geluid omleiden van een externe Windows-workload

Voor Windows-workloads moet het externe geluid automatisch worden overgedragen. Controleer of er apparaten voor geluidsuitvoer (luidsprekers of hoofdtelefoons) zijn verbonden met de externe workload.

Geluid omleiden van een externe macOS-workload

Als u geluidsomleiding van een macOS-workload wilt inschakelen, controleert u het volgende:

- De Bescherming-agent is geïnstalleerd voor de workload.
- Er is een stuurprogramma voor het opnemen van geluid geïnstalleerd voor de workload.
- De workload maakt gebruik van het NEAR-protocol voor externe verbindingen.

Opmerking
Voor een workload met macOS 10.15 Catalina moet de machtiging voor microfoon worden toegekend aan de Connect Agent. Voor meer informatie over het toekennen van de machtiging voor microfoon aan de Connect Agent raadpleegt u "De vereiste systeemmachtigingen toekennen aan Connect Agent" (p. 79).

De agent werkt met de volgende stuurprogramma's voor het opnemen van geluid: Soundflower of Blackhole.

Het installatieproces voor de nieuwste versies wordt beschreven op de Blackhole-wikipagina: https://github.com/ExistentialAudio/BlackHole/wiki/Installation.

Opmerking
Connect Client ondersteunt momenteel alleen de 2-kanaals versie van Blackhole.

Als Homebrew is geïnstalleerd voor de workload, kunt u Blackhole ook installeren via de volgende opdracht:

```
brew install --cask blackhole-2ch
```

Opmerking
Wanneer het geluid van een externe macOS-workload wordt omgeleid, is het geluid niet hoorbaar voor de gebruiker die is aangemeld bij de externe workload.

Geluid omleiden van een externe Linux-workload

De omleiding van extern geluid moet automatisch werken voor de meeste Linux-distributies. Als de omleiding van extern geluid niet standaard werkt, installeer dan het PulseAudio-stuurprogramma via de volgende opdracht:

```
sudo apt-get install pulseaudio
```

Verbinding met beheerde workloads voor extern bureaublad of hulp op afstand

De functionaliteit voor extern bureaublad en hulp op afstand biedt verschillende mogelijkheden om externe directe verbindingen of cloudverbindingen tot stand te brengen met uw workloads.

Directe verbindingen worden tot stand gebracht via TCP/IP in het lokale netwerk (LAN) tussen Connect Client en de externe workload waarvoor geen agent is geïnstalleerd. Er is geen internettoegang vereist.

Cloudverbindingen worden tot stand gebracht tussen Connect Client en de agent of Quick Assist voor de workload via Acronis Cloud.

De volgende tabel bevat meer informatie over de opties voor cloudverbindingen.

Cloudverbinding	Optie voor cloudverbinding	Weergavemodus	Ondersteunde actie op afstand	Beschikbaar voor
via NEAR	van Connect Client naar Connect Agent van Connect Client naar Quick Assist	Beheren Alleen bekijken	Extern bureaublad Hulp op afstand	beheerde workloads
via RDP	van Connect Client naar Connect Agent van webclient naar Connect Agent	Beheren	Extern bureaublad	beheerde workloads
via Schermdeling van Apple	van Connect Client naar Connect Agent	Beheren Alleen bekijken Verbergen	Extern bureaublad Hulp op afstand	beheerde workloads

De volgende tabel bevat meer informatie over de opties voor directe verbindingen.

Directe verbinding	Optie voor directe verbinding	Ondersteunde actie op afstand	Beschikbaar voor
via RDP	van Connect Client naar RDP-server	Extern bureaublad	onbeheerde workloads
via Schermdeling van Apple	van Connect Client naar Schermdelingsserver van Apple	Extern bureaublad Hulp op afstand	onbeheerde workloads

Schema's voor extern beheer

Schema's voor extern beheer zijn schema's die u toepast op de Bescherming-agent om de functionaliteit voor extern bureaublad en hulp op afstand in te schakelen en te configureren voor beheerde workloads.

Als er geen schema voor extern beheer wordt toegepast voor een workload, zijn de functies voor extern bureaublad en hulp op afstand alleen beschikbaar voor acties op afstand (opnieuw opstarten, afsluiten, in de slaapstand zetten, de prullenbak leegmaken en externe gebruiker afmelden).

Opmerking
De beschikbaarheid van de instellingen die u in het schema voor extern beheer kunt configureren, hangt af van het servicepakket dat is toegepast voor de tenant. Activeer het Advanced Management-pakket om toegang te krijgen tot alle instellingen. Zie "Ondersteunde functies van extern bureaublad en hulp op afstand" (p. 1058) voor meer informatie over de functies die deel uitmaken van het Standard- en Advanced Management-pakket.

Een schema voor extern beheer maken

U kunt een schema voor extern beheer maken en dit vervolgens toewijzen aan een workload om de functionaliteit voor extern bureaublad en hulp op afstand te configureren voor de beheerde workload.

Opmerking
De beschikbaarheid van de instellingen van het schema voor extern beheer hangt af van de servicequota die is toegewezen aan de tenant. Als u de standaardfunctionaliteit gebruikt, kunt u alleen verbindingen via RDP configureren.

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een schema voor extern beheer maken:

Vanuit Schema's voor extern beheer

1. Ga in de Cyber Protect-console naar **Beheer** > **Schema's voor extern beheer**.
2. Maak een schema voor extern beheer met een van de volgende twee opties.
   - Als er geen schema's voor extern beheer in de lijst worden weergegeven, klikt u op **Maken**.
   - Als er schema's voor extern beheer in de lijst worden weergegeven, klikt u op **Schema maken**.
3. [Optioneel] Als u de standaardnaam van het schema wilt wijzigen, klikt u op het potloodpictogram, voert u de naam van het schema in en klikt u op **Doorgaan**.
4. Klik op **Verbindingsprotocollen** en schakel de protocollen in die u beschikbaar wilt maken in dit schema voor extern beheer van externe verbindingen: NEAR, RDP of Schermdeling van Apple.
5. [Optioneel] Voor het NEAR-protocol: schakel in het gedeelte **Beveiligingsinstellingen** de selectievakjes in of uit om de bijbehorende instelling in of uit te schakelen en klik vervolgens op **Gereed**.

Instelling	Beschrijving	Beschikbaar voor
De workload vergrendelen wanneer de gebruiker de verbinding met de consolesessie verbreekt	Als u deze instelling selecteert, wordt de externe workload vergrendeld wanneer u de verbinding met de consolesessie verbreekt.	Windows, macOS
Slechts één gebruiker tegelijk toestaan om verbinding te maken met NEAR of bestanden over te dragen	Als u deze instelling selecteert, zijn verbindingen via NEAR en bestandsoverdrachten niet mogelijk zolang er een actieve externe verbinding met de workload is.	Windows, macOS, Linux
De workloadbeheerder toestaan verbinding te maken met elke sessie van gebruikers die geen beheerder zijn	Als u deze instelling selecteert, mag de beheerder verbinding maken met elke standaardgebruikerssessie voor de workload. Als zowel **De workloadbeheerder toestaan verbinding te maken met elke sessie van gebruikers die geen beheerder zijn** als **Het maken van systeemsessies toestaan** is uitgeschakeld, kunt u alleen verbinding maken met actieve	Windows, macOS

Instelling	Beschrijving	Beschikbaar voor
	beheerderssessies voor de externe macOS-workloads.	
Het maken van systeemsessies toestaan	Als u deze instelling selecteert, kan de beheerder externe verbindingen tot stand brengen in een nieuwe sessie in plaats van in een van de bestaande actieve sessies.	macOS
Klembordsynchronisatie toestaan	Als u deze instelling selecteert, kunt u gegevens overdragen tussen uw klembord en het klembord van de externe workload. U kunt bijvoorbeeld tekst uit een bestand in de externe workload kopiëren en in een bestand in uw workload plakken, en omgekeerd.	Windows, macOS, Linux

6. Klik op **Beveiligingsinstellingen**, schakel de selectievakjes in of uit om de bijbehorende instelling in of uit te schakelen en klik vervolgens op **Gereed**.

Instelling	Beschrijving
Weergeven of de workload extern wordt beheerd	Als u deze instelling selecteert, wordt er een melding weergegeven op het bureaublad van de externe workload wanneer de workload een actieve verbinding heeft met een extern bureaublad.
De gebruiker toestemming vragen om momentopnamen van de workload te maken	Als u deze instelling selecteert, krijgt de gebruiker van de externe workload een melding wanneer de beheerder verzoekt om momentopnamen van de workload over te dragen.

7. Klik op **Workloadbeheer**, selecteer de functies die u beschikbaar wilt maken voor de externe workloads en klik vervolgens op **Gereed**.

Instelling	Beschrijving	Beschikbaar voor
Bestandsoverdracht	Maakt bestandsoverdrachten tussen lokale en externe workloads mogelijk.	Windows, macOS, Linux

Instelling	Beschrijving	Beschikbaar voor
Overdracht van momentopname	Maakt het mogelijk om momentopnamen van het bureaublad van de externe workload over te dragen naar de Cyber Protect-console.	Windows, macOS, Linux

8. Klik op **Weergave-instellingen**, schakel de selectievakjes in of uit om de bijbehorende instelling in of uit te schakelen en klik vervolgens op **Gereed**.

Opmerking
Weergave-instellingen zijn alleen beschikbaar voor verbindingen via NEAR.

Instelling	Beschrijving	Beschikbaar voor
Bureaubladdeduplicatie gebruiken voor het vastleggen van bureaubladen	Bureaubladduplicatie is een van de methoden om schermen in Windows op te nemen. In sommige omgevingen kan deze functie instabiel zijn. Als u niet gebruikmaakt van Bureaubladduplicatie, kunt u de basismethode (BitBlt) gebruiken. Deze is veel langzamer, maar stabieler.	Windows
OpenCL-versnelling gebruiken	Met OpenCL-versnelling kan de adaptieve codec (gebruikt in de modus voor de kwaliteit **Balanced**) worden versneld door enkele berekeningen uit te voeren in de GPU (Graphics Processing Unit). Hiervoor moet een OpenCL-stuurprogramma worden geïnstalleerd in de externe Linux-eenheid. De adaptieve codec maakt gebruikt van OpenCL in macOS en Windows (indien beschikbaar in de grafische stuurprogramma's).	Linux
H.264-hardwarecodering	NEAR ondersteunt modi voor	Windows, macOS

Instelling	Beschrijving	Beschikbaar voor
gebruiken	drie kwaliteiten: **Smooth**, **Balanced** en **Sharp**. In de modus **Smooth** wordt H.264-hardwarecodering gebruikt om de bureaubladafbeelding te coderen. In de modus **Balanced** wordt adaptieve codec gebruikt. Deze levert volledige beeldkwaliteit in 32 bits, in tegenstelling tot de 'video'-modus die wordt gebruikt door H.264. De beeldkwaliteit wordt automatisch aangepast aan uw huidige netwerkomstandigheden en de huidige framesnelheid blijft behouden. In de modus **Sharp** wordt adaptieve codec gebruikt. Deze levert volledige beeldkwaliteit in 32 bits, in tegenstelling tot de 'video'-modus die wordt gebruikt door H.264. De beeldkwaliteit is altijd volledig, maar mogelijk met een lagere FPS (frames per seconde) als uw netwerk of processor/videokaart overbelast is.	

9. Als u wilt dat de informatie over de gebruikers die zich het laatst hebben aangemeld bij de workloads, zichtbaar is in de details van de workload, klikt u op **Toolbox**, selecteert u **Laatst aangemelde gebruikers weergeven** en klikt u vervolgens op **Gereed**.

   Zie "Zoek de laatst aangemelde gebruiker" (p. 387) voor meer informatie over de laatst aangemelde gebruikers.
10. [Optioneel] Workloads toevoegen aan het schema:
    a. Klik op **Workloads toevoegen**.
    b. Selecteer de workloads en klik vervolgens op **Toevoegen**.

c. Als er compatibiliteitsproblemen zijn die u wilt oplossen, volgt u de procedure zoals beschreven in "Compatibiliteitsproblemen met schema's voor extern beheer oplossen" (p. 1079).

11. Klik op **Maken**.

Vanuit Alle apparaten

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op de workload waarop u een schema voor extern beheer wilt toepassen.
3. Klik op **Beschermen** en klik vervolgens op **Schema toevoegen**.
4. Klik op **Schema maken** en selecteer **Beheer op afstand**.
5. [Optioneel] Als u de standaardnaam van het schema wilt wijzigen, klikt u op het potloodpictogram, voert u de naam van het schema in en klikt u op **Doorgaan**.
6. Klik op **Verbindingsprotocollen** en schakel de protocollen in die u beschikbaar wilt maken in dit schema voor extern beheer van externe verbindingen: NEAR, RDP of Schermdeling van Apple.
7. [Optioneel] Voor het NEAR-protocol: schakel in het gedeelte **Beveiligingsinstellingen** de selectievakjes in of uit om de bijbehorende instelling in of uit te schakelen en klik vervolgens op **Gereed**.

Instelling	Beschrijving	Beschikbaar voor
De workload vergrendelen wanneer de gebruiker de verbinding met de consolesessie verbreekt	Als u deze instelling selecteert, wordt de externe workload vergrendeld wanneer u de verbinding met de consolesessie verbreekt.	Windows, macOS
Slechts één gebruiker tegelijk toestaan om verbinding te maken met NEAR of bestanden over te dragen	Als u deze instelling selecteert, zijn verbindingen via NEAR en bestandsoverdrachten niet mogelijk zolang er een actieve externe verbinding met de workload is.	Windows, macOS, Linux
De workloadbeheerder toestaan verbinding te maken met elke sessie van gebruikers die geen beheerder zijn	Als u deze instelling selecteert, mag de beheerder verbinding maken met elke standaardgebruikerssessie voor de workload. Als zowel **De workloadbeheerder toestaan verbinding te**	Windows, macOS

Instelling	Beschrijving	Beschikbaar voor
	maken met elke sessie van gebruikers die geen beheerder zijn als **Het maken van systeemsessies toestaan** is uitgeschakeld, kunt u alleen verbinding maken met actieve beheerderssessies voor de externe macOS-workloads.	
Het maken van systeemsessies toestaan	Als u deze instelling selecteert, kan de beheerder externe verbindingen tot stand brengen in een nieuwe sessie in plaats van in een van de bestaande actieve sessies.	macOS
Klembordsynchronisatie toestaan	Als u deze instelling selecteert, kunt u gegevens overdragen tussen uw klembord en het klembord van de externe workload. U kunt bijvoorbeeld tekst uit een bestand in de externe workload kopiëren en in een bestand in uw workload plakken, en omgekeerd.	Windows, macOS, Linux

8. Klik op **Beveiligingsinstellingen**, schakel de selectievakjes in of uit om de bijbehorende instelling in of uit te schakelen en klik vervolgens op **Gereed**.

Instelling	Beschrijving
Weergeven of de workload extern wordt beheerd	Als u deze instelling selecteert, wordt er een melding weergegeven op het bureaublad van de externe workload wanneer de workload een actieve verbinding heeft met een extern bureaublad.
De gebruiker toestemming vragen om momentopnamen van de workload te maken	Als u deze instelling selecteert, krijgt de gebruiker van de externe workload een melding wanneer de beheerder verzoekt om momentopnamen van de workload over te dragen.

9. Klik op **Workloadbeheer**, selecteer de functies die u beschikbaar wilt maken voor de externe workloads en klik vervolgens op **Gereed**.

Instelling	Beschrijving	Beschikbaar voor
Bestandsoverdracht	Maakt bestandsoverdrachten tussen lokale en externe workloads mogelijk.	Windows, macOS, Linux
Overdracht van momentopname	Maakt het mogelijk om momentopnamen van het bureaublad van de externe workload over te dragen naar de Cyber Protect-console.	Windows, macOS, Linux

10. Klik op **Weergave-instellingen**, schakel de selectievakjes in of uit om de bijbehorende instelling in of uit te schakelen en klik vervolgens op **Gereed**.

Opmerking
Weergave-instellingen zijn alleen beschikbaar voor verbindingen via NEAR.

Instelling	Beschrijving	Beschikbaar voor
Bureaubladdeduplicatie gebruiken voor het vastleggen van bureaubladen	Bureaubladduplicatie is een van de methoden om schermen in Windows op te nemen. In sommige omgevingen kan deze functie instabiel zijn. Als u niet gebruikmaakt van Bureaubladduplicatie, kunt u de basismethode (BitBlt) gebruiken. Deze is veel langzamer, maar stabieler.	Windows
OpenCL-versnelling gebruiken	Met OpenCL-versnelling kan de adaptieve codec (gebruikt in de modus voor de kwaliteit **Balanced**) worden versneld door enkele berekeningen uit te voeren in de GPU (Graphics Processing Unit). Hiervoor moet een OpenCL-stuurprogramma worden geïnstalleerd in de externe Linux-eenheid. De adaptieve codec maakt	Linux

Instelling	Beschrijving	Beschikbaar voor
	gebruikt van OpenCL in macOS en Windows (indien beschikbaar in de grafische stuurprogramma's).	
H.264-hardwarecodering gebruiken	NEAR ondersteunt modi voor drie kwaliteiten: **Smooth**, **Balanced** en **Sharp**. In de modus **Smooth** wordt H.264-hardwarecodering gebruikt om de bureaubladafbeelding te coderen. In de modus **Balanced** wordt adaptieve codec gebruikt. Deze levert volledige beeldkwaliteit in 32 bits, in tegenstelling tot de 'video'-modus die wordt gebruikt door H.264. De beeldkwaliteit wordt automatisch aangepast aan uw huidige netwerkomstandigheden en de huidige framesnelheid blijft behouden. In de modus **Sharp** wordt adaptieve codec gebruikt. Deze levert volledige beeldkwaliteit in 32 bits, in tegenstelling tot de 'video'-modus die wordt gebruikt door H.264. De beeldkwaliteit is altijd volledig, maar mogelijk met een lagere FPS (frames per seconde) als uw netwerk of processor/videokaart overbelast is.	Windows, macOS

11. Als u wilt dat de informatie over de gebruikers die zich het laatst hebben aangemeld bij de workloads, zichtbaar is in de details van de workload, klikt u op **Toolbox**, selecteert u **Laatst aangemelde gebruikers weergeven** en klikt u vervolgens op **Gereed**.
    Zie "Zoek de laatst aangemelde gebruiker" (p. 387) voor meer informatie over de laatst aangemelde gebruikers.

12. Klik op **Maken**.

Een workload toevoegen aan een schema voor extern beheer

Afhankelijk van uw behoeften kunt u workloads toevoegen aan een schema voor extern beheer nadat het schema is gemaakt.

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een workload toevoegen aan een schema voor extern beheer:

Vanuit Schema's voor extern beheer

1. Ga in de Cyber Protect-console naar **Beheer** > **Schema's voor extern beheer**.
2. Klik op het schema voor extern beheer.
3. Doe vervolgens het volgende (al naargelang het schema al dan niet is toegepast op een workload):
   - Als het schema nog niet is toegepast op workloads: klik op **Workloads toevoegen**.
   - Als het schema al is toegepast op workloads: klik op **Workloads beheren**.
4. Selecteer een workload in de lijst en klik vervolgens op **Toevoegen**.
5. Klik op **Opslaan**.
6. Klik op **Bevestigen** om de vereiste servicequota toe te voegen aan de workload.

Vanuit Alle apparaten

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op de workload waarop u een schema voor extern beheer wilt toepassen.
3. Klik op **Beschermen** en klik vervolgens op **Schema toevoegen**.
4. Ga naar **Selecteer een schema in onderstaande lijst** en selecteer de optie **Extern beheer** als u alleen de schema's voor extern beheer wilt bekijken.
5. Klik op **Toepassen**.
6. Klik op **Bevestigen** om de vereiste servicequota toe te voegen aan de workload.

Workloads verwijderen uit een schema voor extern beheer

Indien gewenst kunt u workloads beheer verwijderen uit een schema voor extern beheer.

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Workloads verwijderen uit een schema voor extern beheer:

1. Ga in de Cyber Protect-console naar **Beheer** > **Schema's voor extern beheer**.
2. Klik op het schema voor extern beheer.
3. Klik op **Workloads beheren**.
4. Selecteer een of meerdere workloads die u wilt verwijderen uit het schema voor extern beheer en klik vervolgens op **Verwijderen**.
5. Klik op **Gereed**.
6. Klik op **Opslaan**.

Aanvullende acties met bestaande plannen voor extern beheer

Vanuit het scherm **Plannen voor extern beheer** kunt u de volgende aanvullende acties uitvoeren met plannen voor extern beheer: details, activiteiten en waarschuwingen bekijken, namen wijzigen en items bewerken, inschakelen, uitschakelen, klonen, exporteren, verwijderen, instellen als favoriet en instellen als standaard.

Details weergeven

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

De details van een schema voor extern beheer bekijken

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Details weergeven**.

Bewerken

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een schema bewerken:

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Bewerken**.

Activiteiten

De activiteiten voor een schema voor extern beheer bekijken

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Activiteiten**.
3. Klik op een activiteit om meer details te bekijken.

Waarschuwingen

De waarschuwingen bekijken:

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Waarschuwingen**.

Naam wijzigen

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

De naam van een schema voor extern beheer wijzigen

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Naam wijzigen**.
3. Voer de nieuwe naam van het schema in en klik vervolgens op **Doorgaan**.

Inschakelen

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een schema voor extern beheer inschakelen

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Inschakelen**.

Uitschakelen

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een schema voor extern beheer uitschakelen

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Uitschakelen**.

Klonen

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een plan voor extern beheer klonen:

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Klonen**.
3. Klik op **Maken**.

Exporteren

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een plan voor extern beheer exporteren:

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Exporteren**.
   De planconfiguratie wordt geëxporteerd in een JSON-indeling naar de lokale machine.

Instellen als standaard

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een plan voor extern beheer instellen als standaard:

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Instellen als standaard**.
3. Klik in het bevestigingsvenster op **Instellen**.
   In het scherm **Plannen voor extern beheer** wordt de tag **Standaard** weergegeven naast de naam van het plan.

Instellen als favoriet

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een plan voor extern beheer instellen als favoriet

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Toevoegen aan favorieten**.
   In het scherm **Plannen voor extern beheer** wordt een pictogram van een ster weergegeven naast de naam van het plan.

Verwijderen

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een schema voor extern beheer verwijderen

1. Klik in het scherm **Plannen voor extern beheer** op het pictogram **Meer acties** van het plan voor extern beheer.
2. Klik op **Verwijderen**.
3. Selecteer **Ik bevestig** en klik vervolgens op **Verwijderen**.

Compatibiliteitsproblemen met schema's voor extern beheer

In sommige gevallen kunnen compatibiliteitsproblemen optreden wanneer u een schema voor extern beheer toepast op een workload. De volgende compatibiliteitsproblemen kunnen voorkomen:

- Conflicterende schema's: dit probleem doet zich voor wanneer er al een ander schema voor extern beheer is toegepast op de workload (er kan slechts één schema voor extern beheer worden toegepast op een workload).
- Incompatibel besturingssysteem: dit probleem doet zich voor wanneer het besturingssysteem van de workload niet wordt ondersteund.
- Niet-ondersteunde agent: dit probleem doet zich voor wanneer de versie van de beveiligingsagent voor de workload verouderd is en geen ondersteuning biedt voor de functionaliteit van extern bureaublad.
- Onvoldoende quota: dit probleem doet zich voor wanneer de tenant onvoldoende servicequota heeft om aan de geselecteerde workloads toe te wijzen.

Als het schema voor extern beheer wordt toegepast op maximaal 150 afzonderlijk geselecteerde workloads, wordt u gevraagd de bestaande conflicten op te lossen voordat u het schema opslaat. U kunt een conflict oplossen door de hoofdoorzaak ervan weg te nemen of door de betreffende workloads te verwijderen uit het schema. Zie "Compatibiliteitsproblemen met schema's voor extern beheer oplossen" (p. 1079) voor meer informatie. Als u het schema opslaat zonder de conflicten op te lossen, wordt het automatisch uitgeschakeld voor de incompatibele workloads en worden er waarschuwingen weergegeven.

