Cyberbescherming

21.10

Gebruikershandleiding

REVISIE:1-11-2021

Inhoudsopgave

1 Edities en subedities van de Cyber Protection-service

Dit gedeelte bevat informatie over het werken met services, edities en opties die beschikbaar waren als onderdeel van het licentiemodel in Cyber Cloud 21.02 en eerder. Deze opties en edities worden nog steeds ondersteund en kunnen naar behoefte worden geconfigureerd voor tenants, maar worden niet aanbevolen. Ze worden nu beschouwd als verouderd.

Opmerking
De services, edities en opties die voor u beschikbaar zijn, worden overgenomen van de opties die beschikbaar zijn voor uw bovenliggende tenant. Als een optie niet beschikbaar is voor de partner die uw account heeft gemaakt, zal die optie niet beschikbaar zijn voor u, en kunt u deze niet inschakelen voor uw partners of klanten.

Zie "Geavanceerde bescherming" (p. 18) voor informatie over de nieuwe opties.

De volgende edities zijn beschikbaar:

- Cyber Protect
- Cyber Backup

1.0.1 Cyber Protect-editie

Deze editie is gelicentieerd per workload, dat wil zeggen afhankelijk van het aantal beschermde machines, ongeacht de grootte van de gegevens waarvan een back-up is gemaakt.

Binnen de Cyber Protect-editie zijn de volgende subedities beschikbaar:

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

1.0.2 Cyber Backup Edition

Deze editie is gelicentieerd per GB, dat wil zeggen afhankelijk van de grootte van de gegevens waarvan een back-up is gemaakt, ongeacht het aantal beschermde machines.

De Cyber Backup-editie bevat geen subedities, alleen Cyber Backup Standard-opties zijn beschikbaar.

1.0.3 Edities vergelijken

Het aantal en de omvang van de beschikbare functies zijn afhankelijk van de editie van de Cyber Protection-service. Zie Cyber Protection-edities vergelijken voor een gedetailleerde vergelijking tussen de functies in elke editie en subeditie.

1.0.4 Disaster Recovery-add-on

De Disaster Recovery-add-on biedt herstelfunctionaliteit ontworpen voor bedrijven die hoge eisen stellen aan de RPO (Recovery Time Objective). Deze add-on is alleen beschikbaar met de Cyber Protect-editie.

Opmerking
De Disaster Recovery-add-on kan niet worden gebruikt met de Cyber Protect Essentials-editie.

2 Geavanceerde bescherming

Cyber Protect bevat standaard functies die de meeste cyberbeveiligingsrisico's afdekken. U kunt deze functies gebruiken zonder extra kosten. Daarnaast kunt u geavanceerde functies inschakelen om de bescherming van uw workloads te verbeteren.

Als een geavanceerde beschermingsfunctie is ingeschakeld voor u, wordt deze in het beschermingsschema weergegeven met het pictogram voor een geavanceerde functie:  . Wanneer u de functie probeert in te schakelen, ziet u een bericht dat hiervoor extra kosten in rekening worden gebracht.

Als een geavanceerde beschermingsfunctie niet is ingeschakeld voor u, wordt naast de naam van de functie in het beschermingsschema het volgende pictogram weergegeven: . U ziet een bericht dat u contact moet opnemen met uw beheerder om het vereiste geavanceerde pakket voor u in te schakelen.

3 Ondersteunde Cyber Protect-functies per besturingssysteem

Opmerking
Dit onderwerp bevat informatie over alle Cyber Protect-functies en de besturingssystemen waarop ze worden ondersteund. Voor sommige functies zijn mogelijk extra licenties vereist, afhankelijk van het toegepaste licentiemodel.

De Cyber Protect-functies worden ondersteund in de volgende besturingssystemen:

- Windows: Windows 7 Service Pack 1 en later, en Windows Server 2008 R2 Service Pack 1 en later.
  Windows Defender Antivirus-beheer wordt ondersteund op Windows 8.1 en later.
- Linux: CentOS 6.10, 7.8+, CloudLinux 6.10, 7.8+, Ubuntu 16.04.7+ (waarbij plus verwijst naar secundaire versies van deze distributies).
  Andere Linux-distributies en -versies worden mogelijk ook ondersteund, maar zijn niet getest.
- macOS: 10.13.x en later (alleen Antivirus- en antimalwarebeveiliging en apparaatbeheer worden ondersteund). De functionaliteit voor apparaatbeheer wordt ondersteund op macOS 10.15 en later of macOS 11.2.3 en later.
  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 weergeven dat Agent voor preventie van gegevensverlies op de computer is geïnstalleerd, maar de functie voor apparaatbeheer zal niet werken. De functie voor apparaatbeheer werkt alleen op macOS-systemen die worden ondersteund door Agent voor preventie van gegevensverlies.

Opmerking
Antimalwarebeveiliging voor Linux en macOS wordt alleen ondersteund wanneer Geavanceerde antimalwarebeveiliging is ingeschakeld.

Belangrijk
De Cyber Protect-functies worden alleen ondersteund voor machines waarop een beveiligingsagent is geïnstalleerd. Voor virtuele machines die worden beschermd 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, wordt alleen back-up ondersteund.

Cyber Protect-functies	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-	Ja	Nee	Nee

antivirus)			
Cyber Protect Essentials (alleen voor de Cyber Protect Essentials-editie)	Ja	Nee	Nee
Forensische back-up			
Geheugendump genereren	Ja	Nee	Nee
Momentopname van actieve processen	Ja	Nee	Nee
Forensische back-up voor machines met één station zonder opnieuw opstarten	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
Continue gegevensbescherming (CDP)			
CDP voor bestanden en mappen	Ja	Nee	Nee
CDP voor gewijzigde bestanden via applicatie-tracking	Ja	Nee	Nee
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
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	Nee	Nee
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
Antivirus- en antimalwarebeveiliging			
Volledig geïntegreerde Active Protection-functionaliteit	Ja	Nee	Nee
Realtime antimalwarebeveiliging	Ja	Ja, wanneer Geavanceerde antimalware is ingeschakeld	Ja, wanneer Geavanceerde antimalware is ingeschakeld
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
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	Nee
Engine voor gedragsanalyse	Ja	Nee	Ja Niet ondersteund op Apple Silicon-processors, zoals

			Apple M1
Preventie tegen aanvallen	Ja	Nee	Nee
Quarantaine	Ja	Ja	Ja
Automatische opschoning in quarantaine	Ja	Nee	Ja
URL-filtering (http/https)	Ja	Nee	Nee
Witte lijst van het bedrijf	Ja	Nee	Ja
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
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
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
Overzicht van gegevensbescherming			
Aanpasbare definitie van belangrijke bestanden	Ja	Nee	Nee
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
Schijfintegriteit			
Op AI gebaseerd beheer van HDD- en SSD-schijfintegriteit	Ja	Nee	Nee
Slimme beschermingsschema's op basis van Acronis Cyber Protection Operations Center (CPOC)-waarschuwingen			
Bedreigingsfeed	Ja	Nee	Nee
Herstelwizard	Ja	Nee	Nee
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
Veilig herstel			
Antimalwarescan met antivirus- en antimalwarebeveiliging tijdens het herstelproces	Ja	Nee	Nee
Veilig herstel voor versleutelde back-ups	Ja	Nee	Nee
Verbinding met extern bureaublad			
Verbinding via HTML5-client	Ja	Nee	Nee
Verbinding via systeemeigen Windows RDP-client	Ja	Nee	Nee
Hulp op afstand	Ja	Nee	Nee
#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
Preventie van gegevensverlies			
Apparaatbesturing	Ja	Nee	Ja

			ARM CPU-architectuur wordt niet ondersteund
Beheeropties			
Upsellscenario's om Cyber Protect-edities te promoten	Ja	Ja	Ja
Webgebaseerde centrale en externe beheerconsole	Ja	Ja	Ja
Beschermingsopties			
Extern wissen (alleen Windows 10)	Ja	Nee	Nee
Cyber Protect Monitor			
Cyber Protect Monitor-app	Ja	Nee	Ja
Beveiligingsstatus voor Zoom	Ja	Nee	Nee
Beveiligingsstatus voor Cisco Webex	Ja	Nee	Nee
Beveiligingsstatus voor Citrix Workspace	Ja	Nee	Nee
Beveiligingsstatus voor Microsoft Teams	Ja	Nee	Nee
Software-inventaris			
Software-inventarisscan	Ja	Nee	Ja
Software-inventarisbewaking	Ja	Nee	Ja
Hardware-inventaris			
Hardware-inventarisscan	Ja	Nee	Ja
Hardware-inventarisbewaking	Ja	Nee	Ja

* 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.

**** 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.

4 Softwarevereisten

4.1 Ondersteunde webbrowsers

De Cyber Protection-webconsole ondersteunt de volgende webbrowsers:

- Google Chrome 29 of later
- Mozilla Firefox 23 of later
- Opera 16 of later
- Windows Internet Explorer 11 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.

4.2 Ondersteunde besturingssystemen en omgevingen

4.2.1 Agent voor Windows

- 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 Vista – alle edities
- 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 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

4.2.2 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.

4.2.3 Agent voor preventie van gegevensverlies

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

Opmerking
Agent voor preventie van gegevensverlies voor macOS ondersteunt alleen x64-processors (ARM64 wordt niet ondersteund).

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 weergeven dat Agent voor preventie van gegevensverlies op de computer is geïnstalleerd, maar de functie voor apparaatbeheer zal niet werken. De functie voor apparaatbeheer werkt alleen op macOS-systemen die worden ondersteund door Agent voor preventie van gegevensverlies.

4.2.4 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

4.2.5 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

4.2.6 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)

4.2.7 Agent voor Linux

Opmerking
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 Cyberbescherming 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 5.8 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, 8.0, 8.1, 8.2, 8.3, 8,4*

  Belangrijk
  Configuraties met Stratis worden niet ondersteund voor de volgende versies: 8.0, 8.1, 8.2, 8.3, 8.4.

- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

  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
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*

  Belangrijk
  Configuraties met Stratis worden niet ondersteund voor de volgende versies: 8.0, 8.1, 8.2, 8.3, 8.4.

- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4* – zowel Unbreakable Enterprise Kernel als Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*
- AlmaLinux 8.4*
- ALT Linux 7.0

Voordat u het product op een systeem installeert dat geen gebruik maakt van RPM Package Manager, zoals een Ubuntu-systeem, moet u deze software handmatig installeren, bijvoorbeeld door de volgende opdracht uit te voeren (als rootgebruiker): `apt-get install rpm`

* Alleen ondersteund met kernels van 4.18 tot 5.8

4.2.8 Agent voor Mac

Zowel x64- als ARM64- (zoals Apple M1)*-processors worden ondersteund.

- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11

- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12

* Voor Antimalwarebeveiliging, Hardware-inventaris en Software-inventaris is Rosetta 2 op Macs met Apple Silicon-processors vereist.

4.2.9 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

4.2.10 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.

4.2.11 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

4.2.12 Agent voor Virtuozzo

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

4.2.13 Agent voor Virtuozzo Hybrid Infrastructure

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5

4.2.14 Agent voor Scale Computing HC3

Scale Computing Hypercore 8.8, 8.9, 9.0

4.2.15 Agent voor oVirt

Red Hat Virtualization 4.2, 4.3, 4.4

4.3 Ondersteunde versies van Microsoft SQL Server

- 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.

4.4 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.

4.5 Ondersteunde versies van Microsoft SharePoint

Cyberbescherming 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.

4.6 Ondersteunde versies van Oracle Database

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

Alleen configuraties met een enkelvoudig exemplaar worden ondersteund.

4.7 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.

4.8 Ondersteunde virtualisatieplatforms

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

Platform	Back-up op hypervisorniveau (back-ups zonder agent)	Back-up van binnen een gastbesturingssysteem
VMware		
VMware vSphere-versies: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0	+	+

VMware vSphere-edities: VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus		
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server (VMware Virtual server:) VMware Workstation VMware ACE VMware Player		+
Microsoft		
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		
Microsoft Virtual PC 2004, 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8, 8.9, 9.0	+	+
Citrix		
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,		Alleen volledig gevirtualiseerde gasten (HVM). Paravirtual gasten (PV) worden niet ondersteund.

8.0, 8.1, 8.2		
Red Hat en Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1		+
Red Hat Virtualization (beheerd met oVirt) 4.2, 4.3, 4.4	+	+
Kernel-based Virtual Machines (KVM)		+
Kernel-based Virtual Machines (KVM) beheerd met oVirt 4.3 en uitgevoerd op Red Hat Enterprise Linux 7.6, 7.7 of CentOS 7.6, 7.7	+	+
Kernel-based Virtual Machines (KVM) beheerd met oVirt 4.4 en uitgevoerd op Red Hat Enterprise Linux 8.x of CentOS Stream 8.x	+	+
Parallels		
Parallels-werkstation		+
Parallels Server 4 Bare Metal		+

Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Alleen volledig gevirtualiseerde gasten (HVM). Paravirtual gasten (PV) worden niet ondersteund.
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x tot en met 20180425.x		+
Virtuozzo		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	Alleen virtuele machines. Containers worden niet ondersteund.
Virtuozzo 7.0.13, 7.0.14	Alleen ploop-containers. Virtuele machines worden niet ondersteund.	Alleen virtuele machines. Containers worden niet ondersteund.
Virtuozzo Hybrid Server 7.5	+	Alleen virtuele machines. Containers worden niet ondersteund.
Virtuozzo Hybrid Infrastructure		
Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5	+	+
Amazon		
Amazon EC2-exemplaren		+
Microsoft Azure		
Virtuele Azure-machines		+

***** 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.

4.8.1 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.
- **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 VMware en Agent voor Hyper-V maken geen back-up van LUN-volumes die zijn verbonden via een iSCSI-initiator binnen het gastbesturingssysteem. De ESXi- en Hyper-V-hypervisors zijn niet op de hoogte van dergelijke volumes, dus worden de volumes niet opgenomen in momentopnamen op hypervisor-niveau en worden ze 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.
- **Linux-machines met logische volumes (LVM)**

  Agent voor VMware en Agent voor Hyper-V bieden geen ondersteuning voor de volgende bewerkingen voor Linux-machines met LVM:

- P2V-migratie, V2P-migratie en V2V-migratie vanuit Virtuozzo. Agent voor Linux gebruiken om de back-up- en opstartmedia voor herstel te maken.
- Een virtuele machine uitvoeren vanaf een back-up gemaakt met Agent voor Linux.

- **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 GEN2 VM's nadat de virtuele 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.

4.9 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.

4.9.1 Algemene regel voor installatie

Het wordt sterk aanbevolen om eerst de versleutelingssoftware te installeren en vervolgens de beveiligingsagenten.

4.9.2 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.

4.9.3 Algemene regel voor het maken van back-ups

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

4.9.4 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

5 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.

<table>
<tr><th rowspan="2">Bestandssysteem</th><th colspan="3">Ondersteund door</th><th rowspan="2">Beperkingen</th></tr>
<tr><th>Agenten</th><th>Opstartmedia voor Windows en Linux</th><th>Opstartmedia voor Mac</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Alle agenten</td><td>+</td><td>+</td><td rowspan="3">Geen beperkingen</td></tr>
<tr><td>NTFS</td><td>+</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td><td>-</td></tr>
<tr><td>HFS+</td><td rowspan="2">Agent voor Mac</td><td>-</td><td>+</td><td rowspan="2">• 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.</td></tr>
<tr><td>APFS</td><td>-</td><td>+</td></tr>
<tr><td>JFS</td><td rowspan="2">Agent voor Linux</td><td>+</td><td>-</td><td rowspan="2">• Er kunnen geen bestanden worden uitgesloten van een schijfback-up
• Snelle incrementele/differentiële back-up kan niet worden ingeschakeld</td></tr>
<tr><td>ReiserFS3</td><td>+</td><td>-</td></tr>
</table>

ReiserFS4		+	-	• Er kunnen geen bestanden worden uitgesloten van een schijfback-up • Snelle incrementele/differentiële back-up kan niet worden ingeschakeld • De grootte van volumes kan niet worden aangepast tijdens een herstelbewerking
ReFS	Alle agenten	+	+	
XFS		+	+	
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 • Er kunnen geen bestanden worden uitgesloten van een back-up • 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.

5.0.1 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.

6 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.
- **Knop Accountactivering.** Klik op de knop en stel het wachtwoord voor het account in. Het wachtwoord moet minimaal bestaan uit negen tekens.

  Als uw beheerder tweeledige verificatie heeft ingeschakeld, wordt u gevraagd om tweeledige verificatie in ts stellen voor uw account.

6.1 Tweeledige verificatie

Tweeledige verificatie biedt extra beveiliging tegen ongeautoriseerde toegang tot uw account. Wanneer tweeledige verificatie 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 serviceconsole. 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 hij/zij zich nog steeds niet aanmelden zonder toegang tot uw 'tweede-factor-apparaat'.

De eenmalige code wordt gegenereerd op basis van de huidige tijd van het apparaat en het geheim dat door de Cyberbescherming-service als QR-code of alfanumerieke code wordt verstrekt. Tijdens de eerste aanmelding moet u dit geheim invoeren in de verificatietoepassing.

Tweeledige verificatie instellen voor uw account

1. Kies het 'tweede-factor-apparaat'.

   Meestal is dit een mobiele telefoon, maar u kunt ook een tablet, laptop of desktop gebruiken.
2. Zorg ervoor dat de tijdinstellingen van het apparaat juist zijn en de huidige tijd weergeven. Zorg ervoor dat het apparaat zich vergrendelt na een periode van inactiviteit.
3. Installeer de verificatietoepassing op het apparaat. De aanbevolen toepassingen zijn Google Authenticator en Microsoft Authenticator.
4. Ga naar de aanmeldingspagina van de serviceconsole en stel uw wachtwoord in.

   In de serviceconsole worden de QR-code en alfanumerieke code weergegeven.
5. Sla de QR-code en de alfanumerieke code op een handige manier op (bijvoorbeeld door een schermafbeelding, het noteren van de code of het opslaan van de schermafbeelding in de cloudopslag). Als u het 'tweede-factor-apparaat' verliest, kunt u de tweeledige verificatie opnieuw instellen met behulp van deze codes.
6. Open de verificatietoepassing en voer een van de volgende acties uit:
   - Scan de QR-code
   - Voer handmatig de alfanumerieke code in de toepassing in

De verificatietoepassing genereert een eenmalige code. Elke 30 seconden wordt een nieuwe code gegenereerd.

7. Ga terug naar de aanmeldingspagina van de serviceconsole 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 ...** aanvinken. Als u dit doet, is de eenmalige code niet vereist wanneer u zich aanmeldt via deze browser op deze machine.

6.1.1 Wat als ...

... ik het 'tweede-factor-apparaat' kwijt ben?

Als u een vertrouwde browser hebt, kunt u zich aanmelden met deze browser. Wanneer u een nieuw apparaat hebt, herhaalt u de stappen 1-3 en 6-7 van de bovenstaande procedure met het nieuwe apparaat en de opgeslagen QR-code of alfanumerieke code.

Als u de code niet hebt opgeslagen, vraagt u de beheerder of serviceprovider om tweeledige verificatie voor uw account opnieuw in te stellen en herhaalt u de stappen 1-3 en 6-7 van de bovenstaande procedure met het nieuwe apparaat.

... ik een ander 'tweede-factor-apparaat' wil gebruiken?

Wanneer u zich aanmeldt, klikt u op de link **tweeledige verificatie opnieuw instellen**, bevestigt u de bewerking door de eenmalige code in te voeren en herhaalt u de bovenstaande procedure met het nieuwe apparaat.

7 Toegang tot de Cyberbescherming-service

Zodra uw account is geactiveerd, kunt u zich aanmelden bij de Cyberbescherming-service.

Aanmelden bij de Cyberbescherming-service

1. Ga naar de aanmeldingspagina voor de Cyberbescherming-service.
2. Typ de gebruikersnaam en klik op **Volgende**.
3. Typ het wachtwoord en klik op **Volgende**.
4. Als u de rol van beheerder hebt in de Cyberbescherming-service, klikt u op **Cyber Protection**. Gebruikers die niet de rol van beheerder hebben, melden zich rechtstreeks aan bij de serviceconsole.

De time-outperiode voor de serviceconsole is 24 uur voor actieve sessies en 1 uur voor niet-actieve sessies.

Uw wachtwoord opnieuw instellen

1. Ga naar de aanmeldingspagina voor de Cyberbescherming-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. Het wachtwoord moet minimaal acht tekens lang zijn.

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

Als **Cyber Protection** niet de enige service is waarop u bent geabonneerd, kunt u schakelen tussen de services met behulp van het pictogram  in de rechterbovenhoek. Beheerders kunnen dit pictogram ook gebruiken om over te schakelen naar de beheerportal.

Als u bent geabonneerd op een van de Cyberbescherming-edities, kunt u feedback over het product verzenden vanaf de serviceconsole. Klik in het linkernavigatiemenu op **Feedback verzenden**, vul de velden in, voeg bestanden toe (indien van toepassing) en klik op **Verzenden**.

8 De software installeren

8.1 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.

Het wordt aanbevolen om Agent voor Windows te installeren wanneer u ook Agent voor VMware (Windows) en Agent voor Hyper-V installeert.

In Linux werken Agent voor Oracle en Agent voor Virtuozzo alleen als ook Agent voor Linux (64 bits) is geïnstalleerd. Deze drie agenten delen één installatieprogramma.

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	
Applicaties		
SQL-databases	Agent voor SQL	Op de machine met Microsoft SQL Server.
Exchange-databases	Agent voor Exchange	Op de machine met de rol Postvak van Microsoft Exchange Server.*
Microsoft 365-postvakken	Agent voor Microsoft 365	Op een machine met Windows en een verbinding met internet. Mogelijk moet u Agent voor Office 365 installeren, afhankelijk van de gewenste functionaliteit. Zie 'Microsoft 365-gegevens beschermen' voor meer informatie.
Microsoft 365 OneDrive-bestanden en SharePoint Online-sites	—	Van deze gegevens kan alleen een back-up worden gemaakt door een agent die in de cloud is geïnstalleerd. Zie 'Microsoft 365-gegevens

		beschermen' voor meer informatie.
Google Workspace Gmail-postvakken, Google Drive-bestanden en gedeelde Drive-bestanden	—	Van deze gegevens kan alleen een back-up worden gemaakt door een agent die in de cloud is geïnstalleerd. Zie 'Google Workspace beveiligen' voor meer informatie.
Machines met Active Directory Domain Services	Agent voor Active Directory	Op de domeincontroller.
Machines met Oracle Database	Agent voor Oracle	Op de machine met Oracle Database.
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.
Virtuele Virtuozzo Hybrid Infrastructure-machines	Agent voor Virtuozzo Hybrid Infrastructure	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)		

Kernel-based Virtual Machines (KVM)		
Virtuele Oracle-machines		
Virtuele Nutanix AHV-machines		
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. Raadpleeg 'Agent voor VMware – back-up zonder LAN' voor meer 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 Cyberbescherming 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.

8.2 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 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

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

Voor opstartmedia of schijfherstel met opnieuw opstarten is minimaal 1 GB geheugen vereist.

8.3 Voorbereiding

8.3.1 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.

8.3.2 Stap 2

Controleer of er voldoende vrije schijfruimte is op uw harde schijf om een agent te installeren. Zie "Systeemvereisten voor agenten" (p. 47) voor gedetailleerde informatie over de vereiste schijfruimte.

8.3.3 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 Agenten implementeren via Groepsbeleid.

Als u het installatieprogramma 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 Cyberbescherming-service te registreren. Zonder internetverbinding mislukt de installatie.

8.3.4 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.

8.3.5 Stap 5

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

- **443** en **8443** Deze poorten worden gebruikt voor toegang tot de serviceconsole, het registreren van de agenten, het downloaden van de certificaten, gebruikersautorisatie en het downloaden van bestanden uit de cloudopslag.
- **7770...7800** Deze poorten worden door de agenten gebruikt om te communiceren met de beheerserver voor back-ups.
- **44445 en 55556** Deze poorten worden door de agenten gebruikt voor gegevensoverdracht tijdens back-up- en herstelbewerkingen.

Als een proxyserver in uw netwerk is ingeschakeld, raadpleegt u het gedeelte 'Proxyserverinstellingen' om te begrijpen 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

- **TCP 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.
- **TCP 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.
- **TCP 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. Het Downloadprogramma heeft de volgende poorten nodig om te kunnen werken.

- **6888** Gebruikt door BitTorrent-protocol voor torrent peer-to-peer-updates.
- **6771** Gebruikt als de lokale poort voor peer-detectie. Wordt ook gebruikt voor peer-to-peer-updates.
- **18018** Gebruikt voor communicatie tussen updaters die in verschillende modi werken: Updater en UpdaterAgent.
- **18019** Lokale poort, gebruikt voor de communicatie tussen Updater en de <BRAND> Cyber Protection-agent.

8.3.6 Stap 6

Controleer of de volgende lokale poorten niet worden gebruikt door andere processen op de machine waarop u de Cyber Protection-agent 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 service Active Protection luistert op TCP-poort 6109. Controleer of deze niet wordt gebruik door een ander proces.

De poorten wijzigen die door de Cyber Protection-agent worden gebruikt

Sommige poorten die zijn vereist voor de Cyber Protection-agent, worden mogelijk gebruikt door andere toepassingen in uw omgeving. Als u conflicten wilt voorkomen, moet u de standaardpoorten wijzigen die door de Cyber Protection-agent 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

8.4 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.

8.4.1 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.

8.4.2 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.

8.4.3 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.

8.5 Proxyserverinstellingen

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, moeten de proxyserverinstellingen tijdens de installatie of van tevoren worden opgegeven.

8.5.1 In Windows

Als een proxyserver is geconfigureerd in Windows (**Configuratiescherm** > **Internetopties** > **Verbindingen**), worden de proxyserverinstellingen gelezen vanuit het register en automatisch gebruikt door het installatieprogramma. U kunt de proxyinstellingen ook invoeren tijdens de installatie of deze vooraf opgeven via de hieronder beschreven procedure. Gebruik dezelfde procedure als u de proxyinstellingen wilt wijzigen na de installatie.

Proxyinstellingen opgeven in Windows

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

```
Windows Register-editor versie 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 beveiligingsagent nog niet is geïnstalleerd, kunt u deze nu installeren.
9. Open het bestand **%programdata%\Acronis\Agent\etc\aakore.yaml** in een teksteditor.
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
```

8.5.2 In Linux

Voer het installatiebestand uit met de parameters `--http-proxy-host=ADRES --http-proxy-port=POORT --http-proxy-login=GEBRUIKERSNAAM--http-proxy-password=WACHTWOORD`. Gebruik de hieronder beschreven procedure als u de proxyinstellingen wilt wijzigen na de installatie.

Proxyinstellingen wijzigen in Linux

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 agenten, gaat u naar het volgende gedeelte:

     ```
     <key name="HttpProxy">
      <value name="Enabled" type="Tdword">"1"</value>
      <value name="Host" type="TString">"ADRES"</value>
      <value name="Port" type="Tdword">"POORT"</value>
      <value name="Login" type="TString">"GEBRUIKERSNAAM"</value>
      <value name="Password" type="TString">"WACHTWOORD"</value>
     </key>
     ```

   - Kopieer anders de bovenstaande regels en plak deze in het bestand tussen de tags `<registry name="Global">...</registry>`.
3. Vervang `ADRES` door de nieuwe waarden voor de hostnaam/het IP-adres van de proxyserver en vervang `POORT` door de decimale waarde van het poortnummer.
4. Als uw proxyserver verificatie vereist, vervangt u `GEBRUIKERSNAAM` en `WACHTWOORD` 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 volgende opdracht uit te voeren in een willekeurige directory:

```
sudo service acronis_mms restart
```

8.5.3 In macOS

U kunt de proxyinstellingen invoeren tijdens de installatie of deze vooraf opgeven via de hieronder beschreven procedure. Gebruik dezelfde procedure als u de proxyinstellingen wilt wijzigen na de installatie.