Als het schema voor extern beheer wordt toegepast op meer dan 150 workloads of op apparaatgroepen, wordt het eerst opgeslagen en vervolgens gecontroleerd op compatibiliteit. Het schema wordt automatisch uitgeschakeld voor de incompatibele workloads en er worden waarschuwingen weergegeven.

Compatibiliteitsproblemen met schema's voor extern beheer oplossen

Bij het maken van een nieuw schema voor extern beheer kunt u verschillende acties uitvoeren om compatibiliteitsproblemen op te lossen, al naargelang de oorzaak van de problemen.

Opmerking
Wanneer u een compatibiliteitsprobleem oplost door workloads te verwijderen uit een schema, dan is het niet mogelijk de workloads te verwijderen die deel uitmaken van een apparaatgroep.

Compatibiliteitsproblemen oplossen:

1. Klik op **Problemen bekijken**.
2. [Compatibiliteitsproblemen met bestaande schema's voor extern beheer oplossen door workloads te verwijderen uit het nieuwe schema]
   a. Ga naar het tabblad **Conflicterende schema's** en selecteer de workloads die u wilt verwijderen.
   b. Klik op **Workloads verwijderen uit schema**.
   c. Klik op **Verwijderen** en vervolgens op **Sluiten**.
3. [Compatibiliteitsproblemen met schema's voor extern beheer oplossen door de schema's uit te schakelen die al zijn toegepast voor de workloads]
   a. Klik op **Toegepaste schema's uitschakelen**.
   b. Klik op **Uitschakelen** en klik vervolgens op **Sluiten**.
4. [Compatibiliteitsproblemen met incompatibele besturingssystemen oplossen]
   a. Ga naar het tabblad **Niet-compatibel besturingssysteem** en selecteer de workloads die u wilt verwijderen.
   b. Klik op **Workloads verwijderen uit schema**.
   c. Klik op **Verwijderen** en vervolgens op **Sluiten**.
5. [Compatibiliteitsproblemen met niet-ondersteunde agents oplossen door workloads te verwijderen uit het schema]
   a. Ga naar het tabblad **Niet-ondersteunde agents** en selecteer de workloads die u wilt verwijderen.
   b. Klik op **Workloads verwijderen uit schema**.
   c. Klik op **Verwijderen** en vervolgens op **Sluiten**.
6. [Compatibiliteitsproblemen met niet-ondersteunde agents oplossen door de agentversie bij te werken] Klik op **Ga naar lijst met agents**.

   Opmerking
   Deze optie is alleen beschikbaar voor klantbeheerders.

7. [Compatibiliteitsproblemen met onvoldoende quota oplossen door workloads te verwijderen uit het schema]
   a. Ga naar het tabblad **Onvoldoende quota** en selecteer de workloads die u wilt verwijderen.
   b. Klik op **Workloads verwijderen uit schema**.
   c. Klik op **Verwijderen** en vervolgens op **Sluiten**.
8. [Compatibiliteitsproblemen met onvoldoende quota oplossen door de quota van de tenant te verhogen]

   Opmerking
   Deze optie is alleen beschikbaar voor partnerbeheerders.

   a. Klik op het tabblad **Onvoldoende quota** op **Ga naar de beheerportal**.
   b. Verhoog de servicequota voor de klant.

Referenties voor workload

U kunt referenties (gebruikersnaam en wachtwoord of VNC-wachtwoord) voor beheerders en anderen toevoegen, deze opslaan in de cloudopslag voor referenties en ze vervolgens gebruiken voor automatische verificatie wanneer u verbinding maakt met de workloads die u beheert. Op die manier hoeft u de referenties niet elke keer handmatig in te voeren tijdens de verificatiestap van de verbinding, maar kunt u ze eenmalig toevoegen aan de referentieopslag en ze toewijzen aan meerdere workloads. De Connect Client zal deze referenties vervolgens elke keer gebruiken wanneer u op afstand verbinding wilt maken met de workloads.

Opmerking
De referenties die zijn opgeslagen in de referentieopslag worden niet gedeeld tussen verschillende tenantniveaus. Ze worden alleen gedeeld op hetzelfde tenantniveau voor dezelfde klanttenant of partnertenant.

Dus als een klanttenant meerdere beheerders heeft, ziet en deelt de klanttenant de referenties in de referentieopslag, terwijl andere partnerbeheerders of klantbeheerders van andere tenants deze referenties niet kunnen bekijken of gebruiken.

Referenties toevoegen

U kunt referenties toevoegen en deze vervolgens gebruiken voor externe verbindingen met meerdere workloads.

Referenties toevoegen aan een workload en deze opslaan in de referentieopslag

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op de workload waarvoor u referenties wilt toevoegen.
3. Open het menu **Instellingen** op een van de volgende manieren:

- Klik op **Extern bureaublad** en vervolgens op **Instellingen**.
- Klik op **Beheren** en vervolgens op **Instellingen**.

4. Klik op **Referenties toevoegen**.
5. Klik in **Referentieopslag** op **Referenties toevoegen**.
6. Voer de referenties in.

Veld	Beschrijving
Naam van referenties	Id van de referenties die zichtbaar zijn in de referentieopslag.
Gebruikersnaam	Gebruikersnaam die wordt gebruikt voor externe verbindingen met de doelworkload.
Wachtwoord	Wachtwoord dat wordt gebruikt voor externe verbindingen met de doelworkload.
VNC-wachtwoord	Dit veld is alleen beschikbaar voor Schermdeling van Apple.

7. Klik op **Opslaan**.

Referenties toewijzen aan een workload

Wanneer u referenties hebt toegevoegd, kunt u deze gebruiken om automatisch te verifiëren wanneer u verbinding maakt met een door u beheerde workload.

Opgeslagen referenties voor automatische verificatie toewijzen aan een workload

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Open het menu **Instellingen** op een van de volgende manieren:
   - Klik op **Extern bureaublad** en vervolgens op **Instellingen**.
   - Klik op **Beheren** en vervolgens op **Instellingen**.
3. Open het tabblad van het ondersteunde protocol (NEAR, RDP of Schermdeling van Apple) en klik op **Referenties toevoegen**.
4. Ga naar **Referentieopslag**, selecteer de referenties in de lijst en klik vervolgens op **Referenties selecteren**.

Referenties verwijderen

Referenties die u niet meer nodig hebt, kunt u verwijderen.

Referenties verwijderen uit de referentieopslag:

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Open het menu **Instellingen** op een van de volgende manieren:

- Klik op **Extern bureaublad** en vervolgens op **Instellingen**.
- Klik op **Beheren** en vervolgens op **Instellingen**.

3. Open het tabblad van het ondersteunde protocol (NEAR, RDP of Schermdeling van Apple) en klik op **Verwijderen**.
4. Klik in het bevestigingsvenster op **Verwijderen**.

Toewijzing van referenties voor een workload ongedaan maken

U kunt de toewijzing van referenties voor een workload ongedaan maken, maar ze toch in de referentieopslag bewaren.

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Open het menu **Instellingen** op een van de volgende manieren:
   - Klik op **Extern bureaublad** en vervolgens op **Instellingen**.
   - Klik op **Beheren** en vervolgens op **Instellingen**.
3. Open het tabblad van het ondersteunde protocol (NEAR, RDP of Schermdeling van Apple) en klik op **Toewijzing ongedaan maken**.
4. Klik in het bevestigingsvenster op **Toewijzing ongedaan maken**.

Werken met beheerde workloads

Beheerde workloads zijn workloads waarvoor de Bescherming-agent is geïnstalleerd.

U kunt de volgende acties uitvoeren voor de externe beheerde workloads:

- verbinding maken via NEAR voor hulp op afstand of extern bureaublad in de modus Besturen of Alleen bekijken
- verbinding maken via RDP voor extern bureaublad in de modus Besturen
- verbinding maken via Schermdeling van Apple voor hulp op afstand of extern bureaublad in de modus Besturen, Alleen bekijken of Verbergen (Gordijn)
- verbinding maken via een webclient voor extern bureaublad
- opnieuw opstarten, afsluiten, in de slaapstand zetten, de prullenbak leegmaken, externe gebruiker afmelden van de externe workloads
- bestanden overdragen tussen uw workload en de externe workloads
- controles uitvoeren via momentopnamen

Opmerking
Voor verbindingen tussen extern bureaublad en beheerde workloads moet een Bescherming-agent worden geïnstalleerd en moet een schema voor extern beheer worden toegepast op de workload.

RDP-instellingen configureren

U kunt de instellingen configureren die automatisch worden toegepast op RDP-verbindingen met externe besturing voor de beheerde workload.

De RDP-instellingen van een workload configureren

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Open het menu **Instellingen** op een van de volgende manieren:
   - Klik op **Extern bureaublad** en vervolgens op **Instellingen**.
   - Klik op **Beheren** en vervolgens op **Instellingen**.
3. Configureer de instellingen op het tabblad **RDP**.

Instelling	Beschrijving
Audio afspelen	Met deze instelling schakelt u in of uit dat het geluid voor de externe workload wordt omgeleid naar uw lokale workload.
Audio opnemen	Deze instelling bepaalt of audio-opname (spreken in de microfoon) wordt overgedragen naar de externe workload.
Printers omleiden	Als u deze instelling selecteert, zijn de printers van uw workload beschikbaar voor de externe workload.
Bestanden omleiden	Deze instelling definieert of bestanden van uw lokale workload worden gedeeld met een externe workload.
Kleurdiepte	Deze instelling bepaalt hoeveel kleuren in een afbeelding worden overgedragen via RDP. Hoe hoger de waarde, hoe meer bandbreedte is vereist. **Hoge kleur**: 16 bits **Ware kleur**: • 24 bits voor RDP-verbindingen via de webclient • 32 bits voor RDP-verbindingen via Connect Client

4. Klik op de knop Sluiten.

Verbinding maken met beheerde workloads voor een extern bureaublad of voor hulp op afstand

Opmerking
De beschikbaarheid van de verbindingsprotocollen die u kunt gebruiken voor externe verbindingen, hangt af van de configuratie van het schema voor extern beheer en van het besturingssysteem van de externe workload.

Vereisten

- Een schema voor extern beheer met ingeschakeld verbindingsprotocol wordt toegepast op de beheerde workload.
- De vereiste servicequota is toegewezen aan de workload. (De servicequota wordt automatisch opgehaald wanneer u een schema voor extern beheer toepast op de workload.)
- [Voor verbindingen via Schermdeling van Apple]: Schermdeling van Apple is ingeschakeld voor de macOS-workload.
- 2FA is ingeschakeld voor uw gebruikersaccount op Acronis Cyber Protect Cloud.

Op afstand verbinding maken met een beheerde workload voor extern bureaublad of voor hulp op afstand:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik op de workload waarmee u verbinding wilt maken.
3. Klik op **Extern bureaublad**.
   Standaard is NEAR geselecteerd als verbindingsprotocol.
4. [Optioneel] Open de vervolgkeuzelijst **Verbindingsprotocol** en selecteer het verbindingsprotocol dat u wilt gebruiken.
5. Klik op de weergavemodus die u wilt gebruiken.

Protocol	Externe verbindingen naar	Weergavemodus	Ondersteunde actie op afstand
NEAR	Windows Linux macOS	**Beheren**: in deze modus kunt u de externe workload bekijken en uitvoeren. **Alleen bekijken**: in deze modus kunt u de externe workload alleen bekijken.	Extern bureaublad Hulp op afstand
RDP	Windows	**Beheren**: in deze modus kunt u bewerkingen voor de externe workload bekijken en uitvoeren.	Extern bureaublad

Protocol	Externe verbindingen naar	Weergavemodus	Ondersteunde actie op afstand
		Opmerking Als de RDP-functie is uitgeschakeld in de OS-instellingen van de workload, wordt er een pop-up weergegeven. Gebruik dit venster om RDP in te schakelen voor de workload voor de huidige sessie of in het algemeen: • Als u RDP voor deze workload alleen wilt inschakelen voor de huidige sessie, selecteert u **Uitschakelen nadat de sessie is afgelopen** en klikt u vervolgens op **Toestaan**. • Als u RDP wilt inschakelen voor deze workload, klikt u op **Toestaan**.	
Schermdeling van Apple	macOS	**Beheren**: in deze modus kunt u de externe workload bekijken en uitvoeren. **Alleen bekijken**: in deze modus kunt u de externe workload alleen bekijken. **Verbergen**: alleen beschikbaar voor macOS-workloads. Als u verbinding maakt met de externe workload in de modus Verbergen, wordt de weergave van de externe workload gedimd, zodat de externe gebruiker uw acties voor de workload niet kan zien.	Extern bureaublad Hulp op afstand

6. Doe vervolgens het volgende (al naargelang Connect Client al dan niet is geïnstalleerd voor uw workload):
   - Als Connect Client niet is geïnstalleerd: download de toepassing, installeer deze en selecteer **Toestaan** in de bevestigingspop-up die wordt weergegeven.
   - Als Connect Client al is geïnstalleerd: klik op **Connect Client openen** in de bevestigingspop-up die wordt weergegeven.
7. Selecteer in het venster **Verificatie** een verificatieoptie en geef vervolgens de vereiste referenties op.

Opmerking
Als u referenties hebt toegewezen aan de workload, wordt de verificatie automatisch uitgevoerd en wordt deze stap overgeslagen. Zie "Referenties toewijzen aan een workload" (p. 1081) voor meer informatie.

Verificatieoptie	Beschrijving
Met referenties voor externe workload	U mag de externe verbinding tot stand brengen nadat u de gebruikersnaam en het wachtwoord van een beheerder voor de externe workload hebt opgegeven. Deze optie is beschikbaar voor NEAR, RDP en Schermdeling van Apple. U kunt deze optie gebruiken om uw identiteit te verifiëren voor extern bureaublad en hulp op afstand.
Toestemming vragen om te bekijken	U mag de externe verbinding tot stand brengen in de modus Bekijken nadat dit is toegestaan door de gebruiker die is aangemeld bij de externe workload. Deze optie is beschikbaar voor NEAR en Schermdeling van Apple. U kunt deze optie gebruiken om uw identiteit te verifiëren voor hulp op afstand.
Toestemming vragen om te besturen	U mag de externe verbinding tot stand brengen in de modus Besturen nadat dit is toegestaan door de gebruiker die is aangemeld bij de externe workload. Deze optie is beschikbaar voor NEAR en Schermdeling van Apple. U kunt deze optie gebruiken om uw identiteit te verifiëren voor hulp op afstand.

8. Klik op **Verbinden** en klik vervolgens op de sessie die u wilt weergeven (als er meer dan één gebruikerssessie beschikbaar is voor de workload).
   In Connect Client wordt een nieuw viewervenster geopend waarin u het bureaublad van de externe workload kunt zien. De viewer heeft een werkbalk met aanvullende acties die u kunt uitvoeren voor de externe workload nadat de externe verbinding tot stand is gebracht. Zie "De werkbalk in het viewervenster gebruiken" (p. 1095) voor meer informatie.

Verbinding maken met een beheerde workload via een webclient

U kunt een webclient gebruiken om verbinding met een extern bureaublad te maken voor een beheerde workload.

Vereisten

- Standaardservicequota is toegewezen aan de workload.
- Een schema voor extern beheer waarvoor RDP is ingeschakeld, wordt toegepast op de beheerde workload.

- RDP is ingeschakeld voor de beheerde workload.
- Uw browser ondersteunt HTML5.
- 2FA is ingeschakeld voor uw gebruikersaccount op Acronis Cyber Protect Cloud.

Een webclient gebruiken om op afstand verbinding te maken met een workload:

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op de workload waarmee u op afstand verbinding wilt maken en klik vervolgens op **Extern bureaublad** > **Verbinden via webclient**.
3. Voer de gebruikersnaam en het wachtwoord in om toegang te krijgen tot de workload en klik vervolgens op **Verbinden**.

> **Opmerking**
> Als u referenties hebt toegewezen aan de workload, wordt de verificatie automatisch uitgevoerd en wordt deze stap overgeslagen. Zie "Referenties toewijzen aan een workload" (p. 1081) voor meer informatie.

Bestanden overdragen

U kunt eenvoudig bestanden overdragen tussen de lokale workload en een beheerde workload.

Vereisten

- Een schema voor extern beheer met het NEAR-protocol en ingeschakelde functie voor bestandsoverdracht wordt toegepast op de workload.
- De quota voor Advanced Management wordt toegepast op de workload.
- 2FA is ingeschakeld voor uw gebruikersaccount op Acronis Cyber Protect Cloud.

Bestanden op afstand overdragen tussen uw workload en een beheerde workload

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik op de workload waarvoor u bestanden wilt overdragen.
3. Klik op **Beheren** en vervolgens op **Bestanden overdragen**.
4. Doe vervolgens het volgende (al naargelang Connect Client al dan niet is geïnstalleerd voor uw workload):
   - Als Connect Client niet is geïnstalleerd, downloadt en installeert u deze toepassing en klikt u in de bevestigingspop-up op **Toestaan**.
   - Als Connect Client al is geïnstalleerd: klik op **Connect Client openen** in de bevestigingspop-up die wordt weergegeven.
5. Selecteer in het venster **Verificatie** een verificatieoptie en geef vervolgens de vereiste referenties op.

Verificatieoptie	Beschrijving
Met referenties voor externe workload	U mag de externe verbinding tot stand brengen nadat u de gebruikersnaam en het wachtwoord van een beheerder voor de externe workload hebt opgegeven.
Toestemming vragen voor bestandsoverdracht	U mag bestanden overdragen nadat dit is toegestaan door de gebruiker die is aangemeld bij de externe workload.

6. Blader in het venster **Bestandsoverdracht** door bestanden en sleep ze naar de gewenste bestemming.

   Opmerking
   De bestanden van de lokale workload worden weergegeven in het linkerdeelvenster en de bestanden van de externe workload worden weergegeven in het rechterdeelvenster.
   Wanneer een bestandsoverdracht begint, wordt deze vermeld in het deelvenster **Taken**.

7. [Optioneel] Als u de voltooide taken uit het deelvenster **Taken** wilt verwijderen, klikt u op **Voltooide items wissen**.
8. Sluit het venster wanneer alle overdrachten zijn voltooid.

Besturingsacties uitvoeren voor beheerde workloads

U kunt een externe workload beheren via de volgende basisbesturingsacties: de prullenbak leegmaken, in de slaapstand zetten, opnieuw opstarten, afsluiten en externe gebruiker afmelden.

Vereisten

- Standaardservicequota wordt toegepast op de workload.
- 2FA is ingeschakeld voor uw gebruikersaccount op Acronis Cyber Protect Cloud.

Prullenbak leegmaken

De prullenbak voor de externe workload leegmaken:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik op de workload waarvoor u deze actie wilt uitvoeren.
3. Klik op **Beheren** en klik vervolgens op **Prullenbak leegmaken**.
4. Selecteer de gebruikerssessie waarvoor u deze actie wilt uitvoeren en klik vervolgens op **Prullenbak leegmaken**.

Slaapstand

Externe workload in de slaapstand zetten:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik op de workload waarvoor u deze actie wilt uitvoeren.
3. Klik op **Beheren** en klik vervolgens op **Slaapstand**.

Opnieuw opstarten

Een externe workload opnieuw opstarten:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik op de workload waarvoor u deze actie wilt uitvoeren.
3. Klik op **Beheren** en klik vervolgens op **Opnieuw opstarten**.
   - Voor Windows-workloads: selecteer of de gebruiker die momenteel lokaal is aangemeld bij de workload, de wijzigingen mag opslaan voordat de workload opnieuw wordt opgestart. Selecteer vervolgens de gebruiker en klik opnieuw op **Opnieuw opstarten**.
   - Voor macOS-workloads: selecteer of de gebruiker die momenteel lokaal is aangemeld bij de workload, de wijzigingen mag opslaan voordat de workload opnieuw wordt opgestart. Klik vervolgens opnieuw op **Opnieuw opstarten**.
   - Voor Linux-workloads: klik op **Opnieuw opstarten**.

Afsluiten

Een externe workload afsluiten:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik op de workload waarvoor u deze actie wilt uitvoeren.
3. Klik op **Beheren** en klik vervolgens op **Afsluiten**.
   - Voor Windows-workloads: selecteer of de gebruiker die momenteel lokaal is aangemeld bij de workload, de wijzigingen mag opslaan voordat de workload wordt afgesloten. Selecteer vervolgens de gebruiker en klik opnieuw op **Afsluiten**.
   - Voor macOS-workloads: selecteer of de gebruiker die momenteel lokaal is aangemeld bij de workload, de wijzigingen mag opslaan voordat de workload wordt afgesloten. Klik vervolgens opnieuw op **Afsluiten**.
   - Voor Linux-workloads: klik opnieuw op **Afsluiten**.

Externe gebruiker afmelden

De gebruiker afmelden bij een externe workload:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik op de workload waarvoor u deze actie wilt uitvoeren.
3. Klik op **Beheren** en klik vervolgens op **Externe gebruiker afmelden**.
4. Selecteer de gebruiker die u wilt afmelden en klik vervolgens op **Afmelden**.

Workloads controleren via overdracht van momentopnamen

U kunt de status van een workload controleren via de functie voor de overdracht van momentopnamen.

Vereisten

- Op de workload wordt een schema voor extern beheer toegepast waarbij de functie voor het verzenden van momentopnamen is ingeschakeld.
- De versie van de beveiligingsagent is up-to-date en ondersteunt de functie voor de overdracht van momentopnamen.
- De servicequota voor Advanced Management wordt toegepast op de workload.
- De workload is online.
- 2FA is ingeschakeld voor uw gebruikersaccount op Acronis Cyber Protect Cloud.

Een workload controleren via overdracht van momentopnamen

Een workload controleren via overdracht van momentopnamen:

1. Ga in de Cyber Protect-console naar **Apparaten**>**Overdracht van momentopname**.
2. Klik op de workload die u wilt controleren.
3. Selecteer de gebruikerssessie.
4. Selecteer de weergave.
5. Selecteer de vernieuwingsfrequentie waarmee u een nieuwe momentopname van het bureaublad wilt maken.
6. Selecteer de beeldkwaliteit.
7. Klik op het downloadpictogram om de momentopname te downloaden.

Een momentopname maken van een workload

Een momentopname maken van een beheerde workload:

1. Ga in de Cyber Protect-console naar **Apparaten** > **Machines met agents**.
2. Klik op de workload waarvan u een momentopname wilt maken.
3. Klik op **Beheren** en klik vervolgens op **Schermopname van bureaublad maken**.
   Het scherm **Overdracht van momentopname** wordt geopend. De workload is hierin al vooraf geselecteerd. U ziet de momentopname of u ziet de momentopname nadat de gebruiker van de externe workload de aanvraag heeft goedgekeurd (dit hangt af van de instellingen van het schema voor extern beheer dat wordt toegepast op de workload).

Meerdere beheerde workloads tegelijk bekijken

U kunt de bureaubladen van meerdere externe workloads tegelijkertijd bekijken in één venster.

Opmerking
Het aantal bureaubladen dat u tegelijkertijd kunt zien in het venster, hangt af van de grootte van uw monitor.

Vereisten

- NEAR / Apple Schermdeling is ingeschakeld in de schema's voor extern beheer die worden toegepast op de workloads.
- De servicequota voor Advanced Management wordt toegepast op de workload.
- 2FA is ingeschakeld voor uw gebruikersaccount op Acronis Cyber Protect Cloud.

Meerdere workloads tegelijk bekijken:

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer de workloads die u wilt bekijken.
3. Klik op **Multiweergave**.
4. Doe vervolgens het volgende (al naargelang Connect Client al dan niet is geïnstalleerd voor uw workload):
   - Als Connect Client niet is geïnstalleerd: download de toepassing, installeer deze en selecteer **Toestaan** in de bevestigingspop-up die wordt weergegeven.
   - Als Connect Client al is geïnstalleerd: klik op **Connect Client openen** in de bevestigingspop-up die wordt weergegeven.
5. Selecteer in het venster **Verificatie** een verificatieoptie en geef vervolgens de vereiste referenties op.

Verificatieoptie	Beschrijving
Met referenties voor externe workload	U mag de externe verbinding tot stand brengen nadat u de gebruikersnaam en het wachtwoord van een beheerder voor de externe workload hebt opgegeven.
Toestemming vragen om te bekijken	U mag de externe verbinding tot stand brengen in de modus Kijken nadat dit is toegestaan door de gebruiker die is aangemeld bij de externe workload.

6. Als u dezelfde verificatiemethode en referenties wilt gebruiken voor de verbinding met alle externe workloads die u in stap 2 hebt geselecteerd, selecteert u **Gebruiken op andere computers**.
7. Klik op **Verbinden**.
   In de werkbalk van het venster voor multiweergave kunt u een weergavemodus selecteren om verbinding te maken met een workload. Met deze actie wordt een apart viewervenster voor die workload geopend.

Opmerking

Als een van de geselecteerde workloads offline is of als er een verouderde versie van de agent is geïnstalleerd, wordt deze niet weergegeven in het venster voor multiweergave.

Alle verbindingen met externe workloads in de multiweergave worden weergegeven in de modus **Alleen bekijken**.

Werken met onbeheerde workloads

Onbeheerde workloads zijn workloads waarvoor de Bescherming-agent niet is geïnstalleerd.

U kunt de volgende acties uitvoeren voor de externe onbeheerde workloads:

- verbinding maken via Acronis Quick Assist voor hulp op afstand
- verbinding maken via een IP-adres voor extern bureaublad of hulp op afstand
- bestanden overdragen tussen uw workload en de externe workload via Quick Assist

Opmerking

Als u op afstand verbinding wilt maken met onbeheerde workloads via Quick Assist, moet u het volgende controleren:

- Het Advanced Management-pakket is geactiveerd voor uw klanttenant.
- De toepassing Quick Assist wordt uitgevoerd op de externe workload waarmee u verbinding wilt maken.

Verbinding maken met onbeheerde workloads via Acronis Quick Assist

U kunt de Quick Assist-functie gebruiken om op aanvraag een externe verbinding te maken met onbeheerde workloads en eenmalige hulp te bieden.

Vereisten

- Het Advanced Management-pakket is toegewezen aan uw klanttenant.
- 2FA is ingeschakeld voor uw gebruikersaccount op Acronis Cyber Protect Cloud.
- De externe gebruiker heeft de workload-id en toegangscode van Quick Assist opgegeven.
- De externe gebruiker heeft Acronis Quick Assist gedownload en uitgevoerd.

Verbinding maken met een workload voor hulp op afstand via Quick Assist:

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op **Quick Assist**.
3. Voer in het venster **Quick Assist** de workload-id in die is opgegeven door de eindgebruiker en selecteer vervolgens **Verbinden**.

4. Klik op **Verbinden**.
5. Doe vervolgens het volgende (al naargelang Connect Client al dan niet is geïnstalleerd voor uw workload):
   - Als Connect Client niet is geïnstalleerd: download de toepassing, installeer deze en selecteer **Toestaan** in de bevestigingspop-up die wordt weergegeven.
   - Als Connect Client al is geïnstalleerd: klik op **Connect Client openen** in de bevestigingspop-up die wordt weergegeven.
6. Ga naar het venster **Verificatie** en voer de toegangscode in.
7. In Connect Client wordt een nieuw viewervenster geopend waarin u het bureaublad van de externe workload kunt zien. De viewer heeft een werkbalk met aanvullende acties die u kunt uitvoeren voor de externe workload nadat de externe verbinding tot stand is gebracht. Zie "De werkbalk in het viewervenster gebruiken" (p. 1095) voor meer informatie.

Verbinding maken met onbeheerde workloads via IP-adres

Als er een onbeheerde workload is in uw LAN, kunt u het IP-adres gebruiken om hiermee verbinding te maken voor externe besturing of hulp of afstand. Voor deze verbinding is geen internettoegang vereist.

Vereisten

- Het Advanced Management-pakket is toegewezen aan uw klanttenant.
- 2FA is ingeschakeld voor uw gebruikersaccount op Acronis Cyber Protect Cloud.

Het IP-adres gebruiken om verbinding te maken met een workload voor extern bureaublad of hulp op afstand:

1. Ga in de Cyber Protect-console naar **Alle apparaten**.
2. Klik op **Quick Assist**.
3. Klik op het tabblad **Via IP-adres**.
4. Voer het IP-adres en de poort van de workload in.
5. Selecteer een verbindingsprotocol (RDP voor Windows-workloads of Schermdeling van Apple voor macOS-workloads), afhankelijk van het besturingssysteem van de externe workload.

   Opmerking
   Verbindingen via RDP ondersteunen de actie voor extern bureaublad en verbindingen via Schermdeling van Apple ondersteunen zowel de actie voor extern bureaublad als de actie voor hulp op afstand.

6. Klik op **Verbinden**.
7. Geef in het venster **Verificatie** de vereiste referenties op.

Voor verbindingen via Schermdeling van Apple: in Connect Client wordt een nieuw viewervenster geopend waarin u het bureaublad van de externe workload kunt zien. De viewer heeft een werkbalk

met aanvullende acties die u kunt uitvoeren voor de externe workload nadat de externe verbinding tot stand is gebracht. Zie "De werkbalk in het viewervenster gebruiken" (p. 1095) voor meer informatie.

Bestanden overdragen vis Acronis Quick Assist

U kunt de Quick Assist-functie gebruiken om bestanden over te dragen tussen uw workload en onbeheerde workloads.

Vereisten

- Het Advanced Management-pakket is toegewezen aan uw klanttenant.
- 2FA is ingeschakeld voor uw gebruikersaccount op Acronis Cyber Protect Cloud.
- De externe gebruiker heeft Acronis Quick Assist gedownload en uitgevoerd.
- De externe gebruiker heeft de computer-id en toegangscode van Quick Assist opgegeven.

Bestanden overdragen naar een workload via Quick Assist

1. In de Cyber Protect-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op **Quick Assist**.
3. Voer in het venster **Quick Assist** de workload-id in die is opgegeven door de eindgebruiker en selecteer vervolgens **Bestandsoverdracht**.
4. Klik op **Verbinden**.
5. Doe vervolgens het volgende (al naargelang Connect Client al dan niet is geïnstalleerd voor uw workload):
   - Als Connect Client niet is geïnstalleerd: download de toepassing, installeer deze en selecteer **Toestaan** in de bevestigingspop-up die wordt weergegeven.
   - Als Connect Client al is geïnstalleerd: klik op **Connect Client openen** in de bevestigingspop-up die wordt weergegeven.
6. Ga naar het venster **Verificatie** en voer de toegangscode in.
7. Blader in het venster **Bestandsoverdracht** door bestanden en sleep ze naar de gewenste bestemming.

   Opmerking
   De bestanden van de lokale workload worden weergegeven in het linkerdeelvenster en de bestanden van de externe workload worden weergegeven in het rechterdeelvenster.
   Wanneer een bestandsoverdracht begint, wordt deze vermeld in het deelvenster **Taken**.

8. [Optioneel] Als u de voltooide taken uit het deelvenster **Taken** wilt verwijderen, klikt u op **Voltooide items wissen**.
9. Sluit het venster wanneer alle overdrachten zijn voltooid.

De werkbalk in het viewervenster gebruiken

Nadat u verbinding hebt gemaakt met een externe workload, kunt u de werkbalk van het viewervenster gebruiken om snel de verschillende acties uit te voeren.

Pictogram	Beschrijving
	**Ware grootte** Schaalt het bureaublad van de externe workload zodat één pixel van het externe bureaublad overeenkomt met één pixel in het viewervenster.
	**Passend maken** Schaalt het bureaublad van de externe workload zodat deze in het viewervenster past.
	**Scherm vergrendelen** en **ontgrendelen** Geeft een tijdelijke aanduiding weer op het scherm van de externe workload, zodat de externe gebruiker uw acties niet ziet.
	**Momentopname maken** Sla de bureaubladafbeelding van de externe server op in een lokaal bestand.
	**Selecteer weergave** Selecteer de weergave van de externe workload die u wilt bekijken en selecteer de gewenste resolutie. Beschikbaar voor verbindingen van Schermdeling van Apple met macOS en NEAR-verbindingen met elk besturingssysteem.
	**Beeldkwaliteit** Past de beeldkwaliteit van het externe scherm aan van zwart-wit naar de hoogst mogelijke kwaliteit bij verbindingen via Schermdeling van Apple.
	**Beeldkwaliteit van NEAR** Past de verhouding tussen kwaliteit en prestaties aan voor NEAR-verbindingen. Met de linkerkant van de schuifregelaar (Smooth) geeft u voorrang aan prestaties boven beeldkwaliteit. Met de rechterkant (Sharp) kiest u voor de beste kwaliteit van het externe-bureaubladscherm, maar waarschijnlijk mindere prestaties.
	**Ctrl+Alt+Del verzenden** Verzendt een reeks Ctrl + Alt + Delete naar de externe workload.

Pictogram	Beschrijving
	Beschikbaar voor Windows- en Linux-workloads.
	**Bestandsoverdracht** Opent het venster Bestandsbeheer om bestanden uit te wisselen tussen externe en lokale workload. Beschikbaar voor NEAR-verbindingen.
	**Werkbalk vastzetten** Schakelt het automatisch verbergen van de viewerwerkbalk uit. Beschikbaar voor Windows-workloads.
	**Volledig scherm** Schakelt over naar de modus voor volledig scherm en schaalt de externe workload zodat deze uw lokale scherm volledig vult. Beschikbaar voor Windows-workloads.
	**Sluiten** Sluit het viewervenster en beëindigt de sessie voor externe besturing. Beschikbaar voor Windows-workloads.

Wanneer u op het pictogram **Overige** klikt, zijn er mogelijk extra opties beschikbaar. Dit hangt af van het verbindingstype.

Optie	Beschrijving
Opname starten / Opname stoppen	Neem de huidige sessie voor extern bureaublad op. Sessieopnames worden opgeslagen als .crec-bestanden in de lokale workload. U kunt .crec-bestanden openen met Acronis Connect Client. Beschikbaar voor NEAR-verbindingen
Klembord automatisch synchroniseren	Als deze optie is ingeschakeld, synchroniseert de client automatisch uw lokale klembord en het klembord van de externe computer. Beschikbaar voor verbindingen via NEAR en Schermdeling van Apple
Klembord verzenden **Klembord ophalen**	**Klembord verzenden** vervangt de inhoud van het klembord van de externe computer door de inhoud van het lokale klembord. **Klembord ophalen** draagt de inhoud van het klembord van de externe computer over naar het lokale klembord.
Slim toetsenbord /	Wijzigt de modus voor toetsenbordinvoer voor de huidige verbinding.

Optie	Beschrijving
Raw-toetsen / Raw-toetsen met alle snelkoppelingen	**Slim toetsenbord**: de client draagt Unicode-codes van de lokaal getypte symbolen over naar de externe computer **Raw-toetsen**: de client gebruikt de raw-codes van de toetsenbordtoetsen die u indrukt. **Raw-toetsen met alle snelkoppelingen**: de client schakelt lokale systeemsnelkoppelingen uit zodat ze ook naar het externe besturingssysteem worden verzonden.
Toetsenbordfocus op muisaanwijzer	Wanneer deze optie is ingeschakeld, legt de client alleen de toetsenbordinvoer vast wanneer uw lokale muiscursor boven het viewervenster wordt geplaatst. Wanneer deze optie is uitgeschakeld, legt de client uw toetsenbord vast wanneer het venster actief is.
Verbindingsgegevens weergeven/verbergen	Wanneer **Verbindingsgegevens weergeven** is geselecteerd, wordt er een klein gegevensvenster weergegeven op het externe-bureaubladscherm met de meest essentiële informatie over de huidige verbinding.
Extern geluid	Hiermee kan de client het geluid van de externe computer omleiden naar de lokale computer. Beschikbaar voor NEAR-verbindingen
Voorkeuren	Configureer de instellingen van Connect Client. Zie "De Connect Client-instellingen configureren" (p. 1098) voor meer informatie.

Externe sessies opnemen en afspelen

U kunt een externe sessie opnemen via NEAR in Acronis Connect Client.

Een externe sessie opnemen

1. Open de werkbalk van de viewer in Connect Client, klik op **Overig** en selecteer **Opname starten**.
2. Selecteer een naam en locatie voor de record.
   Standaard krijgt het bestand een naam inclusief de huidige datum en tijd en wordt het geplaatst in de map **Documenten** in de huidige basismap van de gebruiker. Zolang de opname actief is, worden in de werkbalk van de **Viewer** de opnametimer en het externe scherm met een knipperende rode cirkel in de rechterbovenhoek weergegeven.
3. Als u de opname wilt stoppen, klikt u op **Overig** en vervolgens op **Opname stoppen**. Op een Mac kunt u ook op **Stop** op de werkbalk klikken.
   Alle .crec-bestanden die zijn gemaakt door Acronis Connect Client, worden standaard geopend met Acronis Connect Client.

Een opname afspelen

1. Zoek een opnamebestand.
2. Open het.

   De opnamespeler van Acronis Connect Client wordt geopend. Let op: Het is niet mogelijk is om door de opname te navigeren. Als u een bepaald moment in de opname wilt vinden, wacht u tot de speler het bereikt.
3. [Optioneel] Als u de afspeelsnelheid wilt aanpassen, gebruikt u de pictogrammen **<<** en **>>** in de sectie Afspeelbesturing.

   De opname wordt opgeslagen als een reeks gebeurtenissen die tijdens een verbinding naar en van de externe server zijn verzonden. Zo worden de beste kwaliteit van de opname en een minimale bestandsgrootte gewaarborgd. Het is daarentegen niet mogelijk is om door de opname te navigeren. Op dit moment is het ook niet mogelijk om de opnames naar een video-indeling te converteren.

De Connect Client-instellingen configureren

Nadat u Connect Client hebt geïnstalleerd voor uw workload, kunt u de instellingen ervan configureren volgens uw voorkeuren.

De instellingen van Connect Client configureren:

1. Zoek in het startmenu naar **Connect Client** en start de toepassing.
2. Configureer de instellingen op het tabblad **Algemeen**.

Optie	Beschrijving
Uitgebreide logboeken schrijven	Selecteer deze optie als u wilt dat er uitgebreide logboeken worden geschreven in Connect Client. Indien deze optie is uitgeschakeld, wordt er door de client alleen algemene informatie in het logbestand geschreven.
Proxyinstellingen	Selecteer of u de standaardsysteemproxy wilt gebruiken of een aangepaste SOCKSS-proxy wilt configureren.

3. Configureer de instellingen op het tabblad **Viewer**.

Optie	Beschrijving
Vragen om bevestiging bij het sluiten van een viewer	Selecteer deze optie als u wilt dat Connect Client een bevestigingsbericht weergeeft wanneer u het viewervenster gaat sluiten, zodat dit niet onbedoeld wordt gesloten.
Wanneer geminimaliseerd	Selecteer of de vieweractiviteit moet worden onderbroken wanneer deze is geminimaliseerd, zodat de CPU minder wordt belast.
Wanneer gemaximaliseerd	Selecteer of u de volledige schermmodus wilt inschakelen wanneer deze is gemaximaliseerd.

Optie	Beschrijving
Klembordoverdracht	Schakel in dat de indicator voor klembordoverdracht wordt weergegeven in het viewervenster wanneer u tekst en afbeeldingen kopieert of plakt.
Toetsenbordmodus	Schakel in dat de indicator voor de invoermodus wordt weergegeven in de titel van het viewervenster wanneer muis- en toetsenbordgebeurtenissen worden verzonden naar de externe machine.
Klembord	Selecteer **Klembord automatisch synchroniseren** om automatische klembordsynchronisatie in te schakelen (wanneer beschikbaar).
Toetsenbordgebeurtenissen verzenden	Kies of u uw lokale toetsenbordinvoer wilt gebruiken wanneer het Connect Client-venster actief is of alleen wanneer u uw lokale muisaanwijzer hierboven beweegt.
Achtergrondkleur van viewer	Wijzig de achtergrondkleur van het viewervenster.
Automatisch opnieuw verbinding maken	Selecteer **Inschakelen om automatisch opnieuw verbinding te maken** als u wilt dat Connect Client de verbinding automatisch herstelt in het geval van een onderbreking.
H.264	U kunt hardwaredecoders uitschakelen.
Sluiten bij inactiviteit	Selecteer na hoeveel tijd inactiviteit het viewervenster moet worden gesloten.

4. Configureer de instellingen op het tabblad **Toetsenbord**.

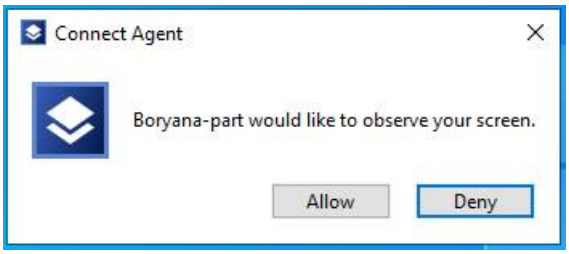
Optie	Beschrijving
Wijzigingstoewijzingen	Wijzig het gedrag van wijzigingstoetsen via een pop-upmenu. Deze instellingen worden apart opgeslagen voor verbindingen via NEAR, Schermdeling van Apple en RDP.
Invoermodus	Selecteer voor elk type verbinding (geselecteerd in de koptekst van het deelvenster) de standaardmodus voor toetsenbordinvoer.

5. Klik op **OK**.

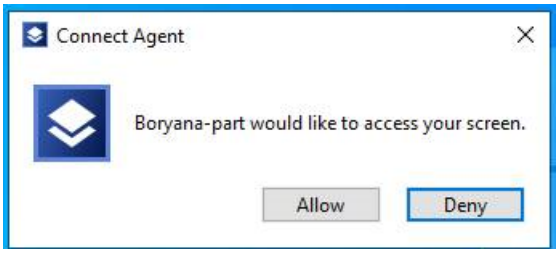
De meldingen van extern bureaublad

Soms worden in Connect Agent actiedialoogvensters (meldingen) weergegeven op het bureaublad van de externe workload. Dit gebeurt:

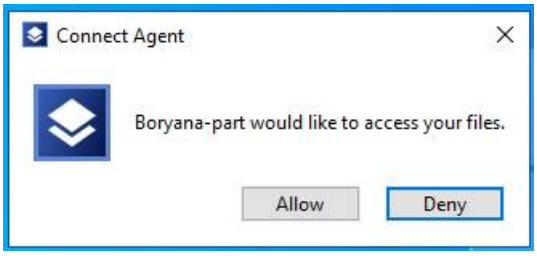
- wanneer u op afstand verbinding probeert te maken met de workload door te vragen om toestemming voor bekijken. De gebruiker die lokaal is aangemeld bij de externe workload, kan het verzoek toestaan of weigeren.



- wanneer u op afstand verbinding probeert te maken met de workload door toestemming te vragen voor besturen. De gebruiker die lokaal is aangemeld bij de externe workload, kan het verzoek toestaan of weigeren.



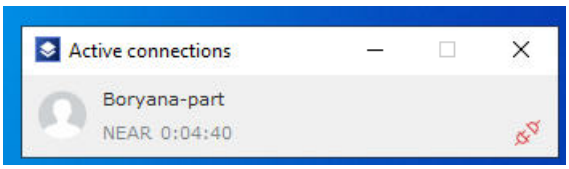
- wanneer u bestanden probeert uit te wisselen tussen uw workload en de externe workload door toestemming te vragen voor bestandsoverdracht. De gebruiker die lokaal is aangemeld bij de externe workload, kan het verzoek toestaan of weigeren.



Wanneer u een extern bureaublad verbindt met een workload, krijgt de gebruiker die is aangemeld bij de workload, een andere verbindingsmelding te zien met de volgende informatie:

- naam van de gebruiker die op afstand is verbonden
- verbindingsprotocol dat wordt gebruikt om de externe verbinding tot stand te brengen
- duur van de externe verbinding

De gebruiker die lokaal is aangemeld bij de externe workload, kan de verbinding op elk moment verbreken door te klikken op het pictogram **Verbinding verbreken** of **Sluiten**.



De status en prestaties van workloads controleren

U kunt de systeemparameters en de status van de workloads in uw organisatie controleren. Als een parameter niet binnen de norm is, wordt u hierover onmiddellijk geïnformeerd, zodat u het probleem snel kunt oplossen. U kunt ook aangepaste waarschuwingen en automatische responsacties configureren. Dit zijn acties die automatisch worden uitgevoerd om anomalieën in workloadgedrag op te lossen.

Opmerking
Als u de controlefunctionaliteit wilt gebruiken, moet Bescherming-agent versie 15.0.35324 of later zijn geïnstalleerd voor de workloads.

Bewakingsschema

Als u wilt beginnen met de controle van de prestatie-, hardware-, software-, systeem- en beveiligingsparameters van uw beheerde workloads, moet u hierop eerst een controleschema toepassen. De controleschema's omvatten verschillende controles die u kunt inschakelen en configureren. Sommige schema's ondersteunen het type controle op basis van anomalieën. Zie "Bewakingsschema" (p. 1140) voor meer informatie over controleschema's. Zie "Configureerbare controles" (p. 1102) voor meer informatie over de beschikbare controles die u kunt configureren in het controleschema.

Als de agent om de een of andere reden geen gegevens van een workload kan verzamelen, wordt automatisch een waarschuwing gegenereerd.

Typen controles

U moet het controletype configureren voor elke controle die u inschakelt in het schema. Het controletype bepaalt het algoritme dat door de controle wordt gebruikt om het normale gedrag en de afwijking van de workload te bepalen. Er zijn twee controletypen: op basis van drempelwaarden en op basis van anomalieën. Sommige controles ondersteunen alleen het type controle op basis van drempelwaarden.

Met controles op basis van drempelwaarden kunt u bijhouden of de waarden van de parameters hoger of lager zijn dan een door u geconfigureerde drempelwaarde. Bij dit controletype bent u verantwoordelijk voor het definiëren van de juiste drempelwaarden voor de workloads. Het systeem bepaalt het normale gedrag op basis van deze statische drempelwaarden en zonder rekening te houden met andere specifieke omstandigheden die het gedrag kunnen veroorzaken. Daarom is controle op basis van drempelwaarden mogelijk minder nauwkeurig dan controle op basis van anomalieën.

Bij controle op basis van anomalieën wordt machine learning gebruikt om de normale gedragspatronen te bepalen voor een workload en om afwijkend gedrag te detecteren. Zie "Controle op basis van anomalieën" (p. 1102) voor meer informatie.

Controle op basis van anomalieën

Bij controle op basis van anomalieën worden machine learning-modellen gebruikt om de normale gedragspatronen vast te stellen voor een bepaalde workload en om anomalieën (onverwachte pieken in de gegevens van tijdreeksen) te detecteren in het gedrag van de workload. Wanneer u dit controletype activeert, wordt automatisch een model gemaakt dat zichzelf begint te trainen en het model aanpast aan de specifieke workload, op basis van de gegevens die het verzamelt uit de workload. Hierdoor zijn de gegevens aan het begin van de trainingsperiode mogelijk niet helemaal nauwkeurig. Er zijn minimaal drie weken training vereist om een betrouwbaar model te maken. Naarmate er meer gegevens worden verzameld en historische gegevenssets worden geanalyseerd, wordt het model geleidelijk verfijnd en worden de dynamische maximale en minimale drempelwaarden gegenereerd voor elke metriek van de workload. Dit controletype is flexibeler dan de op drempelwaarden gebaseerde controle omdat de waarden van de parameters en hun context automatisch worden gecontroleerd. Het kan bijvoorbeeld normaal zijn dat een specifieke workload op bepaalde uren van de dag zwaarder wordt belast. Bij een controletype op basis van drempelwaarden kan dit ten onrechte worden geïnterpreteerd als abnormaal gedrag en wordt er mogelijk een waarschuwing gegenereerd.