Proxyinstellingen opgeven in macOS

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 beveiligingsagent nog niet is geïnstalleerd, kunt u deze nu installeren.
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
```

8.5.4 In opstartmedia

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

8.6 Cyberbescherming-agenten installeren

U kunt agenten installeren op machines met besturingssystemen die worden vermeld in 'Ondersteunde besturingssystemen en omgevingen'. De besturingssystemen die ondersteuning bieden voor de Cyber Protect-functies, worden vermeld in 'Ondersteunde Cyber Protect-functies per besturingssysteem'.

8.6.1 Cyberbescherming-agenten downloaden

Voordat u een agent installeert, moet u het betreffende installatiebestand downloaden van de serviceconsole.

Een agent downloaden terwijl u een workload toevoegt om te beschermen

1. Ga in de Cyberbescherming-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 Cyberbescherming-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**.

8.6.2 Cyberbescherming-agenten installeren in Windows

Vereisten

Download de gewenste agent op de machine die u wilt beschermen. Zie "Cyberbescherming-agenten downloaden" (p. 58).

Agent voor Linux 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:
   - Als u wilt wijzigen welke onderdelen worden geïnstalleerd (bijvoorbeeld om de installatie van Cyberbescherming Monitor of het opdrachtregelprogramma uit te schakelen of om Agent voor antimalwarebeveiliging en URL-filtering te installeren).

     Opmerking
     Voor de functies voor antimalwarebeveiliging en URL-filtering op Windows-machines moet Agent voor antimalwarebeveiliging en URL-filtering zijn geïnstalleerd. Deze wordt automatisch geïnstalleerd voor beschermde workloads als de module **Antivirus- en antimalwarebeveiliging** of de module **URL-filtering** is ingeschakeld in de betreffende beschermingsschema's.

   - De methode voor registratie van de machine in de Cyberbescherming-service 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' 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] Kies de vCenter-server of de standalone ESXi-host waarvan u wilt dat de virtuele machines door de agent worden toegevoegd aan back-ups, en geef het adres en de toegangsreferenties op. Klik vervolgens op **Gereed**. We raden aan een account te gebruiken waaraan de rol **Beheerder** is toegewezen. Anders moet u een account met de nodige rechten beschikbaar maken op de vCenter-server of ESXi.
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.
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. Voer een van de volgende handelingen uit:
   - Klik op **De machine registreren**. Meld u in het geopende browservenster aan bij de serviceconsole, bekijk de registratiegegevens en klik vervolgens op **Registratie bevestigen**.
   - Klik op **Registratiegegevens weergeven**. Het installatieprogramma geeft de registratielink en de registratiecode weer. U kunt deze kopiëren en de registratiestappen uitvoeren op een andere machine. In dit geval moet u de registratiecode invoeren op het registratieformulier. De registratiecode is een uur geldig.
     U kunt het registratieformulier ook als volgt openen: klik op **Alle apparaten** > **Toevoegen**, blader omlaag naar **Registratie via code** en klik vervolgens op **Registreren**.

     Opmerking
     Sluit het installatieprogramma pas af wanneer u de registratie hebt bevestigd. Als u de registratie opnieuw wilt starten, moet u het installatieprogramma opnieuw opstarten en de installatieprocedure herhalen.

     De machine wordt dan toegewezen aan het account dat is gebruikt voor aanmelding bij de serviceconsole.
   - Registreer de machine handmatig via de opdrachtregel. Zie 'Machines handmatig registreren' voor meer informatie over hoe u dit kunt doen.
9. [Als de agent is geregistreerd onder een account met tenant in de modus Verbeterde beveiliging] Stel het versleutelingswachtwoord in.

8.6.3 Cyberbescherming-agenten installeren in Linux

Vereisten

- Download de gewenste agent op de machine die u wilt beschermen. Zie "Cyberbescherming-agenten downloaden" (p. 58).
- 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. Voer het installatiebestand uit als rootgebruiker.

   Als er een proxyserver is ingeschakeld in uw netwerk, geeft u, wanneer het bestand wordt uitgevoerd, de hostnaam/het IP-adres en de poort op in de volgende indeling: `--http-proxy-host=ADRES --http-proxy-port=POORT --http-proxy-login=GEBRUIKERSNAAM--http-proxy-password=WACHTWOORD`.

   Als u de standaardmethode voor registratie van de machine in de Cyberbescherming-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
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 Cyberbescherming-service in of wacht u tot de machine wordt geregistreerd met behulp van het token.
5. Voer een van de volgende handelingen uit:
   - Klik op **De machine registreren**. Meld u in het geopende browservenster aan bij de serviceconsole, bekijk de registratiegegevens en klik vervolgens op **Registratie bevestigen**.
   - Klik op **Registratiegegevens weergeven**. Het installatieprogramma geeft de registratielink en de registratiecode weer. U kunt deze kopiëren en de registratiestappen uitvoeren op een andere machine. In dit geval moet u de registratiecode invoeren op het registratieformulier. De registratiecode is een uur geldig.

     U kunt het registratieformulier ook als volgt openen: klik op **Alle apparaten** > **Toevoegen**, blader omlaag naar **Registratie via code** en klik vervolgens op **Registreren**.

     Opmerking
     Sluit het installatieprogramma pas af wanneer u de registratie hebt bevestigd. Als u de registratie opnieuw wilt starten, moet u het installatieprogramma opnieuw opstarten en de installatieprocedure herhalen.

De machine wordt dan toegewezen aan het account dat is gebruikt voor aanmelding bij de serviceconsole.

- Registreer de machine handmatig via de opdrachtregel. Zie 'Machines handmatig registreren' voor meer informatie over hoe u dit kunt doen.

6. [Als de agent is geregistreerd onder een account met tenant in de modus Verbeterde beveiliging] 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`

8.6.4 Cyberbescherming-agenten installeren in macOS

Vereisten

Download de gewenste agent op de machine die u wilt beschermen. Zie "Cyberbescherming-agenten downloaden" (p. 58).

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. Voer een van de volgende handelingen uit:
   - Klik op **De machine registreren**. Meld u in het geopende browservenster aan bij de serviceconsole, bekijk de registratiegegevens en klik vervolgens op **Registratie bevestigen**.
   - Klik op **Registratiegegevens weergeven**. Het installatieprogramma geeft de registratielink en de registratiecode weer. U kunt deze kopiëren en de registratiestappen uitvoeren op een andere machine. In dit geval moet u de registratiecode invoeren op het registratieformulier. De registratiecode is een uur geldig.

     U kunt het registratieformulier ook als volgt openen: klik op **Alle apparaten** > **Toevoegen**, blader omlaag naar **Registratie via code** en klik vervolgens op **Registreren**.

     Opmerking
     Sluit het installatieprogramma pas af wanneer u de registratie hebt bevestigd. Als u de registratie opnieuw wilt starten, moet u het installatieprogramma opnieuw opstarten en de installatieprocedure herhalen.

     De machine wordt dan toegewezen aan het account dat is gebruikt voor aanmelding bij de serviceconsole.
   - Registreer de machine handmatig via de opdrachtregel. Zie 'Machines handmatig registreren' voor meer informatie over hoe u dit kunt doen.
10. [Als de agent is geregistreerd onder een account met tenant in de modus Verbeterde beveiliging] 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).

8.6.5 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 Agentgebruiker 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, 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: Het wordt niet aanbevolen om aanmeldingsaccounts handmatig te wijzigen nadat de installatie is voltooid.

8.6.6 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 voor een beschermingsschema:

- Agent voor antimalwarebeveiliging en URL-filtering: vereist voor de werking van de functies voor antimalwarebeveiliging en URL-filtering.
- Agent voor preventie van gegevensverlies: vereist voor de werking van de functies voor apparaatbeheer.
- Acronis Cyber Protection Service: vereist voor de werking van de antimalwarebeveiliging.

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

8.7 Installatie zonder toezicht of installatie verwijderen

8.7.1 Installatie zonder toezicht of installatie verwijderen in Windows

In dit gedeelte wordt beschreven hoe u beveiligingsagenten in de modus zonder toezicht op een machine met Windows kunt installeren of verwijderen met behulp van Windows Installer (het programma `msiexec`). In een Active Directory-domein kunt u een installatie zonder toezicht ook uitvoeren via Groepsbeleid. Zie het gedeelte 'Agenten implementeren via Groepsbeleid'.

Tijdens de installatie kunt u ook een zogenaamd **transformatiebestand** (MST-bestand) gebruiken. Een transformatiebestand is een bestand met installatieparameters. In plaats daarvan kunt u installatieparameters rechtstreeks opgeven op de opdrachtregel.

Het MST-transformatiebestand maken en de installatiepakketten uitpakken

1. Meld u aan als beheerder en start het installatieprogramma.
2. Klik op **MST- en MSI-bestanden maken voor installatie zonder toezicht**.
3. Ga naar **Installatie-items** en selecteer de onderdelen die u wilt installeren. De installatiepakketten voor deze onderdelen worden uitgepakt uit het installatieprogramma.
4. Selecteer in **Registratie-instellingen** de optie **Referenties gebruiken** of **Registratietoken gebruiken**. Zie 'Agenten implementeren via Groepsbeleid' voor meer informatie over het genereren van een registratietoken.
5. Controleer of wijzig de andere installatie-instellingen die aan het MST-bestand worden toegevoegd.
6. Klik op **Doorgaan** en selecteer vervolgens de map waar de .mst-transformatie wordt gegenereerd en de .msi- en .cab-installatiepakketten worden uitgepakt.
7. Klik op **Genereren**.

Het product installeren met het MST-transformatiebestand

Voer op de opdrachtregel de volgende opdracht uit.

Opdrachtsjabloon:

```
msiexec /i <pakketnaam> TRANSFORMS=<transformatienaam>
```

Definities:

- `<pakketnaam>` is de naam van het MSI-bestand.
- `<transformatienaam>` is de naam van het transformatiebestand.

Opdrachtvoorbeeld:

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

Installeren of het product verwijderen door parameters handmatig op te geven

Voer op de opdrachtregel de volgende opdracht uit.

Opdrachtsjabloon (installeren):

```
msiexec /i <pakketnaam><PARAMETER 1>=<waarde 1> ... <PARAMETER N>=<waarde n>
```

`<pakketnaam>` is hier de naam van het MSI-bestand. Alle beschikbare parameters en bijbehorende waarden worden beschreven in het gedeelte 'Parameters voor installatie zonder toezicht of installatie verwijderen'.

Opdrachtsjabloon (verwijderen):

```
msiexec /x <pakketnaam> <PARAMETER 1>=<waarde 1> ... <PARAMETER N>=<waarde n>
```

Het .msi-pakket moet dezelfde versie hebben als het product dat u wilt verwijderen.

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 Windows. Naast deze parameters kunt u ook andere parameters van `msiexec` gebruiken, zoals beschreven in https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Installatieparameters

Basisparameters

`ADDLOCAL=<lijst met onderdelen>`

De onderdelen die worden geïnstalleerd, worden gescheiden door komma's zonder spaties. Alle genoemde onderdelen moeten worden uitgepakt uit het installatieprogramma voordat u de installatie begint.

Hier volgt de volledige lijst met onderdelen:

Onderdeel	Moet worden geïnstalleerd in	Bits	Naam / beschrijving van het onderdeel

	combinatie met		
MmsMspComponents		32-bits/64-bits	Kernonderdelen voor agenten
BackupAndRecoveryAgent	MmsMspComponents	32-bits/64-bits	Agent voor Windows
AmpAgentFeature	BackupAndRecoveryAgent	32-bits/64-bits	Agent voor antimalware en URL-filtering
DlpAgentFeature	BackupAndRecoveryAgent	32-bits/64-bits	Agent voor preventie van gegevensverlies
ArxAgentFeature	BackupAndRecoveryAgent	32-bits/64-bits	Agent voor Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32-bits/64-bits	Agent voor SQL
ARADAgentFeature	BackupAndRecoveryAgent	32-bits/64-bits	Agent voor Active Directory
ArxOnlineAgentFeature	MmsMspComponents	32-bits/64-bits	Agent voor Microsoft 365
OracleAgentFeature	BackupAndRecoveryAgent	32-bits/64-bits	Agent voor Oracle
AcronisESXSupport	MmsMspComponents	64 bits	Agent voor VMware ESX (i) (Windows)
HyperVAgent	MmsMspComponents	32-bits/64-bits	Agent voor Hyper-V
CommandLineTool		32-bits/64-bits	Opdrachtregelprogramma
TrayMonitor	BackupAndRecoveryAgent	32-bits/64-bits	Cyber Protection Monitor

BackupAndRecoveryBootableComponents		32-bits/64-bits	Bootable Media Builder

`TARGETDIR=<path>`

De locatie waar het product wordt geïnstalleerd. Deze map is standaard: `C:\Program Files\BackupClient`.

`REBOOT=ReallySuppress`

Als deze parameter is opgegeven, is het opnieuw opstarten van de machine niet toegestaan.

`/l*v <log file>`

Als deze parameter is opgegeven, wordt het installatielogboek in de uitgebreide modus opgeslagen in het opgegeven bestand. Het logbestand kan worden gebruikt om installatieproblemen te analyseren.

`CURRENT_LANGUAGE=<language ID>`

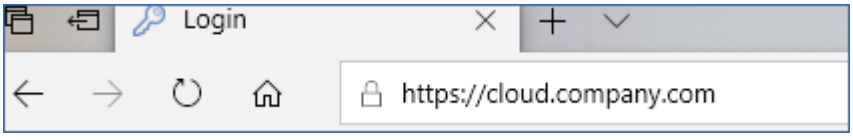
De taal van het product. Beschikbare waarden zijn als volgt: `en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW`.
Als deze parameter niet is opgegeven, wordt de taal van het product bepaald door uw systeemtaal (indien deze in de bovenstaande lijst staat). Anders wordt de taal van het product ingesteld op Engels (`en`).

Registratieparameters

`REGISTRATION_ADDRESS`

Dit is de URL voor de Cyberbescherming-service. U kunt deze parameter gebruiken met de parameters `REGISTRATION_LOGIN` en `REGISTRATION_PASSWORD` of met de parameter `REGISTRATION_TOKEN` .

- Wanneer u `REGISTRATION_ADDRESS` gebruikt met de parameters `REGISTRATION_LOGIN` en `REGISTRATION_PASSWORD`, moet u het adres opgeven dat u gebruikt voor **aanmelding** bij de Cyberbescherming-service. Bijvoorbeeld: `https://cloud.company.com`:



- Wanneer u `REGISTRATION_ADDRESS` gebruikt met de parameter `REGISTRATION_TOKEN`, geeft u het exacte adres van het datacentrum op. Dit is de URL die u ziet **zodra u bent aangemeld** bij de Cyberbescherming-service. Bijvoorbeeld: `https://eu2-cloud.company.com`.

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

`REGISTRATION_LOGIN` and `REGISTRATION_PASSWORD`

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

`REGISTRATION_PASSWORD_ENCODED`

Wachtwoord voor het account waarvoor de agent wordt geregistreerd in de Cyberbescherming-service, gecodeerd met base64. Zie 'Machines handmatig registreren' voor meer informatie over codering van uw wachtwoord.

`REGISTRATION_TOKEN`

Het registratietoken is een reeks van 12 tekens in drie segmenten, gescheiden door koppeltekens. U kunt er een genereren in de serviceconsole, zoals beschreven in 'Agenten implementeren via Groepsbeleid'.

`REGISTRATION_REQUIRED={0,1}`

Hiermee wordt bepaald hoe de installatie wordt beëindigd als de registratie mislukt. Als de waarde `1` is, mislukt de installatie ook. De standaardwaarde is `0`, dus als u deze parameter niet opgeeft, wordt de installatie uitgevoerd, zelfs als de agent niet is geregistreerd.

Aanvullende parameters

Gebruik een van de volgende parameters om het aanmeldingsaccount voor de agentservice in Windows te definiëren:

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`

  Als de waarde `1` is, wordt de agent uitgevoerd voor het **Lokale systeemaccount**.
- `MMS_CREATE_NEW_ACCOUNT={0,1}`

  Als de waarde `1` is, wordt de agent uitgevoerd voor het nieuw gemaakte account **Acronis Agent User**.
- `MMS_SERVICE_USERNAME=<user name>` and `MMS_SERVICE_PASSWORD=<password>`

  Gebruik deze parameters om een bestaand account op te geven waarvoor de agent wordt uitgevoerd.

Raadpleeg 'Het aanmeldingsaccount voor Windows-machines wijzigen' voor meer informatie over aanmeldingsaccounts.

`SET_ESX_SERVER={0,1}`

- Als de waarde `0` is, dan heeft de agent voor VMware die wordt geïnstalleerd, geen verbinding met een vCenter-server of een ESXi-host. Als de waarde `1` is, geeft u de volgende parameters op:
  - `ESX_HOST=<host name>`

    De hostnaam of het IP-adres van vCenter Server of de ESXi-host.
  - `ESX_USER=<user name>` and `ESX_PASSWORD=<password>`

    Referenties voor toegang tot de vCenter-server of ESXi-host.

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

De HTTP-proxyserver die door de agent wordt gebruikt. Zonder deze parameters wordt geen proxyserver gebruikt.

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

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

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

Als de waarde `0` is of als de parameter niet is opgegeven, gebruikt de agent de proxyserver alleen voor back-up en herstel vanuit de cloud. Als de waarde `1` is, maakt de agent ook verbinding met de beheerserver via de proxyserver.

Parameters voor het verwijderen van de installatie

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

De onderdelen die worden verwijderd, worden gescheiden door komma's zonder spaties. Als de waarde `ALL` is, worden alle productonderdelen verwijderd.

U kunt ook de volgende parameter opgeven:

`DELETE_ALL_SETTINGS={0, 1}`

Als de waarde `1` is, worden de logboeken, taken en configuratie-instellingen van het product verwijderd.

`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.

Voorbeelden

- Agent voor Windows, Agent voor Antimalware en URL-filtering, opdrachtregelprogramma en Cyberbescherming Monitor installeren. De machine registreren in de Cyberbescherming-service met 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 Cyberbescherming Monitor installeren. Een nieuw aanmeldingsaccount maken voor de agentservice in Windows. De machine registreren in de Cyberbescherming-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 Cyberbescherming Monitor installeren. De machine registreren in de Cyberbescherming-service met behulp van een gebruikersnaam en gecodeerd met een base64-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 Cyberbescherming Monitor installeren. De machine registreren in de Cyberbescherming-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
```

- Alle agenten verwijderen en hun logboeken, taken en configuratie-instellingen verwijderen.

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

8.7.2 Installatie zonder toezicht of installatie 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 beveiligingsagent installeren of verwijderen

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:

```
<pakketnaam> -a <parameter 1> ... <parameter N>
```

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

- Voer de volgende opdracht uit om de installatie te starten met parameters die zijn opgegeven in een afzonderlijk tekstbestand:

  ```
  <pakketnaam> -a --options-file=<pad naar bestand>
  ```

  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. Zet elke parameter op een nieuwe regel, gevolgd door de gewenste waarde, bijvoorbeeld:

  ```
  --rain=https://cloud.company.com
  --login=janjansen
  --password=janswachtwoord
  --auto
  ```

  of

  ```
  -C
  https://cloud.company.com
  -g
  janjansen
  -w
  janswachtwoord
  -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.

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=}<lijst met onderdelen>`

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

Zonder deze parameter worden alle hier genoemde onderdelen 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 Cyberbescherming-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 Cyberbescherming-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 serviceconsole, zoals beschreven in 'Agenten implementeren via Groepsbeleid'.

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

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

    De URL van de Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-service. Dit mag niet het account van een partnerbeheerder zijn.

- `--skip-registration`

  Gebruik deze parameter als u de agent wilt installeren, maar u van plan bent deze later te registreren in de Cyberbescherming-service. Zie 'Machines handmatig registreren' voor meer informatie over hoe u dit kunt doen.

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. Het gebruik van deze optie wordt niet aanbevolen.

`--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
```

8.7.3 Installatie en verwijderen zonder toezicht in macOS

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

Kan het installatiebestand niet downloaden (.dmg)

1. Ga in de serviceconsole naar **Apparaten** > **Alle apparaten**.
2. Klik op **Toevoegen** en klik vervolgens op **Mac**.

Agent voor Mac installeren

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

   ```
   mkdir <dmg_root>
   ```

   Voor `<dmg_root>` kunt een naam naar eigen keuze opgeven.
2. 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**.
3. Voer het installatieprogramma uit.

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

4. Ontkoppel het installatiebestand (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Voorbeelden

- ```
  mkdir mydirectory
  ```

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

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

  ```
  hdiutil detach mydirectory
  ```

Agent voor Mac registreren

Voer een van de volgende handelingen uit:

- Registreer de agent voor een specifiek account door een gebruikersnaam en wachtwoord op te geven.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -a <adres van
  Cyberbescherming-service> -t cloud -u <gebruikersnaam> -p <wachtwoord> -o register
  ```

  Definities:

  `<Cyberbescherming serviceadres>` is het adres dat u gebruikt voor **aanmelding** bij de Cyberbescherming-service. Bijvoorbeeld:

  `<gebruikersnaam>` en `<wachtwoord>` zijn de referenties voor het account waarvoor de agent wordt geregistreerd. Dit kan niet het account van een partnerbeheerder zijn.
- Registreer de agent met een registratietoken.

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

  Het registratietoken is een reeks van 12 tekens in drie segmenten, gescheiden door koppeltekens. U kunt er een genereren in de serviceconsole, zoals beschreven in 'Agenten implementeren via Groepsbeleid'.

  Wanneer u een registratietoken gebruikt, moet u het exacte adres van het datacenter opgeven. Dit is de URL die u ziet **zodra u bent aangemeld** bij de Cyberbescherming-service. Bijvoorbeeld:

  ```

## Voorbeelden

Registratie met gebruikersnaam en wachtwoord.

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

Registratie met token.

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

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.

Agent voor Mac verwijderen

Voer de volgende opdracht uit:

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

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

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

8.8 Machines handmatig registreren

U kunt een machine registreren in de Cyberbescherming-service tijdens de installatie van de agent of via de opdrachtregelinterface. Mogelijk moet u dit doen als u de agent hebt geïnstalleerd maar de automatische registratie bijvoorbeeld is mislukt of als u een bestaande machine wilt registreren voor een nieuw account.

Een machine registreren

Voer de volgende opdracht uit om een machine te registreren met een gebruikersnaam en wachtwoord.

In Windows

Opdracht voor het registreren van een machine onder het huidige account:

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

Opdrachtsjabloon voor het registreren van een machine onder een ander account:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <serviceadres> -u <gebruikersnaam> -p <wachtwoord>
```

Opdrachtvoorbeeld:

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

In Linux

Opdracht voor het registreren van een machine onder het huidige account:

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

Opdrachtsjabloon voor het registreren van een machine onder een ander account:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
<serviceadres> -u <gebruikersnaam> -p <wachtwoord>
```

Opdrachtvoorbeeld:

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

In macOS

Opdracht voor het registreren van een machine onder het huidige account:

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

Opdrachtsjabloon voor het registreren van een machine onder een ander account:

```
sudo "/Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
<serviceadres> -u <gebruikersnaam> -p <wachtwoord>
```

Opdrachtvoorbeeld:

```
sudo "/Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.bedrijf.com -u janjansen -p janswachtwoord
```

Opmerking
Gebruik de gebruikersnaam en het wachtwoord voor het specifieke account waarvoor de agent wordt geregistreerd. Dit mag niet het account van een partnerbeheerder zijn.
Het serviceadres is de URL die u gebruikt voor **aanmelding** bij de Cyberbescherming-service. Bijvoorbeeld: `https://cloud.company.com`:

Indien gewenst, kunt u een machine ook registreren met een registratietoken. Voer hiervoor de volgende opdracht uit.

In Windows

Opdrachtsjabloon:

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

Opdrachtvoorbeeld:

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

In Linux

Opdrachtsjabloon:

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

Opdrachtvoorbeeld:

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

In macOS

Opdrachtsjabloon:

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

Opdrachtvoorbeeld:

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

Opmerking
Wanneer u een registratietoken gebruikt, moet u het exacte adres van het datacenter opgeven. Dit is de URL die u ziet **zodra u bent aangemeld** bij de Cyberbescherming-service. Bijvoorbeeld: `https://eu2-cloud.company.com`.

In dit geval moet u niet `https://cloud.company.com` gebruiken.
Het registratietoken is een reeks van 12 tekens in drie segmenten, gescheiden door koppeltekens. Zie 'Agenten implementeren via Groepsbeleid' voor meer informatie over het genereren van een agent.

Registratie van een machine ongedaan maken

Voer de volgende opdracht uit:

In Windows

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

In Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o registratie verwijderen
```

In macOS

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

8.8.1 Wachtwoorden met speciale tekens of spaties

Als uw wachtwoord speciale tekens of spaties bevat, plaats het dan tussen aanhalingstekens wanneer u het op de opdrachtregel typt.

Voer bijvoorbeeld in Windows deze opdracht uit.

Opdrachtsjabloon:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <serviceadres> -u <gebruikersnaam> -p <"wachtwoord">
```

Opdrachtvoorbeeld:

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

Als u nog steeds een foutmelding krijgt:

- Codeer 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 deze opdracht uit.

Opdrachtsjabloon:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <serviceadres> -u <gebruikersnaam> -b -p <gecodeerd wachtwoord>
```

Opdrachtvoorbeeld:

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

8.9 Automatische detectie van machines

Met de functie voor machinedetectie kunt u het volgende doen:

- De installatie van beveiligingsagenten en machineregistratie automatiseren door machines automatisch te detecteren in uw Active Directory-domein (AD) of lokale netwerk.
- De beveiligingsagent installeren en bijwerken op meerdere machines.
- Synchronisatie met Active Directory gebruiken om het werk en de overhead voor resource-inrichting en machinebeheer in een grote AD-omgeving te verminderen.

Belangrijk
Machinedetectie kan alleen worden uitgevoerd door agenten op Windows-machines. Momenteel kunnen alleen Windows-machines door de detectieagent worden gedetecteerd en ook software-installatie op afstand is alleen mogelijk op Windows-machines.
Als er geen machine is waarop de agent is geïnstalleerd, wordt de functionaliteit van automatische detectie verborgen en het gedeelte **Meerdere apparaten** wordt verborgen in de wizard Nieuw apparaat toevoegen.

Wanneer machines zijn toegevoegd aan de serviceconsole, worden deze als volgt gecategoriseerd:

- **Gedetecteerd**: machines die zijn gedetecteerd, maar waarop geen beveiligingsagent is geïnstalleerd.
- **Beheerd**: machines waarop de beveiligingsagent is geïnstalleerd.

- **Onbeschermd**: machines waarop het beschermingsschema niet wordt toegepast. Onbeschermde machines kunnen zowel gedetecteerde als beheerde machines zijn waarop geen beschermingsschema is toegepast.
- **Beschermd**: machines waarop het beschermingsschema wordt toegepast.

8.9.1 Zo werkt het

De detectieagent maakt gebruik van de volgende technologieën voor scans van het lokale netwerk: NetBIOS-detectie, Web Service Discovery (WSD) en de ARP-tabel (Address Resolution Protocol). De agent probeert de volgende parameters op te halen van elke machine:

- Naam (korte naam/NetBIOS-hostnaam)
- FQDN
- Domein/werkgroep
- IPv4/IPv6-adressen
- MAC-adressen
- Besturingssysteem (naam/versie/familie)
- Machinecategorie (werkstation/server/domeincontroller)

Wanneer AD-scans worden uitgevoerd, probeert de agent bijna dezelfde parameters van elke machine op te halen als hierboven vermeld. Het verschil is dat ook de parameter Organisatie-eenheid (OU) en meer volledige informatie over de naam en het besturingssysteem worden opgehaald, maar geen IP-adres en MAC-adres.

8.9.2 Vereisten

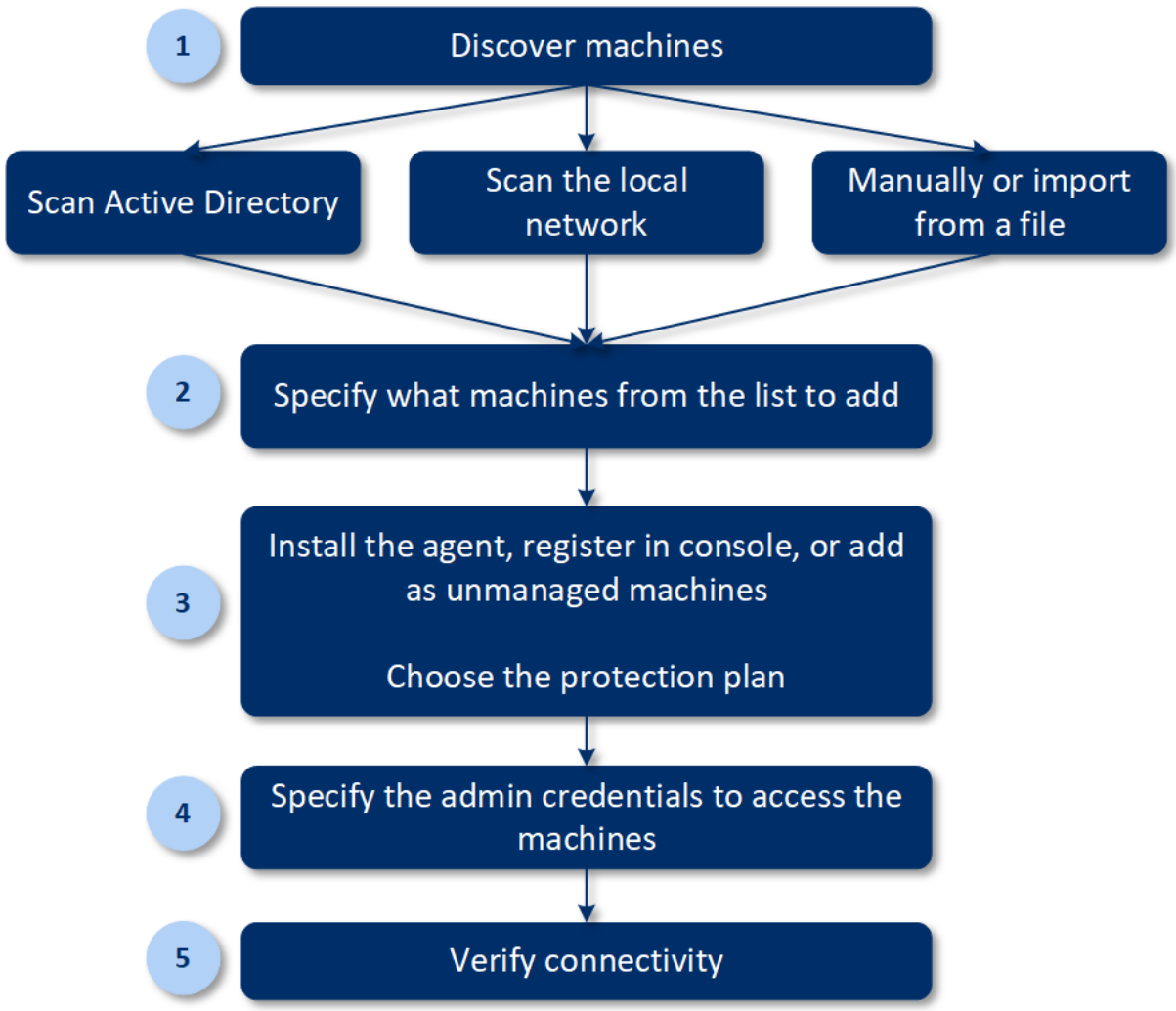
Voordat u machines detecteert, moet u de beveiligingsagent installeren op ten minste één machine in uw lokale netwerk om deze als detectieagent te gebruiken.

Als u van plan bent machines in het Active Directory-domein te detecteren, moet u de agent op ten minste één machine in het AD-domein installeren. Deze agent wordt gebruikt als detectieagent tijdens de AD-scan.

Opmerking
Agent voor Windows kan niet worden geïnstalleerd op een externe machine met Windows XP.
Als u Agent voor Windows wilt installeren op een machine met Windows Server 2012 R2, moet Windows-update KB2999226 zijn geïnstalleerd op deze machine.

8.9.3 Machinedetectie

In het volgende schema ziet u de belangrijkste stappen van het proces voor machinedetectie:



Automatische detectie bestaat doorgaans uit de volgende stappen:

1. Selecteer de methode voor machinedetectie:
   - Active Directory-scan
   - Lokalenetwerkscan
   - Handmatig: een machine toevoegen op IP-adres of hostnaam of een lijst met machines importeren uit een bestand

   Met de eerste twee methoden worden de resultaten automatisch gefilterd om machines met geïnstalleerde agenten uit te sluiten.

   Met de handmatige methode wordt een upgrade uitgevoerd voor de bestaande agenten en worden deze opnieuw geregistreerd. Wanneer u automatische detectie uitvoert via hetzelfde account, betekent dit dat de agent alleen wordt bijgewerkt naar de nieuwste versie als dat nodig is. Als u een ander account gebruikt, wordt de agent bijgewerkt en opnieuw geregistreerd onder de tenant waartoe het account behoort.
2. Selecteer machines om toe te voegen uit de lijst die u ontvangt bij de vorige stap.
3. Selecteer hoe de machines worden toegevoegd:

- De beveiligingsagent en extra onderdelen worden op de machines geïnstalleerd en worden ook geregistreerd in de serviceconsole.
- De machines worden geregistreerd in de serviceconsole (als de agent al is geïnstalleerd).
- De machines worden als **onbeheerde machines** toegevoegd aan de serviceconsole, zonder installatie van een agent of onderdeel.

Als u een van de eerste twee methoden hebt geselecteerd om een machine toe te voegen, kunt u ook het beschermingsschema uit de bestaande schema's selecteren en op machines toepassen.

4. Geef de referenties op van de gebruiker die de beheerdersrechten heeft voor het beheer van de machines.
5. Controleer de connectiviteit met machines met behulp van de verstrekte referenties.

In de volgende onderwerpen krijgt u meer gedetailleerde informatie over de detectieprocedure.

8.9.4 Automatische detectie n handmatige detectie

Voordat u met de detectie begint, moet u controleren of dat aan de voorwaarden is voldaan.

Machines detecteren

1. Ga in de serviceconsole 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 vanuit 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. [Als de detectiemethode met Active Directory of het lokale netwerk is geselecteerd] Gebruik een lijst om de machines te selecteren die u wilt toevoegen.

[Als de handmatige detectiemethode is geselecteerd] Geef de machine-IP-adressen of hostnamen op of importeer de machinelijst 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 welke acties moeten worden uitgevoerd na de detectie:
   - **Agenten installeren en machines registreren**. U kunt selecteren welke onderdelen op de machines moeten worden geïnstalleerd door te klikken op **Onderdelen selecteren**. Zie "Onderdelen selecteren voor installatie" (p. 91) voor meer informatie.

     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 Agentgebruiker 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, 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.
   - **Machines met geïnstalleerde agenten registreren**. Deze optie wordt gebruikt als de agent al is geïnstalleerd op de machines en u deze alleen hoeft te registreren in Cyberbescherming. Als er geen agent wordt gevonden op de machines, dan worden de machines toegevoegd als **Onbeheerd**.
   - **Toevoegen als onbeheerde machines**. De agent wordt niet op de machines geïnstalleerd. U kunt ze later in de console bekijken en de agent later installeren of registreren.

[Als de actie **Agenten installeren en machines registreren** na detectie is geselecteerd] **De machine indien nodig opnieuw opstarten**: als de optie is ingeschakeld, wordt de machine zo vaak als nodig opnieuw opgestart om de installatie te voltooien.

De machine moet mogelijk opnieuw worden opgestart in een van de volgende gevallen:

- De vereiste onderdelen zijn geïnstalleerd en de machine moet opnieuw worden opgestart om door te gaan met de installatie
- De installatie is voltooid, maar opnieuw opstarten is vereist omdat sommige bestanden tijdens de installatie zijn vergrendeld
- De installatie is voltooid, maar opnieuw opstarten is vereist voor andere eerder geïnstalleerde software

[Als **De machine indien nodig opnieuw opstarten** is geselecteerd]: **Niet opnieuw opstarten als de gebruiker is aangemeld**: als de optie is ingeschakeld, 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 opnieuw moet worden opgestart, wordt het systeem niet opnieuw opgestart.

Als de vereiste onderdelen zijn geïnstalleerd en het opnieuw opstarten niet is voltooid omdat een gebruiker is aangemeld, moet u de machine opnieuw opstarten om de installatie van de agent te voltooien en de installatie opnieuw te starten.

Als de agent is geïnstalleerd maar het systeem niet opnieuw is opgestart, moet u de machine opnieuw opstarten.

[Als er eenheden in uw organisatie zijn] **Gebruiker voor wie de machines moeten worden geregistreerd**: selecteer de gebruiker van uw eenheid of ondergeschikte eenheden waarvoor de machines worden geregistreerd.

Als u een van de eerste twee acties na detectie hebt geselecteerd, is er ook een optie om het beschermingsschema toe te passen op de machines. Als u verschillende beschermingsschema's 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 enkele aangepaste beheerdersreferenties wilt definiëren, moet u aanvullende handmatige voorbereidingen treffen, zoals beschreven in 'Externe installatie van een agent voor een aangepaste beheerder inschakelen' hieronder.

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 **Dashboard** > **Activiteiten** > **Machines detecteren**.

Een machine voorbereiden voor externe installatie

1. Als u de installatie wilt uitvoeren op een externe machine met Windows Vista of later, moet de optie **Configuratiescherm > Mapopties > Weergave > Wizard Delen gebruiken** zijn *uitgeschakeld* op die machine.
2. 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.
3. 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.
4. 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 Vista, Windows Server 2008, Windows 7 of later: ga naar **Configuratiescherm > Windows Firewall > Netwerkcentrum > Geavanceerde instellingen voor delen wijzigen**.
5. Voor een externe installatie van Cyberbescherming 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 Vista 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 bevelen we aan dat u na het beëindigen van de beheerbewerking (zoals externe installatie) beide instellingen herstelt naar hun 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 URL-	Met dit onderdeel kunnen de modules Antivirus- en antimalwarebeveiliging en

filtering	URL-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 wordt 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.
Cyberbescherming 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.

8.9.5 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 **Uitzonderingen**, 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 **Uitzonderingen**, selecteert u deze in de lijst en klikt u op **Toevoegen aan uitzonderingen**. Als u een machine wilt verwijderen uit **Uitzonderingen**, gaat u naar **Onbeheerde machines** > **Uitzonderingen**, selecteert u de machine en klikt u op **Verwijderen uit uitzonderingen**.

U kunt de beveiligingsagent installeren en meerdere gedetecteerde machines registreren in Cyberbescherming 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.

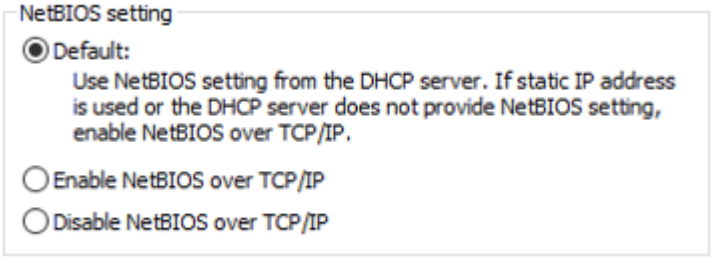
Wanneer de beveiligingsagent op machines is geïnstalleerd, worden deze machines weergegeven in het gedeelte **Apparaten** > **Machines met agenten**.

Als u de beveiligingsstatus wilt controleren, gaat u naar **Dashboard** > **Overzicht** en voegt u de widget **Beveiligingsstatus** of de widget **Gedetecteerde machine** toe.

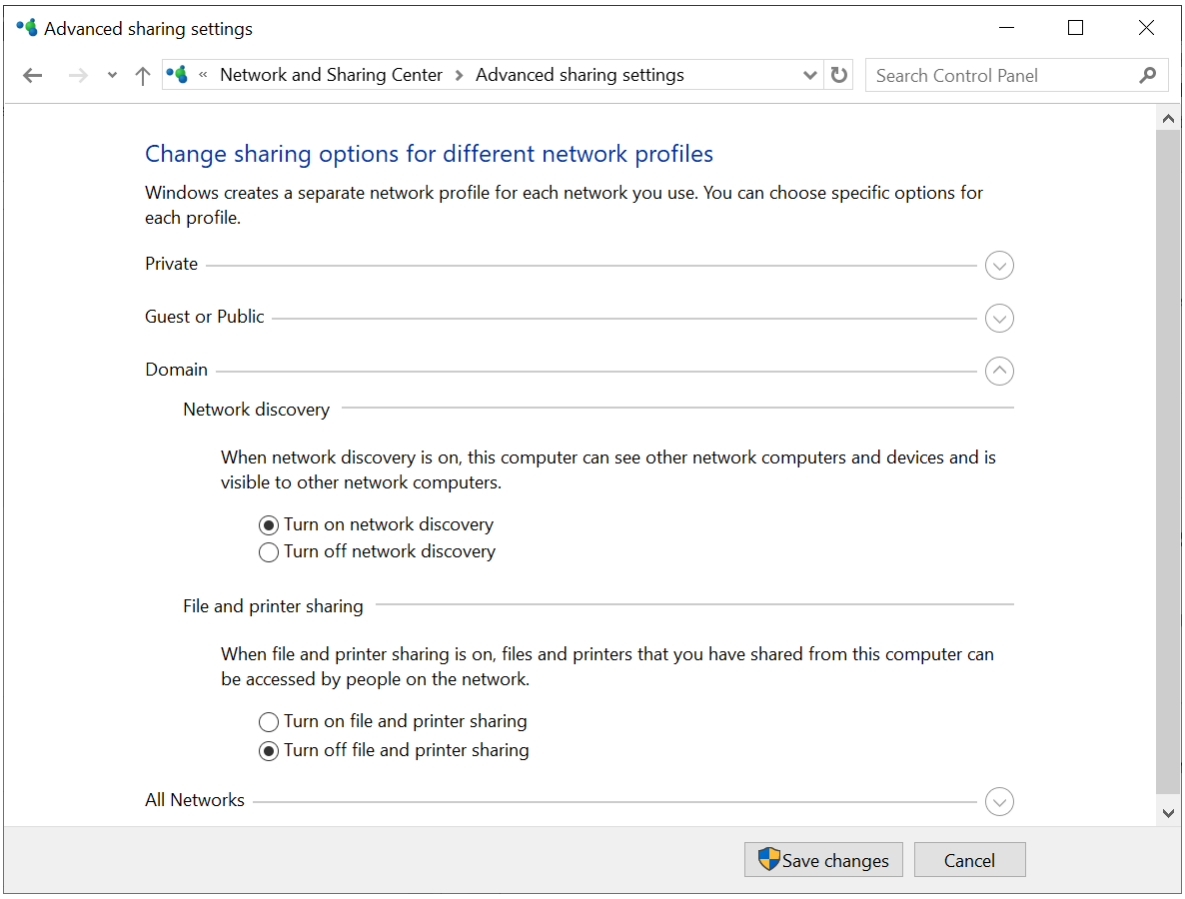
8.9.6 Problemen oplossen

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.

8.10 Agent voor VMware (Virtual Appliance) implementeren

8.10.1 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 wanneer u verwacht dat de bandbreedte van het back-upverkeer de 100 MB per seconde overschrijdt (bijvoorbeeld in netwerken van 10 GBit), raden we u aan deze bronnen uit te breiden tot 8 GB RAM en 4 vCPU's.

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 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**.

8.10.2 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.

8.10.3 De virtuele toepassing configureren

1. Geef in vSphere Client de optie **Inventaris** weer, klik met de rechtermuisknop op de naam van de virtuele toepassing en selecteer **Aan/uit** > **Inschakelen**. Selecteer het tabblad **Console**.
2. De netwerkverbinding van de agent wordt automatisch geconfigureerd met Dynamic Host Configuration Protocol (DHCP). Als u de standaardconfiguratie wilt wijzigen, gaat u naar **Agentopties** in **eth0**, klikt u op **Wijzigen** en geeft u de gewenste netwerkinstellingen op.

3. Ga naar **Agentopties** in **vCenter/ESX(i)**, klik op **Wijzigen** en geef de naam of het IP-adres van vCenter Server op. De agent kan dan een back-up maken en een herstelbewerking uitvoeren voor elke virtuele machine die wordt beheerd met vCenter Server.

   Als u geen gebruik maakt van vCenter Server, geeft u de naam of het IP-adres van de ESXi-host op met de virtuele machines waarvan u een back-up wilt maken of die u wilt herstellen. Doorgaans worden back-ups sneller uitgevoerd wanneer de agent back-ups maakt van virtuele machines die worden gehost op de eigen host.

   Geef de referenties op die de agent moet gebruiken om verbinding te maken met vCenter Server of ESXi. We raden aan een account te gebruiken waaraan de rol **Beheerder** is toegewezen. Anders moet u een account met de nodige rechten beschikbaar maken op de vCenter-server of ESXi.

   U kunt op **Verbinding controleren** klikken om te controleren of de toegangsreferenties juist zijn.
4. Ga naar **Agentopties** in **Beheerserver** en klik op **Wijzigen**.
   a. Selecteer bij **Servernaam/IP** de optie **Cloud**. Het adres van de Cyberbescherming-service wordt weergegeven. Wijzig dit adres niet tenzij anders wordt aangegeven.
   b. Geef bij **Gebruikersnaam** en **Wachtwoord** de gebruikersnaam en het wachtwoord op voor de Cyberbescherming-service. De agent en de virtuele machines die door de agent worden beheerd, worden geregistreerd onder dit account.
5. Ga naar **Virtuele machine** in **Tijdzone** en klik op **Wijzigen**. Selecteer de tijdzone van uw locatie om te waarborgen dat de geplande bewerkingen op de juiste tijd worden uitgevoerd.
6. [Optioneel] Lokale opslag toevoegen.

   U kunt een aanvullende schijf koppelen aan de virtuele toepassing, zodat de Agent voor VMware back-ups kan maken naar deze lokaal gekoppelde opslag.

   U kunt de schijf toevoegen door de instellingen van de virtuele machine te bewerken en op **Vernieuwen** te klikken. De link **Opslag maken** is dan beschikbaar. Klik op deze link, selecteer de schijf en geef een naam op voor de schijf.
7. [Als een proxyserver is ingeschakeld in uw netwerk] Configureer de proxyserver.
   a. Als u de opdrachtshell wilt starten, drukt u op CTRL+SHIFT+F2 in de gebruikersinterface van de virtuele toepassing.
   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 `ADRES` door de nieuwe waarden voor de hostnaam/het IP-adres van de proxyserver en vervang `POORT` door de decimale waarde van het poortnummer.

e. Als uw proxyserver verificatie vereist, vervangt u `GEBRUIKERSNAAM` en `WACHTWOORD` 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 automatische of handmatige updates wilt uitvoeren van een virtuele toepassing die zich achter een proxy bevindt, moet u de proxyserver in de toepassing als volgt configureren.

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
```

8.11 Agent voor Scale Computing HC3 (Virtual Appliance) implementeren ...

8.11.1 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. We raden aan deze resources uit te breiden naar 4 vCPU's en 8 GiB RAM als u verwacht dat de bandbreedte van het back-upverkeer de 100 MB per seconde zal overschrijden (bijvoorbeeld in netwerken van 10 Gb). Op die manier kunt u de prestaties van back-ups verbeteren.

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 uit de Cyberbescherming-serviceconsole hebt verwijderd.

Controleren door welke agent een specifieke machine word beheerd

1. Klik in de Cyberbescherming-serviceconsole 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.

8.11.2 De QCOW2-sjabloon implementeren

1. Meld u aan bij uw Cyberbescherming-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. 101) 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. 99) 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.

8.11.3 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 Cyberbescherming-service.

De virtuele toepassing configureren

1. Meld u aan bij uw Scale Computing HC3-account.
2. Selecteer de virtuele machine van de toepassing die u wilt configureren en klik vervolgens op het **Console**-pictogram.
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 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. 101) voor meer informatie over deze rollen.

c. [Optioneel] Klik op **Verbinding controleren** om te controleren of de verstrekte referenties juist zijn.
d. Klik op **OK**.

5. Klik in het veld **Beheerserver** op **Wijzigen** om het adres van de Cyberbescherming-service en de referenties voor toegang op te geven.
   a. Selecteer in het veld **Servernaam/IP** de optie **Cloud** en geef vervolgens het Cyberbescherming-serviceadres op.
   b. Voer in de velden **Gebruikersnaam** en **Wachtwoord** de referenties in voor uw account in de Cyberbescherming-service.
   c. Klik op **OK**.
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 Cyberbescherming-serviceconsole.
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. Als u de opdrachtshell wilt starten, drukt u op CTRL+SHIFT+F2 in de gebruikersinterface van de virtuele toepassing.
   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 `ADRES` door de nieuwe waarden voor de hostnaam/het IP-adres van de proxyserver en vervang `POORT` door de decimale waarde van het poortnummer.
   e. Als uw proxyserver verificatie vereist, vervangt u `GEBRUIKERSNAAM` en `WACHTWOORD` 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 automatische of handmatige updates wilt uitvoeren van een virtuele toepassing die zich achter een proxy bevindt, moet u de proxyserver in de toepassing als volgt configureren.