U kunt de machine learning-modellen voor een workload opnieuw instellen. In dit geval verwijdert het systeem alle gegevens en modellen voor de controles die op de workload zijn toegepast. Zie "Machine learning-modellen opnieuw instellen" (p. 1151) voor meer informatie.

Ondersteunde platforms voor controles

De controlefunctionaliteit wordt ondersteund voor de volgende besturingssystemen.

Ondersteunde Windows-versies	Ondersteunde macOS-versies
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x (Big Sur) • macOS 12.x (Monterey) • macOS 13.x (Ventura)

Configureerbare controles

De controlefunctionaliteit ondersteunt de volgende controles, onderverdeeld in zes categorieën: Hardware, prestaties, software, systeem, beveiliging en aangepast.

Controle	Beschrijving	Ondersteunde besturingssystemen	Frequentie van gegevensverzameling	Ondersteuning van controle op basis van anomalieën	Beschikbaar in Standard Protection of Advanced Management
Hardware					
Schijfruimte	Controleert de vrije schijfruimte op een specifiek station van de workload.	Windows macOS	1 minuut	Ja	Standard Protection
CPU-temperatuur	Controleert de temperatuur van de CPU.	Windows macOS	30 sec	Ja	Advanced Management
GPU-temperatuur	Hiermee wordt de temperatuur van de GPU gecontroleerd.	Windows macOS	30 sec	Ja	Advanced Management
Hardwarewijzigingen	Hiermee worden de hardwarewijzigingen gecontroleerd, zoals het toevoegen, verwijderen of vervangen van hardware voor een workload	Windows macOS	24 uur	Nee	Standard Protection
Prestaties					
CPU-gebruik	Controleert het totale CPU-gebruik (door alle CPU's voor	Windows macOS	30 sec	Ja	Advanced Management

Controle	Beschrijving	Ondersteunde besturingssystemen	Frequentie van gegevensverzameling	Ondersteuning van controle op basis van anomalieën	Beschikbaar in Standard Protection of Advanced Management
	de workload).				
Geheugengebruik	Hiermee wordt het totale geheugengebruik (door alle geheugensleuven voor de workload) gecontroleerd.	Windows macOS	30 sec	Ja	Advanced Management
Schijfoverdrachtssnelheid	Controleert de lees- en schrijfsnelheid van elke fysieke schijf voor de workload.	Windows macOS	30 sec	Ja	Advanced Management
Netwerkgebruik	Hiermee wordt het inkomende en uitgaande verkeer voor elke netwerkadapter voor de workload gecontroleerd.	Windows macOS	30 sec	Ja	Advanced Management
CPU-gebruik per proces	Hiermee wordt het CPU-gebruik door bepaalde processen gecontroleerd.	Windows macOS	30 sec	Nee	Advanced Management
Geheugengebruik per proces	Hiermee wordt het	Windows macOS	30 sec	Nee	Advanced

Controle	Beschrijving	Ondersteunde besturingssystemen	Frequentie van gegevensverzameling	Ondersteuning van controle op basis van anomalieën	Beschikbaar in Standard Protection of Advanced Management
	geheugengebruik door het geselecteerde proces gecontroleerd.				Management
Schijfoverdrachtssnelheid per proces	Controleert de lees- en schrijfsnelheid van het geselecteerde proces.	Windows macOS	30 sec	Nee	Advanced Management
Netwerkgebruik per proces	Controleert het inkomende en uitgaande verkeer van het geselecteerde proces.	Windows macOS	30 sec	Nee	Advanced Management
Software					
Windows-servicestatus	Hiermee wordt de status van de geselecteerde Windows-service (Actief of Gestopt) gecontroleerd.	Windows	30 sec	Nee	Advanced Management
Processtatus	Hiermee wordt de status van het geselecteerde proces (Actief of Gestopt)	Windows macOS	30 sec	Nee	Advanced Management

Controle	Beschrijving	Ondersteunde besturingssystemen	Frequentie van gegevensverzameling	Ondersteuning van controle op basis van anomalieën	Beschikbaar in Standard Protection of Advanced Management
	gecontroleerd.				
Geïnstalleerde software	Controleert de installatie, update of verwijdering van softwaretoepassingen.	Windows macOS	24 uur	Nee	Advanced Management
Systeem					
Laatste herstart van systeem	Controleert wanneer de workload opnieuw is opgestart.	Windows macOS	1 uur	Nee	Standard Protection
Windows-gebeurtenislogboek	Controleert specifieke bedrijfskritieke gebeurtenissen in de Windows-gebeurtenislogboeken.	Windows	10 min	Nee	Advanced Management
Grootte van bestanden en mappen	Controleert de totale grootte van de geselecteerde bestanden of mappen.	Windows macOS	10 min	Nee	Standard Protection
Beveiliging					
Windows Update-status	Controleert de Windows Update-status	Windows	15 min	Nee	Advanced Manage

Controle	Beschrijving	Ondersteunde besturingssystemen	Frequentie van gegevensverzameling	Ondersteuning van controle op basis van anomalieën	Beschikbaar in Standard Protection of Advanced Management
	van de workload en of de nieuwste updates zijn geïnstalleerd.				ment
Firewallstatus	Controleert de status van de ingebouwde of externe firewall die is geïnstalleerd voor de workload.	Windows macOS	5 min	Nee	Advanced Management
Status van antimalwaresoftware	Controleert de status van de ingebouwde of externe antimalwaresoftware die is geïnstalleerd voor de workload.	Windows macOS	5 min	Nee	Advanced Management
Mislukte aanmeldingen	Controleert mislukte aanmeldingspogingen voor de workload.	Windows	1 uur	Nee	Advanced Management
Status van AutoRun	Controleert of de AutoRun-functie voor verwisselbare opslagmedia is ingeschakeld.	Windows	1 uur	Nee	Advanced Management

Controle	Beschrijving	Ondersteunde besturingssystemen	Frequentie van gegevensverzameling	Ondersteuning van controle op basis van anomalieën	Beschikbaar in Standard Protection of Advanced Management
Aangepast					
Aangepast	Controleert aangepaste objecten via actieve scripts.	Windows macOS	aangepast	Nee	Advanced Management

Instellingen voor controle van Schijfruimte

Schijfruimte: hiermee wordt de vrije schijfruimte gecontroleerd voor een specifiek station van de workload.

Opmerking
Bij de controle van de vrije schijfruimte worden binaire bytes berekend (1024 bytes per kB, 1024 kB per MB en 1024 MB per GB) voor zowel Windows- als macOS-workloads.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Controle op basis van drempelwaarden	
Station	Het station dat u wilt controleren. De volgende waarden zijn beschikbaar. • **Systeemstation**: Dit is de standaardwaarde. • **Elk station**
Operator	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Minder dan**: Dit is de standaardwaarde. • **Minder dan of gelijk aan**
Drempelwaarde voor vrije schijfruimte	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek.

Instelling	Beschrijving
	Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in het bereik 1-100 (%) in. De standaardwaarde is 20.
Verwisselbare stations opnemen	Deze instelling is beschikbaar als de waarde voor **Station** is ingesteld op **Elk station**. Selecteer deze instelling als u verwisselbare stations, zoals USB-flashstations, wilt toevoegen voor controle. Deze instelling is standaard uitgeschakeld.
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 30.
Controle op basis van anomalieën	
Station	Het station dat u wilt controleren. De volgende waarden zijn beschikbaar. • **Systeemstation**: Dit is de standaardwaarde. • **Elk station**
Trainingsperiode van model	Dit is een periode waarin de machine learning-modellen worden getraind op basis van gegevens die zijn verzameld van de agents. In deze periode worden ook de normale gedragspatronen vastgesteld voor de workload. Hoe langer het model wordt getraind, hoe nauwkeuriger het gedragspatroon op de lange termijn kan worden vastgesteld. De aanbevolen minimale periode voor training van het model is eenentwintig dagen. Voer een geheel getal in (dagen). De standaardwaarde is 21.
Anomaliewaarschuwingen ontvangen tijdens trainingsperiode	Als u deze instelling selecteert, ontvangt u waarschuwingen over anomalieën tijdens de trainingsperiode van het model. Deze waarschuwingen kunnen ten onrechte zijn, omdat de modellen nog worden getraind en mogelijk niet nauwkeurig genoeg zijn. Deze instelling is standaard ingeschakeld.
Gevoeligheidsniveau	Het gevoeligheidsniveau fungeert als een voorlopig filter voor anomalieën in het geval van waarden binnen een bepaald

Instelling	Beschrijving
	bereik. Dit filter werkt onafhankelijk van het algoritme voor detectie van anomalieën. Het doel is om te voorkomen dat de anomalieën binnen het opgegeven bereik worden verwerkt door het algoritme voor detectie van anomalieën. Gedurende de trainingsperiode: 1. Het algoritme wordt getraind met behulp van de gegevens die tijdens de training worden verzameld. 2. Het algoritme detecteert anomalieën in de trainingsgegevens. 3. Er wordt een filterproces toegepast op basis van de gemiddelde en standaardafwijking. 4. Eventuele anomalieën binnen het opgegeven interval worden gefilterd. 5. Voor de resterende datapunten met anomalieën wordt de anomalie met het laagste niveau geselecteerd. Dit niveau (een zwevendekommagetal tussen 0 en 1) wordt vastgelegd in het model. Gedurende de voorspelling: 1. Het algoritme voorspelt anomalieën voor de inferentiegegevens. 2. De voorspelde anomalieën worden gefilterd op basis van de gemiddelde en standaardafwijking, volgens het gevoeligheidsniveau. 3. De resterende anomalieën worden verder gefilterd op basis van het volgende principe: waarden boven het drempelniveau worden als een anomalie beschouwd, en waarden onder het drempelniveau worden als normaal gedrag beschouwd. De volgende waarden zijn beschikbaar. • **Laag**: het lage niveau is gelijk aan de waarde van de gemiddelde afwijking en de standaardafwijking. • **Normaal**: dit is de standaardwaarde. Het normale niveau is gelijk aan de waarde van de gemiddelde afwijking en tweemaal de waarde van de standaardafwijking. • **Hoog**: het hoge niveau is gelijk aan de waarde van de gemiddelde afwijking en driemaal de waarde van de standaardafwijking.
Duur van de anomalie	Er wordt alleen een waarschuwing voor een gedetecteerde anomalie gegenereerd als het afwijkende gedrag zich blijft voordoen gedurende de opgegeven periode. De standaardwaarde is 30 minuten.

Instellingen voor controle van de CPU-temperatuur

CPU-temperatuur: hiermee wordt de CPU-temperatuur van de workload gecontroleerd.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Controle op basis van drempelwaarden	
CPU-temperatuur is hoger dan (°C)	De maximale waarde van de gecontroleerde metriek. Als deze waarde wordt overschreden, wordt er een waarschuwing gegenereerd. Voer een geheel getal in (C). De standaardwaarde is 80.
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.
Controle op basis van anomalieën	
Trainingsperiode van model	Dit is een periode waarin de machine learning-modellen worden getraind op basis van gegevens die zijn verzameld van de agents. In deze periode worden ook de normale gedragspatronen vastgesteld voor de workload. Hoe langer het model wordt getraind, hoe nauwkeuriger het gedragspatroon op de lange termijn kan worden vastgesteld. De aanbevolen minimale periode voor training van het model is eenentwintig dagen. Voer een geheel getal in (dagen). De standaardwaarde is 21.
Gevoeligheidsniveau	Het gevoeligheidsniveau fungeert als een voorlopig filter voor anomalieën in het geval van waarden binnen een bepaald bereik. Dit filter werkt onafhankelijk van het algoritme voor detectie van anomalieën. Het doel is om te voorkomen dat de anomalieën binnen het opgegeven bereik worden verwerkt door het algoritme voor detectie van anomalieën. Gedurende de trainingsperiode: 1. Het algoritme wordt getraind met behulp van de gegevens die tijdens de training worden verzameld. 2. Het algoritme detecteert anomalieën in de trainingsgegevens. 3. Er wordt een filterproces toegepast op basis van de gemiddelde en standaardafwijking. 4. Eventuele anomalieën binnen het opgegeven interval

Instelling	Beschrijving
	worden gefilterd. 5. Voor de resterende datapunten met anomalieën wordt de anomalie met het laagste niveau geselecteerd. Dit niveau (een zwevendekommagetal tussen 0 en 1) wordt vastgelegd in het model. Gedurende de voorspelling: 1. Het algoritme voorspelt anomalieën voor de inferentiegegevens. 2. De voorspelde anomalieën worden gefilterd op basis van de gemiddelde en standaardafwijking, volgens het gevoeligheidsniveau. 3. De resterende anomalieën worden verder gefilterd op basis van het volgende principe: waarden boven het drempelniveau worden als een anomalie beschouwd, en waarden onder het drempelniveau worden als normaal gedrag beschouwd. De volgende waarden zijn beschikbaar. • **Laag**: het lage niveau is gelijk aan de waarde van de gemiddelde afwijking en de standaardafwijking. • **Normaal**: dit is de standaardwaarde. Het normale niveau is gelijk aan de waarde van de gemiddelde afwijking en tweemaal de waarde van de standaardafwijking. • **Hoog**: het hoge niveau is gelijk aan de waarde van de gemiddelde afwijking en driemaal de waarde van de standaardafwijking.
Duur van de anomalie	Er wordt alleen een waarschuwing voor een gedetecteerde anomalie gegenereerd als het afwijkende gedrag zich blijft voordoen gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 15.

Instellingen voor controle van de GPU-temperatuur

GPU-temperatuur: hiermee wordt de GPU-temperatuur van de workload gecontroleerd.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Controle op basis van drempelwaarden	
GPU-temperatuur is overschreden	De maximale waarde van de gecontroleerde metriek. Als deze waarde wordt overschreden, wordt er een anomalie gedetecteerd.

Instelling	Beschrijving
	Voer een geheel getal in (C). De standaardwaarde is 80.
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.
Controle op basis van anomalieën	
Trainingsperiode van model	Dit is een periode waarin de machine learning-modellen worden getraind op basis van gegevens die zijn verzameld van de agents. In deze periode worden ook de normale gedragspatronen vastgesteld voor de workload. Hoe langer het model wordt getraind, hoe nauwkeuriger het gedragspatroon op de lange termijn kan worden vastgesteld. De aanbevolen minimale periode voor training van het model is eenentwintig dagen. Voer een geheel getal in (dagen). De standaardwaarde is 21.
Gevoeligheidsniveau	Het gevoeligheidsniveau fungeert als een voorlopig filter voor anomalieën in het geval van waarden binnen een bepaald bereik. Dit filter werkt onafhankelijk van het algoritme voor detectie van anomalieën. Het doel is om te voorkomen dat de anomalieën binnen het opgegeven bereik worden verwerkt door het algoritme voor detectie van anomalieën. Gedurende de trainingsperiode: 1. Het algoritme wordt getraind met behulp van de gegevens die tijdens de training worden verzameld. 2. Het algoritme detecteert anomalieën in de trainingsgegevens. 3. Er wordt een filterproces toegepast op basis van de gemiddelde en standaardafwijking. 4. Eventuele anomalieën binnen het opgegeven interval worden gefilterd. 5. Voor de resterende datapunten met anomalieën wordt de anomalie met het laagste niveau geselecteerd. Dit niveau (een zwevendekommagetal tussen 0 en 1) wordt vastgelegd in het model. Gedurende de voorspelling: 1. Het algoritme voorspelt anomalieën voor de inferentiegegevens. 2. De voorspelde anomalieën worden gefilterd op basis van de gemiddelde en standaardafwijking, volgens het gevoeligheidsniveau. 3. De resterende anomalieën worden verder gefilterd op basis van

Instelling	Beschrijving
	het volgende principe: waarden boven het drempelniveau worden als een anomalie beschouwd, en waarden onder het drempelniveau worden als normaal gedrag beschouwd. De volgende waarden zijn beschikbaar. • **Laag**: het lage niveau is gelijk aan de waarde van de gemiddelde afwijking en de standaardafwijking. • **Normaal**: dit is de standaardwaarde. Het normale niveau is gelijk aan de waarde van de gemiddelde afwijking en tweemaal de waarde van de standaardafwijking. • **Hoog**: het hoge niveau is gelijk aan de waarde van de gemiddelde afwijking en driemaal de waarde van de standaardafwijking.
Duur van de anomalie	Er wordt alleen een waarschuwing voor een gedetecteerde anomalie gegenereerd als het afwijkende gedrag zich blijft voordoen gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 15.

Instellingen voor controle van hardwarewijzigingen

Hardwarewijzigingen: hiermee worden de hardwarewijzigingen gecontroleerd, zoals het toevoegen, verwijderen of vervangen van hardware voor een workload.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Hardwareonderdelen	Selecteer een of meer hardwareonderdelen die u wilt controleren op wijzigingen. De volgende waarden zijn beschikbaar. • **Alles**: Dit is de standaardwaarde. • **Moederbord** • **CPU** • **RAM** • **Schijf** • **GPU** • **Netwerkadapter**
Wat moet er worden gecontroleerd	Geef aan op welke wijzigingen u de geselecteerde hardwareonderdelen wilt controleren. U kunt meerdere items selecteren in de lijst. De volgende waarden zijn beschikbaar.

Instelling	Beschrijving
	• **Elke wijziging**: Dit is de standaardwaarde. • **Nìeuw toegevoegde onderdelen** • **Vervangen onderdelen** • **Verwijderde onderdelen**

Instellingen voor controle van CPU-gebruik

CPU-gebruik: hiermee wordt het totale CPU-gebruik (processorgebruik) van de workload gecontroleerd. Als de workload meerdere CPU's heeft, is het totale CPU-gebruik de som van het CPU-gebruik van elke CPU.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Controle op basis van drempelwaarden	
Operator	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempelwaarde voor CPU-gebruik	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in het bereik 1-100 (%) in. De standaardwaarde is 90.
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.
Controle op basis van anomalieën	
Trainingsperiode van model	Dit is een periode waarin de machine learning-modellen worden getraind op basis van gegevens die zijn verzameld van de agents. In deze periode worden ook de normale gedragspatronen vastgesteld voor de workload. Hoe langer

Instelling	Beschrijving
	het model wordt getraind, hoe nauwkeuriger het gedragspatroon op de lange termijn kan worden vastgesteld. De aanbevolen minimale periode voor training van het model is eenentwintig dagen. Voer een geheel getal in (dagen). De standaardwaarde is 21.
Anomaliewaarschuwingen ontvangen tijdens trainingsperiode	Als u deze instelling selecteert, ontvangt u waarschuwingen over anomalieën tijdens de trainingsperiode van het model. Deze waarschuwingen kunnen ten onrechte zijn, omdat de modellen nog worden getraind en mogelijk niet nauwkeurig genoeg zijn. Deze instelling is standaard ingeschakeld.
Gevoeligheidsniveau	Het gevoeligheidsniveau fungeert als een voorlopig filter voor anomalieën in het geval van waarden binnen een bepaald bereik. Dit filter werkt onafhankelijk van het algoritme voor detectie van anomalieën. Het doel is om te voorkomen dat de anomalieën binnen het opgegeven bereik worden verwerkt door het algoritme voor detectie van anomalieën. Gedurende de trainingsperiode: 1. Het algoritme wordt getraind met behulp van de gegevens die tijdens de training worden verzameld. 2. Het algoritme detecteert anomalieën in de trainingsgegevens. 3. Er wordt een filterproces toegepast op basis van de gemiddelde en standaardafwijking. 4. Eventuele anomalieën binnen het opgegeven interval worden gefilterd. 5. Voor de resterende datapunten met anomalieën wordt de anomalie met het laagste niveau geselecteerd. Dit niveau (een zwevendekommagetal tussen 0 en 1) wordt vastgelegd in het model. Gedurende de voorspelling: 1. Het algoritme voorspelt anomalieën voor de inferentiegegevens. 2. De voorspelde anomalieën worden gefilterd op basis van de gemiddelde en standaardafwijking, volgens het gevoeligheidsniveau. 3. De resterende anomalieën worden verder gefilterd op basis van het volgende principe: waarden boven het drempelniveau worden als een anomalie beschouwd, en waarden onder het drempelniveau worden als normaal

Instelling	Beschrijving
	gedrag beschouwd. De volgende waarden zijn beschikbaar. • **Laag**: het lage niveau is gelijk aan de waarde van de gemiddelde afwijking en de standaardafwijking. • **Normaal**: dit is de standaardwaarde. Het normale niveau is gelijk aan de waarde van de gemiddelde afwijking en tweemaal de waarde van de standaardafwijking. • **Hoog**: het hoge niveau is gelijk aan de waarde van de gemiddelde afwijking en driemaal de waarde van de standaardafwijking.
Duur van de anomalie	Er wordt alleen een waarschuwing voor een gedetecteerde anomalie gegenereerd als het afwijkende gedrag zich blijft voordoen gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 15.

Instellingen voor controle van geheugengebruik

Geheugengebruik: hiermee wordt het totale geheugengebruik door alle geheugenmodules voor de workload gecontroleerd.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Controle op basis van drempelwaarden	
Operator	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempelwaarde voor geheugengebruik	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in het bereik 1-100 (%) in. De standaardwaarde is 90.

Instelling	Beschrijving
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.
Controle op basis van anomalieën	
Trainingsperiode van model	Dit is een periode waarin de machine learning-modellen worden getraind op basis van gegevens die zijn verzameld van de agents. In deze periode worden ook de normale gedragspatronen vastgesteld voor de workload. Hoe langer het model wordt getraind, hoe nauwkeuriger het gedragspatroon op de lange termijn kan worden vastgesteld. De aanbevolen minimale periode voor training van het model is eenentwintig dagen. Voer een geheel getal in (dagen). De standaardwaarde is 21.
Anomaliewaarschuwingen ontvangen tijdens trainingsperiode	Als u deze instelling selecteert, ontvangt u waarschuwingen over anomalieën tijdens de trainingsperiode van het model. Deze waarschuwingen kunnen ten onrechte zijn, omdat de modellen nog worden getraind en mogelijk niet nauwkeurig genoeg zijn. Deze instelling is standaard ingeschakeld.
Gevoeligheidsniveau	Het gevoeligheidsniveau fungeert als een voorlopig filter voor anomalieën in het geval van waarden binnen een bepaald bereik. Dit filter werkt onafhankelijk van het algoritme voor detectie van anomalieën. Het doel is om te voorkomen dat de anomalieën binnen het opgegeven bereik worden verwerkt door het algoritme voor detectie van anomalieën. Gedurende de trainingsperiode: 1. Het algoritme wordt getraind met behulp van de gegevens die tijdens de training worden verzameld. 2. Het algoritme detecteert anomalieën in de trainingsgegevens. 3. Er wordt een filterproces toegepast op basis van de gemiddelde en standaardafwijking. 4. Eventuele anomalieën binnen het opgegeven interval worden gefilterd. 5. Voor de resterende datapunten met anomalieën wordt de anomalie met het laagste niveau geselecteerd. Dit niveau (een zwevendekommagetal tussen 0 en 1) wordt vastgelegd in het model.

Instelling	Beschrijving
	Gedurende de voorspelling: 1. Het algoritme voorspelt anomalieën voor de inferentiegegevens. 2. De voorspelde anomalieën worden gefilterd op basis van de gemiddelde en standaardafwijking, volgens het gevoeligheidsniveau. 3. De resterende anomalieën worden verder gefilterd op basis van het volgende principe: waarden boven het drempelniveau worden als een anomalie beschouwd, en waarden onder het drempelniveau worden als normaal gedrag beschouwd. De volgende waarden zijn beschikbaar. • **Laag**: het lage niveau is gelijk aan de waarde van de gemiddelde afwijking en de standaardafwijking. • **Normaal**: dit is de standaardwaarde. Het normale niveau is gelijk aan de waarde van de gemiddelde afwijking en tweemaal de waarde van de standaardafwijking. • **Hoog**: het hoge niveau is gelijk aan de waarde van de gemiddelde afwijking en driemaal de waarde van de standaardafwijking.
Duur van de anomalie	Er wordt alleen een waarschuwing voor een gedetecteerde anomalie gegenereerd als het afwijkende gedrag zich blijft voordoen gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 30 minuten.

Instellingen voor controle van de schijfoverdrachtssnelheid

Schijfoverdrachtssnelheid: hiermee worden de lees- en schrijfsnelheid van elke fysieke schijf voor de workload gecontroleerd.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Controle op basis van drempelwaarden	
Wat moet er worden gecontroleerd	Selecteer de snelheid die u wilt controleren. De volgende waarden zijn beschikbaar. • **Leessnelheid en schrijfsnelheid**. Dit is de standaardwaarde. • **Leessnelheid**

Instelling	Beschrijving
	• **Schrijfsnelheid**
Operator voor leessnelheid	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**. Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempelwaarde voor leessnelheid	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in (kb/s). De standaardwaarde is 0 kb/s.
Periode voor leessnelheid	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.
Operator voor schrijfsnelheid	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempelwaarde voor schrijfsnelheid	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in (kb/s). De standaardwaarde is 0 kb/s.
Periode voor schrijfsnelheid	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.

Instelling	Beschrijving
Controle op basis van anomalieën	
Trainingsperiode van model	Dit is een periode waarin de machine learning-modellen worden getraind op basis van gegevens die zijn verzameld van de agents. In deze periode worden ook de normale gedragspatronen vastgesteld voor de workload. Hoe langer het model wordt getraind, hoe nauwkeuriger het gedragspatroon op de lange termijn kan worden vastgesteld. De aanbevolen minimale periode voor training van het model is eenentwintig dagen. Voer een geheel getal in (dagen). De standaardwaarde is 21.
Anomaliewaarschuwingen ontvangen tijdens trainingsperiode	Als u deze instelling selecteert, ontvangt u waarschuwingen over anomalieën tijdens de trainingsperiode van het model. Deze waarschuwingen kunnen ten onrechte zijn, omdat de modellen nog worden getraind en mogelijk niet nauwkeurig genoeg zijn. Deze instelling is standaard ingeschakeld.
Wat moet er worden gecontroleerd	Selecteer de snelheid die u wilt controleren. De volgende waarden zijn beschikbaar. • **Leessnelheid en schrijfsnelheid**. Dit is de standaardwaarde. • **Leessnelheid** • **Schrijfsnelheid**
Gevoeligheidsniveau	Het gevoeligheidsniveau fungeert als een voorlopig filter voor anomalieën in het geval van waarden binnen een bepaald bereik. Dit filter werkt onafhankelijk van het algoritme voor detectie van anomalieën. Het doel is om te voorkomen dat de anomalieën binnen het opgegeven bereik worden verwerkt door het algoritme voor detectie van anomalieën. Gedurende de trainingsperiode: 1. Het algoritme wordt getraind met behulp van de gegevens die tijdens de training worden verzameld. 2. Het algoritme detecteert anomalieën in de trainingsgegevens. 3. Er wordt een filterproces toegepast op basis van de gemiddelde en standaardafwijking. 4. Eventuele anomalieën binnen het opgegeven interval worden gefilterd. 5. Voor de resterende datapunten met anomalieën wordt de anomalie met het laagste niveau geselecteerd. Dit niveau

Instelling	Beschrijving
	(een zwevendekommagetal tussen 0 en 1) wordt vastgelegd in het model. Gedurende de voorspelling: 1. Het algoritme voorspelt anomalieën voor de inferentiegegevens. 2. De voorspelde anomalieën worden gefilterd op basis van de gemiddelde en standaardafwijking, volgens het gevoeligheidsniveau. 3. De resterende anomalieën worden verder gefilterd op basis van het volgende principe: waarden boven het drempelniveau worden als een anomalie beschouwd, en waarden onder het drempelniveau worden als normaal gedrag beschouwd. De volgende waarden zijn beschikbaar. • **Laag**: het lage niveau is gelijk aan de waarde van de gemiddelde afwijking en de standaardafwijking. • **Normaal**: dit is de standaardwaarde. Het normale niveau is gelijk aan de waarde van de gemiddelde afwijking en tweemaal de waarde van de standaardafwijking. • **Hoog**: het hoge niveau is gelijk aan de waarde van de gemiddelde afwijking en driemaal de waarde van de standaardafwijking.
Duur van de anomalie (leessnelheid)	Er wordt alleen een waarschuwing voor een gedetecteerde anomalie gegenereerd als het afwijkende gedrag zich blijft voordoen gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 25.
Duur van de anomalie (schrijfsnelheid)	Er wordt alleen een waarschuwing voor een gedetecteerde anomalie gegenereerd als het afwijkende gedrag zich blijft voordoen gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 25.

Instellingen voor controle van netwerkgebruik

Netwerkgebruik: hiermee wordt het inkomende en uitgaande verkeer voor elke netwerkadapter voor de workload gecontroleerd.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Controle op basis van drempelwaarden	
Verkeersrichting	De verkeersrichting die u wilt controleren. De volgende waarden zijn beschikbaar. • **Inkomend verkeer en uitgaand verkeer**. Dit is de standaardwaarde. • **Inkomend verkeer** • **Uitgaand verkeer**
Operator voor inkomend verkeer	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempelwaarde voor inkomend verkeer	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in (kb/s). De standaardwaarde is 0 kb/s.
Periode voor inkomend verkeer	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.
Operator voor uitgaand verkeer	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempelwaarde voor uitgaand verkeer	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd.

Instelling	Beschrijving
	Voer een geheel getal in (kb/s). De standaardwaarde is 0 kb/s.
Periode voor uitgaand verkeer	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.
Controle op basis van anomalieën	
Trainingsperiode van model	Dit is een periode waarin de machine learning-modellen worden getraind op basis van gegevens die zijn verzameld van de agents. In deze periode worden ook de normale gedragspatronen vastgesteld voor de workload. Hoe langer het model wordt getraind, hoe nauwkeuriger het gedragspatroon op de lange termijn kan worden vastgesteld. De aanbevolen minimale periode voor training van het model is eenentwintig dagen. Voer een geheel getal in (dagen). De standaardwaarde is 21.
Anomaliewaarschuwingen ontvangen tijdens trainingsperiode	Als u deze instelling selecteert, ontvangt u waarschuwingen over anomalieën tijdens de trainingsperiode van het model. Deze waarschuwingen kunnen ten onrechte zijn, omdat de modellen nog worden getraind en mogelijk niet nauwkeurig genoeg zijn. Deze instelling is standaard ingeschakeld.
Verkeersrichting	• **Inkomend verkeer en uitgaand verkeer**. Dit is de standaardwaarde. • **Inkomend verkeer** • **Uitgaand verkeer**
Gevoeligheidsniveau	Het gevoeligheidsniveau fungeert als een voorlopig filter voor anomalieën in het geval van waarden binnen een bepaald bereik. Dit filter werkt onafhankelijk van het algoritme voor detectie van anomalieën. Het doel is om te voorkomen dat de anomalieën binnen het opgegeven bereik worden verwerkt door het algoritme voor detectie van anomalieën. Gedurende de trainingsperiode: 1. Het algoritme wordt getraind met behulp van de gegevens die tijdens de training worden verzameld. 2. Het algoritme detecteert anomalieën in de trainingsgegevens.

Instelling	Beschrijving
	3. Er wordt een filterproces toegepast op basis van de gemiddelde en standaardafwijking. 4. Eventuele anomalieën binnen het opgegeven interval worden gefilterd. 5. Voor de resterende datapunten met anomalieën wordt de anomalie met het laagste niveau geselecteerd. Dit niveau (een zwevendekommagetal tussen 0 en 1) wordt vastgelegd in het model. Gedurende de voorspelling: 1. Het algoritme voorspelt anomalieën voor de inferentiegegevens. 2. De voorspelde anomalieën worden gefilterd op basis van de gemiddelde en standaardafwijking, volgens het gevoeligheidsniveau. 3. De resterende anomalieën worden verder gefilterd op basis van het volgende principe: waarden boven het drempelniveau worden als een anomalie beschouwd, en waarden onder het drempelniveau worden als normaal gedrag beschouwd. De volgende waarden zijn beschikbaar. • **Laag**: het lage niveau is gelijk aan de waarde van de gemiddelde afwijking en de standaardafwijking. • **Normaal**: dit is de standaardwaarde. Het normale niveau is gelijk aan de waarde van de gemiddelde afwijking en tweemaal de waarde van de standaardafwijking. • **Hoog**: het hoge niveau is gelijk aan de waarde van de gemiddelde afwijking en driemaal de waarde van de standaardafwijking.
Duur van de anomalie (inkomend)	Er wordt alleen een waarschuwing voor een gedetecteerde anomalie gegenereerd als het afwijkende gedrag zich blijft voordoen gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 25.
Duur van de anomalie (uitgaand)	Er wordt alleen een waarschuwing voor een gedetecteerde anomalie gegenereerd als het afwijkende gedrag zich blijft voordoen gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 25.

Instellingen voor controle van het CPU-gebruik per proces

CPU-gebruik per proces: hiermee wordt het CPU-gebruik van het geselecteerde proces gecontroleerd. Als er meerdere instanties van hetzelfde proces zijn, wordt het totale gebruik door alle procesinstanties gecontroleerd en wordt er een waarschuwing gegenereerd wanneer aan de voorwaarden is voldaan.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Naam van proces	Naam van het proces dat u wilt controleren. Voer de procesnaam in zonder de extensie.
Operator	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempel	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in het bereik 1-100 (%) in. De standaardwaarde is 90.
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.

Instellingen voor controle van het Geheugengebruik per proces

Geheugengebruik per proces: hiermee wordt het geheugengebruik van het geselecteerde proces gecontroleerd. Als er meerdere instanties van hetzelfde proces zijn, wordt het totale gebruik door alle procesinstanties gecontroleerd en wordt er een waarschuwing gegenereerd wanneer aan de voorwaarden is voldaan.

Opmerking
De agents gebruiken de totale proceswerkset (privé en gedeeld) om de grootte van het geheugengebruik per proces te schatten. Daarom kan de weergegeven grootte in de widget verschillen van de grootte van het geheugengebruik dat wordt weergegeven in Windows Taakbeheer (privéwerkset).

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Naam van proces	Naam van het proces dat u wilt controleren. Voer de procesnaam in zonder de extensie.
Operator	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempel	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in (kb). De standaardwaarde is 1.
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.

Instellingen voor controle van de schijfoverdrachtssnelheid per proces

Schijfoverdrachtssnelheid per proces: hiermee wordt de lees- en schrijfsnelheid van het geselecteerde proces gecontroleerd. Als er meerdere instanties van hetzelfde proces zijn, wordt het totale gebruik door alle procesinstanties gecontroleerd en wordt er een waarschuwing gegenereerd wanneer aan de voorwaarden is voldaan.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Naam van proces	Klik op de naam van het proces dat u wilt controleren. Voer de procesnaam in zonder de extensie.
Wat moet er worden gecontroleerd	De snelheid die u wilt controleren. De volgende waarden zijn beschikbaar. • **Leessnelheid en schrijfsnelheid**. Dit is de standaardwaarde. • **Leessnelheid**

Instelling	Beschrijving
	• **Schrijfsnelheid**
Operator voor leessnelheid	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempelwaarde voor leessnelheid	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in (kb/s). De standaardwaarde is 0 kb/s.
Periode voor leessnelheid	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.
Operator voor schrijfsnelheid	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempelwaarde voor schrijfsnelheid	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in (kb/s). De standaardwaarde is 0 kb/s.
Periode voor schrijfsnelheid	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.

Instellingen voor controle van het netwerkgebruik per proces

Netwerkgebruik per proces: hiermee wordt het inkomende en uitgaande verkeer van het geselecteerde proces gecontroleerd. Als er meerdere instanties van hetzelfde proces zijn, wordt het totale gebruik door alle procesinstanties gecontroleerd en wordt er een waarschuwing gegenereerd wanneer aan de voorwaarden is voldaan voor alle instanties.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Naam van proces	Naam van het proces dat u wilt controleren. Voer de procesnaam in zonder de extensie.
Verkeersrichting	De verkeersrichting die u wilt controleren. De volgende waarden zijn beschikbaar. • **Inkomend verkeer en uitgaand verkeer**. Dit is de standaardwaarde. • **Inkomend verkeer** • **Uitgaand verkeer**
Operator voor inkomend verkeer	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempelwaarde voor inkomend verkeer	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in (kb/s). De standaardwaarde is 0 kb/s.
Periode voor inkomend verkeer	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.
Operator voor uitgaand verkeer	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar.

Instelling	Beschrijving
	• **Meer dan**: Dit is de standaardwaarde. • **Meer dan of gelijk aan** • **Minder dan** • **Minder dan of gelijk aan**
Drempelwaarde voor uitgaand verkeer	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in (kb/s). De standaardwaarde is 0 kb/s.
Periode voor uitgaand verkeer	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 5.

Instellingen voor controle van de Windows-servicestatus

Windows-servicestatus: hiermee wordt gecontroleerd of de Windows-service actief of gestopt is.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Servicenaam	Klik op de naam van de Windows-service die u wilt controleren. U kunt een servicenaam selecteren in de lijst met Windows-services. De lijst wordt gevuld door alle agents van de tenant nadat de scan van de software-inventaris is voltooid voor de workloads. U kunt ook een servicenaam toevoegen die niet in de lijst voorkomt. Dit is de enige beschikbare optie als er geen scan van de software-inventaris is uitgevoerd voor de workloads.
Servicestatus	Als de service de geselecteerde status heeft, wordt er een gebeurtenis gegenereerd. De volgende waarden zijn beschikbaar. • **Wordt uitgevoerd** • **Gestopt**: Dit is de standaardwaarde.
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 1.

Instellingen voor controle van de processtatus

Processtatus: hiermee wordt gecontroleerd of het geselecteerde proces actief of gestopt is. Als er meerdere instanties van hetzelfde proces zijn, wordt elke instantie van het proces gecontroleerd en wordt er een waarschuwing gegenereerd wanneer aan de voorwaarden is voldaan voor alle instanties van het proces.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Naam van proces	Klik op de naam van het proces dat u wilt controleren. Geef de naam van het uitvoerbare bestand op zonder de extensie.
Processtatus	Als het proces de geselecteerde status heeft, wordt er automatisch een gebeurtenis gegenereerd. De volgende waarden zijn beschikbaar. • **Wordt uitgevoerd** • **Gestopt**: Dit is de standaardwaarde.
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-60 (min.) in. De standaardwaarde is 1.

Instellingen voor controle van geïnstalleerde software

Geïnstalleerde software: hiermee worden de installatie, updates of verwijdering van softwaretoepassingen voor de workload gecontroleerd.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Welke software moet er worden gecontroleerd	Geef de software op die u wilt controleren. De volgende waarden zijn beschikbaar. • **Elke software**: Dit is de standaardwaarde. • **Specifieke software**
Namen van software	Deze instelling is beschikbaar als u de waarde **Specifieke software** selecteert voor **Welke software moet er worden gecontroleerd**. Voer de naam van een of meer softwaretoepassingen in. U kunt de naam van een softwaretoepassing selecteren in de lijst met Windows-services. De lijst wordt gevuld door alle agents van de tenant nadat de scan van de software-inventaris is voltooid voor de workloads. U

Instelling	Beschrijving
	kunt ook de naam van een softwaretoepassing toevoegen die niet in de lijst voorkomt. Dit is de enige beschikbare optie als er geen scan van de software-inventaris is uitgevoerd voor de workloads.
Status van installatie	Geef op of u geïnstalleerde, niet-geïnstalleerde of bijgewerkte software wilt controleren. De volgende waarden zijn beschikbaar. • **Geïnstalleerd**: Dit is de standaardwaarde. als u deze waarde selecteert, krijgt u een waarschuwing wanneer er een nieuwe softwaretoepassing wordt geïnstalleerd voor de workload. • **Bijgewerkt**: als u deze waarde selecteert, krijgt u een waarschuwing wanneer een softwaretoepassing wordt bijgewerkt. • **Niet geïnstalleerd**: Als u deze waarde selecteert, wordt er bij de controle een waarschuwing gegenereerd wanneer een softwaretoepassing wordt verwijderd of niet beschikbaar is voor de workload.

Instellingen voor controle van laatste herstart van systeem

Laatste herstart van systeem: geeft aan wanneer de workload de laatste keer opnieuw is opgestart.

U kunt de volgende instelling configureren voor de controle.

Instelling	Beschrijving
De workload is niet opnieuw gestart voor	De periode (aantal dagen) sinds de laatste keer dat de workload opnieuw is opgestart. Als de workload gedurende een langere periode dan de door u opgegeven periode niet opnieuw is opgestart, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in het bereik 1-180 (dagen) in. De standaardwaarde is 30.

Instellingen voor controle van het Windows-gebeurtenislogboek

Windows-gebeurtenislogboek: hiermee worden specifieke bedrijfskritieke gebeurtenissen in de Windows-gebeurtenislogboeken gecontroleerd.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Naam van gebeurtenislogboek	Selecteer een bepaald gebeurtenislogboek in een lijst met Windows-gebeurtenislogboeken die beschikbaar zijn in Windows Logboeken. De volgende waarden zijn beschikbaar.

Instelling	Beschrijving
	• **Elke**: Dit is de standaardwaarde. • **Toepassing** • **Beveiliging** • **Systeem**
Gebeurtenisbron	Naam van gebeurtenisbron U kunt de waarde selecteren in een lijst met gebeurtenisbronnen die zijn verzameld van alle agents van de tenant, of u kunt handmatig een nieuwe bronnaam invoeren. Als de scan van de software-inventaris is uitgeschakeld voor de tenant, is de lijst met gebeurtenisbronnen leeg.
Matching-modus	In dit veld kunt u opgeven of u de instellingen voor **Gebeurtenis-id's**, **Gebeurtenistype** en **Gebeurtenisbeschrijving** wilt koppelen met de operator **Elke** of **Alle**. De volgende waarden zijn beschikbaar. • **Elke**: Dit is de standaardwaarde. er wordt alleen een waarschuwing gegenereerd als aan een van de geselecteerde criteria wordt voldaan. • **Alle**-: Er wordt alleen een waarschuwing gegenereerd als aan alle geselecteerde criteria wordt voldaan.
Gebeurtenis-id's	Voer een of meerdere gebeurtenis-id's in (gescheiden door een komma) Als in het gebeurtenislogboek een van de gebeurteniscodes wordt gedetecteerd die u in dit veld hebt ingevoerd, wordt er een waarschuwing gegenereerd.
Gebeurtenistype	Selecteer een of meer typen gebeurtenissen die u wilt controleren. De volgende waarden zijn beschikbaar. • **Elke**: Dit is de standaardwaarde. • **Fout** • **Waarschuwing** • **Informatie** • **Voltooid-audit** • **Mislukt-audit**
Beschrijving van gebeurtenis	Specifieke trefwoorden of woordgroepen in de beschrijving van de gebeurtenis waarnaar u wilt zoeken. Trefwoorden en woordgroepen moeten worden ingevoerd tussen aanhalingstekens en gescheiden door een komma. Als een van de trefwoorden of woordgroepen worden gevonden die u hebt ingevoerd, wordt er een waarschuwing gegenereerd.
Aantal gevallen	Het minimum aantal gebeurtenissen met een gebeurtenis in het

Instelling	Beschrijving
	logboek gedurende de opgegeven periode voordat er een waarschuwing wordt gegenereerd. Voer een geheel getal in het bereik 1-1000 in.
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in en selecteer vervolgens de eenheid: minuten of uren. De standaardwaarde is 60 minuten.

Instellingen voor controle van de grootte van bestanden en mappen

Grootte van bestanden en mappen: hiermee wordt de totale grootte van de geselecteerde bestanden en mappen gecontroleerd.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Bestanden of mappen om te controleren	De paden van de bestanden of mappen die u wilt controleren. U kunt ook bestanden of mappen opgeven die u wilt uitsluiten van de controle. U kunt een van de volgende jokertekens gebruiken. • *: het sterretje komt overeen met nul of meer tekens in de naam van een bestand of map • ?: het vraagteken komt overeen met exact één teken in de naam van een bestand of map Voor Windows-workloads: • Het volledige pad moet beginnen met de stationsletter gevolgd door het scheidingsteken :\. • U kunt een slash of backslash gebruiken als scheidingsteken in een pad. • De naam van het bestand of de map mag niet eindigen met een spatie of punt. Voor macOS-workloads: • Het volledige pad moet beginnen vanuit de hoofdmap. • U kunt een slash gebruiken als scheidingsteken in een pad. • De naam van het bestand of de map mag niet eindigen met een spatie of punt. Het is niet verplicht om een specifieke locatie op te geven voor uitsluitingsfilters. De bestanden die zonder specifieke locatie worden ingevoerd, worden uitgesloten in de gecontroleerde mappen.

Instelling	Beschrijving
Operator	De operator is een voorwaardelijke functie die definieert hoe de prestaties voor de metriek moeten worden gemeten. De volgende waarden zijn beschikbaar. • **Meer dan**: Dit is de standaardwaarde. • **Minder dan**
Drempelwaarde	De drempelwaarde en de waarde van de **Operator** bepalen de normale prestaties van de gecontroleerde metriek. Wanneer de waarde van de gecontroleerde metriek niet binnen de norm is, wordt er automatisch een waarschuwing gegenereerd. Voer een geheel getal in (MB).
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 10-60 (min.) in. De standaardwaarde is 10.

Instellingen voor controle van de Windows Update-status

Windows Update-status: hiermee wordt de Windows Update-status van de workload gecontroleerd en wordt gecontroleerd of de nieuwste updates zijn geïnstalleerd.

Als u deze controle inschakelt, wordt er een waarschuwing gegenereerd voor de volgende gevallen.

- Windows Update is uitgeschakeld voor de workload.
- Windows Update is ingeschakeld voor de workload, maar de meest recente updates zijn niet geïnstalleerd.

Instellingen voor controle van de firewallstatus

Firewallstatus: hiermee wordt de status gecontroleerd van de ingebouwde of externe firewall die is geïnstalleerd voor de workload.

Als u deze controle inschakelt, wordt er een waarschuwing gegenereerd voor de volgende gevallen.

- De ingebouwde firewall van het besturingssysteem (Windows Defender Firewall of macOS-firewall) is uitgeschakeld en er is geen firewall van derden actief.
- Windows Defender Firewall is uitgeschakeld voor openbare netwerken.
- Windows Defender Firewall is uitgeschakeld voor privénetwerken.
- Windows Defender Firewall is uitgeschakeld voor domeinnetwerken.

Instellingen voor controle van mislukte aanmeldingen

Mislukte aanmeldingen: hiermee worden de mislukte aanmeldingspogingen voor de workload gecontroleerd.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Drempelwaarde voor mislukte aanmeldingspogingen	De drempelwaarde bepaalt de grenzen voor de normale prestaties van de gecontroleerde metriek. Wanneer de drempelwaarde wordt overschreden, is de waarde niet binnen de norm. Voer een geheel getal in. De standaardwaarde is 60.
Periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode. Voer een geheel getal in het bereik 1-24 in en selecteer een eenheid: uren of dagen. De standaardwaarde is 12.

Instellingen voor statuscontrole van antimalwaresoftware

Status van antimalwaresoftware: hiermee wordt een controle uitgevoerd van de ingebouwde of externe antimalwaresoftware die is geïnstalleerd voor de workload.

Als u deze controle inschakelt, genereert het systeem een waarschuwing wanneer een van de volgende toestanden wordt gedetecteerd.

- Antimalwaresoftware is niet geïnstalleerd voor de workload.
- Antimalwaresoftware is geïnstalleerd, maar is niet actief.
- Antimalwaresoftware is geïnstalleerd en actief, maar de malwaredefinities zijn niet up-to-date.

Opmerking
Deze voorwaarde wordt gecontroleerd voor Windows- en Windows Server-besturingssystemen.