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
```

Virtuele machines in het Scale Computing HC3-cluster beschermen

1. Meld u aan bij uw Cyberbescherming-account.
2. Ga naar **Apparaten** > **Scale Computing HC3**> <uw cluster> of zoek uw machines in **Apparaten** > **Alle apparaten**.
3. Selecteer de gewenste machines en pas een beschermingsschema toe op deze machines.

8.11.4 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

8.12 Agent voor Virtuozzo Hybrid Infrastructure (Virtual Appliance) implementeren

8.12.1 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. We raden aan deze resources uit te breiden naar 4 vCPU's en 8 GB RAM als u verwacht dat de bandbreedte van het back-upverkeer de 100 MB per seconde zal overschrijden (bijvoorbeeld in netwerken van 10 GB). Op die manier kunt u de prestaties van back-ups verbeteren.

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 Cyberbescherming-webinterface hebt verwijderd.

Controleren door welke agent een specifieke machine word beheerd

1. Klik in de Cyberbescherming-serviceconsole 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.

8.12.2 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 Vereisten voor het compute-cluster in de Virtuozzo-documentatie voor meer informatie over het configureren van de netwerken.

8.12.3 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 Domeingebruikers 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.

8.12.4 De QCOW2-sjabloon implementeren

1. Meld u aan bij uw Cyberbescherming-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 Infrastructuur-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.

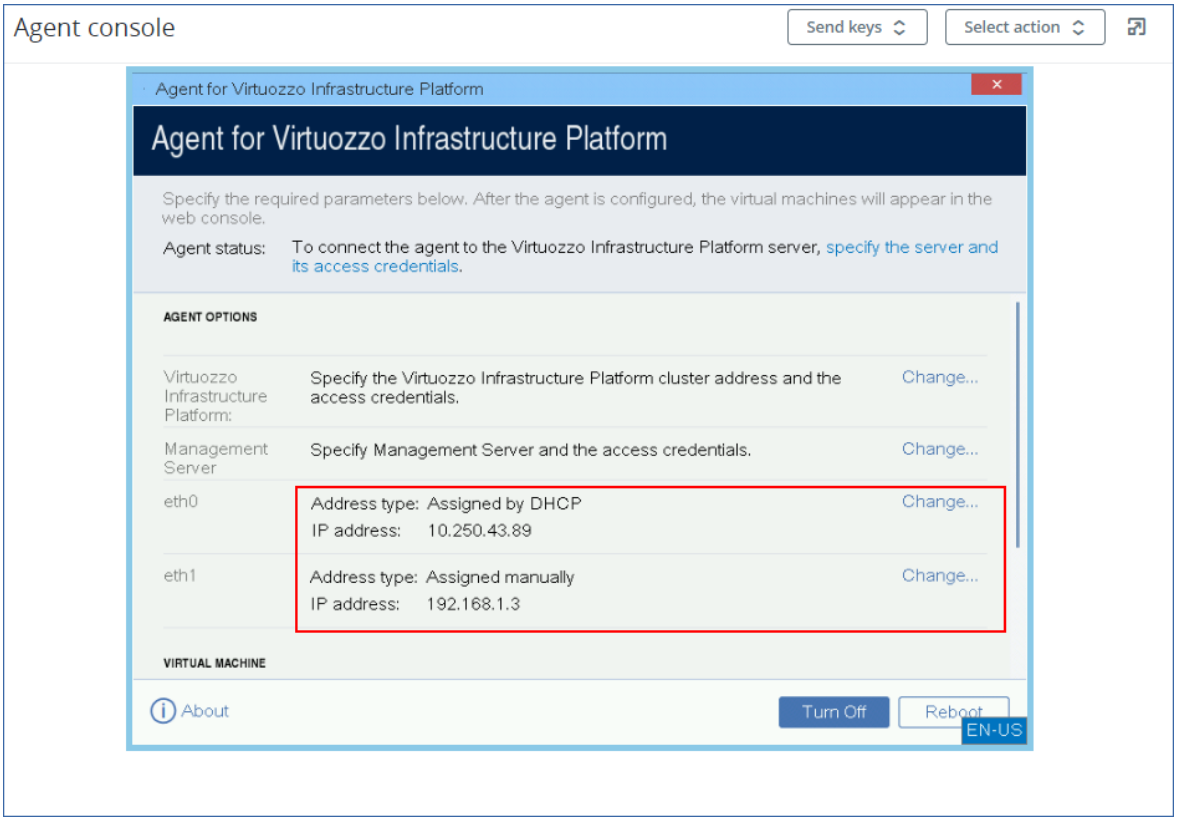
7. Klik op **Gereed**.
8. Wanneer u weer terug bent in het venster **Virtuele machine maken**, klikt u op **Implementeren** om de virtuele machine te maken en op te starten.

8.12.5 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 Cyberbescherming-cloudservice.

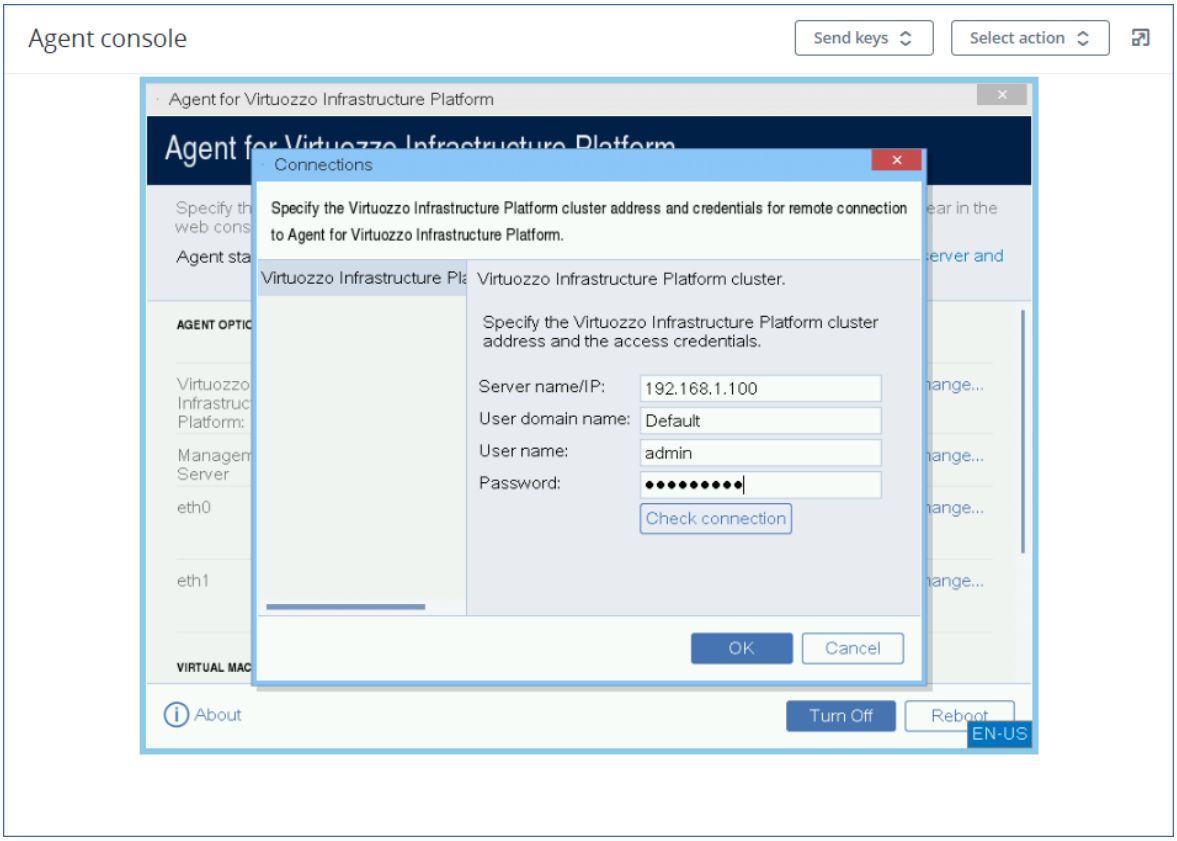
De virtuele toepassing configureren

1. Meld u aan bij uw Virtuozzo Hybrid Infrastructuur-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.

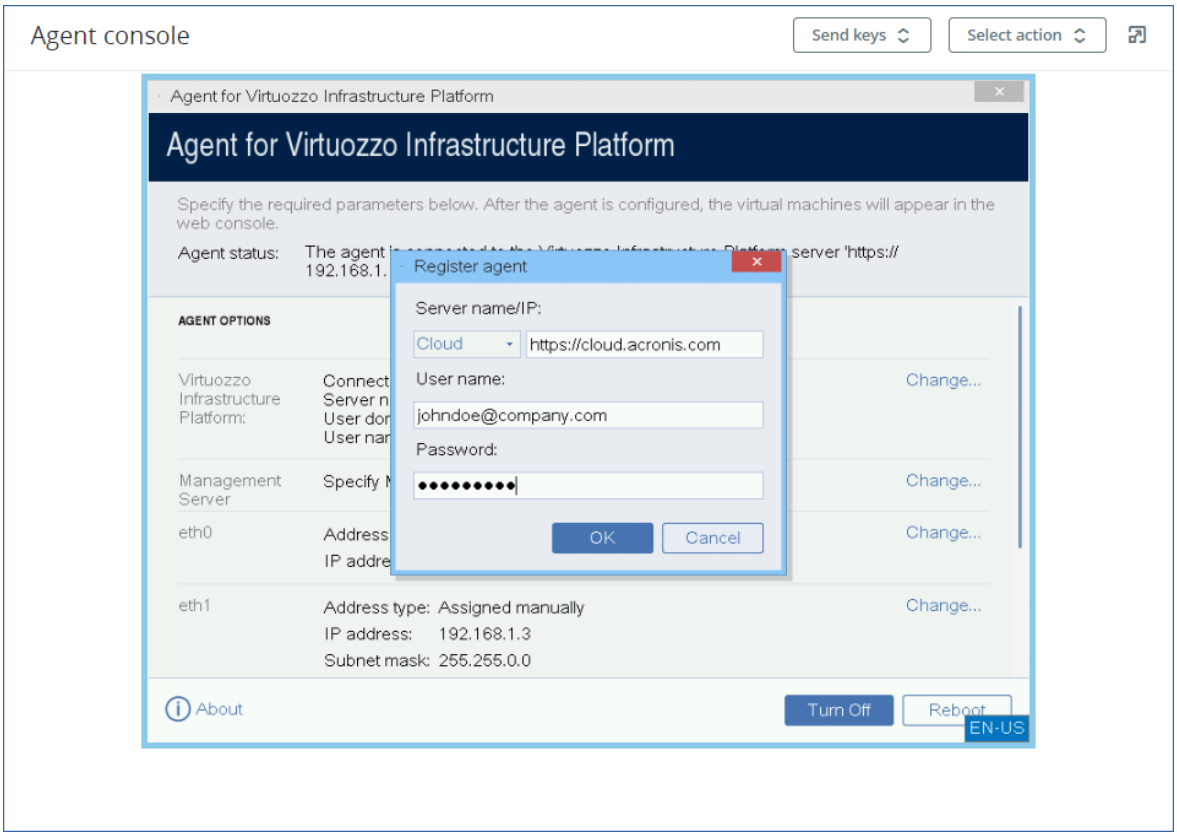


4. Geef het adres en de referenties van het Virtuozzo-cluster op:
   - DNS-naam of IP-adres van het Virtuozzo Hybrid Infrastructure-cluster (dit is het adres van het beheerknooppunt van het cluster). De standaardpoort 5000 wordt automatisch ingesteld. Als u een andere poort gebruikt, moet u deze handmatig 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. Geef het adres en de referenties op voor de Cyberbescherming-beheerserver om toegang te krijgen.



6. [Als een proxyserver is ingeschakeld in uw netwerk] Configureer de proxyserver.
   a. Als u de opdrachtshell wilt starten, drukt u op CTRL+SHIFT+F2 in de gebruikersinterface van de virtuele toepassing.
   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 `ADRES` door de nieuwe waarden voor de hostnaam/het IP-adres van de proxyserver en vervang `POORT` door de decimale waarde van het poortnummer.
   e. Als uw proxyserver verificatie vereist, vervangt u `GEBRUIKERSNAAM` en `WACHTWOORD` 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

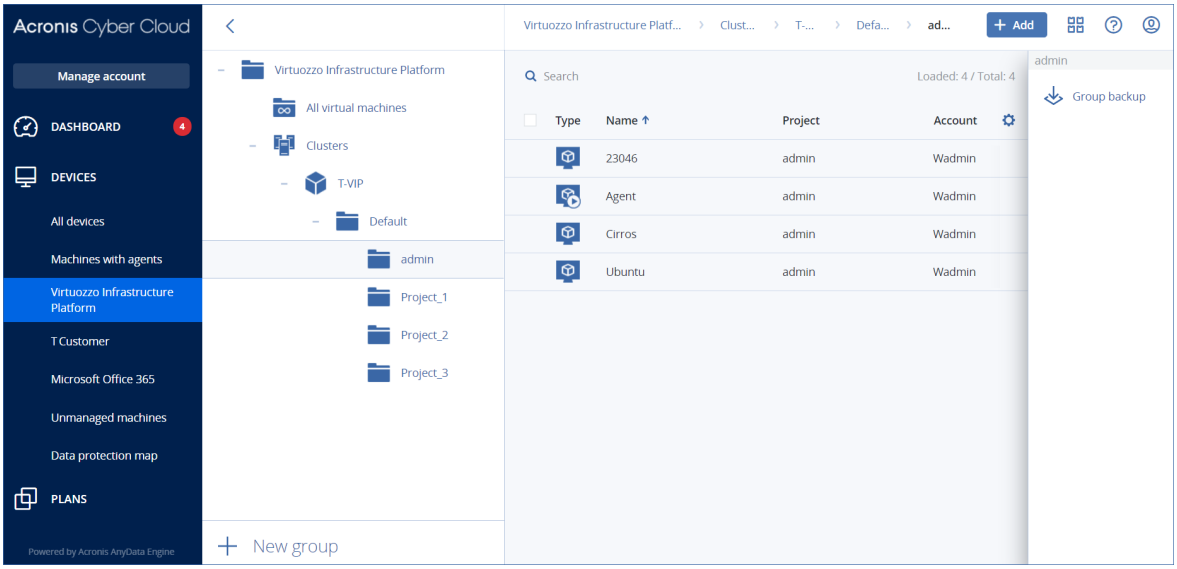
Als u automatische of handmatige updates wilt uitvoeren van een virtuele toepassing die zich achter een proxy bevindt, moet u de proxyserver in de toepassing als volgt configureren.

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
```

De virtuele machines in het Virtuozzo Hybrid Infrastructure-cluster beschermen

1. Meld u aan bij uw Cyberbescherming-account.
2. Ga naar **Apparaten** > **Virtuozzo Hybrid Infrastructure**> <uw cluster> > **Standaardproject** > **admin** of zoek uw machines in **Apparaten** > **Alle apparaten**.
3. Selecteer de gewenste machines en pas een beschermingsschema toe op deze machines.



8.13 Agent voor oVirt (Virtual Appliance) implementeren ...

8.13.1 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. We raden aan deze resources uit te breiden naar 4 vCPU's en 8 GiB RAM als u verwacht dat de bandbreedte van het back-upverkeer de 100 MB per seconde zal overschrijden (bijvoorbeeld in netwerken van 10 Gb). Op die manier kunt u de prestaties van back-ups verbeteren.

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 uit de Cyberbescherming-serviceconsole hebt verwijderd.

Controleren door welke agent een specifieke machine word beheerd

1. Klik in de Cyberbescherming-serviceconsole 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

8.13.2 De OVA-sjabloon implementeren

1. Meld u aan bij uw Cyberbescherming-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. 115) 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. 113) 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 Cyberbescherming-serviceconsole. 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.

8.13.3 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 Cyberbescherming-service.

De virtuele toepassing configureren

1. Meld u aan bij de Red Hat Virtualization/oVirt-beheerportal.
2. Selecteer de virtuele machine met de agent die u wilt configureren en klik vervolgens op het **Console**-pictogram.
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. 115) voor meer informatie over deze rollen.
   c. [Optioneel] Klik op **Verbinding controleren** om te controleren of de verstrekte referenties

juist zijn.

d. Klik op **OK**.

5. Klik in het veld **Beheerserver** op **Wijzigen** om het adres van de Cyberbescherming-service en de referenties voor toegang op te geven.
   a. Selecteer in het veld **Servernaam/IP** de optie **Cloud** en geef vervolgens het Cyberbescherming-serviceadres op.
   b. Voer in de velden **Gebruikersnaam** en **Wachtwoord** de referenties in voor uw account in de Cyberbescherming-service.
   c. Klik op **OK**.
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 Cyberbescherming-serviceconsole.
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. Als u de opdrachtshell wilt starten, drukt u op CTRL+SHIFT+F2 in de gebruikersinterface van de virtuele toepassing.
   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 `ADRES` door de nieuwe waarden voor de hostnaam/het IP-adres van de proxyserver en vervang `POORT` door de decimale waarde van het poortnummer.
   e. Als uw proxyserver verificatie vereist, vervangt u `GEBRUIKERSNAAM` en `WACHTWOORD` 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 automatische of handmatige updates wilt uitvoeren van een virtuele toepassing die zich achter een proxy bevindt, moet u de proxyserver in de toepassing als volgt configureren.

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
```

Virtuele machines in het Red Hat Virtualization/oVirt-datacenter beschermen

1. Meld u aan bij uw Cyberbescherming-account.
2. Ga naar **Apparaten** > **oVirt** > <uw cluster> of zoek uw machines in **Apparaten** > **Alle apparaten**.
3. Selecteer de gewenste machines en pas een beschermingsschema toe op deze machines.

8.13.4 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

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4

- 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.

8.14 Agenten implementeren via Groepsbeleid

U kunt 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.

8.14.1 Vereisten

Voordat u de agent implementeert, moet u zorgen voor het volgende:

- U hebt een Active Directory-domein met een domeincontroller waarop Microsoft Windows Server 2003 of later wordt uitgevoerd.
- U bent lid van de groep **Domeinadministrators** in het domein.
- U hebt het installatieprogramma voor **Alle agenten voor Windows** gedownload. De downloadlink is beschikbaar op de pagina **Apparaten toevoegen** in de serviceconsole.

8.14.2 Stap 1: Een registratietoken genereren

Een registratietoken geeft de identiteit van een gebruiker door aan het installatieprogramma van de agent zonder de gebruikersreferenties voor de serviceconsole op te slaan. Hierdoor kunnen gebruikers een willekeurig aantal machines registreren voor hun account zonder dat ze zich hoeven aan te melden. Om veiligheidsredenen hebben tokens een beperkte levensduur, maar u kunt deze aanpassen. De standaardperiode is 3 dagen.

Een registratietoken genereren voor uw account

1. Meld u aan bij de serviceconsole.
2. Klik op **Apparaten** > **Alle apparaten** > **Toevoegen**.
3. Blader omlaag naar **Registratietoken** en klik vervolgens op **Genereren**.

4. Geef de levensduur van het token op.
5. [Optioneel] Als u wilt dat de gebruiker van het token een beschermingsschema kan toepassen en intrekken op de toegevoegde machines, selecteert u het schema in de vervolgkeuzelijst.
6. Klik op **Token genereren**.
7. Kopieer het token of noteer het.
   Sla het token op als u het nodig hebt voor later gebruik.

U kunt klikken op **Actieve tokens beheren** om de reeds gegenereerde tokens voor uw account te bekijken en te verwijderen.

Opmerking
In de tabel Actieve tokens worden om veiligheidsredenen niet de volledige tokenwaarden weergegeven.

Een registratietoken genereren namens een gebruiker in de tenants die u kunt beheren

1. Meld u als partner of klantbeheerder aan bij de serviceconsole.
   Als u al bent aangemeld bij de beheerconsole, klikt u op het tabblad **Cyber Protection** op **Service beheren** om naar de serviceconsole te navigeren.
2. Selecteer in de vervolgkeuzelijst linksboven de tenant met de gebruiker namens wie u een token wilt maken.
3. Klik onder **Apparaten** op **Alle apparaten** > **Toevoegen**.
   Het dialoogvenster Apparaten toevoegen wordt geopend aan de rechterkant.
4. Blader omlaag naar **Registratietoken** en klik vervolgens op **Genereren**.
5. Geef de levensduur van het token op.
6. Selecteer de gebruiker voor wie u een token wilt genereren.

   Opmerking
   Agenten die met het token zijn geregistreerd, worden geregistreerd onder het gebruikersaccount dat u hier selecteert.

7. [Optioneel] Als u wilt dat de gebruiker van het token een beschermingsschema kan toepassen en intrekken op de toegevoegde machines, selecteert u het schema in de vervolgkeuzelijst.
8. Klik op **Token genereren**.
9. Kopieer het token of noteer het.
   Sla het token op als u het nodig hebt voor later gebruik.

U kunt klikken op **Actieve tokens beheren** als u de reeds gegenereerde tokens wilt bekijken en verwijderen voor de gebruikers die u kunt beheren.

Opmerking
In de tabel Actieve tokens worden om veiligheidsredenen niet de volledige tokenwaarden weergegeven.

8.14.3 Stap 2: Het MST-transformatiebestand maken en het installatiepakket uitpakken

1. Meld u als beheerder aan bij een van de machines in het 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. Start het installatieprogramma.
4. Klik op **MST- en MSI-bestanden maken voor installatie zonder toezicht**.
5. Klik op **Opgeven** naast **Registratie-instellingen** en voer vervolgens het token in dat u hebt gegenereerd.
   U kunt de methode voor registratie van de machine in de Cyberbescherming-service wijzigen van **Registratietoken gebruiken** (standaard) in **Referenties gebruiken** of **Registratie overslaan**. Als u **Registratie overslaan** kiest, wordt ervan uitgegaan dat u de machine later wilt registreren.
6. Controleer of wijzig de installatie-instellingen die aan het MST-bestand worden toegevoegd en klik vervolgens op **Doorgaan**.
7. Ga naar **De bestanden opslaan in** en geef het pad op naar de map die u hebt gemaakt.
8. Klik op **Genereren**.

Het MST-transformatiebestand wordt gegenereerd en de MSI- en CAB-installatiepakketten worden uitgepakt naar de map die u hebt gemaakt.

8.14.4 Stap 3: De groepsbeleidobjecten 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 de agent in een organisatie-eenheid wilt implementeren, moet u ervoor zorgen dat de organisatie-eenheid bestaat in het domein. Anders kunt u deze stap overslaan.
3. Wijs in het menu **Start** de optie **Systeembeheer** aan en klik vervolgens op **Active Directory: gebruikers en computers** (in Windows Server 2003) of op **Groepsbeleidsbeheer** (in Windows Server 2008 of later).
4. In 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**.

   In 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. Geef **Agent voor Windows** als naam van het nieuwe groepsbeleidobject.

6. Ga als volgt te werk om het groepsbeleidobject **Agent voor Windows** te openen en te bewerken:
   - Klik in Windows Server 2003 op het groepsbeleidobject en klik vervolgens op **Bewerken**.
   - Klik in Windows Server 2008 of later in het gedeelte **Groepsbeleidobjecten** met de rechtermuisknop op het groepsbeleidobject en klik vervolgens op **Bewerken**.
7. Vouw in de module Groepsbeleidobjecteditor de optie **Computerconfiguratie** uit.
8. In Windows Server 2003 en Windows Server 2008:
   - Vouw **Software-instellingen** uit.

   In Windows Server 2012 of later:
   - Vouw **Beleidsregels** > **Software-instellingen** uit.
9. Klik met de rechtermuisknop op **Software-installatie**, wijs **Nieuw** aan en klik vervolgens op **Pakket**.
10. Selecteer het MSI-installatiepakket van de agent in de gedeelde map die u eerder hebt gemaakt en klik vervolgens op **Openen**.
11. Klik in het dialoogvenster **Software distribueren** op **Geavanceerd** en klik vervolgens op **OK**.
12. Klik op het tabblad **Wijzigingen** op **Toevoegen** en selecteer vervolgens het eerder gemaakte MST-transformatiebestand.
13. Klik op **OK** om het dialoogvenster **Software distribueren** te sluiten.

8.15 Agenten bijwerken

U kunt alle agenten handmatig bijwerken.

U kunt automatische updates configureren voor de volgende agenten:

- Agent voor Windows
- Agent voor Linux
- Agent voor Mac

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
```

8.15.1 Agenten handmatig bijwerken

U kunt agenten bijwerken via de serviceconsole of door het installatiebestand te downloaden en uit te voeren.

Virtuele toepassingen met de volgende versies kunnen alleen worden bijgewerkt met de serviceconsole:

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

Agenten met de volgende versies kunnen ook worden bijgewerkt met de serviceconsole:

- Agent voor Windows, Agent voor VMware (Windows), Agent voor Hyper-V: versie 11.9.191 en later.
- Agent voor Linux: versie 11.9.179 en later.
- Andere agenten: elke versie kan worden bijgewerkt.

Als u de versie van de agent wilt vinden, selecteert u de machine in de serviceconsole 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 serviceconsole

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 rol Updater 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.

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**.

8.15.2 Agenten 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. Cyberbescherming-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 serviceconsole naar **Instellingen** > **Agenten**.
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 serviceconsole naar **Instellingen** > **Agenten**.
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 serviceconsole naar **Instellingen** > **Agenten**.
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**.

8.16 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.

8.17 Agenten verwijderen

8.17.1 In Windows

Als u afzonderlijke productonderdelen wilt verwijderen (bijvoorbeeld een van de agenten of Cyber Protection Monitor), voert u het installatieprogramma **Alle agenten voor Windows** uit, kiest u de optie om het product te wijzigen en deselecteert u de onderdelen die u wilt verwijderen. De link naar het installatieprogramma vindt u op de pagina **Downloads** (klik op het accountpictogram in de rechterbovenhoek > **Downloads**).

Als u alle productonderdelen van een machine wilt verwijderen, voert u de volgende stappen uit.

1. Meld u aan als beheerder.
2. Ga naar **Configuratiescherm** en selecteer **Programma's en onderdelen** (**Software** in Windows XP) > **Acronis Cyberbescherming Agent** > **Verwijderen**.
3. [Voor een met een wachtwoord beveiligde agent] Geef het wachtwoord op dat u nodig hebt om de agent te verwijderen en klik vervolgens op **Volgende**.
4. [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, wordt de machine mogelijk gedupliceerd in de serviceconsole en de back-ups van de oude machine worden dan mogelijk niet gekoppeld aan de nieuwe machine.
5. Klik op **Verwijderen**.

8.17.2 In Linux

1. 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, wordt de machine mogelijk gedupliceerd in de serviceconsole en de back-ups van de oude machine worden dan mogelijk niet gekoppeld aan de nieuwe machine.
3. Bevestig uw beslissing.

8.17.3 In macOS

1. Dubbelklik op het installatiebestand (.dmg).
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.

8.17.4 Agent voor VMware (Virtual Appliance) verwijderen

1. Start vSphere Client en meld u aan bij vCenter Server.
2. Als de virtuele toepassing (VA) is ingeschakeld, klikt u erop met de rechtermuisknop en klikt u vervolgens op **Aan/uit** > **Uitschakelen**. Bevestig uw beslissing.
3. Als de virtuele toepassing gebruikmaakt van lokaal gekoppelde opslag op een virtuele schijf en u de gegevens op die schijf wilt behouden, gaat u als volgt te werk:
   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**. Klik onder **Opties voor verwijderen** op **Verwijderen van virtuele machine**.
   c. 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 van plan bent de agent opnieuw te installeren, slaat u deze stap over. Klik anders in de serviceconsole op **Back-upopslag** > **Locaties** en verwijder vervolgens de locatie die overeenkomt met de lokaal gekoppelde opslag.

8.17.5 Machines verwijderen uit de serviceconsole

Wanneer u een agent hebt verwijderd, wordt de registratie van de agent bij de Cyberbescherming-service ongedaan gemaakt en de machine waarop de agent was geïnstalleerd, wordt automatisch verwijderd uit de serviceconsole.

Als tijdens deze bewerking de verbinding met de service verloren gaat, bijvoorbeeld door een netwerkprobleem, kan de agent worden verwijderd, maar de betreffende machine wordt mogelijk nog steeds weergegeven in de serviceconsole. In dit geval moet u de machine handmatig verwijderen uit de serviceconsole.

Een machine handmatig verwijderen uit de serviceconsole

1. Meld u als beheerder aan bij de Cyberbescherming-service.
2. Ga in de serviceconsole naar **Instellingen** > **Agenten**.

3. Selecteer de machine waar de agent is geïnstalleerd.
4. Klik op **Verwijderen**.

8.18 Beveiligingsinstellingen

Als u de algemene beveiligingsinstellingen voor Cyberbescherming wilt configureren, gaat u in de serviceconsole naar **Instellingen** > **Beveiliging**.

8.18.1 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.

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 (publiek, 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 serviceconsole naar **Instellingen** > **Agenten**.
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.

8.18.2 De Cyberbescherming-definities bijwerken volgens een schema

Op het tabblad **Schema** kunt u het schema instellen voor automatische update van de Cyberbescherming-definities voor elk van de volgende onderdelen:

- Antimalware
- Evaluatie van beveiligingsproblemen
- Patchbeheer

U kunt de instelling van de definitie-updates wijzigen via **Instellingen** > **Beveiliging** > **Update van beveiligingsdefinities** > **Schema**.

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.

8.18.3 De Cyberbescherming-definities op aanvraag bijwerken

De Cyberbescherming-definities op aanvraag bijwerken voor een bepaalde machine

1. Ga in de serviceconsole naar **Instellingen** > **Agenten**.
2. Selecteer de machines waarop u de beveiligingsdefinities wilt bijwerken en klik vervolgens op **Definities bijwerken**.

8.18.4 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** > **Beveiliging** > **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.

8.18.5 Externe verbinding

De externe verbinding met machines inschakelen via RDP- of HTML-client

1. Ga in de serviceconsole naar **Instellingen** > **Beveiliging**.
2. Klik op **Verbinding met extern bureaublad** en schakel vervolgens de optie **Verbinding met extern bureaublad** in.
   Als deze schakelaar is uitgeschakeld, worden de opties **Verbinden via RDP-client** / **Verbinden via HTML5-client** verborgen in de serviceconsole en kunnen gebruikers niet op afstand verbinding maken met machines. Deze optie is van invloed op alle gebruikers van uw organisatie.

Het delen van de externe verbinding inschakelen

1. Ga in de serviceconsole naar **Instellingen** > **Beveiliging**.
2. Schakel het selectievakje **Verbinding met extern bureaublad delen** in.

Hierdoor wordt de optie **Externe verbinding delen** weergegeven onder **Cyberbescherming-bureaublad** in het rechtermenu. Het rechtermenu wordt geopend wanneer u een machine selecteert op het tabblad **Apparaten**.

Als u op **Verbinding op afstand delen** klikt, genereert u een link die u met andere gebruikers kunt delen. Via deze link kunt u op afstand toegang krijgen tot de geselecteerde machine.

8.19 De servicequota van machines wijzigen

De servicequota wordt automatisch toegewezen wanneer een beschermingsschema voor het eerst wordt toegepast op een machine.

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 quota's aanschaft die meer geschikt zijn. Er wordt bijvoorbeeld een quota voor **werkstations** toegewezen aan een virtuele machine. Na aankoop van een quota voor **Virtuele machines** kunt u

deze handmatig toewijzen aan deze machine. U kunt ook de momenteel toegewezen servicequota vrijgeven en vervolgens toewijzen aan een andere machine.

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 Protection-serviceconsole naar **Apparaten**.
2. Selecteer de gewenste machine en klik op **Details**.
3. Klik in het gedeelte **Servicequota** op **Wijzigen**.
4. Open het venster **Licentie 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 Protection-serviceconsole naar **Apparaten**.
2. Selecteer meer dan één machine en klik vervolgens op **Quota toewijzen**.
3. Open het venster **Licentie wijzigen**, selecteer de gewenste servicequota of **Geen quota** en klik vervolgens op **Wijzigen**.

8.20 Cyberbescherming-services geïnstalleerd in uw omgeving

Cyberbescherming installeert enkele of alle van de volgende services, afhankelijk van de Cyberbescherming-opties die u gebruikt.

8.20.1 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

8.20.2 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-`	Zorgt voor de detectie van malware

`service.plist`	
`/Library/LaunchDaemons/com.acronis.mms.plist`	Biedt back-up- en herstelfuncties
`/Library/LaunchDaemons/com.acronis.schedule.plist`	Voert geplande taken uit

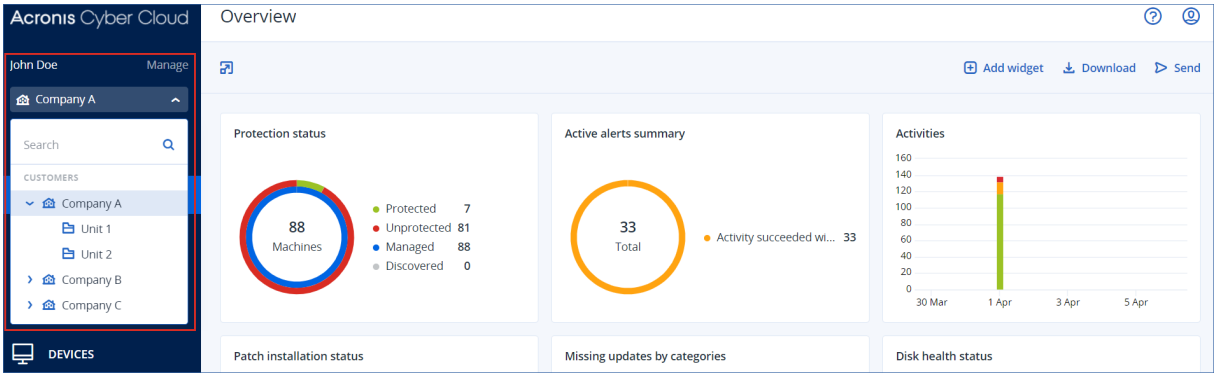
9 Serviceconsole

In de serviceconsole kunt u apparaten en beschermingsschema's beheren, de beveiligingsinstellingen wijzigen, rapporten configureren en de back-upopslag controleren.

Op het dashboard vindt u de belangrijkste informatie over uw bescherming.