Besturingssysteem	Ondersteunde antimalwaresoftware
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton Antivirus • SentinelOne • Trend Micro Endpoint Security met Apex One • Trend Micro Worry-Free Business

Besturingssysteem	Ondersteunde antimalwaresoftware
	• McAfee Endpoint Security • McAfee Endpoint Protection for SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud • BitDefender Antivirus • Sophos Intercept X Endpoint • Avast Business Antivirus • AVG AntiVirus Business Edition • AVG Internet Security Business Edition • Panda Endpoint Protection • Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security • Avira Antivirus • Comodo Internet Security • Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security **Opmerking** De controlefunctie werkt mogelijk ook met andere antimalwaretoepassingen, maar dit kan niet worden gegarandeerd.
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Antivirus voor Mac • Sophos Home • Sophos Endpoint Protection • Avast Security voor Mac • AVG AntiVirus voor Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus voor Mac

Besturingssysteem	Ondersteunde antimalwaresoftware
	• Comodo Antivirus voor Mac • K7 Antivirus voor Mac • Vipre Advanced Security • Total AV voor Mac **Opmerking** De controlefunctie werkt mogelijk ook met andere antimalwaretoepassingen, maar dit kan niet worden gegarandeerd.

Instellingen voor statuscontrole van de AutoRun-functie

Status van AutoRun-functie: hiermee wordt gecontroleerd of de AutoRun-functie voor verwisselbare media is ingeschakeld.

Vanwege de veiligheid raden we aan de AutoRun-functie voor verwisselbare media uit te schakelen voor de workload. Als de functie is ingeschakeld, wordt automatisch een waarschuwing gegenereerd.

Instellingen voor controle van aangepaste items

Aangepast: hiermee worden aangepaste objecten gecontroleerd door een script uit te voeren.

U kunt de volgende instellingen configureren voor de controle.

Instelling	Beschrijving
Script om uit te voeren	Lijst met vooraf gedefinieerde scripts uit de opslagplaats voor scripts.
Planning	Het tijdstip waarop het script wordt uitgevoerd en eventueel aanvullende voorwaarden waaraan moet worden voldaan om het script uit te voeren. De volgende waarden zijn beschikbaar. • **Planning op tijd**: het script wordt uitgevoerd op de exacte tijd, dagen, weken of maanden die u opgeeft. Dit is de standaardwaarde. **Type schema**: **Elk uur**, **Dagelijks** of **Maandelijks** **Uitvoeren binnen een datumbereik**: een tijdbereik waarbinnen het script moet worden uitgevoerd. • **Wanneer de gebruiker zich aanmeldt bij het systeem**: het script wordt uitgevoerd wanneer een gebruiker zich aanmeldt bij de workload. • **Wanneer de gebruiker zich afmeldt bij het systeem**: het script wordt uitgevoerd wanneer een gebruiker zich afmeldt bij de workload. • **Wanneer het systeem wordt opgestart**: het script wordt

Instelling	Beschrijving
	uitgevoerd wanneer het besturingssysteem van de workload start. • **Wanneer het systeem wordt uitgeschakeld**: het script wordt uitgevoerd wanneer de workload wordt uitgeschakeld. • **Wanneer het systeem online gaat**: het script wordt uitgevoerd zodra de workload online beschikbaar is. **Startvoorwaarden**: de taak wordt alleen uitgevoerd op een opgegeven tijdstip/bij een bepaalde gebeurtenis als aan de voorwaarde is voldaan. Als er meerdere voorwaarden zijn geselecteerd, moet tegelijkertijd aan al deze voorwaarden worden voldaan om een taak te kunnen starten. De voorwaarde **Voorkomen dat een geplande taak wordt gestart tijdens de slaap- of sluimerstand** is standaard geselecteerd. **Voer de taak na de start uit, zelfs als niet aan de startvoorwaarden wordt voldaan**: deze voorwaarde is standaard ingeschakeld. De standaardwaarde is 1 uur.
Account waarvoor het script wordt uitgevoerd	Het account waarvoor het script wordt uitgevoerd. De volgende waarden zijn beschikbaar. • **Systeemaccount**: Dit is de standaardwaarde. • **Momenteel aangemeld account**
Maximale duur	De maximale periode gedurende welke het script kan worden uitgevoerd voor de workload. Als het script tijdens deze periode niet wordt voltooid, mislukt de bewerking. Voer een geheel getal in het bereik 1-1440 (minuten) in. De standaardwaarde is 3.
Uitvoeringsbeleid voor PowerShell	Het uitvoeringsbeleid voor PowerShell. De volgende waarden zijn beschikbaar. • **Undefined** • **AllSigned** • **Bypass**: Dit is de standaardwaarde. • **RemoteSigned** • **Restricted** • **Unrestricted** Zie de Microsoft-documentatie voor meer informatie over deze velden.

Bewakingsschema

Controleschema's zijn schema's die u toepast voor uw beheerde workloads om de controlefunctionaliteit in te schakelen en te configureren.

Als er geen controleschema wordt toegepast voor een workload, zijn de controlefuncties niet beschikbaar voor de workload.

Opmerking
De beschikbaarheid van de instellingen die u in het controleschema kunt configureren, hangt af van het servicepakket dat is toegepast voor de tenant. Activeer het Advanced Management-pakket om toegang te krijgen tot alle instellingen.

Een controleschema maken

U kunt een controleschema maken en hieraan vervolgens workloads toewijzen om de controlefunctionaliteit te configureren voor de beheerde workloads.

Vereisten

De versie van de agent die is geïnstalleerd voor de workload, ondersteunt de controlefunctionaliteit.

Een controleschema maken:

Vanuit Controleschema's

1. Ga in de Bescherming-console naar **Beheer** > **Bewakingsschema**.
2. Maak een controleschema met een van de volgende twee opties.
   - Als er geen controleschema's worden weergegeven in de lijst, klikt u op **Maken**.
   - Als er wel controleschema's worden weergegeven in de lijst, klikt u op **Schema maken**.
3. Ga naar het venster **Controleschema maken** en doe het volgende (al naargelang het Advanced Management-pakket al dan niet is ingeschakeld voor uw tenant):
   - Als uw tenant standaardbeveiliging gebruikt, worden de volgende vier controles automatisch toegevoegd aan het controleschema: Schijfruimte, hardwarewijzigingen, laatste systeemherstart en Grootte van bestanden en mappen.
   - Als het Advanced Management-pakket is ingeschakeld voor uw tenant, selecteert u een van de sjabloonopties en klikt u op **Volgende**.

Optie	Beschrijving
Aanbevolen	Selecteer deze optie om een controleschema te maken met de standaardconfiguratie voor controles.
Aangepast	Gebruik deze optie om een volledig nieuw controleschema te maken.

4. [Optioneel] Als u de standaardnaam van het schema wilt wijzigen, klikt u op het potloodpictogram, voert u de naam van het schema in en klikt u op **OK**.
5. [Optioneel] Als u een controle wilt toevoegen aan het schema, klikt u op **Controle toevoegen**, selecteert u een controle in de lijst en klikt u vervolgens op **Toevoegen**.

   Opmerking
   De instellingen van de controle worden automatisch gevuld met de standaardwaarden.
   U kunt maximaal drie controles van hetzelfde type en maximaal 30 controles in totaal toevoegen aan een controleschema.

6. [Optioneel] Ga naar het scherm voor de controleparameters en wijzig de standaardinstellingen van de controle en waarschuwingen. Klik vervolgens op **Gereed**.

   Opmerking
   U kunt voor elke controle verschillende instellingen configureren. Zie "Configureerbare controles" (p. 1102) en "Controlewaarschuwingen configureren" (p. 1151) voor meer informatie.

7. [Optioneel] Als u een controle wilt verwijderen, klikt u op het prullenbakpictogram en vervolgens op **Verwijderen**.
8. [Optioneel] Workloads toevoegen aan het schema:
   a. Klik op **Workloads toevoegen**.
   b. Selecteer de workloads en klik vervolgens op **Toevoegen**.
   c. Als er compatibiliteitsproblemen zijn die u wilt oplossen, volgt u de procedure zoals beschreven in "Compatibiliteitsproblemen met controleschema's oplossen" (p. 1150).
9. Klik op **Maken**.

Vanuit Alle apparaten

1. In de Bescherming-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op de workload waarop u een controleschema wilt toepassen.
3. Klik op **Beschermen**.
4. Doe vervolgens het volgende (al naargelang er al dan niet een schema is toegepast op de workload):
   - Als er al een controleschema is toegepast voor de workload, klikt u op **Schema maken** en selecteert u **Controle**.
   - Als er geen controleschema is toegepast voor de workload, klikt u op **Schema toevoegen** en vervolgens op **Schema maken** en selecteert u **Controle**.
5. Ga naar het venster **Controleschema maken**, selecteer een van de sjabloonopties en klik vervolgens op **Volgende**.

Optie	Beschrijving
Aanbevolen	Selecteer deze optie om een controleschema te maken met de

Optie	Beschrijving
	standaardconfiguratie voor controles.
Aangepast	Gebruik deze optie om een volledig nieuw controleschema te maken.

6. [Optioneel] Als u de standaardnaam van het schema wilt wijzigen, klikt u op het potloodpictogram, voert u de naam van het schema in en klikt u op **OK**.
7. [Optioneel] Als u de standaardinstellingen van de controle en waarschuwingen wilt wijzigen, configureert u de nieuwe waarden en klikt u op **Gereed**.

   Opmerking
   U kunt maximaal drie controles van hetzelfde type en maximaal 30 controles in totaal toevoegen aan een controleschema.

8. [Optioneel] Ga naar het scherm voor de controleparameters en wijzig de standaardinstellingen van de controle en waarschuwingen. Klik vervolgens op **Gereed**.

   Opmerking
   U kunt voor elke controle verschillende instellingen configureren. Zie "Configureerbare controles" (p. 1102) en "Controlewaarschuwingen configureren" (p. 1151) voor meer informatie.

9. [Optioneel] Als u een controle wilt verwijderen, klikt u op het prullenbakpictogram en vervolgens op **Verwijderen**.
10. Klik op **Maken**.

Workloads toevoegen aan controleschema's

Indien gewenst, kunt u workloads achteraf toevoegen aan een controleschema (nadat het schema is gemaakt).

Vereisten

- 2FA is ingeschakeld voor uw gebruikersaccount.
- De versie van de agent die is geïnstalleerd voor de workload, ondersteunt de controlefunctionaliteit.
- Er is ten minste één controleschema beschikbaar.

Een workload toevoegen aan een controleschema:

Vanuit Bewakingsschema

1. Ga in de Bescherming-console naar **Beheer** > **Bewakingsschema**.
2. Klik op het controleschema.
3. Al naargelang het schema al dan niet is toegepast op een workload, doet u het volgende:

- Als het schema nog niet is toegepast op workloads: klik op **Workloads toevoegen**.
- Als het schema wel al is toegepast op workloads: klik op **Workloads beheren**.

4. Selecteer een workload in de lijst en klik vervolgens op **Toevoegen**.
5. Klik op **Opslaan**.
6. Klik indien nodig op **Bevestigen** om de vereiste servicequota toe te voegen aan de workload.

Vanuit Alle apparaten

1. In de Bescherming-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op de workload waarop u een controleschema wilt toepassen.
3. Klik op **Beschermen**.
4. Zoek het controleschema waaraan u de workload wilt toevoegen en klik op **Toepassen**.
5. Klik indien nodig op **Bevestigen** om de vereiste servicequota toe te voegen aan de workload.

Controleschema's intrekken

U kunt een controleschema intrekken voor een workload waarop het schema is toegepast.

Vereisten

Er wordt ten minste één controleschema toegepast op de workload.

Een controleschema intrekken:

1. In de Bescherming-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op de workload en klik vervolgens op **Beschermen**.
3. Klik op het pictogram **Meer acties** van het controleschema dat u wilt intrekken en klik vervolgens op **Intrekken**.

Automatische responsacties configureren

Automatische responsacties voor de gebeurtenissen met een waarschuwing zijn vooraf gedefinieerde acties of maatregelen die automatisch worden geactiveerd als reactie op gedetecteerde gebeurtenissen of incidenten. Deze acties zijn bedoeld om potentiële bedreigingen te beperken en schade tot een minimum te beperken.

U kunt een of meerdere automatische responsacties configureren voor de gebeurtenissen met een waarschuwing. Er kunnen maximaal 20 automatische responsacties per controle worden uitgevoerd.

Automatische responsacties configureren:

1. Ga in de Bescherming-console naar **Beheer** > **Controleschema's**.
2. Selecteer het controleschema waarvoor u automatische responsacties wilt configureren.

3. Selecteer de controle waarvoor u automatische responsacties wilt configureren, of, als u nog geen controles hebt toegevoegd: klik op **Controle toevoegen**, klik op de controle in de lijst, klik op **Toevoegen** en selecteer vervolgens de controle.
4. Klik op de link naast **Automatische responsacties**.
5. Voeg in het venster **Automatische responsacties** een of meerdere responsacties toe die automatisch worden uitgevoerd wanneer een waarschuwing wordt gegenereerd.
6. Configureer elke responsactie. Als u bijvoorbeeld de responsactie **Een Windows-service starten** hebt toegevoegd, doet u het volgende:
   a. Klik naast **Windows service** op **Opgeven**.
   b. Selecteer in het veld **Service** een service die als responsactie moet worden gestart.
   c. Klik op **Gereed**.
7. Gebruik de pijlen omhoog en omlaag in de lijst met alle toegevoegde responsacties of sleep de responsacties om de volgorde in te stellen.
8. Configureer hoe opeenvolgende responsacties moeten worden afgehandeld als een eerdere responsactie mislukt. Selecteer een van de volgende opties:
   a. **Doorgaan met de volgende responsactie**.
   b. **Niet doorgaan met de volgende responsactie**.
9. Klik op **Gereed**.

   U ziet het aantal geconfigureerde acties naast de instelling voor **Automatische responsacties** van uw controleschema. U kunt deze acties bewerken of verwijderen en de nieuwe acties later op elk gewenst moment toevoegen.

De volgende tabel bevat alle automatische responsacties die beschikbaar zijn in de controle-instellingen, met een beschrijving.

Automatische responsactie	Beschrijving	Ondersteund besturingssysteem
Een script uitvoeren	Als u deze actie toevoegt, kunt u: 1. Een script selecteren dat u wilt uitvoeren voor de workload. 2. Het account opgeven waarvoor u het script wilt uitvoeren. 3. De maximale duur van de bewerking opgeven. 4. Het uitvoeringsbeleid voor PowerShell opgeven. 5. Een script uitvoeren. Als u deze actie wilt uitvoeren, hebt u een licentie voor een Advanced Management-pakket nodig voor de workload (indien nog niet toegewezen).	Windows, macOS

Automatische responsactie	Beschrijving	Ondersteund besturingssysteem
	Het geselecteerde externe script met opgegeven parameters wordt automatisch uitgevoerd wanneer aan de voorwaarden is voldaan.	
De workload opnieuw opstarten	Als u deze actie toevoegt, wordt de workload op afstand automatisch opnieuw opgestart wanneer aan de voorwaarden is voldaan.	Windows, macOS
Het proces stoppen	Als u deze actie toevoegt, kunt u aangeven welk proces moet worden gestopt door de procesnaam handmatig in te voeren. Het proces wordt automatisch gestopt wanneer aan de voorwaarden is voldaan.	Windows, macOS
De Windows-service starten	Als u deze actie toevoegt, kunt u selecteren welke Windows-service u wilt starten in de dynamische lijst van services die door de agents wordt ingevuld. De service wordt automatisch gestart wanneer aan de voorwaarden is voldaan.	Windows
De Windows-service stoppen	Als u deze actie toevoegt, kunt u selecteren welke Windows-service u wilt stoppen in de dynamische lijst van services die door de agents wordt ingevuld. De service wordt automatisch gestopt wanneer aan de voorwaarden is voldaan.	Windows
Windows Update inschakelen	Als u deze actie toevoegt, wordt Windows Update automatisch ingeschakeld wanneer aan de voorwaarden is voldaan. Deze actie is alleen beschikbaar voor controle van de status van Windows Update.	Windows
AutoRun uitschakelen	Als u deze actie toevoegt, wordt de	Windows

Automatische responsactie	Beschrijving	Ondersteund besturingssysteem
voor verwisselbare stations	AutoRun-functie op verwisselbare opslagmedia automatisch uitgeschakeld voor de workload wanneer aan de voorwaarden is voldaan. Deze actie is alleen beschikbaar voor controle van de status van de AutoRun-functie.	

Aanvullende acties met monitoringplannen

Vanuit het scherm **Monitoringplannen** kunt u de volgende extra bewerkingen uitvoeren met monitoringplannen: details, activiteiten en waarschuwingen bekijken, namen wijzigen en items bewerken, inschakelen, uitschakelen, klonen, exporteren, verwijderen, instellen als favoriet en instellen als standaard.

Details weergeven

De details van een controleschema bekijken:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Details weergeven**.
3. [Optioneel] Als u de details wilt bekijken van een controle die is ingeschakeld in het schema, klikt u op de naam van de betreffende controle.

Bewerken

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een schema bewerken:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Bewerken**.
3. [Optioneel] Als u een controle uit het schema wilt verwijderen, klikt u op het pictogram van de prullenbak rechts van de naam van de controle.
4. [Optioneel] Gebruik de schakelaar naast de naam van de controle om een controle in het schema in of uit te schakelen.
5. [Optioneel] Als u de parameters van de controle wilt bewerken, doet u het volgende.
   a. Klik op de naam van de controle.
   b. Klik op het overzicht van de controleparameters.
   c. Ga naar het scherm **Controleparameters**, configureer de parameters en klik vervolgens op **Gereed**.

Opmerking
U kunt voor elke controle verschillende instellingen configureren. Zie "Configureerbare controles" (p. 1102) en "Controlewaarschuwingen configureren" (p. 1151) voor meer informatie.

d. Sluit het scherm en bevestig de wijzigingen.

6. [Optioneel] Als u een controle wilt toevoegen, klikt u op **Controle toevoegen** en bewerkt u indien nodig de parameters, zoals uitgelegd in de vorige stap.
7. Klik op **Opslaan**.

Activiteiten

De activiteiten voor een controleschema bekijken:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Activiteiten**.
3. Klik op een activiteit om meer details te bekijken.

Waarschuwingen

De waarschuwingen bekijken:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Waarschuwingen**.

Naam wijzigen

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

De naam van een controleschema wijzigen

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Naam wijzigen**.
3. Voer de nieuwe naam van het schema in en klik vervolgens op **OK**.

Inschakelen

Vereisten

- 2FA is ingeschakeld voor uw gebruikersaccount.
- Het controleschema wordt toegepast op ten minste één workload.

Een controleschema inschakelen:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Inschakelen**.

Uitschakelen

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een controleschema uitschakelen:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Uitschakelen**.

Klonen

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een controleplan klonen:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Klonen**.
3. Klik op **Maken**.

Exporteren

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een controleplan exporteren:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Exporteren**.
   De planconfiguratie wordt geëxporteerd in een JSON-indeling naar de lokale machine.

Verwijderen

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Een controleschema verwijderen:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Verwijderen**.
3. Selecteer **Ik bevestig** en klik vervolgens op **Verwijderen**.

Instellen als standaard

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Monitoringplan instellen als standaard:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Instellen als standaard**.
3. Klik in het bevestigingsvenster op **Instellen**.
   In het scherm **Monitoringplannen** wordt de tag **Standaard** weergegeven naast de naam van het plan.

Toevoegen aan favorieten

Vereisten

2FA is ingeschakeld voor uw gebruikersaccount.

Monitoringplan instellen als favoriet:

1. Klik in het scherm **Monitoringplannen** op het pictogram **Meer acties** van het monitoringplan.
2. Klik op **Toevoegen aan favorieten**.
   In het scherm **Monitoringplannen** wordt een pictogram van een ster weergegeven naast de naam van het plan.

Compatibiliteitsproblemen met controleschema's

In sommige gevallen kunnen compatibiliteitsproblemen optreden wanneer u een controleschema toepast op een workload. De volgende compatibiliteitsproblemen kunnen voorkomen:

- Incompatibel besturingssysteem: dit probleem doet zich voor wanneer het besturingssysteem van de workload niet wordt ondersteund.
- Niet-ondersteunde agent: dit probleem doet zich voor wanneer de versie van de beveiligingsagent voor de workload verouderd is en geen ondersteuning biedt voor de controlefunctionaliteit.
- Onvoldoende quota: dit probleem doet zich voor wanneer de tenant onvoldoende servicequota heeft om aan de geselecteerde workloads toe te wijzen.

Als het controleschema wordt toegepast op maximaal 150 afzonderlijk geselecteerde workloads, wordt u gevraagd de bestaande conflicten op te lossen voordat u het schema opslaat. U kunt een conflict oplossen door de hoofdoorzaak ervan weg te nemen of door de betreffende workloads te verwijderen uit het schema. Zie "Compatibiliteitsproblemen met controleschema's oplossen" (p. 1150) voor meer informatie. Als u het schema opslaat zonder de conflicten op te lossen, wordt het automatisch uitgeschakeld voor de incompatibele workloads en worden er waarschuwingen weergegeven.

Als het controleschema wordt toegepast op meer dan 150 workloads of op apparaatgroepen, wordt het eerst opgeslagen en vervolgens gecontroleerd op compatibiliteit. Het schema wordt automatisch uitgeschakeld voor de incompatibele workloads en er worden waarschuwingen weergegeven.

Compatibiliteitsproblemen met controleschema's oplossen

Bij het maken van een nieuw controleschema kunt u verschillende acties uitvoeren om compatibiliteitsproblemen op te lossen, al naargelang de oorzaak van de problemen.

Compatibiliteitsproblemen oplossen:

1. Klik op **Problemen bekijken**.
2. [Optioneel] Compatibiliteitsproblemen met incompatibele agents oplossen door workloads te verwijderen uit het schema:
   a. Ga naar het tabblad **Niet-compatibel besturingssysteem** en selecteer de workloads die u wilt verwijderen.
   b. Klik op **Workloads verwijderen uit schema**.
   c. Klik op **Verwijderen** en vervolgens op **Sluiten**.
3. [Optioneel] Compatibiliteitsproblemen met incompatibele besturingssystemen oplossen door een controle uit te schakelen in het schema:
   a. Ga naar het tabblad **Niet-compatibel besturingssysteem** en selecteer de controles die u wilt verwijderen.
   b. Klik op **Controle uitschakelen**.
   c. Klik op **Uitschakelen** en klik vervolgens op **Sluiten**.
4. [Optioneel] Compatibiliteitsproblemen met niet-ondersteunde agents oplossen door workloads te verwijderen uit het schema:
   a. Ga naar het tabblad **Niet-ondersteunde agents** en selecteer de workloads die u wilt verwijderen.
   b. Klik op **Workloads verwijderen uit schema**.
   c. Klik op **Verwijderen** en vervolgens op **Sluiten**.
5. [Optioneel] Als u compatibiliteitsproblemen met niet-ondersteunde agents wilt oplossen door de agentversie bij te werken, klikt u op **Ga naar lijst met agents**.

   Opmerking
   Deze optie is alleen beschikbaar voor klantbeheerders.

6. [Optioneel] Compatibiliteitsproblemen met onvoldoende quota oplossen door workloads te verwijderen uit het schema:
   a. Ga naar het tabblad **Onvoldoende quota** en selecteer de workloads die u wilt verwijderen.
   b. Klik op **Workloads verwijderen uit schema**.

c. Klik op **Verwijderen** en vervolgens op **Sluiten**.

7. [Optioneel] Compatibiliteitsproblemen met onvoldoende quota oplossen door de quota van de tenant te verhogen:
   a. Klik op het tabblad **Onvoldoende quota** op **Ga naar beheerportal**.
   b. Verhoog de servicequota voor de klant.

> **Opmerking**
> Deze optie is alleen beschikbaar voor partnerbeheerders.

Machine learning-modellen opnieuw instellen

U kunt de modellen van een workload opnieuw instellen wanneer ze om een of andere reden verouderd zijn of ongeldig zijn geworden. Met deze actie worden de gemaakte modellen verwijderd, evenals de gegevens die voor de workload zijn verzameld tijdens de controles van het type op basis van anomalieën. De machine learning-modellen voor de workload worden vervolgens helemaal opnieuw getraind.