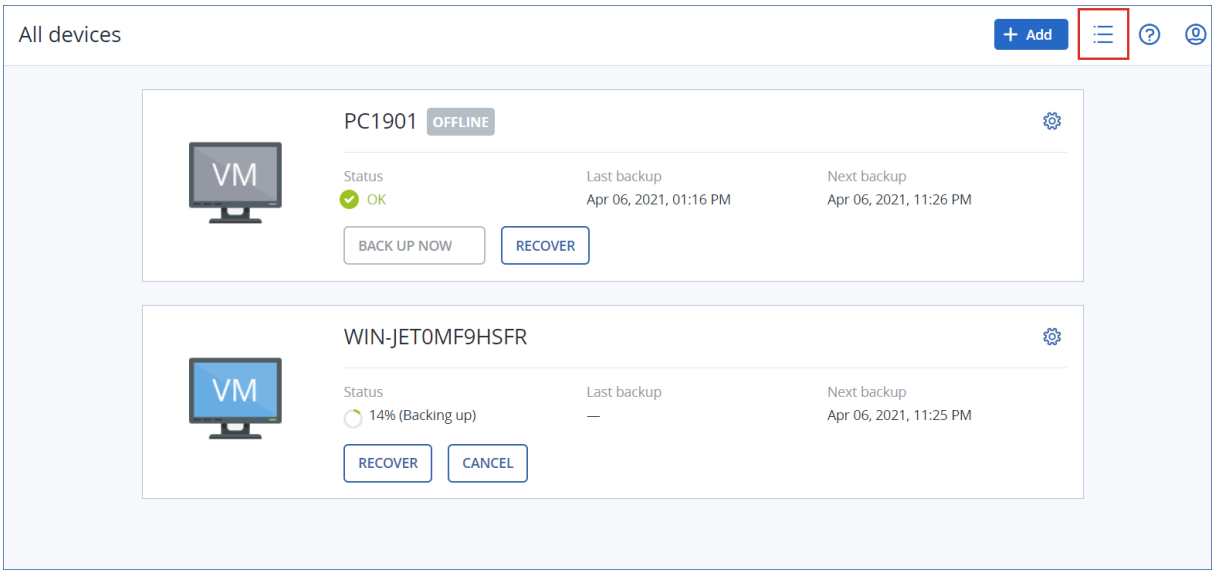
Via de serviceconsole hebt u ook toegang tot extra services en functies van Cyberbescherming, zoals File Sync & Share, Antivirus- en antimalwarebeveiliging, Patchbeheer, Apparaatbeheer en Evaluatie van beveiligingsproblemen. Het type en het aantal kunnen variëren, afhankelijk van uw Cyberbescherming-licentie.

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.

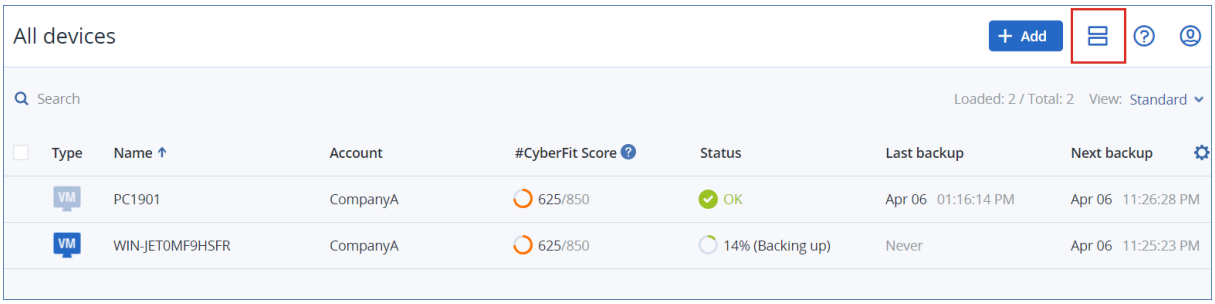


Het gedeelte **Apparaten** is beschikbaar in eenvoudige en tabelweergave. U kunt tussen de weergaven schakelen door te klikken op het betreffende pictogram in de rechterbovenhoek.

De eenvoudige weergave wordt gebruikt als er slechts enkele machines zijn.



De tabelweergave wordt automatisch ingeschakeld wanneer er een groot aantal machines is.



Beide weergaven bieden toegang tot dezelfde functies en bewerkingen. In dit document wordt beschreven hoe u de bewerkingen uitvoert vanuit de tabelweergave.

Een machine verwijderen uit de serviceconsole

1. Schakel het selectievakje naast de gewenste machine in.
2. Klik op **Verwijderen** en bevestig uw keuze.

Belangrijk
Wanneer u een machine verwijdert uit de serviceconsole, worden de beveiligingsagent en de op deze machine toegepaste beschermingsschema's niet verwijderd. De back-ups van de verwijderde machine worden ook bewaard.

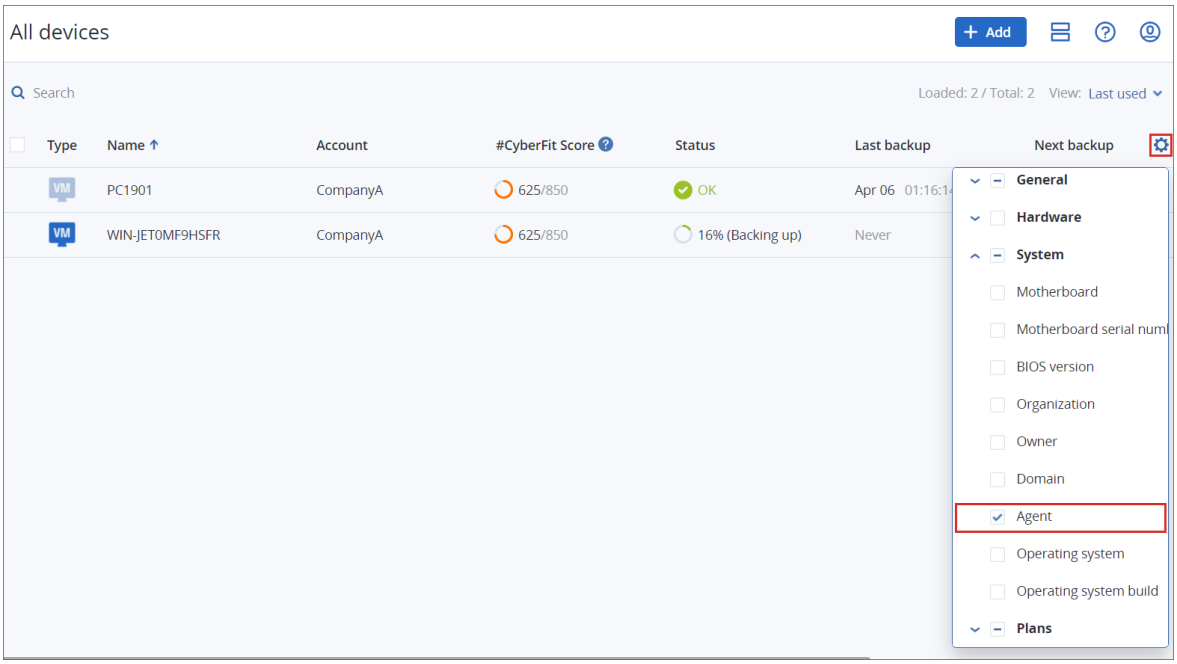
Op de volgende virtualisatieplatforms kunnen back-ups worden gemaakt van ESXi-hosts en virtuele machines door een agent die niet hierop is geïnstalleerd, d.w.z. in de modus zonder agent:

- Hyper-V
- VMware
- Virtuozzo Hybrid Infrastructure
- Scale Computing
- Red Hat Virtualization/oVirt

U kunt dergelijke machines niet afzonderlijk verwijderen. Als u ze wilt verwijderen, moet u de machine zoeken waarop de betreffende agent (Agent voor Hyper-V, Agent voor VMware, Agent voor Virtuozzo Hybrid Infrastructure, Agent voor Scale Computing of Agent voor oVirt) is geïnstalleerd, en moet u deze machine verwijderen.

Een virtuele machine of ESXi-host verwijderen zonder een agent

1. Selecteer onder **Apparaten** de optie **Alle apparaten**.
2. Klik op het tandwielpictogram in de rechterbovenhoek en schakel de kolom **Agent** in.



3. Controleer in de kolom **Agent** de naam van de machine waarop de betreffende agent is geïnstalleerd.
4. Verwijder deze machine uit de serviceconsole. Hiermee worden ook alle machines verwijderd waarvan een back-up is gemaakt door de agent.
5. Verwijder de agent uit de verwijderde machine, zoals beschreven in "Agenten verwijderen" (p. 125).

10 Apparaatgroepen

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Apparaatgroepen zijn bedoeld om het beheer van een groot aantal geregistreerde apparaten te vergemakkelijken.

U kunt een beschermingsschema toepassen op een groep. Zodra een nieuw apparaat wordt weergegeven in de groep, wordt het apparaat beschermd via het schema. Als een apparaat uit de groep wordt verwijderd, is het apparaat niet langer beschermd via het schema. Een schema dat wordt toegepast op een groep kan niet worden ingetrokken vanuit een lid van de groep, alleen vanuit de groep zelf.

Alleen apparaten van hetzelfde type kunnen aan een groep worden toegevoegd. Zo kunt u bijvoorbeeld onder **Hyper-V** een groep van Hyper-V virtuele machines maken. Onder **Machines met agenten** kunt u een groep machines met geïnstalleerde agenten maken. Onder **Alle Apparaten** kunt u geen groep maken.

Een enkel apparaat kan lid zijn van meer dan één groep.

10.1 Ingebouwde groepen

Wanneer een apparaat is geregistreerd, wordt het weergegeven in een van de ingebouwde rootgroepen op het tabblad **Apparaten**.

Rootgroepen kunnen niet worden bewerkt of verwijderd. U kunt geen schema's toepassen op rootgroepen.

Sommige rootgroepen bevatten ingebouwde subrootgroepen. Deze groepen kunnen niet worden bewerkt of verwijderd. U kunt echter wel schema's toepassen op ingebouwde subrootgroepen.

10.2 Aangepaste groepen

Bescherming van alle apparaten in een ingebouwde groep met een enkel beschermingsschema is mogelijk niet adequaat vanwege de verschillende rollen van de machines. Per afdeling verschillen de gegevens waarvan een back-up wordt gemaakt; van bepaalde gegevens moet veelvuldig een back-up worden gemaakt, terwijl dat voor andere gegevens maar tweemaal per jaar gebeurt. Daarom wilt u wellicht liever verschillende beschermingsschema's maken voor toepassing op verschillende reeksen machines. In dat geval kunt u overwegen aangepaste groepen te maken.

Een aangepaste groep kan een of meer geneste groepen bevatten. Elke aangepaste groep kan worden bewerkt of verwijderd. De volgende typen aangepaste groepen zijn beschikbaar:

- **Statische groepen**

  Statische groepen bevatten de machines die hieraan handmatig zijn toegevoegd. De inhoud van statische groepen verandert alleen als u expliciet een machine toevoegt of verwijdert.

  Voorbeeld: U kunt een aangepaste groep maken voor de boekhoudafdeling en handmatig de machines van de boekhouder toevoegen aan deze groep. Wanneer u een beschermingsschema toepast op de groep, worden de machines van de boekhouder beschermd. Als een nieuwe boekhouder in dienst wordt genomen, moet u de nieuwe machine handmatig toevoegen aan de groep.
- **Dynamisch groepen**

  Dynamische groepen bevatten de machines die automatisch zijn toegevoegd op basis van de zoekcriteria die zijn opgegeven bij het maken van een groep. De inhoud van de dynamische groep verandert automatisch. Een machine blijft deel uitmaken van de groep zolang deze aan de opgegeven criteria voldoet.

  Voorbeeld 1: De hostnamen van de machines die deel uitmaken van de boekhoudafdeling bevatten het woord "boekhouding". U geeft de gedeeltelijke machinenaam op als criterium voor lidmaatschap van de groep en past een beschermingsschema toe op de groep. Als een nieuwe boekhouder in dienst wordt genomen, wordt de nieuwe machine toegevoegd aan de groep zodra deze is geregistreerd en daarmee is de machine automatisch beschermd.

  Voorbeeld 2: De boekhoudafdeling creëert een afzonderlijke Active Directory-organisatie-eenheid (OU). U geeft de organisatie-eenheid van de boekhouding op als criterium voor lidmaatschap van de groep en past een beschermingsschema toe op de groep. Als een nieuwe accountant in dienst wordt genomen, wordt de nieuwe machine aan de groep toegevoegd zodra deze is geregistreerd en aan de organisatie-eenheid is toegevoegd (ongeacht wat het eerst gebeurt) en daarmee is de machine automatisch beschermd.

10.3 Een statische groep maken

1. Klik op **Apparaten** en selecteer vervolgens de ingebouwde groep die de apparaten bevat waarvoor u een statische groep wilt maken.
2. Klik op het tandwielpictogram naast de groep waarin u een groep wilt maken.
3. Klik op **Nieuwe groep**.
4. Geef de groepsnaam op en klik vervolgens op **OK**.

   De nieuwe groep wordt weergegeven in de groepsstructuur.

10.4 Apparaten toevoegen aan statische groepen

1. Klik op **Apparaten** en selecteer vervolgens een of meer apparaten die u wilt toevoegen aan een groep.
2. Klik op **Toevoegen aan groep**.

   De software toont een structuur van groepen waaraan het geselecteerde apparaat kan worden toegevoegd.

3. Als u een nieuwe groep wilt maken, volgt u de volgende stappen. Anders kunt u deze stap overslaan.
   a. Selecteer de groep waarin u een groep wilt maken.
   b. Klik op **Nieuwe groep**.
   c. Geef de groepsnaam op en klik vervolgens op **OK**.
4. Selecteer de groep waaraan u het apparaat wilt toevoegen en klik vervolgens op **Gereed**.

U kunt apparaten ook toevoegen aan een statische groep door de groep te selecteren en te klikken op **Apparaten toevoegen**.

10.5 Een dynamische groep maken

1. Klik op **Apparaten** en selecteer vervolgens de groep die de apparaten bevat waarvoor u een dynamische groep wilt maken.

   Opmerking
   U kunt geen dynamische groepen maken voor de groep Alle apparaten.

2. Zoek naar apparaten met behulp van het zoekveld. U kunt meerdere zoekcriteria en operators gebruiken, zoals hieronder beschreven.
3. Klik op **Opslaan als** naast het zoekveld.

   Opmerking
   Sommige zoekcriteria worden niet ondersteund voor het maken van groepen. Zie de tabel in het gedeelte Zoekcriteria hieronder.

4. Geef de groepsnaam op en klik vervolgens op **OK**.

10.5.1 Zoekcriteria

De volgende tabel bevat een overzicht van de beschikbare zoekcriteria.

Criterium	Betekenis	Voorbeelden van query's zoeken	Ondersteund voor het maken van groepen
`naam`	• Hostnaam voor fysieke machines • Naam voor virtuele machines • Databasenaam • E-mailadres voor postvakken	`name = 'en-00'`	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
	Wanneer er handmatig tekst in het opmerkingenveld wordt toegevoegd, wordt de automatische synchronisatie met de Windows-beschrijving uitgeschakeld. Wis de opmerking die u hebt toegevoegd en schakel deze weer in.
	
	Als u de automatisch gesynchroniseerde opmerkingen voor uw apparaten wilt vernieuwen, start u de Managed Machine Service in **Windows-services** opnieuw op of voert u de volgende opdrachten uit op de opdrachtprompt:
	
	`net stop mms`
	
	`net start mms`
	
	Als u een opmerking over een apparaat wilt bekijken,
		`comment = 'important machine'`
		
		`comment = ''` (alle machines zonder een opmerking)
			Ja

	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.
	• 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 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**. **Opmerking** Wanneer er handmatig tekst in het opmerkingenveld wordt toegevoegd, wordt de automatische synchronisatie met de Windows-beschrijving uitgeschakeld. Wis de opmerking die u hebt toegevoegd en schakel deze weer in.		
`ip`	IP-adres (uitsluitend voor fysieke machines).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Ja
`memorySize`	RAM-grootte in megabytes	`memorySize < 1024`	Ja

	(MiB).		
`diskSize`	Grootte van de harde schijf in gigabytes of megabytes (alleen voor fysieke machines).	`diskSize < 300GB` `diskSize >= 3000000MB`	Nee
`insideVm`	Virtuele machine met een agent. Mogelijke waarden: • `true` • `false`	`insideVm = true`	Ja
`osName`	Naam van besturingssysteem.	`osName LIKE '%Windows XP%'`	Ja
`osType`	Type besturingssysteem. Mogelijke waarden: • `'windows'` • `'linux'` • `'macosx'`	`osType IN ('linux', 'macosx')`	Ja
`osProductType`	Het producttype van het besturingssysteem. Mogelijke waarden: • `'dc'` Staat voor Domeincontroller. **Opmerking** Wanneer de rol van de domeincontroller op een Windows-server wordt toegewezen, verandert osProductType van 'server' in 'dc'. Zulke machines worden niet opgenomen in de zoekresultaten voor het filter osProductType='server'. • `'server'` • `'workstation'`	`osProductType = 'server'`	Ja
`tenant`	De naam van de eenheid waarvan het apparaat deel	`tenant = 'Unit 1'`	Ja

	uitmaakt.		
`tenantId`	De id van de eenheid waarvan het apparaat deel uitmaakt. U kunt de eenheid-id opvragen door onder **Apparaten** het apparaat te selecteren en op **Details** > **Alle eigenschappen** te klikken. De id wordt weergegeven in het veld `ownerId`.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Ja
`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
`protectedByPlan`	Apparaten die worden beschermd door een beschermingsschema met een bepaalde id. U kunt de schema-id opvragen door op **Schema's** > **Back-up** te klikken, het schema te selecteren, op het diagram in de kolom **Status** te klikken en vervolgens op een status te	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nee

	klikken. 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 status **Interactie vereist** hebben.	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nee
`ou`	Machines die behoren tot de opgegeven Active Directory-organisatie-eenheid.	`ou IN ('RnD', 'Computers')`	Ja
`id`	Apparaat-id. U kunt de apparaat-id opvragen door onder **Apparaten** het apparaat te selecteren en op **Details** > **Alle eigenschappen** te klikken. De id wordt	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Ja

	weergegeven in het veld `id`.		

`lastBackupTime`*	De datum en tijd van de laatste geslaagde back-up.
	De notatie is `'JJJJ-MM-DD UU:MM'`.
		`lastBackupTime > '2020-03-11'`
		`lastBackupTime <= '2019-03-11 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 >= '2020-03-11'`	Nee
`nextBackupTime`*	Het tijdstip van de volgende back-up. De notatie is `'JJJJ-MM-DD UU:MM'`.	`nextBackupTime >= '2021-03-11'`	Nee
`agentVersion`	Versie van de geïnstalleerde beveiligingsagent.	`agentVersion LIKE '12.0.*'`	Ja
`hostId`	Interne id van de beveiligingsagent. U kunt de id van de beveiligingsagent opvragen door onder **Apparaten** de machine te selecteren en op **Details** > **Alle eigenschappen** te klikken. Gebruik de `'id'`-waarde van de `agent`-eigenschap.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Ja
`resourceType`	Resourcetype. Mogelijke waarden: • `'machine'` • `'virtual_machine.vmwesx'` • `'virtual_machine.mshyperv'` • `'virtual_machine.scale'` • `'virtual_machine.hci'` • `'virtual_machine.ovirt'` • `virtual_machine.pcs`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Ja

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 = 2020-02-20 betekent bijvoorbeeld dat de zoekresultaten alle back-ups bevatten van het interval tussen lastBackupTime> = 2020-02-20 00:00 en lastBackup time <= 2020-02-20 23:59:59

10.5.2 Operators

De volgende tabel bevat een overzicht van de beschikbare operators.

Operator	Betekenis	Voorbeelden
`AND`	Operator voor logische samenvoeging	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Operator voor logische scheiding	`state = 'backup' OR state = 'interactionRequired'`
`NOT`	Operator voor logische negatie	`NOT(osProductType = 'workstation')`

`LIKE 'wildcard pattern'`	Deze operator wordt gebruikt om te testen of een uitdrukking overeenkomt met het jokertekenpatroon. Deze operator is niet hoofdlettergevoelig.
	De volgende jokertekens kunnen worden gebruikt:
	• * 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*'`
		`name LIKE 'en-00_'`

`IN (<value1>,... <valueN>)`	Deze operator wordt gebruikt om te testen of een expressie overeenkomt met een waarde in een lijst met waarden. Deze operator is hoofdlettergevoelig.	`osType IN ('windows', 'linux')`
`RANGE (<starting_value>, <ending_value>)`	Deze operator wordt gebruikt om te testen of een expressie deel uitmaakt van een bereik van waarden (inbegrepen).	`ip RANGE ('10.250.176.1','10.250.176.50')`
`<`	Kleiner dan operator.	`memorySize < 1024`
`>`	Groter dan operator.	`diskSize > 300GB`
`<=`	Kleiner dan of gelijk aan operator.	`lastBackupTime <= '2019-03-11 00:15'`

>=	Groter dan of gelijk aan operator.	`nextBackupTime >= '2021-03-11'`
= or ==	Gelijk aan operator.	`osProductType = 'server'`
!= or <>	Niet gelijk aan operator.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`

10.6 Een beschermingsschema toepassen op een groep

1. Klik op **Apparaten** en selecteer vervolgens de ingebouwde groep met de groep waarop u een beschermingsschema wilt toepassen.

   De software geeft de lijst met kindergroepen weer.
2. Selecteer de groep waarop u een beschermingsschema wilt toepassen.
3. Klik op **Back-up van groep**.

   U ziet dan de lijst met Beschermingsschema's die kunnen worden toegepast op de groep.
4. Voer een van de volgende handelingen uit:
   - Vouw een bestaand beschermingsschema uit en klik vervolgens op **Toepassen**.
   - Klik op **Nieuw maken** en maak vervolgens een nieuw beschermingsschema zoals beschreven in 'Beschermingsschema'.

11 Ondersteuning voor meerdere tenants

Cyberbescherming biedt ondersteuning voor meerdere tenants. Dit betekent dat een tenantbeheerder/-gebruiker objecten kan beheren die zijn gerelateerd aan de eigen tenant of sub-tenants (eenheden). Een beheerder/gebruiker van een eenheid kan geen objecten van de bovenliggende tenant beheren.

Een klantbeheerder heeft bijvoorbeeld een beschermingsschema gemaakt en toegepast op een machine. Een klantbeheerder kan ook beschermingsschema's beheren die zijn gemaakt door een eenheidbeheerder. Een eenheidbeheerder kan echter niet het beschermingsschema beheren dat door de klantbeheerder is gemaakt. Een eenheidbeheerder kan een eigen beschermingsschema maken als dit niet conflicteert met het schema van de klantbeheerder.

Meerdere tenants houdt ook in dat een tenantbeheerder/-gebruiker alle objecten kan zien die zijn gerelateerd aan de eigen tenant of sub-tenants (eenheden). Een beheerder/gebruiker van een eenheid kan geen objecten van de bovenliggende tenant zien.

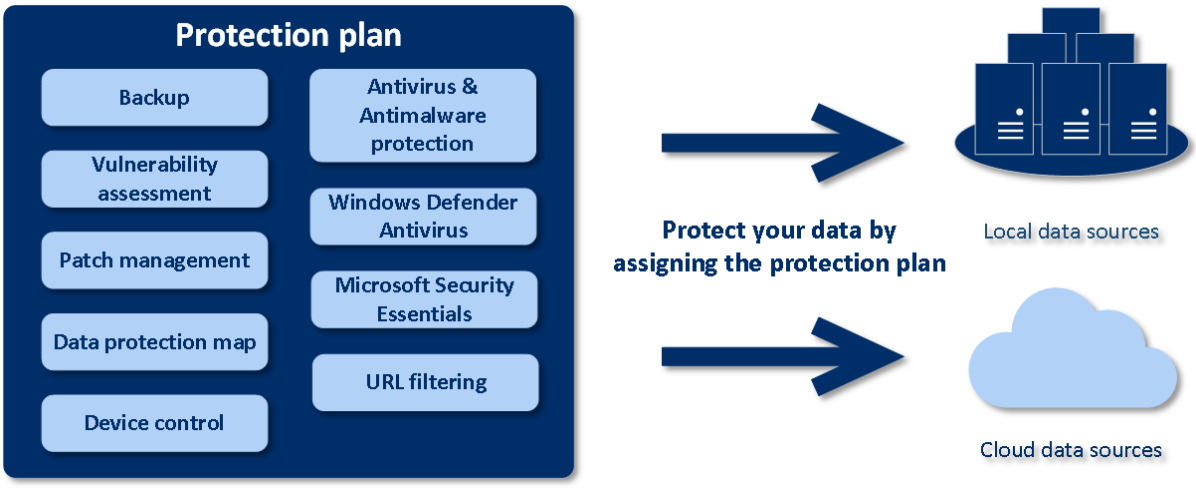
De gegevens van de patchlijst, quarantaine, bedreigingsfeed, waarschuwingen en activiteiten worden bijvoorbeeld alleen weergegeven voor de huidige tenants en sub-tenants. De gegevens over de bovenliggende tenant worden niet weergegeven.

12 Beschermingsschema en modules

Het beschermingsschema is een schema dat verschillende gegevensbeschermingsmodules combineert, waaronder

- Back-up: hiermee kunt u een back-up van uw gegevensbronnen maken naar een lokale of cloudopslag.
- "Noodherstel" (p. 407): hiermee kunt u exacte kopieën van uw machines op de cloudsite starten en de workload van de beschadigde oorspronkelijke machines verplaatsen naar de herstelservers in de cloud.
- Antivirus- en antimalwarebeveiliging: hiermee kunt u uw machines controleren met de ingebouwde antimalwareoplossing.
- URL-filtering: hiermee kunt u uw machines beschermen tegen bedreigingen via internet door de toegang tot schadelijke URL's en downloads van schadelijke inhoud te blokkeren.
- Windows Defender Antivirus: hiermee kunt u de instellingen van Windows Defender Antivirus beheren om uw omgeving te beschermen.
- Microsoft Security Essentials - hiermee kunt u de instellingen van Microsoft Security Essentials beheren om uw omgeving te beschermen.
- Evaluatie van beveiligingsproblemen: hiermee wordt automatisch gecontroleerd op beveiligingsproblemen met de producten van Microsoft, Linux, macOS en de producten van derden voor Microsoft en macOS die op uw machines zijn geïnstalleerd, en er worden waarschuwingen hierover gegenereerd.
- Patchbeheer: hiermee kunt u patches en updates voor de producten van Microsoft en van derden op uw machines installeren om de ontdekte beveiligingsproblemen te verhelpen.
- Overzicht van gegevensbescherming: hiermee kunt u de gegevens detecteren om de beveiligingsstatus van belangrijke bestanden te controleren.
- Apparaatbeheer: Hiermee kunt u apparaten opgeven die gebruikers op uw machines mogen gebruiken of waarvoor beperkingen gelden.

Gebruik het beschermingsschema om uw gegevensbronnen volledig te beschermen tegen externe en interne bedreigingen. Door verschillende modules in en uit te schakelen en de module-instellingen te configureren kunt u flexibele schema's maken die voldoen aan diverse bedrijfsbehoeften.



12.1 Een beschermingsschema maken

Een beschermingsschema kan worden toegepast op meerdere machines wanneer u het schema aanmaakt of later. Wanneer u een schema maakt, worden het besturingssysteem en het apparaattype (bijvoorbeeld werkstation, virtuele machine, enzovoort) gecontroleerd. Alleen de schemamodules die van toepassing zijn op uw apparaten, worden weergegeven.

Een beschermingsschema kunt u als volgt maken.

- In het gedeelte **Apparaten**: u selecteert het apparaat of de apparaten die u wilt beschermen en maakt hier vervolgens een plan voor.
- In het gedeelte **Schema's**: u maakt een schema en selecteert vervolgens de machines waarop u het wilt toepassen.

Het eerste beschermingsschema maken in het gedeelte Apparaten

1. Ga in de serviceconsole 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. [Optioneel] Klik op het potloodpictogram naast de naam om de naam van het beschermingsschema te wijzigen.
5. [Optioneel] Klik op de optie naast de modulenaam om de schemamodule in of uit te schakelen.
6. [Optioneel] Als u de parameters van de module wilt wijzigen, klikt u op het desbetreffende gedeelte van het beschermingsschema.
7. Wanneer u klaar bent, klikt u op **Maken**.

De modules Back-up, Antivirus- en antimalwarebeveiliging, Evaluatie van beveiligingsproblemen, Patchbeheer en Overzicht van gegevensbescherming kunnen op aanvraag worden uitgevoerd door te klikken op **Nu uitvoeren**.

Bekijk de instructievideo Het eerste beschermingsplan maken.

Zie "Een beschermingsschema voor noodherstel maken" (p. 410) voor meer informatie over de module Noodherstel.

Zie "Apparaatbesturing" (p. 560) voor meer informatie over de Apparaatbeheermodule.

12.2 Standaardbeschermingsschema's

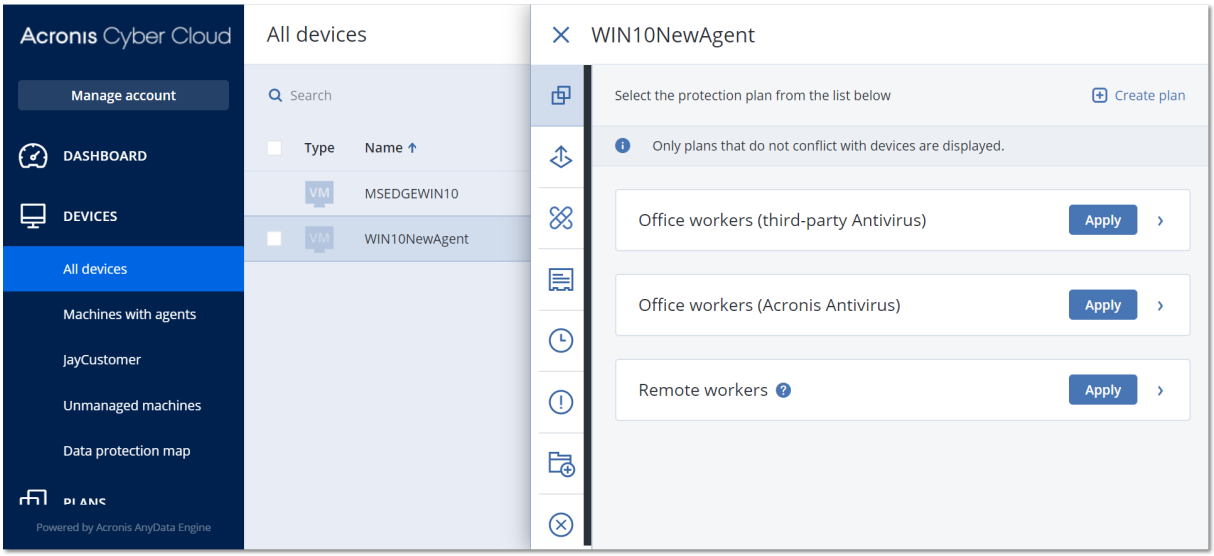
U kunt drie vooraf geconfigureerde schema's, die standaard beschikbaar zijn, gebruiken voor snelle bescherming van specifieke workloads:

- Medewerkers op kantoor (Acronis Antivirus)

  Dit schema is geoptimaliseerd voor gebruikers die op kantoor werken en bij voorkeur werken met de Acronis-antivirussoftware.
- Medewerkers op kantoor (antivirus van derden)

  Dit plan is geoptimaliseerd voor gebruikers die op kantoor werken en bij voorkeur werken met antivirussoftware van derden. Het belangrijkste verschil is dat in dit schema de module **Antivirus- en antimalwarebeveiliging** en **Active Protection** zijn uitgeschakeld.
- Medewerkers op afstand

  Dit schema is speciaal geoptimaliseerd voor gebruikers die op afstand werken. Het heeft frequentere taken (zoals back-up, antimalwarebeveiliging, evaluatie van beveiligingsproblemen), strengere beschermingsacties en geoptimaliseerde prestatie- en energieopties.



Een standaardbeschermingsschema toepassen

1. Ga in de serviceconsole naar **Apparaten** > **Alle apparaten**.
2. Selecteer de machines die u wilt beschermen.
3. Klik op **Beschermen**.
4. Selecteer een van de standaardschema's en klik vervolgens op **Toepassen**.

Opmerking
U kunt ook uw eigen beschermingsschema configureren door te klikken op **Schema maken**.

Een toegepast standaardbeschermingsschema wijzigen

1. Ga in de serviceconsole naar **Schema's** > **Bescherming**.
2. Selecteer het schema dat u wilt wijzigen en klik vervolgens op **Bewerken**.
3. Wijzig de modules of moduleopties van dit schema en klik op **Opslaan**.

Belangrijk
Sommige instellingen kunnen niet worden gewijzigd voor een bestaand beschermingsschema.

12.2.1 Standaardopties voor het schema

Voor de vooraf geconfigureerde schema's worden de standaardopties voor elke module* gebruikt, met de volgende wijzigingen:

Modules en opties/schema	Medewerkers op kantoor (Acronis Antivirus)	Medewerkers op kantoor (antivirus van derden)	Medewerkers op afstand
"Back-up" (p. 165)			
BACK-UP VAN	Volledige machine	Volledige machine	Volledige machine
Continue gegevensbescherming (CDP)	Uitgeschakeld	Uitgeschakeld	Ingeschakeld
Waar back-up maken	Cloudopslag	Cloudopslag	Cloudopslag
Back-upschema	Altijd incrementeel (één bestand)	Altijd incrementeel (één bestand)	Altijd incrementeel (één bestand)
Planning	Dagelijks schema, standaard	Dagelijks schema, standaard	Dagelijks: 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 besparen: Niet starten bij gebruik van batterijstroom • Niet starten bij verbinding met een datalimiet
Bewaartijd	Maandelijks: 12 maanden Wekelijks: 4 weken Dagelijks: 7 dagen	Maandelijks: 12 maanden Wekelijks: 4 weken Dagelijks: 7 dagen	Maandelijks: 12 maanden Wekelijks: 4 weken Dagelijks: 7 dagen
Back-upopties	Standaardopties	Standaardopties	Standaardopties, plus: Prestatie- en back-upvenster (de groene set): • CPU-prioriteit: Laag • Uitvoersnelheid: 50%
"Antivirus- en antimalwarebeveiliging" (p. 475)			
Scan plannen	Type scan: Snel	N.v.t.	Type scan: Volledig 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
"URL-filtering" (p. 493)			
Toegang via schadelijke websites	Altijd vragen aan gebruiker	Altijd vragen aan gebruiker	Blokkeren
"Evaluatie van beveiligingsproblemen" (p. 513)			
	Standaard	Standaard	Standaard
"Patchbeheer" (p. 521)			
Planning	Standaard	Standaard	Dagelijks: Maandag t/m vrijdag om 14:20 uur

Back-up vóór update	Uit	Uit	Aan
"Overzicht van gegevensbescherming" (p. 553)			
Extensies	Standaardopties	Standaardopties	Standaardopties, plus: **Afbeeldingen:** • .bmp • .png • .ico • .wbmp • .gif • .bmp • .xcf • .psd • .tiff • .jpeg, .jpg • .dwg **Audio:** • .wav • .aif, .aifc, .aiff • .au, .snd • .mid, .midi • .mid • .mpga, .mp3 • .oga • .flac • .oga • .oga • .opus • .oga • .spx • .oga • .ogg • .ogx • .ogx • .mp4
"Apparaatbesturing" (p. 560)			
Apparaatbesturing	Uitgeschakeld	Uitgeschakeld	Uitgeschakeld

*Het aantal modules in het standaardbeschermingsschema kan verschillen al naargelang de editie van de Cyberbescherming-service.

12.3 Conflicten tussen schema's oplossen

Een beschermingsschema kan de volgende statussen hebben:

- **Actief**: een schema dat wordt toegewezen aan apparaten en dat wordt uitgevoerd op die apparaten.
- **Inactief**: een schema dat is toegewezen aan apparaten maar is uitgeschakeld en dus niet op die apparaten wordt uitgevoerd.

12.3.1 Meerdere schema's toepassen op een apparaat

U kunt meerdere beschermingsschema's toepassen op één apparaat. Hierdoor wordt een combinatie van verschillende beschermingsschema's toegewezen op één apparaat. U kunt bijvoorbeeld een schema toepassen waarbij alleen de module Antivirus- en antimalwarebeveiliging is ingeschakeld in het schema, en een ander schema dat alleen de back-upmodule bevat. De beschermingsschema's kunnen alleen worden gecombineerd als ze geen modules delen. Als er vergelijkbare modules zijn ingeschakeld in de toegepaste beschermingsschema's, moet u conflicten tussen dergelijke modules oplossen.

12.3.2 Conflicten tussen schema's oplossen

Er zijn conflicten met reeds toegepaste schema's

Wanneer u een nieuw schema maakt op een apparaat of apparaten met reeds toegepaste schema's die conflicteren met het nieuwe schema, dan kunt u het conflict op een van de volgende manieren oplossen:

- Maak een nieuw schema, pas het toe en schakel alle reeds toegepaste conflicterende schema's uit.
- Maak een nieuw schema en schakel het uit.

Wanneer u een schema bewerkt op een apparaat of apparaten met al eerder toegepaste schema's die conflicteren met de door u gemaakte wijzigingen, dan kunt u het conflict op een van de volgende manieren oplossen:

- Sla wijzigingen in het schema op en schakel alle reeds toegepaste conflicterende schema's uit.
- Sla wijzigingen in het schema op en schakel het uit.

Een apparaatschema conflicteert met een groepsschema

Als een apparaat is opgenomen in een groep apparaten met een toegewezen groepsschema en u probeert een nieuw schema aan een apparaat toe te wijzen dat hiermee conflicteert, dan wordt u gevraagd om het conflict op te lossen op een van de volgende manieren:

- Verwijder een apparaat uit de groep en pas een nieuw schema toe op het apparaat.
- Pas een nieuw schema toe op de hele groep of bewerk het huidige groepsschema.

Licentieprobleem

De toegewezen quota op een apparaat moet geschikt zijn voor het uitvoeren, bijwerken of toepassen van het beschermingsschema. Voer een van de volgende handelingen uit om het licentieprobleem op te lossen:

- Schakel de modules uit die niet worden ondersteund door de toegewezen quota en blijf het beschermingsschema gebruiken.
- Wijzig de toegewezen quota handmatig: ga naar **Apparaten** > **<specifiek_apparaat>** > **Details** > **Servicequota**, trek de bestaande quota in en wijs een nieuwe quota toe.

12.4 Bewerkingen met beschermingsschema's

Beschikbare acties voor een beschermingsschema

U kunt de volgende acties uitvoeren voor een beschermingsschema:

- Naam van een schema wijzigen.
- Modules in-/uitschakelen en alle module-instellingen bewerken.
- Een schema in-/uitschakelen.

  Een uitgeschakeld schema wordt niet uitgevoerd op het apparaat waarop het wordt toegepast.

  Deze actie is handig voor beheerders die van plan zijn om hetzelfde apparaat later met hetzelfde schema te beschermen. Het schema wordt niet ingetrokken van het apparaat en u hoeft het schema alleen maar opnieuw in te schakelen om de bescherming te herstellen.
- Een schema toepassen op een apparaat of groep apparaten.
- Een schema intrekken van een apparaat.

  Een ingetrokken schema wordt niet meer toegepast op een apparaat.

  Deze actie is handig voor beheerders als hetzelfde apparaat niet snel opnieuw hoeft te worden beschermd met hetzelfde schema. Als u de bescherming van een ingetrokken schema wilt herstellen, moet u de naam van dit schema kennen, het schema selecteren in de lijst met beschikbare schema's en het schema vervolgens opnieuw toepassen op het gewenste apparaat.
- Een schema importeren/exporteren.

  Opmerking
  U kunt beschermingsschema's importeren die zijn gemaakt in Cyberbescherming 9.0 (uitgebracht in maart 2020) en later. Schema's gemaakt in eerdere productversies zijn niet compatibel met versie 9.0 en later.
- Een schema verwijderen.

Een bestaand beschermingsschema toepassen

1. Selecteer de machines die u wilt beschermen.
2. Klik op **Beschermen**. Als er al een beschermingsschema wordt toegepast op de geselecteerde machines, klikt u op **Schema toevoegen**.
3. De eerder gemaakte beschermingsschema's worden weergegeven.
4. Selecteer een beschermingsschema om toe te passen en klik op **Toepassen**.

Een beschermingsschema bewerken

1. Als u het beschermingsschema wilt bewerken voor alle machines waarop het wordt toegepast, selecteert u een van deze machines. Of selecteer de machines waarvoor u het beschermingsschema wilt bewerken.
2. Klik op **Beschermen**.
3. Selecteer het beschermingsschema dat u wilt bewerken.
4. Klik op het ellipspictogram naast de naam van het beschermingsschema en klik vervolgens op **Bewerken**.
5. Als u de schemaparameters te wijzigen, klikt u op het betreffende gedeelte in het deelvenster voor het beschermingsschema.
6. Klik op **Wijzigingen opslaan**.
7. Als u het beschermingsschema wilt wijzigen voor alle machines waarop het wordt toegepast, klikt u op **De wijzigingen toepassen op dit beschermingsschema**. Anders klikt u op **Alleen een nieuw beschermingsschema maken voor de geselecteerde apparaten**.

Een beschermingsschema intrekken voor machines

1. Selecteer de machines waarvan u het beschermingsschema wilt intrekken.
2. Klik op **Beschermen**.
3. Als er verschillende beschermingsschema's worden toegepast op de machines, selecteert u het beschermingsschema dat u wilt intrekken.
4. Klik op het ellipspictogram naast de naam van het beschermingsschema en klik vervolgens op **Intrekken**.

Een beschermingsschema verwijderen

1. Selecteer een van de machines waarop het beschermingsschema wordt toegepast dat u wilt verwijderen.
2. Klik op **Beschermen**.
3. Als er meerdere beschermingsschema's worden toegepast op de machine, selecteert u het beschermingsschema dat u wilt verwijderen.
4. Klik op het ellipspictogram naast de naam van het beschermingsschema en klik vervolgens op **Verwijderen**.

   Het beschermingsschema wordt ingetrokken voor alle machines en volledig verwijderd uit de webinterface.

13 #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

13.1 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.

13.1.1 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) • U hebt geen antimalwarebeveiliging, er is mogelijk een risico voor uw systeem (0 punten) Aanbevelingen van #CyberFit-score:	275: er is antimalwaresoftware geïnstalleerd op een machine 0: er is geen antimalwaresoftware geïnstalleerd op een machine

		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.	
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 uw omgeving. De agent doet het volgende: 1. Controleert Windows Firewall- en netwerkbeveiliging, of er	Bevindingen: • U hebt een firewall ingeschakeld voor openbare en particuliere netwerken, of er is een firewalloplossing van derden gevonden (+175 punten) • U hebt alleen een firewall ingeschakeld voor	100: openbare firewall van Windows is ingeschakeld 75: particuliere firewall van Windows is ingeschakeld 175: openbare en particuliere firewall van Windows zijn ingeschakeld

	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 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: Het wordt aanbevolen om een firewall in te schakelen voor uw openbare en particuliere netwerken 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 Geavanceerde regels maken in Windows Firewall	OF een firewalloplossing van derden is ingeschakeld 0: er is geen Windows-firewall en geen firewalloplossing van derden ingeschakeld
Virtueel particulier netwerk (VPN)	De agent controleert of een VPN-oplossing is geïnstalleerd op een machine en of het VPN is	Bevindingen: • U hebt een VPN-oplossing en u kunt veilig gegevens ontvangen en verzenden	75: VPN is ingeschakeld en actief 0: VPN is niet ingeschakeld

	ingeschakeld en actief is.	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: Het wordt aanbevolen 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 • SonicWall GVPN • LANCOM VPN	
Schijfversleuteling	De agent controleert of schijfversleuteling is ingeschakeld op een	Bevindingen: • U hebt volledige	125: alle schijven zijn versleuteld

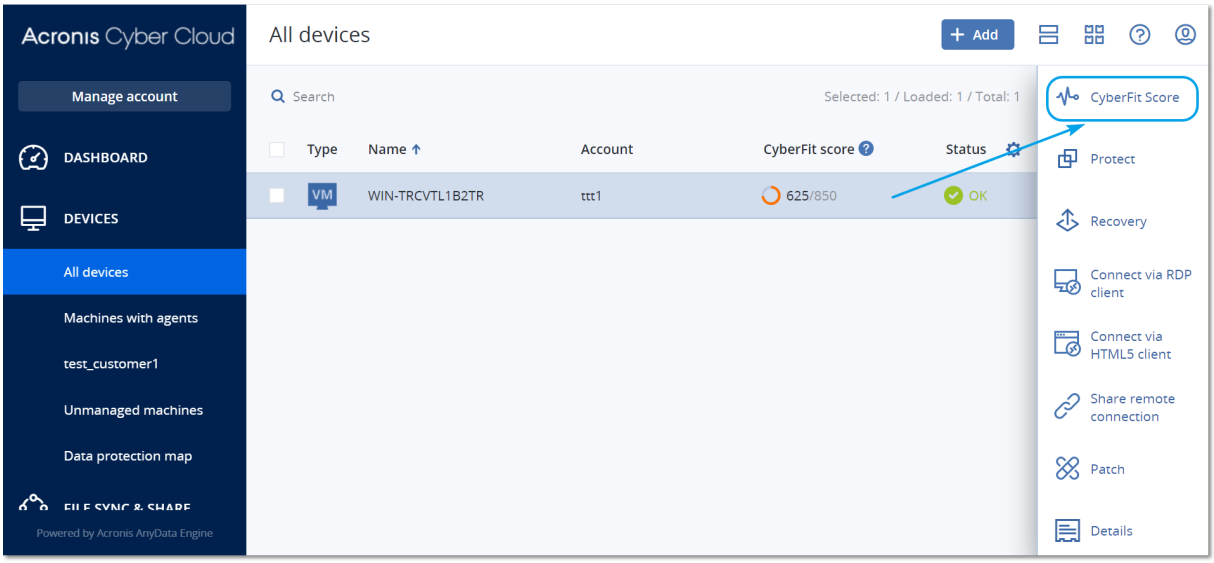
	machine. De agent controleert of Windows BitLocker is ingeschakeld.	schijfversleuteling ingeschakeld, uw machine is beschermd tegen ongewenste wijzigingen (+125 punten) • Slechts enkele harde schijven zijn versleuteld, er is mogelijk een risico van ongewenste wijzigingen op uw machine (+75 punten) • Er is geen schijfversleuteling gevonden, er is een risico van ongewenste wijzigingen op uw machine (0 punten) Aanbevelingen van #CyberFit-score: Het wordt aanbevolen om Windows BitLocker in te schakelen om de bescherming van uw gegevens en bestanden te verbeteren. Handleiding: Apparaatversleuteling inschakelen in Windows	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) Aanbevelingen van #CyberFit-score: Voor een betere beveiliging wordt het aanbevolen om al het uitgaande NTLM-verkeer	25: uitgaand NTLM-verkeer is ingesteld op DenyAll (alles weigeren) 0: uitgaand NTLM-verkeer is ingesteld op een andere waarde

		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 serviceconsole 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.

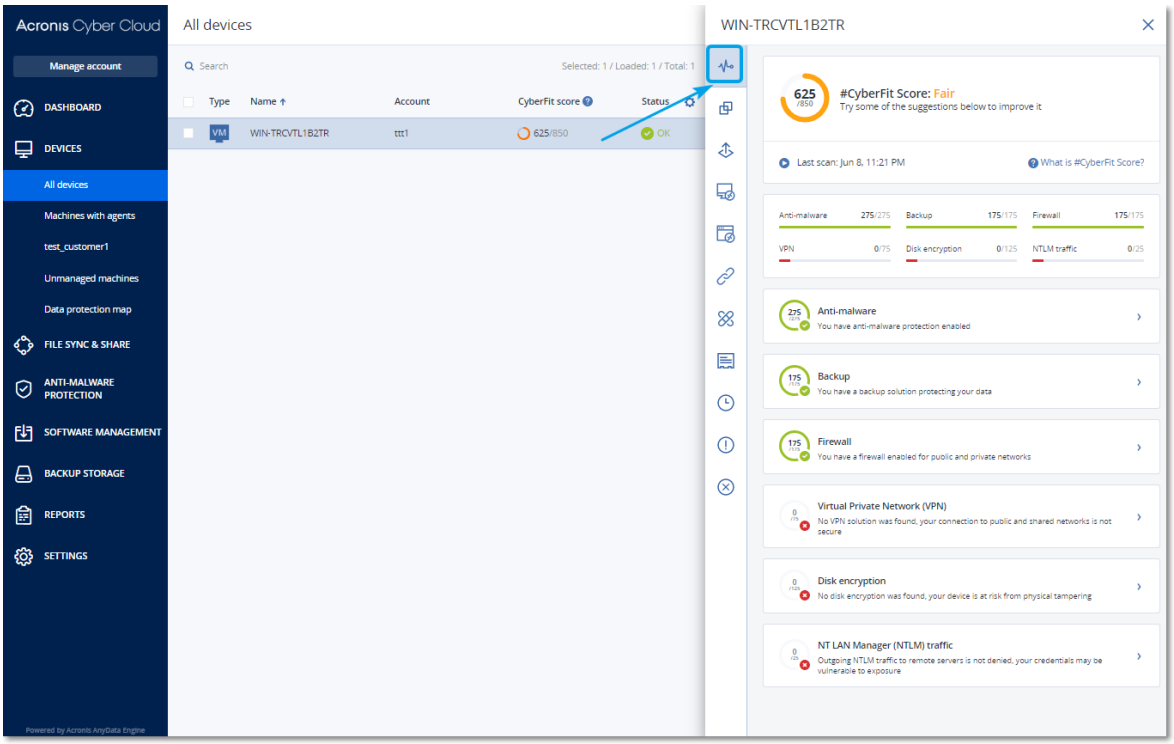


Informatie over de #CyberFit-score vindt u ook op de betreffende pagina's van de widget en het rapport.

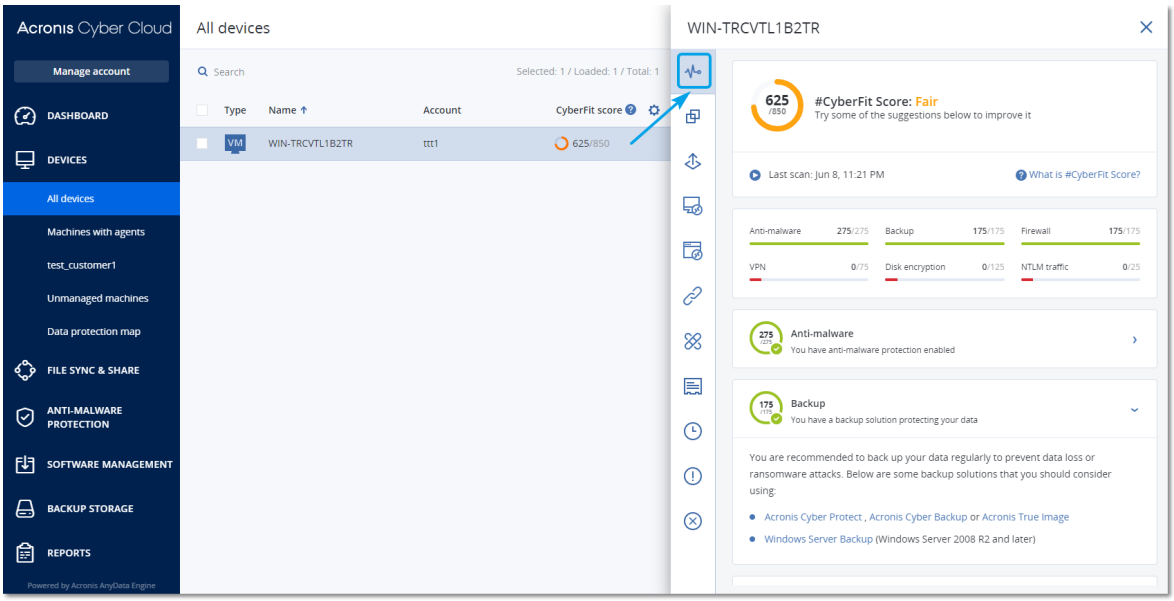
13.2 Scan van een #CyberFit-score uitvoeren

Scan van een #CyberFit-score uitvoeren

1. Ga in de serviceconsole 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.

14 Back-up en herstel

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.

14.1 Back-up

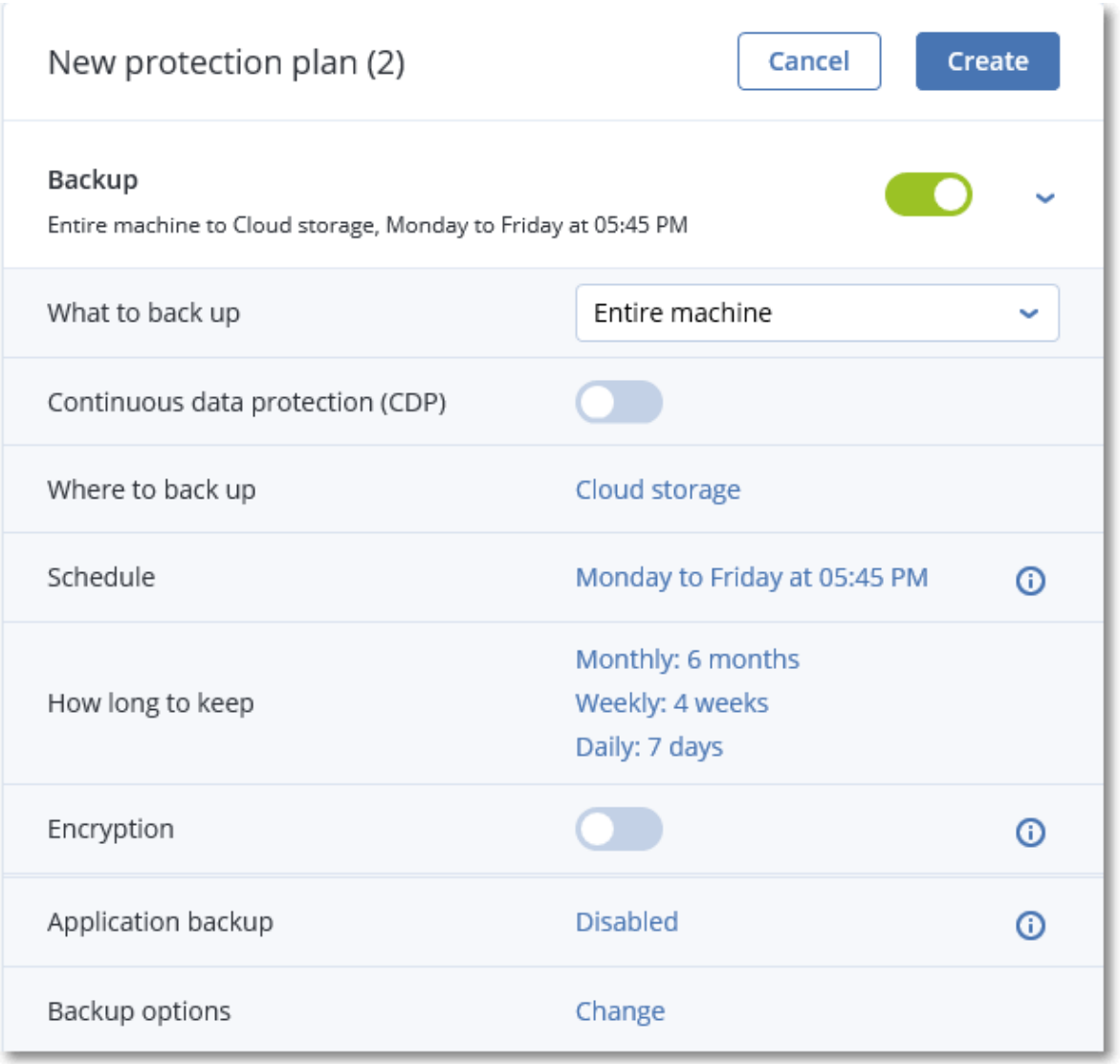
Een beschermingsschema in de back-upmodule is een set regels die bepaalt hoe de desbetreffende gegevens op een bepaalde machine worden beschermd.