De machine learning-modellen voor een workload opnieuw instellen:

1. In de Bescherming-console: ga naar **Apparaten** > **Alle apparaten**.
2. Klik op een workload in de lijst en klik vervolgens op et tabblad **Details**.
3. Klik in het gedeelte **Machine learning-modellen opnieuw instellen** op **Opnieuw instellen**.
4. Klik in het bevestigingsvenster op **Opnieuw instellen**.

Controlewaarschuwingen

Controlewaarschuwingen worden weergegeven in de Bescherming-console en worden via e-mail verzonden wanneer het gecontroleerde gedrag van workloads buiten de norm is. Dankzij de waarschuwingen worden belanghebbenden zo snel mogelijk geïnformeerd over problemen in de IT-omgeving van de organisatie.

> **Opmerking**
> Als u controlewaarschuwingen via e-mail wilt inschakelen, moet u minstens één beleid voor e-mailmeldingen configureren voor het betreffende waarschuwingstype. Voor meer informatie: zie "Beleid voor e-mailmeldingen configureren" (p. 1160).

Controlewaarschuwingen configureren

U kunt de instellingen voor waarschuwingen van de controle configureren wanneer u een controle toevoegt aan een controleschema of wanneer u een controle bewerkt die al beschikbaar is in een controleschema.

Controlewaarschuwingen configureren:

1. Ga in het venster **Controleparameters** naar het gedeelte **Waarschuwingen genereren**.
2. Ga naar **Ernstgraad van de waarschuwing** en selecteer de ernstgraad die overeenkomt met de prioriteit van de waarschuwing.

Optie	Beschrijving
Kritiek	Deze waarschuwingen hebben de hoogste prioriteit en zijn gerelateerd aan problemen die essentieel zijn voor de werking van de workload. Los deze problemen zo snel mogelijk op.
Fout	Een foutmelding is niet zo ernstig en geeft aan dat er iets mis is of zich niet normaal gedraagt. Los de problemen tijdig op om te voorkomen dat ze ernstigere problemen veroorzaken.
Waarschuwing	Een waarschuwingsmelding geeft aan dat er een toestand is waarvan u op de hoogte moet zijn, maar die mogelijk nog geen probleem veroorzaakt. Los deze problemen op nadat u de problemen hebt opgelost die kritieke waarschuwingen en foutmeldingen veroorzaken. Dit is de standaardwaarde.
Informatie	Deze waarschuwingen hebben de laagste prioriteit. De ernstgraad Informatie duidt niet op een probleem. Dergelijke waarschuwingen geven informatie over acties in verband met een gecontroleerd object.

3. Ga naar **Frequentie van de waarschuwing** en selecteer hoe vaak er een waarschuwing moet worden gegenereerd wanneer aan de voorwaarde wordt voldaan.

Optie	Beschrijving
Eén keer tot de controle is voltooid	Er wordt eenmalig een waarschuwing gegenereerd totdat de controle met goed gevolg is voltooid. Dit is de standaardwaarde.
Na X opeenvolgende mislukte controles	Er wordt een waarschuwing gegenereerd na X opeenvolgende mislukte controles (waarbij X een geheel getal is).

4. Klik in **Bericht van de waarschuwing** op het potloodpictogram om het standaardwaarschuwingsbericht te bewerken dat zal worden gebruikt voor de automatisch gegenereerde waarschuwingen. U kunt een aangepast waarschuwingsbericht met variabelen opgeven. Zie "Variabelen van controlewaarschuwingen" (p. 1153) voor meer informatie over de variabelen die u kunt gebruiken.

   Opmerking
   Voor sommige controles kunt u meer dan één waarschuwingsbericht configureren.

5. Schakel **Automatische oplossing van waarschuwingen** in als u wilt dat de waarschuwing automatisch wordt ingesteld op opgelost wanneer de gecontroleerde metriek weer de status Normaal heeft en het gedrag weer normaal is. Deze instelling is standaard ingeschakeld.

Variabelen van controlewaarschuwingen

U kunt verschillende waarschuwingsvariabelen configureren voor verschillende controles. Alleen variabelen tussen {{}} kunnen worden gebruikt.

De volgende tabel bevat meer informatie over de beschikbare variabelen.

Variabele	Beschrijving	Beschikbaar voor controle
naam_schema	De naam van het beleid	Alle controles
naam_controle	De naam van het subbeleid in het controleschema	Alle controles
naam_workload	De naam van de workload	Alle controles
drempelwaarde	Specifieke controlevoorwaarden of drempelwaarden voor het genereren van een waarschuwing	Alle controles die controles op basis van op drempelwaarden ondersteunen.
drempelwaarde-eenheid	De eenheid die is gekoppeld aan de drempelwaarde. Bijvoorbeeld: %, MB of mb/s.	Alle controles die controles op basis van op drempelwaarden ondersteunen.
periode	Er wordt alleen een waarschuwing voor een gedetecteerd probleem gegenereerd als de waarde van de metriek niet binnen de norm is gedurende de opgegeven periode.	Alle controles die controles op basis van op drempelwaarden ondersteunen.
tijdeenheid	De eenheid die wordt gekoppeld aan de periode (sec/min/uur/dag).	Alle controles die controles op basis van op drempelwaarden ondersteunen.
waarde_anomalie	De waarde van de anomalie	Alle controles die controles op basis van anomalieën ondersteunen.
anomalie-eenheid	De eenheid die wordt gekoppeld aan de waarde van de anomalie	Alle controles die controles op basis van anomalieën ondersteunen.
waarde_afwijking	De waarde van de afwijking	Alle controles die controles op basis van anomalieën ondersteunen.
afwijking-eenheid	De eenheid die wordt gekoppeld aan	Alle controles die controles

Variabele	Beschrijving	Beschikbaar voor controle
	de waarde van de afwijking	op basis van anomalieën ondersteunen.
naam_station	Het station voor Windows of partitie voor macOS	Schijfruimte,
CPU-model	Het model van de gecontroleerde CPU	CPU-temperatuur
GPU-model	Het model van de gecontroleerde GPU	GPU-temperatuur
hardwaremodel	Het model van het gecontroleerde onderdeel	Hardwarewijzigingen
hardwareonderdeel	Het type van de gecontroleerde hardware	Hardwarewijzigingen
hardwaremodel_oud	Het model van het gecontroleerde onderdeel dat is vervangen	Hardwarewijzigingen
hardwaremodel_nieuw	Het model van het nieuwe gecontroleerde onderdeel dat is toegevoegd	Hardwarewijzigingen
schijfmodel	Het model van de schijf	Schijfoverdrachtssnelheid
netwerkadaptermodel	Het model van de netwerkadapter	Netwerkgebruik
procesnaam	De naam van het proces	CPU-gebruik per proces Geheugengebruik per proces Schijfoverdrachtssnelheid per proces Netwerkgebruik per proces Processtatus
servicenaam	De naam van de service	Windows-servicestatus
softwarenaam	De naam van de softwaretoepassing	Geïnstalleerde software
softwareversie	De versie van de softwaretoepassing	Geïnstalleerde software
softwareversie_oud	De versie van de softwaretoepassing vóór de update	Geïnstalleerde software

Variabele	Beschrijving	Beschikbaar voor controle
softwareversie_nieuw	De versie van de nieuwe of bijgewerkte softwaretoepassing	Geïnstalleerde software
aantal_gevallen	Het aantal keer dat een gebeurtenis is vermeld in het logboek	Windows-gebeurtenislogboek
gebeurtenistypen	Het type gebeurtenis	Windows-gebeurtenislogboek
bron_gebeurtenis	De bron van de gebeurtenis	Windows-gebeurtenislogboek
naam_ gebeurtenislogboek	De naam van de gebeurtenis	Windows-gebeurtenislogboek
naam_firewallsoftware	De naam van de firewallsoftware	Firewallstatus
naam_ antimalwaresoftware	De naam van de antimalwaresoftware	Status van antimalwaresoftware
gebruikersnaam	De naam van de gebruiker	Status van AutoRun-functie
scriptnaam	De naam van het script	Aangepast

Handmatige responsacties

Wanneer u een waarschuwing ziet, kunt u een responsactie selecteren die u wilt uitvoeren voor de gebeurtenissen met waarschuwingen.

Een handmatige responsactie uitvoeren

1. Ga in de Bescherming-console naar **Waarschuwingen**.
2. Open de waarschuwing die u wilt bekijken.
3. Klik op **Responsactie** en selecteer vervolgens een reactieactie in de vervolgkeuzelijst.

De lijst met beschikbare responsacties voor een bepaalde waarschuwing is afhankelijk van het waarschuwingstype, de beschikbaarheid van functies voor een bepaalde tenant en het besturingssysteem van de workload.

De volgende tabel bevat alle mogelijke handmatige responsacties, met een beschrijving. U kunt deze gebruiken als referentie.

Handmatige responsactie	Beschrijving	Ondersteund besturingssysteem
Trend van schijfruimtegebruik bekijken	Hiermee opent u een venster met de grafiek **Schijfruimtegebruik**. Hier kunt u het volgende kunt doen:	Windows, macOS

Handmatige responsactie	Beschrijving	Ondersteund besturingssysteem
	• Bekijken hoe het schijfruimtegebruik in de loop van de tijd is veranderd (gedurende de laatste 1 dag / 7 dagen / 1 maand). • De delta voor schijfruimtegebruik in relatieve waarde (%) bekijken voor de geselecteerde periode.	
Trend van toename van bestandsgrootte bekijken	Hiermee opent u een venster met de grafiek **Toename van bestandsgrootte**. Hier kunt u het volgende doen: • Bekijken hoe de totale grootte van de gecontroleerde bestanden en mappen in de loop van de tijd is veranderd (gedurende de laatste 1 dag / 7 dagen / 1 maand). • De delta voor de totale bestandsgrootte in relatieve waarde (%) bekijken voor de geselecteerde periode.	Windows, macOS
Een script uitvoeren	Hiermee opent u een venster waarin u het volgende kunt doen: 1. Een script selecteren dat u wilt uitvoeren voor de workload. 2. Het account opgeven waarvoor u het script wilt uitvoeren. 3. De maximale duur van de bewerking opgeven. 4. Het uitvoeringsbeleid voor PowerShell opgeven. 5. Een script uitvoeren. Als u deze actie wilt uitvoeren, hebt u een licentie voor een Advanced Management-pakket nodig voor de workload (indien nog niet toegewezen).	Windows, macOS
Verbinding maken via NEAR	Acronis Connect Client maakt een externe verbinding.	Windows, macOS
Verbinding maken via RDP	Acronis Connect Client maakt een externe verbinding.	Windows

Handmatige responsactie	Beschrijving	Ondersteund besturingssysteem
Hardware-inventaris openen	U wordt omgeleid naar het tabblad **Hardware-inventaris** voor de huidige workload.	Windows, macOS
De top 10 processen bekijken waarbij de CPU is geladen	Hiermee opent u een venster met de top 10 processen waarbij de CPU is geladen en die mogelijk oververhitting hebben veroorzaakt (de momentopname van het systeem op het moment dat de waarschuwing is gegenereerd).	Windows, macOS
De top 10 processen bekijken waarbij de GPU is geladen	Hiermee opent u een venster met de top 10 processen waarbij de GPU is geladen en die mogelijk oververhitting hebben veroorzaakt (de momentopname van het systeem op het moment dat de waarschuwing is gegenereerd).	Windows, macOS
De top 10 processen bekijken waarbij het geheugen is geladen	Hiermee opent u een venster met de top 10 processen waarbij het geheugen is geladen (de momentopname van het systeem op het moment dat de waarschuwing is gegenereerd).	Windows, macOS
De top 10 processen bekijken waarbij de schijf is geladen	Hiermee opent u een venster met de top 10 processen waarbij de schijf is geladen (de momentopname van het systeem op het moment dat de waarschuwing is gegenereerd).	Windows, macOS
De top 10 processen bekijken waarbij het netwerk is geladen	Hiermee opent u een venster met de top 10 processen waarbij de netwerkinterfaceadapter is geladen (de momentopname van het systeem op het moment dat de waarschuwing is gegenereerd).	Windows, macOS
Resourcegebruik bekijken per proces	Hiermee opent u een venster met gedetailleerde informatie over het gebruik van hardwareresources door het betreffende proces: CPU-gebruik, geheugengebruik, schijf-I/O, netwerkgebruik.	Windows, macOS

Handmatige responsactie	Beschrijving	Ondersteund besturingssysteem
Workload opnieuw opstarten	Hiermee opent u een bevestigingsvenster. Na de bevestiging wordt de workload opnieuw opgestart.	Windows, macOS
Windows-service starten	Hiermee opent u een bevestigingsvenster. Na de bevestiging wordt de Windows-service gestart.	Windows
Windows-service stoppen	Hiermee opent u een bevestigingsvenster. Na de bevestiging wordt de Windows-service gestopt.	Windows
Proces stoppen	Hiermee opent u een bevestigingsvenster. Na de bevestiging wordt het in de waarschuwing vermelde proces gestopt.	Windows, macOS
Windows Update inschakelen	Hiermee opent u een bevestigingsvenster. Na de bevestiging wordt Windows Update ingeschakeld.	Windows
AutoRun-functie uitschakelen voor verwisselbare stations	Hiermee opent u een bevestigingsvenster. Na de bevestiging wordt de AutoRun-functie uitgeschakeld op het systeemniveau van de workload.	Windows

Belangrijk
Om veiligheidsredenen is tweeledige verificatie vereist voor de volgende handmatige responsacties:

- Een script uitvoeren
- Verbinding maken via NEAR
- Verbinding maken via RDP
- Workload opnieuw opstarten
- Windows-service starten
- Windows-service stoppen
- Proces stoppen
- Windows Update inschakelen
- AutoRun-functie uitschakelen voor verwisselbare stations

Controlewaarschuwingen bekijken voor een workload

Op het tabblad **Waarschuwingen** kunt u de controlewaarschuwingen van een specifieke workload bekijken en diverse acties in verband met een waarschuwing uitvoeren.

Controlewaarschuwingen bekijken voor een workload:

1. Ga in de Bescherming-console naar **Alle apparaten**.
2. Klik op een workload en selecteer het tabblad **Waarschuwingen**.
3. [Optioneel] In het deelvenster voor controlewaarschuwingen voert u een van de volgende acties uit:
   - Als u de waarschuwing wilt wissen: klik op **Wissen**.
   - Voor een responsactie klikt u op **Responsactie** en op de betreffende actie.
   - Als u contact wilt opnemen met het ondersteuningsteam, klikt u op **Ondersteuning ontvangen**.
4. [Optioneel] Als u alle controlewaarschuwingen voor de workload wilt wissen, klikt u op **Alles wissen**.

Het waarschuwingslogboek met controlewaarschuwingen bekijken

U kunt alle gebeurtenissen in verband met een controlewaarschuwing bekijken in chronologische volgorde: de uitgevoerde responsacties (zowel automatisch als handmatig) en de e-mailmeldingen die zijn verzonden.

Het auditlogboek van een controlewaarschuwing bekijken

1. Ga in de Bescherming-console naar **Waarschuwingen**.
2. Open de **Tabelweergave**.
3. Ga naar de lijst met waarschuwingen en selecteer de controlewaarschuwing die u wilt verwijderen.
4. Klik op **Details** en klik vervolgens op **Waarschuwingslogboek**.

Beleid voor e-mailmeldingen configureren

Het beleid voor e-mailmeldingen bepaalt welke gebruikers e-mailmeldingen ontvangen over diverse controles.

Met het beleid voor e-mailmeldingen kunt u de volgende acties uitvoeren vanuit het scherm **E-mailmeldingen**: items toevoegen, bewerken, inschakelen, uitschakelen en verwijderen.

Toevoegen

Een nieuw beleid voor e-mailmeldingen toevoegen:

1. Ga in de Bescherming-webconsole naar **Instellingen** > **E-mailmeldingen**.
2. Klik op **Beleid toevoegen**.
3. Klik op **Ontvangers selecteren**.
4. Ga naar het scherm **Ontvangers selecteren**, selecteer de gebruikers die e-mail met waarschuwingen moeten ontvangen en klik op **Selecteren**.
5. Ga naar **Typen waarschuwingen** en selecteer de controles waarvoor waarschuwingen per e-mail moeten worden gegenereerd.
6. Klik op **Toevoegen**.

Bewerken

Een beleid voor e-mailmeldingen bewerken:

1. Ga in de Bescherming-webconsole naar **Instellingen** > **E-mailmeldingen**.
2. Klik op het ellipspictogram van het meldingenbeleid en klik vervolgens op **Bewerken**.
3. [Optioneel] Als u de ontvangers wilt wijzigen, klikt u op **Ontvangers bewerken**. Voeg gebruikers toe of verwijder ze uit de lijst en klik op **Selecteren**.
4. [Optioneel] Ga naar **Typen waarschuwingen** en selecteer de typen controlewaarschuwingen die u wilt laten verzenden naar de geselecteerde ontvangers.
5. Klik op **Opslaan**.

Inschakelen

Een beleid voor e-mailmeldingen inschakelen:

1. Ga in de Bescherming-webconsole naar **Instellingen** > **E-mailmeldingen**.
2. Ga naar het scherm **E-mailmeldingen** en klik op het ellipspictogram (**...**) van het beleid voor e-mailmeldingen.
3. Klik op **Inschakelen**.

Uitschakelen

Een beleid voor e-mailmeldingen uitschakelen:

1. Ga in de Bescherming-webconsole naar **Instellingen** > **E-mailmeldingen**.
2. Ga naar het scherm **E-mailmeldingen** en klik op het ellipspictogram (**...**) van het beleid voor e-mailmeldingen.
3. Klik op **Uitschakelen**.

Verwijderen

Een beleid voor e-mailmeldingen verwijderen:

1. Ga in de Bescherming-webconsole naar **Instellingen** > **E-mailmeldingen**.
2. Ga naar het scherm **E-mailmeldingen** en klik op het ellipspictogram (**...**) van het beleid voor e-mailmeldingen.
3. Klik op **Verwijderen** en klik op **Bevestigen**.

Controlegegevens bekijken

Voor elke workload kunt u het volgende bekijken: de lijst met toegepaste controles, de huidige status van de controles en de historische prestatiegegevens in een grafisch overzicht. U kunt deze informatie gebruiken om de status van de workload te analyseren en hoe de status in de loop van de tijd is veranderd.

Vereisten

- Er wordt een controleschema toegepast op de workload.
- De workload is online en bevat gegevens voor de betreffende controle.
- De versie van de agent die is geïnstalleerd voor de workload, ondersteunt de controleschema's.

De op een workload toegepaste controles en de controlegegevens bekijken

1. In de Bescherming-console: ga naar **Apparaten** > **Alle apparaten**.
2. Selecteer een workload en klik vervolgens op het tabblad **Controle**.
   Het tabblad **Controle** bevat een widget voor elke controle die is ingeschakeld voor de workload. Elke widget bevat de volgende informatie:

Weergegeven informatie	Beschrijving
Naam van controle	De naam van de controle
Laatste resultaat	De laatste waarde van de gecontroleerde metriek of de meest recente status van de gebeurtenis
Laatste controle	De datum en tijd waarop de laatste gegevens zijn verzameld voor controle
Waarschuwingen	Het aantal waarschuwingen dat door de controle is gegenereerd en nog steeds niet is opgelost. Als er minstens één onopgeloste waarschuwing is gegenereerd door deze controle u op het betreffende nummer klikt, dan wordt het tabblad **Waarschuwingen** geopend. De waarschuwingen worden gefilterd en alleen de waarschuwingen voor deze controle worden vermeld.

Opmerking
De widgets worden zichtbaar op het tabblad 15 minuten (of de minimale controlefrequentie die is ingesteld) nadat u een controleschema hebt toegepast voor de workload.

3. [Optioneel] Als u meer details van de controle wilt bekijken en, indien van toepassing, de historische gegevens die zijn verzameld voor de gecontroleerde metriek, klikt u in de widget van de controle op het pictogram met de drie puntjes en vervolgens op **Details**.
   Zie "Controlewidgets" (p. 1162) voor meer informatie over de controlegegevens die u kunt zien in de widgets.

Controlewidgets

De controlewidget bevat de volgende details over de controle.

Detail	Beschrijving
Controleschema	De naam van het controleschema dat de controle bevat. De naam van het controleschema is een link waarmee het controleschema in weergavemodus wordt geopend.
Frequentie van controle	Het tijdinterval waarmee de controle gegevens van de workload verzamelt
Laatste resultaat	De laatste waarde van de gecontroleerde metriek of de meest recente status van de gebeurtenis
Laatste controle	De datum en tijd waarop de laatste gegevens zijn verzameld voor controle

Detail	Beschrijving
Laatste waarschuwing	De datum en tijd waarop de laatste waarschuwing is gegenereerd. Het veld wordt alleen weergegeven als er ten minste één waarschuwing is gegenereerd voor de controle.
Historische grafiek	In het geval van controles waarbij tijdreeksgegevens worden verzameld, kunt u de historische gegevens voor een geselecteerde periode (1 uur, 6 uur, 12 uur, 1 dag, 1 week of 1 maand) ook bekijken in een grafische weergave in de widget. De grafiek toont de werkelijke waarden van de maatstaven gedurende een periode die u selecteert. Als om een of andere reden de agent de verzamelde gegevens niet naar de cloud heeft verzonden, worden de ontbrekende waarden weergegeven als een gestippelde lijn die de gegevenspunten verbindt met werkelijke waarden vóór en na de ontbrekende waarde. Voor controles op **basis van anomalieën** geeft de grafiek het gebied van de basislijnen weer, plus een lijn met de werkelijke waarden van de maatstaf en de anomalieën. De anomalieën zijn de pieken of waarden die niet binnen de basislijnen zijn. De anomalieën worden weergegeven als rode stippen in de grafiek. Als u met de muis over de grafiek beweegt, ziet u de werkelijke waarde en de drempelwaarden voor een bepaalde tijd. 

Detail	Beschrijving
	Opmerking De gegevens in de grafieken worden weergegeven in de tijdzone van het lokale systeem. Dat is de tijdzone van de browser van de workload van waaruit u toegang krijgt tot de Bescherming-console.

Aanvullende Cyber Protection-tools

Compliancemodus

De compliancemodus is bedoeld voor klanten met hogere beveiligingsvereisten. In deze modus is verplichte versleuteling voor alle back-ups vereist en worden alleen lokaal ingestelde versleutelingswachtwoorden toegestaan.

Met de compliancemodus worden alle back-ups die in een klanttenant en de eenheden daarvan zijn gemaakt, automatisch versleuteld met het AES-algoritme en een 256-bits sleutel. Gebruikers kunnen hun versleutelingswachtwoorden alleen instellen op de beschermde apparaten en niet in de beschermingsplannen.

Belangrijk
De compliancemodus kan niet worden uitgeschakeld.

Beperkingen

- De compliancemodus is alleen compatibel met agents met versie 15.0.26390 of hoger.
- De compliancemodus is niet beschikbaar voor apparaten met Red Hat Enterprise Linux 4.x of 5.x en afgeleiden.
- Cloudservices hebben geen toegang tot de versleutelingswachtwoorden. Als gevolg van deze beperking zijn bepaalde functies niet beschikbaar voor tenants in de compliancemodus.

Niet-ondersteunde functies

De volgende functies zijn niet beschikbaar voor tenants in de compliancemodus:

- Herstel via de Cyber Protect-console
- Bladeren door back-ups op bestandsniveau via de Cyber Protect-console
- Cloud-to-cloud back-up
- Back-ups van websites
- Back-up van applicatie
- Back-up van mobiele apparaten
- Antimalwarescan van back-ups
- Veilig herstel
- Automatische aanmaak van witte lijsten voor bedrijven
- Overzicht van gegevensbescherming
- Noodherstel
- Rapporten en dashboards over niet-beschikbare functies

Het versleutelingswachtwoord instellen

U moet het versleutelingswachtwoord lokaal instellen op het beschermde apparaat. U kunt het versleutelingswachtwoord niet instellen in het beschermingsschema. Anders zullen nieuwe back-ups mislukken.