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**.

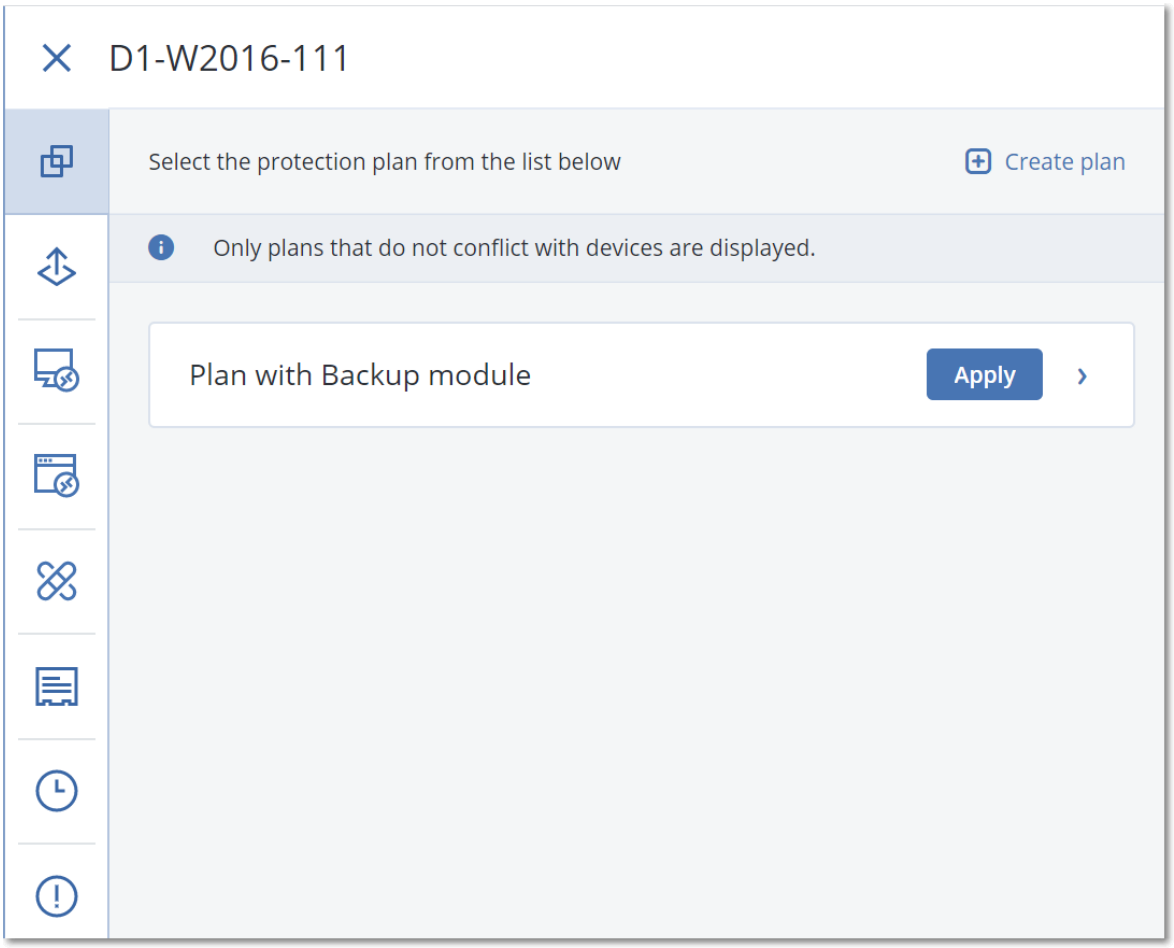
   De beschermingsschema's die op de machine worden toegepast, worden weergegeven. Als er nog geen schema's aan de machine zijn toegewezen, dan ziet u het standaardbeschermingsschema dat kan worden toegepast. U kunt de instellingen naar wens aanpassen en dit schema toepassen of een nieuw schema maken.
3. 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**.

14.2 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**		
ESXi-configuratie	Rechtstreekse selectie	Lokale map Netwerkmap NFS*	Wekelijks volledig, dagelijks incrementeel Maandelijks volledig, Wekelijks differentieel, Dagelijks incrementeel (GFS) Aangepast (F-D-I)	
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)</td><td rowspan="4"></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></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">—</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">—</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.

14.3 Gegevens voor de back-up selecteren

14.3.1 Schijven/volumes selecteren

Een back-up op schijfniveau bevat een kopie van een schijf of volume in pakketvorm. U kunt afzonderlijk schijven, volumes of bestanden herstellen uit een back-up op schijfniveau. Een back-up van een volledige machine is een back-up van alle bijbehorende niet-verwisselbare schijven.

Opmerking
Schijf/volumeback-ups worden niet ondersteund voor versleutelde APFS-volumes die zijn vergrendeld.

Tijdens een back-up van een volledige machine worden dergelijke volumes overgeslagen.

U kunt ook een back-up maken van schijven die via het iSCSI-protocol zijn verbonden met een fysieke machine, maar er zijn 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.

U kunt schijven/bestanden op twee manieren selecteren: rechtstreeks op elke machine of door beleidsregels. U kunt bestanden uitsluiten voor de back-up van een schijf door bestandsfilters in te stellen.

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 machines in het beschermingsschema de selectievakjes in naast de schijven of volumes waarvan u een back-up wilt maken.
5. Klik op **Gereed**.

Beleidsregels gebruiken

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.
   De beleidsregels worden toegepast op alle machines die in het beschermingsschema zijn opgenomen. Als bij het starten van de back-up geen gegevens op de machine worden gevonden

die minimaal aan een van de criteria voldoen, mislukt de back-up voor de desbetreffende machine.

5. Klik op **Gereed**.

Regels voor Windows, Linux en macOS

- `[Alle volumes]`: hiermee worden alle volumes op machines met Windows en alle gekoppelde volumes op machines met Linux of macOS geselecteerd.

Regels voor Windows

- Stationsletter (bijvoorbeeld **C:**): hiermee wordt het volume met de opgegeven stationsletter geselecteerd.
- `[Vaste volumes (fysieke machines)]`: hiermee worden alle volumes van fysieke machines 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.
- `[OPSTARTEN+SYSTEEM]`: hiermee worden het systeem en de opstartvolumes geselecteerd. Deze combinatie is de minimale set gegevens die ervoor zorgt dat de back-up van het besturingssysteem wordt hersteld.
- `[Schijf 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.

Regels voor Linux

- `/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, voert u het volgende in:

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

Regels voor macOS

- `[Schijf 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.

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.

14.3.2 Bestanden/mappen selecteren

Back-up op bestandsniveau is beschikbaar voor fysieke machines en virtuele machines waarvan een back-up wordt gemaakt door een agent die is geïnstalleerd in het gastsysteem. U kunt ook een back-up maken van mappen en bestanden op schijven die via het iSCSI-protocol zijn verbonden met een fysieke machine, maar er zijn beperkingen als u Agent voor VMware of Agent voor Hyper-V gebruikt voor het maken van back-ups van de gegevens op de schijven die zijn verbonden via iSCSI.

Als u het besturingssysteem wilt herstellen, kunt u niet volstaan met een back-up op bestandsniveau. Kies voor een bestandsback-up als u alleen bepaalde gegevens veilig wilt stellen (bijvoorbeeld het huidige project). Zodoende reduceert u de back-upgrootte en bespaart u dus opslagruimte.

U kunt bestanden op twee manieren selecteren: rechtstreeks op elke machine of door beleidsregels. Beide methoden bieden u de mogelijkheid uw selectie verder te verfijnen door bestandsfilters in te stellen.

Rechtstreekse selectie

1. Selecteer bij **Back-up maken van** de optie **Bestanden/mappen**.
2. Geef **Items om een back-up van te maken** op.
3. Selecteer bij **Items voor back-up selecteren** de optie **Rechtstreeks**.

4. Voor elk van de machines die in het beschermingsschema zijn opgenomen:
   a. Klik op **Bestanden en mappen selecteren**.
   b. Klik op **Lokale map** of **Netwerkmap**.
      De share moet toegankelijk zijn vanaf de geselecteerde machine.
   c. Blader naar de benodigde bestanden/mappen of geef het pad op en klik op de pijlknop. Geef desgevraagd de gebruikersnaam en het wachtwoord voor de gedeelde map op.
      Een back-up maken van een map met anonieme toegang wordt niet ondersteund.
   d. Selecteer de vereiste bestanden/mappen.
   e. Klik op **Gereed**.

Beleidsregels gebruiken

1. Selecteer bij **Back-up maken van** de optie **Bestanden/mappen**.
2. Geef **Items om een back-up van te maken** op.
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.
   De beleidsregels worden toegepast op alle machines die in het beschermingsschema zijn opgenomen. Als bij het starten van de back-up geen gegevens op de machine worden gevonden die minimaal aan een van de criteria voldoen, mislukt de back-up voor de desbetreffende machine.
5. Klik op **Gereed**.

Selectieregels voor Windows

- Volledig pad naar een bestand of map, bijvoorbeeld **D:\Work\Text.doc** of **C:\Windows**.
- Sjablonen:
  - `[All Files]`: hiermee worden alle bestanden op alle volumes van de machine geselecteerd.
  - `[All Profiles Folder]`: hiermee wordt de map geselecteerd waar alle gebruikersprofielen zijn opgeslagen (doorgaans **C:\Users** of **C:\Documents and Settings**).
- Omgevingsvariabelen:
  - `%ALLUSERSPROFILE%`: hiermee wordt de map met de algemene gegevens van alle gebruikersprofielen geselecteerd (doorgaans **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 met 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, typt u **%PROGRAMFILES%\Java**.

Selectieregels voor Linux

- Volledig pad naar een bestand of directory. Als u bijvoorbeeld een back-up wilt maken van **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.
  - `/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.
- Sjablonen:
  - `[Map Alle profielen]`: hiermee wordt **/home** geselecteerd. Dit is de map waar standaard alle gebruikersprofielen zijn opgeslagen.

Selectieregels voor macOS

- Volledig pad naar een bestand of directory.
- Sjablonen:
  - `[Map Alle profielen]`: hiermee wordt **/Users** geselecteerd. Dit is de map waar standaard alle gebruikersprofielen zijn opgeslagen.

Voorbeelden:

- Als u een back-up van **file.txt** op uw desktop wilt maken, geeft u **/Users/<username>/Desktop/file.txt** op, waarbij <username> uw gebruikersnaam is.
- Als u een back-up van alle home directory's van alle gebruikers wilt maken, geeft u **/Users** op.
- Als u een back-up wilt maken van de directory waar de toepassingen zijn geïnstalleerd, geeft u **/Applications** op.

14.3.3 Systeemstatus selecteren

Back-up van systeemstatus is beschikbaar voor machines met Windows Vista en later.

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

14.3.4 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-up van ESXi-configuratie wordt niet ondersteund voor VMware vSphere 7.0.
- 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.

14.4 Continue gegevensbescherming (CDP)

Back-ups worden meestal uitgevoerd op regelmatige, maar vrij lange tijdsintervallen om prestatieproblemen te voorkomen. Als het systeem plotseling beschadigd raakt, gaan wijzigingen van de gegevens tussen de laatste back-up en de systeemfout verloren.

Met de functie **Continue gegevensbescherming** worden er tussen de geplande back-ups continu back-ups gemaakt van de wijzigingen van de geselecteerde gegevens:

- Door wijzigingen bij te houden in de opgegeven bestanden/mappen
- Door wijzigingen bij te houden van de bestanden die zijn gewijzigd door de opgegeven toepassingen

U kunt bepaalde bestanden voor continue gegevensbescherming selecteren uit de gegevens die zijn geselecteerd voor back-up. Er wordt dan automatisch een back-up gemaakt van elke wijziging van deze bestanden. U kunt deze bestanden herstellen tot de tijd van de laatste wijziging.

Momenteel wordt de functie **Continue gegevensbescherming** ondersteund voor de volgende besturingssystemen:

- Windows 7 en later
- Windows Server 2008 R2 en later

Het ondersteunde bestandssysteem: Alleen NTFS, alleen lokale mappen (gedeelde mappen worden niet ondersteund).

De optie **Continue gegevensbescherming** is niet compatibel met de optie **Applicatieback-up**.

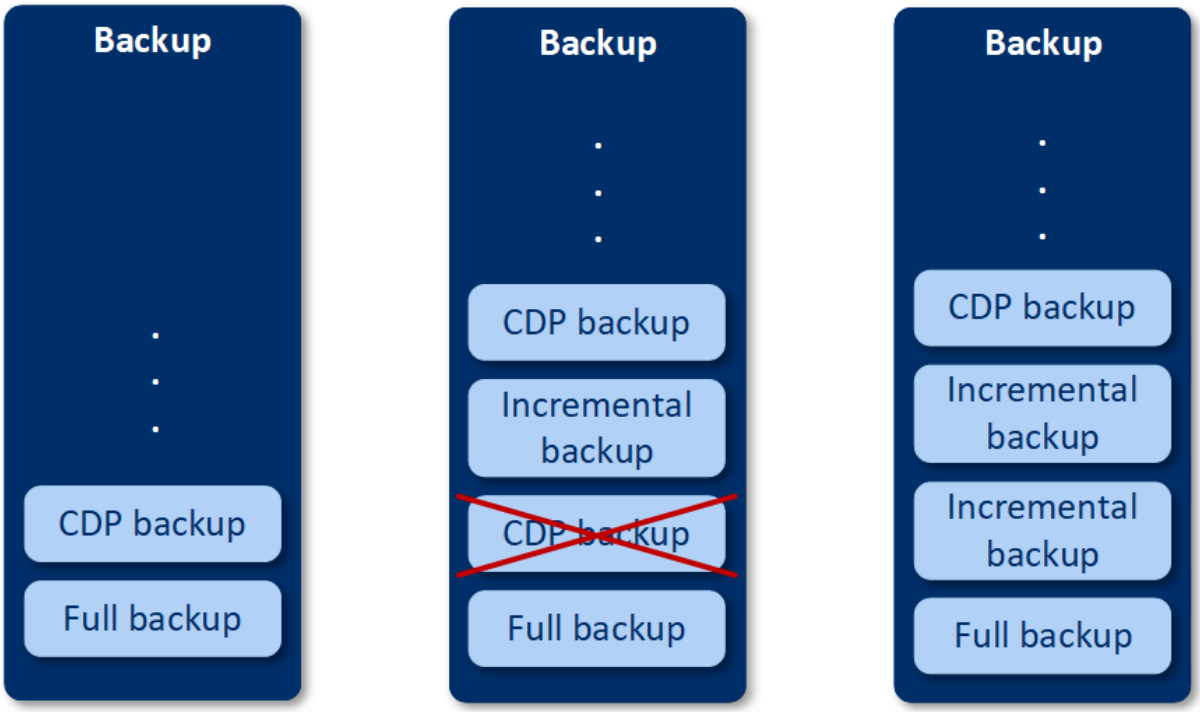
Zo werkt het

Laten we de back-up die continu wordt gemaakt, de CDP-back-up noemen. Voor het maken van de CDP-back-up moet van te voren een volledige back-up of incrementele back-up worden gemaakt.

Wanneer u het beschermingsschema voor het eerst uitvoert met de back-upmodule terwijl **Continue gegevensbescherming** is ingeschakeld, dan wordt eerst een volledige back-up gemaakt. Direct daarna wordt de CDP-back-up voor de geselecteerde of gewijzigde bestanden/mappen gemaakt. De CDP-back-up bevat altijd de nieuwste versie van de door u geselecteerde gegevens. Wanneer u wijzigingen aanbrengt in de geselecteerde bestanden/mappen, wordt er geen nieuwe CDP-back-up gemaakt, alle wijzigingen worden opgenomen in dezelfde CDP-back-up.

Wanneer het tijd is voor een geplande incrementele back-up, wordt de CDP-back-up verwijderd en wordt een nieuwe CDP-back-up gemaakt nadat de incrementele back-up is voltooid.

De CDP-back-up blijft dus altijd de nieuwste back-up in de back-upketen met de meest recente actuele versie van de beschermde bestanden/mappen.



Als u al een beschermingsschema hebt waarvoor de back-upmodule is ingeschakeld en u besluit **Continue gegevensbescherming** in te schakelen, dan wordt de CDP-back-up gemaakt direct na het inschakelen van de optie, omdat de back-upketen al volledige back-ups heeft.

Ondersteunde gegevensbronnen en bestemmingen voor continue gegevensbescherming

Voor een goede werking van continue gegevensbescherming moet u de volgende items opgeven voor de volgende gegevensbronnen:

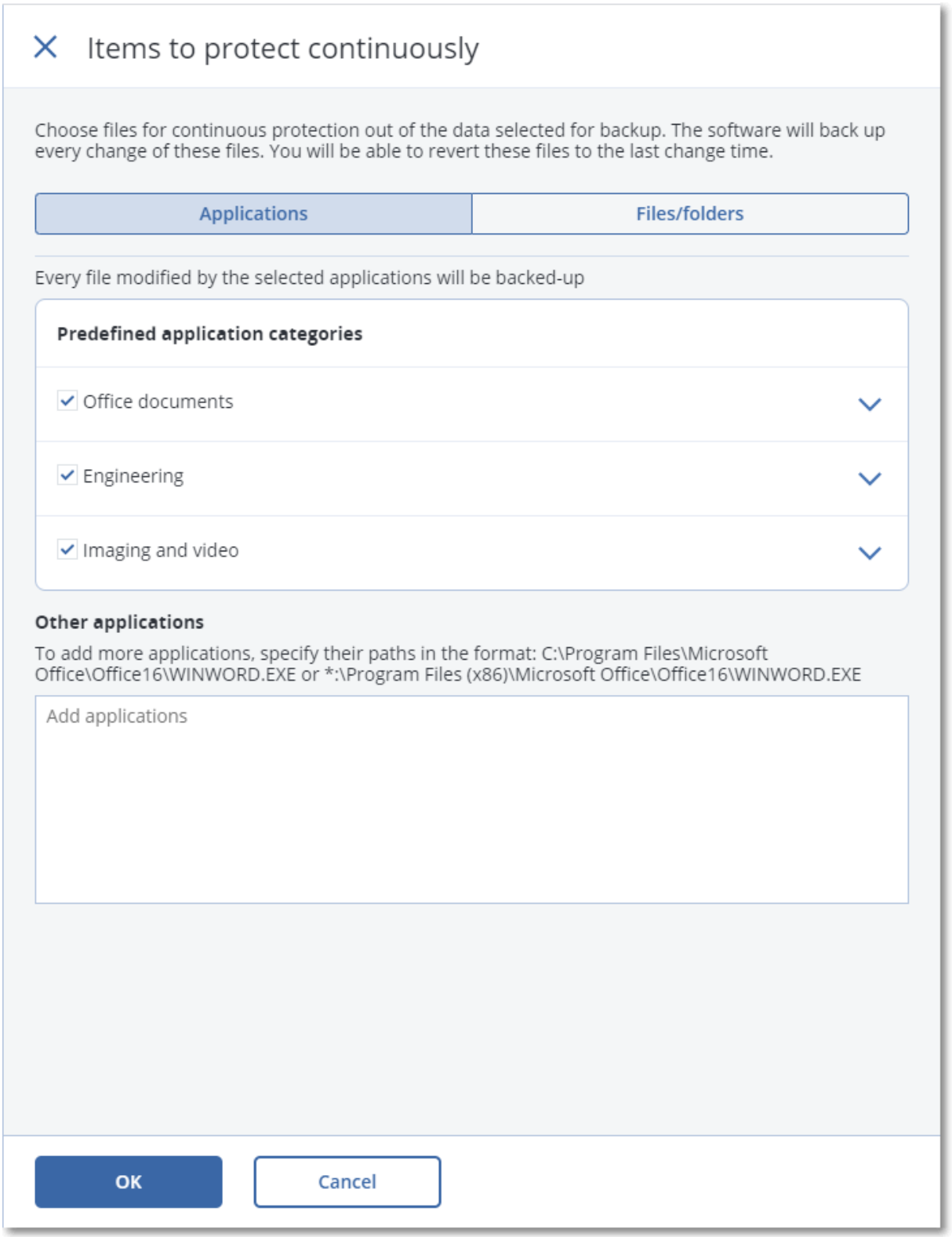
BACK-UP VAN	Items waarvan u een back-up wilt maken
Volledige machine	U moet bestanden/mappen of toepassingen opgeven
Schijven/volumes	U moet schijven/volumes of bestanden/mappen opgeven
Bestanden/mappen	U moet bestanden/mappen opgeven U moet toepassingen opgeven (niet verplicht)

De volgende back-upbestemmingen worden ondersteund voor continue gegevensbescherming:

- Lokale map
- Netwerkmap
- Locatie gedefinieerd door een script
- Cloudopslag
- Acronis Cyber Infrastructure

Apparaten beschermen met continue gegevensbescherming

1. Kies in de serviceconsole de optie Een beschermingsschema maken terwijl de **Back-up**module is ingeschakeld.
2. Schakel de optie **Continue gegevensbescherming (CDP)** in.
3. Geef de **Items die voortdurend moeten worden beschermd** op:
   - **Toepassingen** (er wordt een back-up gemaakt van elk bestand dat is gewijzigd door de geselecteerde toepassingen). We raden aan deze optie te gebruiken om uw Office-documenten te beschermen met de CDP-back-up.



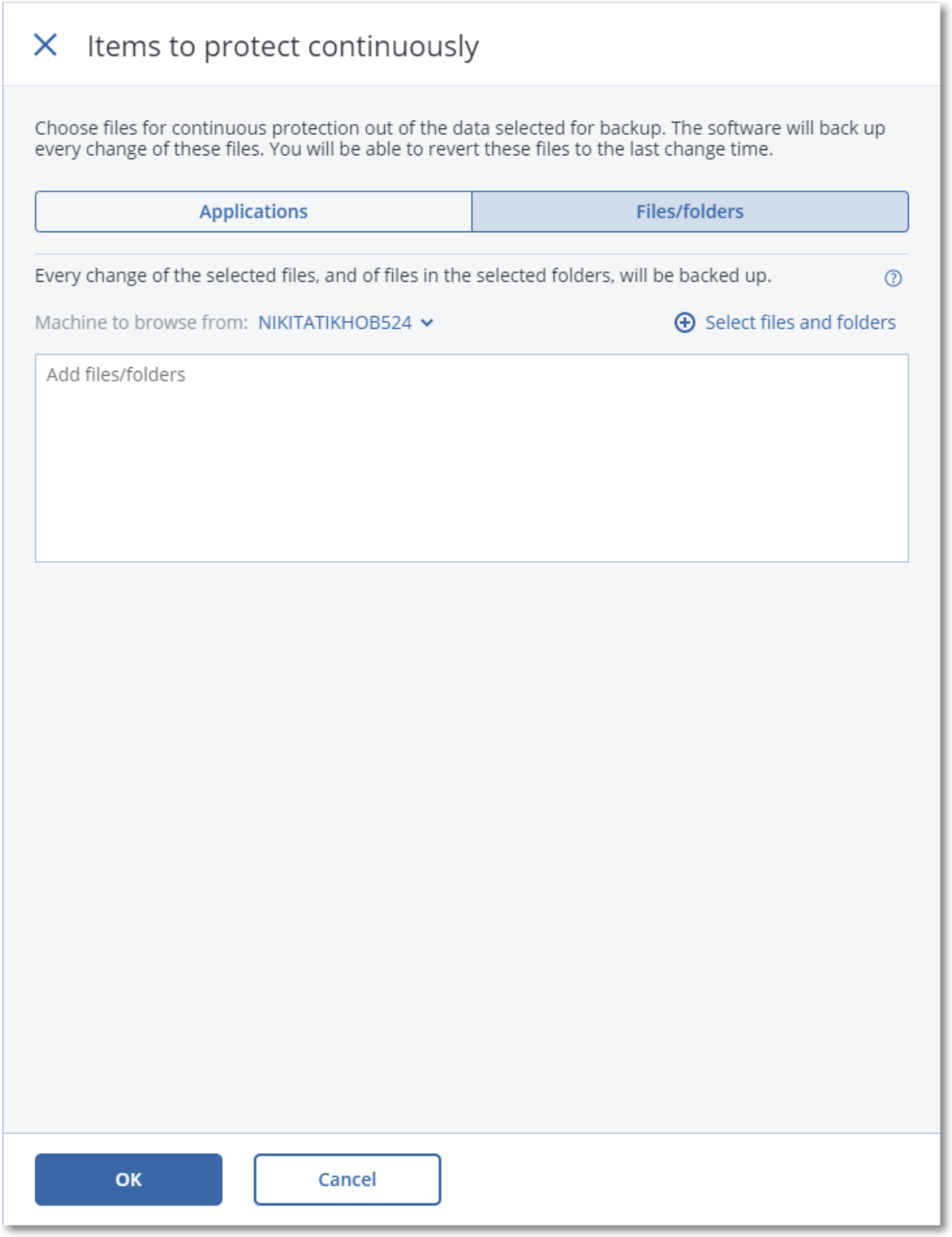
- U kunt de toepassingen uit de vooraf gedefinieerde categorieën selecteren of andere toepassingen opgeven door het pad naar het uitvoerbare bestand van de toepassing te definiëren. Gebruik een van de volgende indelingen:

  `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

  OF

```
*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
```

- **Bestanden/mappen** (er wordt een back-up gemaakt van elk bestand dat is gewijzigd in de opgegeven locatie). We raden aan deze optie te gebruiken om bestanden en mappen te beschermen die voortdurend worden gewijzigd.



1. **Machine waarmee u wilt bladeren**: geef de machine op waarvan u de bestanden/mappen wilt selecteren voor continue gegevensbescherming.

   Klik op **Bestanden en mappen selecteren** om bestanden/mappen op de opgegeven machine te selecteren.

   Belangrijk
   Als u handmatig een hele map opgeeft met bestanden waarvan continu een back-up wordt gemaakt, gebruik dan een masker, bijvoorbeeld:
   Juist pad: D:\Data*
   Onjuist pad: D:\Data\

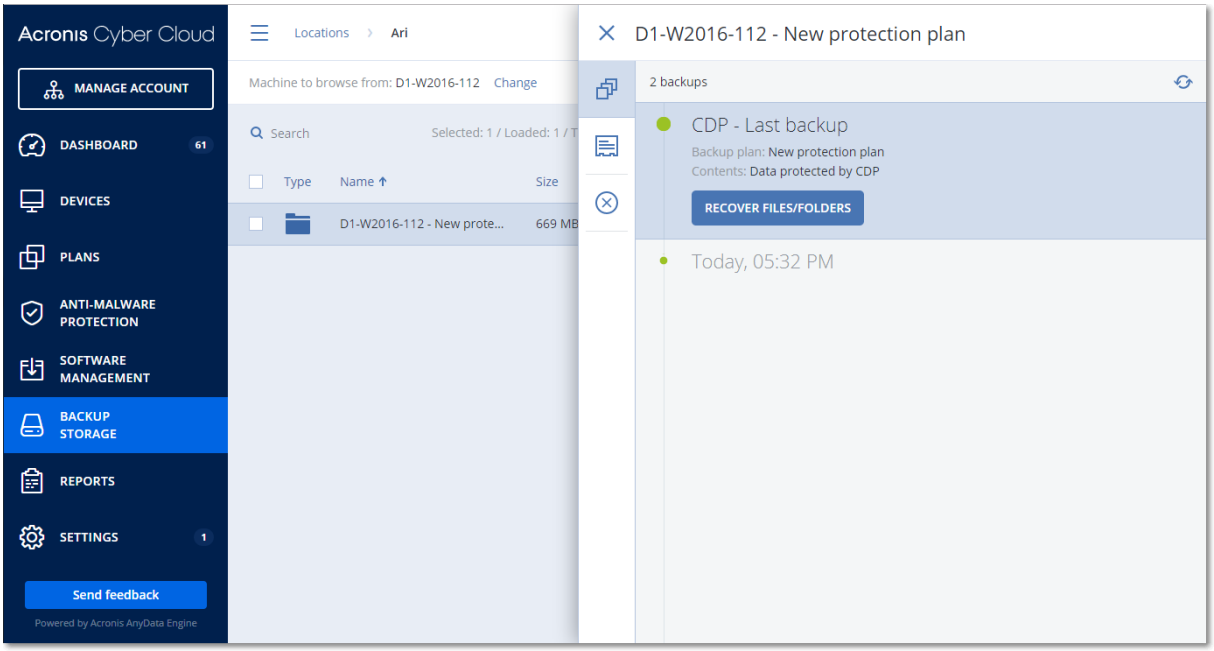
   In het tekstveld kunt u ook regels opgeven voor het selecteren van bestanden/mappen waarvan een back-up wordt gemaakt. Raadpleeg 'Bestanden/mappen selecteren' voor meer informatie over het definiëren van regels. Wanneer u klaar bent, klikt u op **Gereed**.
2. Klik op **Maken**.