Waarschuwing!
Er is geen manier om versleutelde back-ups te herstellen als u het wachtwoord verliest of vergeet.

U kunt het versleutelingswachtwoord als volgt instellen:

1. Tijdens de installatie van een beveiligingsagent (voor Windows, macOS en Linux).
2. Via de opdrachtregel (voor Windows en Linux).
   Dit is de enige manier om een versleutelingswachtwoord in te stellen in een virtuele toepassing.
   Meer informatie over hoe u een versleutelingswachtwoord instelt met de tool **Acropsh** vindt u in "Versleuteling" (p. 469).
3. In Cyber Protect Monitor (voor Windows en macOS).

Het versleutelingswachtwoord instellen in Cyber Protect Monitor

1. Meld u aan als beheerder op het beschermde apparaat.
2. Klik op het pictogram van Cyber Protect Monitor in het systeemvak (in Windows) of de menubalk (in macOS).
3. Klik op het tandwielpictogram.
4. Klik op **Versleuteling**.
5. Stel het versleutelingswachtwoord in.
6. Klik op **OK**.

Versleutelingswachtwoord wijzigen

U kunt het versleutelingswachtwoord wijzigen voordat er back-ups worden gemaakt voor een beschermingsschema.

We raden u niet aan om het versleutelingswachtwoord te wijzigen nadat er back-ups zijn gemaakt, want de daaropvolgende back-ups zullen dan mislukken. Als u dezelfde machine wilt blijven beschermen, moet u hiervoor een nieuw beschermingsschema maken. Als u zowel het versleutelingswachtwoord als het beschermingsschema wijzigt, worden er nieuwe back-ups gemaakt die zijn versleuteld met het gewijzigde wachtwoord. De back-ups die vóór deze wijzigingen zijn gemaakt, worden niet beïnvloed.

U kunt ook het toegepaste beschermingsschema behouden, en alleen de naam van het back-upbestand daarin wijzigen. Ook in dit geval worden er dan nieuwe back-ups gemaakt die zijn versleuteld met het gewijzigde wachtwoord. Zie "Naam van back-upbestand" (p. 478) voor meer informatie over de naam van het back-upbestand.

U kunt het versleutelingswachtwoord als volgt wijzigen:

1. In Cyber Protect Monitor (voor Windows en macOS).
2. Via de opdrachtregel (voor Windows en Linux).
   Meer informatie over hoe u een versleutelingswachtwoord instelt met de tool **Acropsh** vindt u in "Versleuteling" (p. 469).

Back-ups herstellen voor tenants in de compliancemodus

Met de compliancemodus kunt u geen back-ups herstellen in de Cyber Protect-console.

De volgende opties zijn beschikbaar:

- De hele machine, de bijbehorende schijven of bestanden herstellen via een opstartmedium.
- Bestanden uitpakken uit lokale back-ups van Windows-machines met geïnstalleerde agent, met behulp van Windows Verkenner.

Onveranderbare opslag

Met onveranderbare opslag hebt u toegang tot verwijderde back-ups gedurende een opgegeven retentieperiode. U kunt inhoud van deze back-ups herstellen, maar u kunt ze niet wijzigen, verplaatsen of verwijderen. Wanneer de retentieperiode afloopt, worden de verwijderde back-ups permanent verwijderd.

De onveranderbare opslag bevat de volgende back-ups:

- Back-ups die handmatig worden verwijderd.
- Back-ups die automatisch worden verwijderd, volgens de instellingen in het gedeelte **Bewaartijd** in een beschermingsschema of het gedeelte **Bewaarregels** in een opschoonschema.

Verwijderde back-ups in de onveranderbare opslag nemen nog altijd opslagruimte in beslag die ook in rekening wordt gebracht.

Verwijderde tenants worden voor geen enkele opslag, inclusief onveranderbare opslag, in rekening gebracht.

Modi voor onveranderbare opslag

Voor klanttenants is onveranderbare opslag beschikbaar in de volgende modi:

Onveranderbare opslag is beschikbaar in de volgende modi:

- **Governancemodus**
  U kunt de onveranderbare opslag uitschakelen en opnieuw inschakelen. U kunt de retentieperiode wijzigen of overschakelen naar Compliancemodus.
- **Compliancemodus**

Waarschuwing!
Wanneer u Compliancemodus selecteert, kan dit niet meer ongedaan worden gemaakt.

U kunt de onveranderbare opslag niet uitschakelen. U kunt de retentieperiode niet wijzigen en u kunt niet terugschakelen naar de Governancemodus.

Ondersteunde opslag en agents

- Onveranderbare opslag wordt alleen ondersteund in de cloudopslag.
  Onveranderbare opslag is beschikbaar voor door Acronis gehoste en door partners gehoste cloudopslag waarvoor Acronis Cyber Infrastructure versie 4.7.1 of later wordt gebruikt.
  Alle opslagruimten die kunnen worden gebruikt met Acronis Cyber Infrastructure Backup Gateway, worden ondersteund. Bijvoorbeeld Acronis Cyber Infrastructure-opslag, Amazon S3- en EC2opslagruimten en Microsoft Azure-opslag.
  In het geval van onveranderbare opslag moet TCP-poort 40440 zijn geopend voor de Backup Gateway-service in Acronis Cyber Infrastructure. In versie 4.7.1 en later wordt TCP-poort 40440 automatisch geopend met het verkeerstype **Backup (ABGW) openbaar**. Raadpleeg de documentatie van Acronis Cyber Infrastructure voor meer informatie over de verkeerstypen.
- Voor onveranderbare opslag is een beveiligingsagent versie 21.12 (build 15.0.28532) of later vereist.
- Alleen TIBX (versie 12)-back-ups worden ondersteund.

Onveranderbare opslag inschakelen

U kunt de instellingen voor onveranderbare opslag configureren in de Cyber Protect-console of in de beheerportal. Ze bieden beide toegang tot dezelfde instellingen. In de onderstaande procedure wordt de Cyber Protect-console gebruikt. Informatie over het configureren van de instellingen voor onveranderbare opslag in de beheerportal vindt u onder Onveranderbare opslag configureren in de beheerdershandleiding.

Als u de instellingen voor onveranderlijke opslag wilt configureren, is tweeledige verificatie vereist in de tenant waartoe het beheerdersaccount behoort.

Onveranderbare opslag inschakelen

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Ga naar **Instellingen** > **Systeeminstellingen**.
3. Blader door de lijst met standaardback-upopties en klik vervolgens op **Onveranderbare opslag**.
4. Zet de schakelaar **Onveranderbare opslag** aan.
5. Geef een retentieperiode tussen de 14 en 3650 dagen op.
   De standaardretentieperiode is 14 dagen. Een langere retentieperiode kan leiden tot een hoger opslaggebruik.

6. Selecteer de Onveranderbare-opslagmodus en bevestig vervolgens uw keuze als daarom wordt gevraagd.
   In de Governancemodus kunt u onveranderbare opslag inschakelen of uitschakelen en de retentieperiode wijzigen. U kunt overschakelen van de Governancemodus naar de Compliancemodus.

   Waarschuwing!
   Overschakelen naar de Compliancemodus is onomkeerbaar. Nadat u de Compliancemodus hebt geselecteerd, kunt u de onveranderbare opslag niet uitschakelen en kunt u de modus of retentieperiode niet meer wijzigen.

7. Klik op **Opslaan**.
8. Als u wilt dat een bestaand archief de onveranderbare opslag ondersteunt, maakt u een nieuwe back-up in dat archief.
   Als u een nieuwe back-up wilt maken, voert u het beschermingsschema handmatig of volgens een schema uit.

   Waarschuwing!
   Als u een back-up verwijdert zonder in te stellen dat het archief de onveranderbare opslag moet ondersteunen, wordt de back-up permanent verwijderd.

Onveranderbare opslag uitschakelen

Opmerking
U kunt de onveranderbare opslag alleen uitschakelen in de Governancemodus.

Onveranderbare opslag uitschakelen

1. Meld u als beheerder aan bij de Cyber Protect-console.
2. Klik in het navigatiemenu op **Instellingen** > **Systeeminstellingen**.
3. Blader door de lijst met standaardback-upopties en klik vervolgens op **Onveranderbare opslag**.
4. Zet de schakelaar **Onveranderbare opslag** uit.
5. Bevestig uw keuze door te klikken op **Uitschakelen**.

Waarschuwing!
Het uitschakelen van de onveranderbare opslag wordt niet onmiddellijk van kracht. Tijdens een respijtperiode van 14 dagen is de onveranderbare opslag nog steeds actief en hebt u toegang tot de verwijderde back-ups volgens de oorspronkelijke retentieperiode. Wanneer de respijtperiode afloopt, worden alle back-ups in de onveranderbare opslag permanent verwijderd.

Toegang tot verwijderde back-ups in onveranderbare opslag

Tijdens de retentieperiode hebt u toegang tot verwijderde back-ups en kunt u hieruit gegevens herstellen.

Opmerking
Als u toegang wilt geven tot verwijderde back-ups, moet poort 40440 in de back-upopslag zijn ingeschakeld voor inkomende verbindingen.

Toegang krijgen tot een verwijderde back-up:

1. Ga naar het tabblad **Back-upopslag** en selecteer de cloudopslag die de verwijderde back-up bevat.
2. [Alleen voor verwijderde archieven] Als u de verwijderde archieven wilt zien, klikt u op **Verwijderde weergeven**.
3. Selecteer het archief dat de back-up bevat die u wilt herstellen.
4. Klik op **Back-ups weergeven** en vervolgens op **Verwijderde weergeven**.
5. Selecteer de back-up die u wilt herstellen.
6. Ga verder met de herstelbewerking, zoals beschreven in "Herstel" (p. 525).

Geografisch redundante opslag

Met Geo-redundante opslag wordt de duurzaamheid van gegevens gewaarborgd door ze asynchroon te kopiëren naar een secundaire locatie die geografisch ver verwijderd is van de primaire locatie. Met geo-redundantie zijn uw gegevens toegankelijk, zelfs als de primaire locatie niet beschikbaar is.

Belangrijk
De gerepliceerde gegevens nemen dezelfde opslagruimte in beslag als de oorspronkelijke gegevens.

Geo-redundante opslag inschakelen en uitschakelen

Vereisten

- De geo-redundante opslag wordt pas beschikbaar in de Cyber Protect-console nadat een partnerbeheerder dit heeft ingeschakeld in de beheerportal of via API.
- Alleen beheerders kunnen de geo-redundante opslag in- of uitschakelen in de Cyber Protect-console. Controleer of u beheerdersrechten hebt.

Geografisch redundante opslag inschakelen:

1. [Alleen als de geo-redundante opslag is ingeschakeld via API] Klik in de waarschuwing bovenaan 'Geo-redundantie is beschikbaar voor al uw gegevens in de cloud' op **Geo-redundant Cloud**

Storage inschakelen.

2. Ga in de Cyber Protect-console naar **Instellingen** > **Systeeminstellingen**.
3. Blader door de lijst met standaardback-upopties en klik vervolgens op **Geo-redundant Cloud Storage**.
4. Gebruik de schakelaar om **Geo-redundant Cloud Storage** in te schakelen.
5. Klik op **Opslaan**.

   Nu worden uw gegevens gerepliceerd naar een secundaire locatie en blijven ze beschikbaar, zelfs als de primaire locatie uitvalt.

Geo-redundante opslag uitschakelen:

Waarschuwing!
De gerepliceerde gegevens worden binnen één dag verwijderd nadat u de geo-redundantie hebt uitgeschakeld.

1. Ga in de Cyber Protect-console naar **Instellingen** > **Systeeminstellingen**.
2. Blader door de lijst met back-upopties en klik vervolgens op **Geo-redundant Cloud Storage**.
3. Gebruik de schakelaar om **Geo-redundant Cloud Storage** uit te schakelen.
4. Bevestig uw keuze door **Uitschakelen** te typen en klik vervolgens op **Uitschakelen**.

Status van geo-replicatie

Geo-redundantie houdt in dat gegevens worden gerepliceerd naar een secundaire locatie. De status van geo-replicatie geeft de fasen van dit proces weer. De status kan de volgende waarden hebben:

- **Gesynchroniseerd**: de gegevens zijn gerepliceerd naar de secundaire locatie.
- **Wordt gesynchroniseerd**: de gegevens worden gerepliceerd naar de secundaire locatie. De duur van deze bewerking hangt af van de grootte van de gegevens.
- **In wachtstand**: gegevensreplicatie is tijdelijk opgeschort.
- **Uitgeschakeld**: gegevensreplicatie is uitgeschakeld.

De replicatiestatus in de Cyber Protect-console controleren:

1. Ga in de Cyber Protect-console naar **Back-upopslag**.
2. Selecteer de locatie en de back-upset.
3. Klik op **Details** en controleer vervolgens de status in **Status van geo-replicatie**.

Beperkingen

- Momenteel zijn secundaire locaties voor gerepliceerde gegevens alleen beschikbaar in de Verenigde Staten, Duitsland en Canada.
- Zie de documentatie van Disaster Recovery voor informatie over de beperkingen van de Disaster Recovery-service bij gebruik van geo-redundantie.

Trefwoordenlijst

A

Agent voor de preventie van gegevensverlies

Een clientonderdeel van het systeem voor preventie van gegevensverlies dat de hostcomputer beschermt tegen ongeoorloofd gebruik, ongeoorloofde overdracht en ongeoorloofde opslag van vertrouwelijke, beschermde of gevoelige gegevens door een combinatie van context- en inhoudanalysetechnieken toe te passen en een centraal beheerd beleid voor preventie van gegevensverlies af te dwingen. Cyber Protection biedt een volledig functionele agent voor preventie van gegevensverlies. De functionaliteit van de agent op een beschermde computer is echter beperkt tot de reeks functies voor preventie van gegevensverlies waarvoor in Cyber Protection een licentie kan worden verkregen, en is afhankelijk van het beschermingsschema dat op die computer wordt toegepast.

Apparaatbeheermodule

De apparaatbeheermodule, die deel uitmaakt van een beschermingsschema, maakt gebruik van een functionele subset van de agent voor preventie van gegevensverlies op elke beschermde computer om ongeoorloofde toegang en overdracht van gegevens via lokale computerkanalen te detecteren en te voorkomen. Dit geldt onder meer voor gebruikerstoegang tot randapparatuur en poorten, afdrukken van documenten, kopiëren/plakken van klembord, formatteren en uitwerpen van media en synchronisaties met lokaal aangesloten mobiele apparaten. De apparaatbeheermodule biedt gedetailleerde, contextuele controle over de typen apparaten en poorten waartoe gebruikers op de beschermde computer toegang hebben, en de acties die gebruikers op die apparaten kunnen uitvoeren.

B

Back-upset

Een groep back-ups waarop een afzonderlijke bewaarregel kan worden toegepast. Voor het back-upschema Aangepast komen de back-upsets overeen met de back-upmethoden (Volledig, Differentieel en Incrementeel). In alle andere gevallen zijn de back-upsets Maandelijks, Dagelijks, Wekelijks en Elk uur. Een maandelijkse back-up is de eerste back-up die na het begin van de maand wordt gemaakt. Een wekelijkse back-up is de eerste back-up die wordt gemaakt op de dag van de week zoals geselecteerd in de optie Wekelijkse back-up (klik op het tandwielpictogram en vervolgens op Back-upopties > Wekelijkse back-up). Als een wekelijkse back-up de eerste back-up is die na het begin van de maand wordt gemaakt, wordt deze back-up beschouwd als een maandelijkse back-up. In dit geval wordt een wekelijkse back-up gemaakt op de geselecteerde dag van de volgende week. Een dagelijkse back-up is de eerste back-up die na het begin van de dag wordt gemaakt, tenzij deze back-up valt onder de definitie van een maandelijkse of wekelijkse back-up. Een back-up per uur is de eerste back-up die na het begin van een uur wordt gemaakt, tenzij deze back-up valt onder de definitie van een maandelijkse, wekelijkse of dagelijkse back-up.

Beschermingsschema

Beschermingsschema is een schema dat de gegevensbeschermingsmodules omvat, waaronder Back- up, Antivirus- en antimalwarebeveiliging, URL-filtering, Windows Defender Antivirus, Microsoft Security Essentials, Evaluatie van beveiligingsproblemen, Patchbeheer en Overzicht van gegevensbescherming en Apparaatbeheer.

Beveiligingsagent

Beveiligingsagent is de agent die op machines moet worden geïnstalleerd voor gegevensbescherming.

C

Cloudserver

[Noodherstel] Algemene verwijzing naar een herstelserver of primaire server.

Cloudsite (of DR-site)

[Noodherstel] Externe site gehost in de cloud en gebruikt voor het uitvoeren van herstelinfrastructuur, in het geval van een ramp.

D

Database van USB-apparaten

[Apparaatbeheer] In de apparaatbeheermodule wordt een database van USB- apparaten onderhouden waaruit u apparaten kunt toevoegen aan de uitsluitingslijst van het apparaattoegangsbeheer. De database registreert USB-apparaten per apparaat-id, die met de hand kan worden ingevoerd of kan worden geselecteerd in de lijst met bekende apparaten in de Cyber Protect-console.

Differentiële back-up

Een differentiële back-up wordt gebruikt voor het opslaan van de wijzigingen in de gegevens sinds de laatste volledige back- up. U hebt toegang tot de bijbehorende volledige back-up nodig om gegevens uit een differentiële back-up te herstellen.

E

Enkelvoudig back-upbestand

Een nieuwe back-upindeling waarin de initiële volledige back- up en de daaropvolgende incrementele back-ups worden opgeslagen in één TIBX-bestand. Deze indeling maakt gebruik van de snelheid van de incrementele back-upmethode, terwijl tegelijkertijd het grootste nadeel, namelijk het feit dat verouderde back-ups moeilijk verwijderbaar zijn, wordt vermeden. De software markeert de blokken die worden gebruikt door verouderde back-ups, als 'vrij' en schrijft nieuwe back-ups naar deze blokken. Dit resulteert in een zeer snel opschoonproces met een minimum aan resourceverbruik. Enkelvoudig back-upbestand is niet beschikbaar wanneer u een back- up maakt naar locaties die geen ondersteuning bieden voor lees - en schrijfbewerkingen via random-access.

F

Failback

Een workload van een reserveserver (zoals een replica van een virtuele machine of een herstelserver in de cloud) terugverplaatsen naar de productieserver.

Failover

Een workload van een productieserver verplaatsen naar een reserveserver (zoals een replica van een virtuele machine of een herstelserver in de cloud).

Fysieke machine

Een machine waarvan een back-up wordt gemaakt door een agent die in het besturingssysteem is geïnstalleerd.

H

Herstelserver

[Noodherstel] Een VM-replica van de oorspronkelijke machine, gebaseerd op de beschermde serverback-ups die in de cloud zijn opgeslagen. Herstelservers worden gebruikt om workloads te verplaatsen van de oorspronkelijke servers in geval van een ramp.

I

Incrementele back-up

Een back-up waarin de wijzigingen in de gegevens sinds de laatste back-up worden opgeslagen. U hebt toegang tot andere back-ups nodig om gegevens uit een incrementele back-up te herstellen.

IP-adres testen

[Noodherstel] Een IP-adres dat nodig is in geval van een testfailover, om duplicatie van het productie-IP-adres te voorkomen.

L

Lokale site

[Noodherstel] De lokale infrastructuur die is geïmplementeerd op de locatie van uw bedrijf.

M

Module

Module is een onderdeel van het beschermingsschema en biedt een bepaalde functionaliteit voor gegevensbescherming, bijvoorbeeld de back-upmodule, de module Antivirus- en antimalwarebeveiliging, enzovoort.

O

Openbaar IP-adres

[Noodherstel] Een IP-adres dat nodig is om cloudservers beschikbaar te maken vanaf internet.

P

Point-to-site-verbinding (P2S)

[Noodherstel] Een veilige externe VPN-verbinding naar de cloudsite en lokale site via uw eindpuntapparaten (zoals een computer of laptop).

Preventie van gegevensverlies (vroeger: preventie van gegevenslekken)

Een systeem van geïntegreerde technologieën en organisatorische maatregelen bedoeld om onopzettelijke of opzettelijke openbaarmaking van/toegang tot vertrouwelijke, beschermde of gevoelige gegevens door onbevoegde entiteiten buiten of binnen de organisatie, of de overdracht van dergelijke gegevens naar niet-vertrouwde omgevingen, te detecteren en voorkomen.

Primaire server

[Noodherstel] Een virtuele machine die geen gekoppelde machine op de lokale site heeft

(zoals een herstelserver). Primaire servers worden gebruikt om een toepassing te beveiligen of om diverse ondersteunende diensten (zoals een webserver) uit te voeren.

Productienetwerk

[Noodherstel] Het interne netwerk dat via een VPN-tunnel is uitgebreid naar lokale sites en cloudsites. Lokale servers en cloudservers kunnen met elkaar communiceren in het productienetwerk.

R

Recovery point objective (RPO)

[Noodherstel] Hoeveelheid gegevens die verloren zijn gegaan door een bedrijfsonderbreking, gemeten als de hoeveelheid tijd vanaf een geplande onderbreking of een ramp. De RPO-drempel bepaalt het maximaal toegestane tijdsinterval tussen het laatste geschikte herstelpunt voor een failover en de huidige tijd.

Runbook

[Noodherstel] Gepland scenario bestaande uit configureerbare stappen waarmee de acties voor noodherstel worden geautomatiseerd.

S

Site-to-site-verbinding (S2S)

[Noodherstel] Verbinding waarmee uw lokale netwerk wordt uitgebreid naar de cloud via een veilige VPN-tunnel.

T

Testnetwerk

[Noodherstel] Geïsoleerd virtueel netwerk dat wordt gebruikt om het failoverproces te testen.

V

Validatie

Een bewerking waarmee wordt gecontroleerd of het mogelijk is gegevens te herstellen vanuit een back-up. Bij validatie van een bestandsback-up wordt het herstel van alle bestanden vanuit de back-up naar een dummy-bestemming geïmiteerd. Bij validatie van een schijfback-up wordt een controlesom berekend voor elk gegevensblok dat is opgeslagen in de back-up. Voor beide procedures zijn veel resources vereist. Wanneer validatie lukt, is er een grote kans dat het herstel zal slagen, maar niet alle factoren die van invloed zijn op het herstelproces, worden gecontroleerd.

Virtuele machine

Een virtuele machine waarvan een back-up op hypervisorniveau wordt gemaakt door een externe agent zoals Agent voor VMware of Agent voor Hyper-V. Back-ups voor een virtuele machine met agent worden op dezelfde manier gemaakt als voor een fysieke machine.

Volledige back-up

Een zelfvoorzienende back-up die alle geselecteerde gegevens bevat waarvan u een back-up wilt maken. U hebt geen toegang tot een andere back-up nodig om de gegevens uit een volledige back-up te herstellen.

Voltooien

De bewerking waarmee een tijdelijke virtuele machine die wordt uitgevoerd vanaf een back-up, wordt omgevormd tot een permanente virtuele machine. Fysiek betekent dit dat alle schijven van de virtuele machine, samen met de wijzigingen die zijn aangebracht toen de machine werd uitgevoerd, worden hersteld

naar de gegevensopslag waar deze wijzigingen worden opgeslagen.

VPN-gateway (voorheen VPN-server of connectiviteitsgateway)

[Noodherstel] Een speciale virtuele machine die een verbinding via een beveiligde VPN-tunnel tot stand brengt tussen het netwerk van de lokale site en het netwerk van de cloudsite. De VPN-gateway wordt geïmplementeerd op de cloudsite.

VPN-toepassing

[Noodherstel] Een speciale virtuele machine die een verbinding via een beveiligde VPN-tunnel tot stand brengt tussen het lokale netwerk en de cloudsite. De VPN-toepassing wordt geïmplementeerd op de lokale site.

Z

Zwevende back-up

Een zwevende back-up is een back-up die niet meer is gekoppeld aan een beschermingsschema.

Index

B

C

E

F

G

I

N

O

P

T

U

V

W

Z