Het beschermingsschema met ingeschakelde continue gegevensbescherming wordt dan toegewezen aan de geselecteerde machine. Na de eerste reguliere back-up worden continu back-ups met de nieuwste kopie van de met CDP beschermde gegevens gemaakt. Er worden back-ups gemaakt van zowel de gegevens die zijn gedefinieerd via Toepassingen als via Bestanden/mappen.

Gegevens waarvan een continu back-up wordt gemaakt, worden bewaard volgens het bewaarbeleid dat is gedefinieerd voor de back-upmodule.

Back-ups herkennen die continu worden beschermd

De back-ups waarvan continu een back-up wordt gemaakt, hebben het voorvoegsel CDP.



Uw hele machine herstellen naar de meest recente status

Als u een volledige machine wilt herstellen naar de meest recente status, kunt u de optie **Continue gegevensbescherming (CDP)** in de back-upmodule van een beschermingsschema gebruiken.

U kunt een volledige machine of bestanden/mappen herstellen vanaf een CDP-back-up. In het eerste geval krijgt u een volledige machine met de meest recente status, in het tweede geval bestanden/mappen met de meest recente status.

14.5 Een bestemming selecteren

Klik op **Locatie van back-up** 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.
- **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. 184).

14.5.1 Geavanceerde opslagoptie

Opmerking
Deze functionaliteit is alleen beschikbaar in de Advanced Edition van de Cyberbescherming-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.

Voorbeeld. 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**.

14.5.2 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.

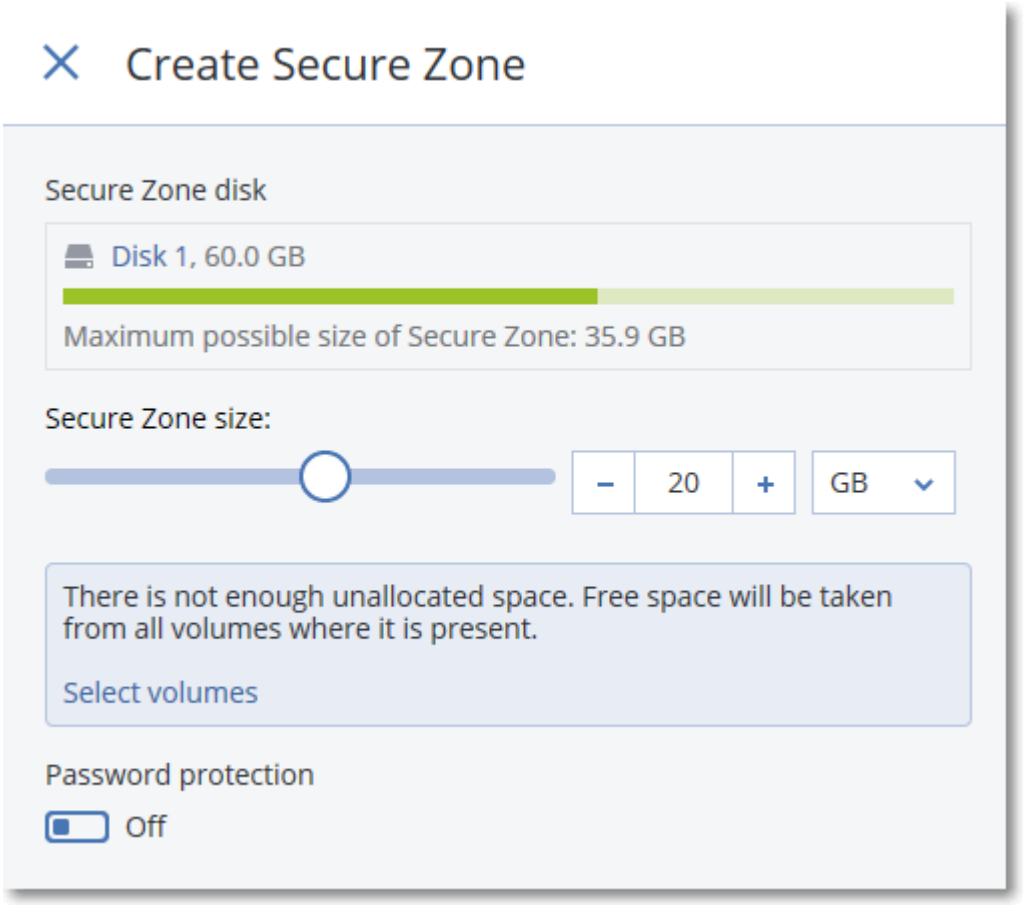
Belangrijk
Als u het volume waarvan het systeem wordt opgestart, verplaatst of de grootte ervan verandert, moet het systeem opnieuw worden opgestart.

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 **Locatie van back-up** 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.

14.6 Planning

Het schema maakt gebruik van de tijdinstellingen (inclusief de tijdzone) van het besturingssysteem waarop de agent is geïnstalleerd. De tijdzone van Agent voor VMware (Virtual Appliance) kan worden geconfigureerd in de interface van de agent.

Als een beschermingsschema volgens schema bijvoorbeeld moet worden uitgevoerd om 21:00 uur en het schema wordt toegepast op verschillende machines in verschillende tijdzones, dan wordt de back-up op elke machine gestart om 21:00 uur lokale tijd.

14.6.1 Back-upschema's

U kunt een van de vooraf gedefinieerde back-upschema's kiezen of een aangepast schema maken. Een back-upschema is onderdeel van een beschermingsschema dat zowel het back-upschema als de back-upmethoden bevat.

Selecteer bij **Back-upschema** een van de volgende opties:

- **Altijd incrementeel (één bestand)**

  Er worden standaard dagelijks back-ups gemaakt, van maandag tot en met vrijdag. U kunt de tijd voor het uitvoeren van de back-up selecteren.

  Als u de back-upfrequentie wilt aanpassen, verplaatst u de schuifregelaar en geeft u het back-upschema op.

  Voor de back-ups wordt de indeling voor enkelvoudig back-upbestand[1] (één bestand) gebruikt.

  De eerste back-up is een volledige back-up. Dit betekent dat deze back-up vrij veel tijd in beslag neemt. Alle volgende back-ups zijn incrementele back-ups en nemen aanzienlijk minder tijd in beslag.

  Dit schema wordt sterk aangeraden als de back-uplocatie de cloudopslag is. Andere back-upschema's omvatten mogelijk meerdere volledige back-ups die veel tijd en netwerkverkeer verbruiken.
- **Altijd volledig**

  Er worden standaard dagelijks back-ups gemaakt, van maandag tot en met vrijdag. U kunt de tijd voor het uitvoeren van de back-up selecteren.

  Als u de back-upfrequentie wilt aanpassen, verplaatst u de schuifregelaar en geeft u het back-upschema op.

  Alle back-ups zijn volledige back-ups.
- **Wekelijks volledig, dagelijks incrementeel**

  Er worden standaard dagelijks back-ups gemaakt, van maandag tot en met vrijdag. U kunt wijzigen op welke dag van de week en op welk tijdstip de back-up wordt uitgevoerd.

  Er wordt eens per week een volledige back-up gemaakt. Alle andere back-ups zijn incrementele back-ups. Op welke dag de volledige back-up wordt gemaakt, is afhankelijk van de optie **Wekelijkse back-up** (klik op het tandwielpictogram en vervolgens op **Back-upopties** > **Wekelijkse back-up**).
- **Maandelijks volledig, Wekelijks differentieel, Dagelijks incrementeel (GFS)**

  Er worden standaard dagelijks incrementele back-ups gemaakt, van maandag tot en met vrijdag; differentiële back-ups worden elke zaterdag gemaakt; volledige back-ups worden op de eerste dag van de maand gemaakt. U kunt de dag en tijd voor het uitvoeren van de back-up selecteren.

  Dit back-upschema wordt weergegeven als een **Aangepast** schema in het deelvenster voor het beschermingsschema.
- **Aangepast**

  Hier kunt u schema's voor volledige, differentiële en incrementele back-ups opgeven.

  Differentiële back-up is niet beschikbaar wanneer er een back-up van SQL-gegevens, Exchange-gegevens of de systeemstatus wordt gemaakt.

---

[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.

Met een back-upschema kunt u de back-up plannen op gebeurtenissen, in plaats van op tijd. Selecteer hiervoor het gebeurtenistype in de schemakiezer. Zie Plannen op gebeurtenissen voor meer informatie.

14.6.2 Aanvullende planningsopties

U kunt voor elke bestemming het volgende doen:

- Geef de back-up startvoorwaarden op, zodat een geplande back-up alleen wordt uitgevoerd als aan de voorwaarden wordt voldaan. Zie voor meer informatie 'Startvoorwaarden'.
- 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. Terwijl het schema is uitgeschakeld, worden de bewaarregels niet toegepast tenzij een back-up handmatig wordt gestart.
- Een vertraging ten opzichte van de geplande tijd instellen. 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.

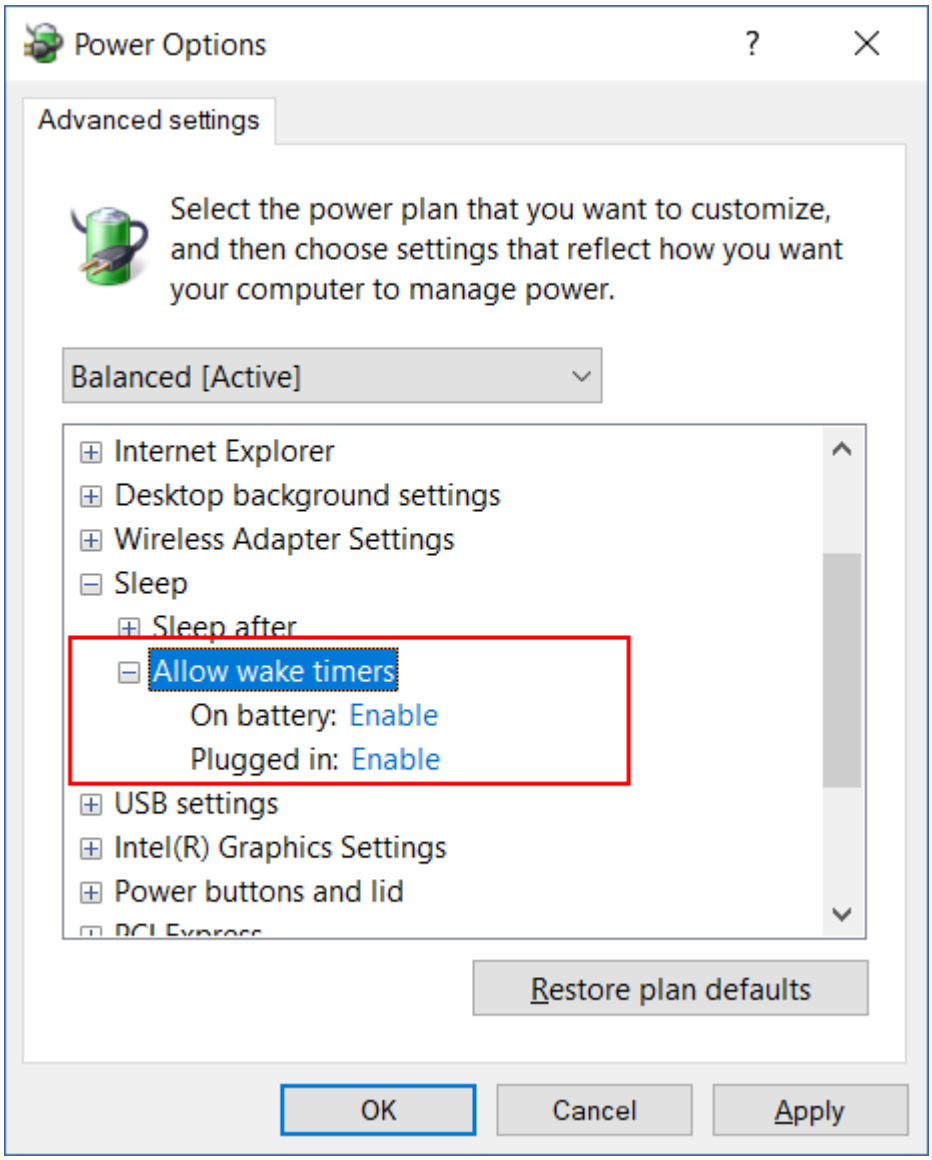
  Ga in het beschermingsschema in de instellingen van de back-upmodule naar **Back-upopties** > **Plannen**. Selecteer **Starttijden van back-ups binnen een tijdvenster distribueren** en geef de maximale vertraging op. De waarde van de vertraging voor elke machine wordt bepaald op het moment dat het beschermingsschema wordt toegepast op de machine. Deze waarde verandert niet totdat u het beschermingsschema bewerkt en de maximumwaarde voor de vertraging wijzigt.

  Opmerking
  Deze optie is standaard ingeschakeld en ingesteld op een maximale vertraging van 30 minuten.

- Klik op **Meer weergeven** voor toegang tot de volgende opties:
  - **Als de machine is uitgeschakeld, gemiste taken uitvoeren wanneer de machine wordt opgestart** (standaard uitgeschakeld)
  - **De slaapstand of de stand-bymodus verhinderen tijdens het maken van een back-up** (standaard ingeschakeld)

    Deze optie werkt alleen voor machines met Windows.
  - **De slaapstand of stand-bymodus beëindigen om een geplande back-up te starten** (standaard uitgeschakeld)

    Deze optie werkt alleen voor machines met Windows waarop de instelling **Activeringstimers toestaan** is ingeschakeld voor het energiebeheerschema.



Deze optie werkt niet wanneer de machine is uitgeschakeld, dat wil zeggen dat de optie geen gebruik maakt van de functie Wake-on-LAN.

14.6.3 Planning op gebeurtenissen

Wanneer u een schema instelt voor de back-upmodule van het beschermingsschema, kunt u het gebeurtenistype selecteren in de schemakiezer. De back-up wordt uitgevoerd en gestart zodra de gebeurtenis zich voordoet.

U kunt een van de volgende gebeurtenissen selecteren:

- **Op tijd sinds de laatste back-up**
  Dit is het tijdstip sinds de voltooiing van de laatst uitgevoerde back-up binnen hetzelfde beschermingsschema. U kunt de tijdsduur opgeven.

Opmerking
Omdat het schema is gebaseerd op een succesvolle back-up, zal de planner, als een back-up mislukt, de taak niet opnieuw uitvoeren totdat een operator het schema handmatig uitvoert en de run met succes is voltooid.

- **Wanneer een gebruiker zich aanmeldt bij het systeem**
  Standaard zal het aanmelden van een gebruiker tot een back-up leiden. U kunt elke gebruiker wijzigen naar een specifieke gebruikersaccount.
- **Wanneer een gebruiker zich afmeldt bij het systeem**
  Standaard zal het afmelden van een gebruiker tot een back-up leiden. U kunt elke gebruiker wijzigen naar een specifieke gebruikersaccount.

Opmerking
De back-up wordt niet uitgevoerd wanneer het systeem wordt afgesloten omdat afsluiten niet hetzelfde is als afmelden.

- **Wanneer het systeem wordt opgestart**
- **Wanneer het systeem wordt afgesloten**
- **Bij een gebeurtenis in het Windows-gebeurtenislogboek**
  U moet de gebeurteniseigenschappen opgeven.

De onderstaande tabel toont de gebeurtenissen die beschikbaar zijn voor verschillende gegevens onder Windows, Linux en macOS.

BACK-UP MAKEN VAN	Op tijd sinds de laatste back-up	Wanneer een gebruiker zich aanmeldt bij het systeem	Wanneer een gebruiker zich afmeldt bij het systeem	Wanneer het systeem wordt opgestart	Wanneer het systeem wordt afgesloten	Bij een gebeurtenis in het Windows-gebeurtenislogboek
Schijven/volumes of bestanden (fysieke machines)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Schijven/volumes (virtuele machines)	Windows, Linux	–	–	–	–	–
ESXi-configuratie	Windows, Linux	–	–	–	–	–
Microsoft 365-postvakken	Windows	–	–	–	–	Windows

Databases en postvakken uitwisselen	Windows	–	–	–	–	Windows
SQL-databases	Windows	–	–	–	–	Windows

Bij een gebeurtenis in het Windows-gebeurtenislogboek

U kunt een back-up laten beginnen wanneer een bepaalde Windows-gebeurtenis is vastgelegd in een van de gebeurtenislogboeken, zoals het logboek **Toepassing**, **Beveiliging** of **Systeem**.

U wilt bijvoorbeeld mogelijk een beschermingsschema instellen waarin er automatisch een volledige noodback-up van uw gegevens wordt gemaakt zodra er in Windows wordt gedetecteerd dat er sprake is van een defect aan uw hardeschijfstation.

Als u door de gebeurtenissen wilt bladeren en de eigenschappen van een gebeurtenis wilt weergeven, gebruikt u de module **Gebeurtenisviewer** in de console **Computerbeheer**. U moet lid zijn van de groep **Administrators** op deze machine om het logboek **Beveiliging** te kunnen openen.

Gebeurteniseigenschappen

Logboeknaam

Geeft de naam van het logboek weer. Selecteer de naam van een standaard logboek (**Toepassing**, **Beveiliging**, of **Systeem**) in de lijst, of typ een logboeknaam, bijvoorbeeld: **Microsoft Office-sessies**

Gebeurtenisbron

Geeft de gebeurtenisbron aan: doorgaans het programma of het systeemonderdeel waardoor 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. Dus als u de tekenreeks **service** opgeeft, wordt een back-up geactiveerd door zowel de gebeurtenisbron **Servicebesturingsbeheer** als de gebeurtenisbron **Tijdservice**.

Gebeurtenistype

Geeft het soort gebeurtenis weer: **Fout**, **Waarschuwing**, **Informatie**, **Audit voltooid**, of **Audit mislukt**.

Gebeurtenis-id

Geeft het gebeurtenisnummer weer, dat het specifieke soort gebeurtenis van gebeurtenissen uit dezelfde bron identificeert.

Bijvoorbeeld een gebeurtenis **Fout** met gebeurtenisbron **schijf** en gebeurtenis-id **7** doet zich voor als Windows een slecht blok op een schijf ontdekt, terwijl een gebeurtenis **Fout** met gebeurtenisbron **schijf** en gebeurtenis-id **15** zich voordoet wanneer een schijf nog niet klaar is voor toegang.

Bijvoorbeeld: Noodback-up bij "beschadigd blok"

Als er plotseling een of meer beschadigde blokken zijn verschenen op een harde schijf, betekent dit doorgaans dat er binnen afzienbare tijd een fout in de harde schijf zal optreden. Stel dat u een beschermingsschema wilt maken waarin er een back-up van de gegevens van de harde schijf wordt gemaakt zodra een dergelijke situatie zich voordoet.

Wanneer er in Windows een beschadigd blok op een harde schijf wordt gedetecteerd, wordt in het logboek **Systeem** de **schijf** met de gebeurtenisbron en het gebeurtenisnummer **7** vastgelegd. Het type gebeurtenis is **Fout**.

Wanneer u het schema maakt, typt of selecteert u het volgende in het gedeelte **Planning**:

- **Logboeknaam**: **Systeem**
- **Gebeurtenisbron**: **schijf**
- **Gebeurtenistype**: **Fout**
- **Gebeurtenis-id**: **7**

Belangrijk
Als u er zeker van wilt zijn dat een dergelijke back-up wordt voltooid ondanks de aanwezigheid van beschadigde blokken, moet u instellen dat beschadigde blokken worden geneerd tijdens de back-up. Hiervoor gaat u in **Back-upopties** naar **Foutafhandeling** en schakelt u het selectievakje **Beschadigde sectoren negeren** in.

14.6.4 Startvoorwaarden

Deze instellingen voegen meer flexibiliteit toe aan de planner, waardoor het mogelijk is om een back-up uit te voeren met betrekking tot bepaalde voorwaarden. Als er meerdere voorwaarden zijn, moet tegelijkertijd aan al deze voorwaarden worden voldaan om een back-up te kunnen starten. Startvoorwaarden werken niet wanneer een back-up handmatig wordt gestart.

Klik voor toegang tot deze instellingen op **Meer weergeven** wanneer u een beschermingsschema instelt.

Het gedrag van de planner, als aan een (of meer van meerdere voorwaarden) niet wordt voldaan, wordt gedefinieerd door de back-upoptie Startvoorwaarden voor back-up. Voor het geval dat er te lang niet aan de voorwaarden wordt voldaan en het te risicovol wordt om de back-up nog langer uit te stellen, kunt u een tijdinterval instellen waarna de back-up wordt uitgevoerd, of nu wel of niet aan de voorwaarden is voldaan.

De onderstaande tabel toont de startvoorwaarden die beschikbaar zijn voor verschillende gegevens onder Windows, Linux en macOS.

BACK-UP MAKEN VAN	Schijven/volumes of bestanden	Schijven/volumes (virtuele machines)	ESXi-configuratie	Microsoft 365-postvakke	Databases en postvakke	SQL-databases

	(fysieke machines)			n	n uitwisselen	
Gebruiker is niet-actief	Windows	–	–	–	–	–
De host voor de back-uplocatie is beschikbaar	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Gebruikers zijn afgemeld	Windows	–	–	–	–	–
Past in het tijdinterval	Windows, Linux, macOS	Windows, Linux	–	–	–	–
Batterijstroom besparen	Windows	–	–	–	–	–
Niet starten bij verbinding met een datalimiet	Windows	–	–	–	–	–
Niet starten indien verbonden met de volgende wifinetwerken	Windows	–	–	–	–	–
IP-adres van apparaat controleren	Windows	–	–	–	–	–

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 de back-up elke dag om 21:00 uit op de machine, bij voorkeur als de gebruiker niet actief is. Als de gebruiker om 23:00 nog actief is, wordt de back-up toch uitgevoerd.

- Planning: Dagelijks, iedere dag uitvoeren Starten om: **21:00**.
- Voorwaarde: **Gebruiker is niet-actief**.
- Startvoorwaarden voor back-up: **Wachten tot aan de voorwaarden is voldaan**, **De back-up hoe dan ook uitvoeren na 2** uur.

Het resultaat:

(1) Als de gebruiker niet meer actief is om 21:00, begint de back-up om 21:00.

(2) Als de gebruiker inactief wordt tussen 21:00 en 23:00, gaat de back-up van start zodra de gebruiker niet meer actief is.

(3) Als de gebruiker nog actief is om 23:00, begint de back-up om 23:00.

De host voor de back-uplocatie is beschikbaar

'De host voor de back-uplocatie is beschikbaar' betekent dat de machine die de bestemming host voor back-ups beschikbaar is via het netwerk.

Deze voorwaarde is van kracht 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

Er wordt elke werkdag om 21:00 een back-up van de gegevens gemaakt 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 een geplande start op de volgende werkdag.

- Planning: Dagelijks, uitvoeren van maandag tot vrijdag Starten om: **21:00**.
- Voorwaarde: **De host voor de back-uplocatie is beschikbaar**.
- Startvoorwaarden voor back-up: **De geplande back-up overslaan**.

Het resultaat:

(1) Als het 21:00 is en de host beschikbaar is, start de back-up onmiddellijk.

(2) Als het 21:00 is en de host niet beschikbaar is, start de back-up op de volgende werkdag als de host beschikbaar is.

(3) Als de host nooit beschikbaar is op werkdagen om 21:00, start de back-up nooit.

Gebruikers zijn afgemeld

Hiermee is het mogelijk om een back-up in de wachtstand te plaatsen tot alle gebruikers bij Windows zijn afgemeld.

Voorbeeld

De back-up elke vrijdag om 20:00 uitvoeren, bij voorkeur als alle gebruikers afgemeld zijn. Als er om 23.00 nog een gebruiker is aangemeld, wordt de back-up toch uitgevoerd.

- Planning: Wekelijks op vrijdag Starten om: **20:00**.
- 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:

(1) Als alle gebruikers zijn afgemeld om 20:00, begint de back-up om 20:00.

(2) Als de laatste gebruiker zich afmeldt tussen 20:00 en 23:00, gaat de back-up onmiddellijk na de afmelding van start.

(3) Als er nog een gebruiker aangemeld is om 23:00, begint de back-up om 23:00.

Past in het tijdinterval

Hiermee wordt de begintijd van een back-up beperkt 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 een back-up van hun gegevens worden gemaakt. Elke dag om 23:00 uur wordt een back-up gemaakt van de servers van het bedrijf. Dus verdient het de voorkeur vóór die tijd een back-up te maken van alle gebruikersgegevens, om netwerkbandbreedte vrij te maken. Er wordt van uitgegaan dat het maken van een back-up van gebruikersgegevens niet meer dan één uur vergt, dus de uiterste starttijd voor een back-up is 22:00 uur. Als een gebruiker nog steeds is aangemeld binnen het opgegeven tijdinterval of zich op enig ander tijdstip afmeldt, wordt geen back-up van de gegevens van de gebruiker gemaakt en wordt de back-upbewerking dus overgeslagen.

- Gebeurtenis: **Wanneer een gebruiker zich afmeldt bij het systeem**. Geef het gebruikersaccount op: **Elke gebruiker**.
- Voorwaarde: **Past in het tijdinterval** van **16:30** tot **22:00**.
- Startvoorwaarden voor back-up: **De geplande back-up overslaan**.

Het resultaat:

(1) als de gebruiker zich afmeldt tussen 16:30 en 22:00 uur, gaat de back-up onmiddellijk na de afmelding van start.

(2) als de gebruiker zich afmeldt op enig ander tijdstip, wordt de back-up overgeslagen.

Batterijstroom besparen

Verhindert het maken van back-ups als het apparaat (een laptop of tablet) niet is aangesloten op een stroombron. Afhankelijk van de waarde van de back-upoptie Startvoorwaarden voor back-up, wordt de overgeslagen back-up al dan niet gestart wanneer het apparaat wordt aangesloten op een stroombron. De volgende opties zijn beschikbaar:

- **Niet starten bij gebruik van batterijstroom**
  Een back-up start alleen als het apparaat is aangesloten op een stroombron.
- **Starten bij gebruik van batterijstroom als het batterijniveau hoger is dan**
  Een back-up start als het apparaat is aangesloten op een stroombron of als het batterijniveau hoger is dan de opgegeven waarde.

Voorbeeld

Elke werkdag wordt er om 21:00 uur een back-up van de gegevens gemaakt. Als het apparaat niet is aangesloten op een stroombron (bijvoorbeeld wanneer de gebruiker een late bijeenkomst bijwoont), wilt u de back-up mogelijk overslaan om batterijstroom te sparen en wacht u totdat de gebruiker het apparaat aansluit op een stroombron.

- Schema: Dagelijks, uitvoeren van maandag tot vrijdag Starten om: 21:00.
- Voorwaarde: **Batterijstroom besparen**, **Niet starten bij gebruik van batterijstroom**.
- Startvoorwaarden voor back-up: **Wachten tot aan de voorwaarden is voldaan**.

Het resultaat:

(1) Als het 21:00 is en het apparaat is aangesloten op een stroombron, start de back-up onmiddellijk.

(2) Als het 21:00 is en het apparaat batterijstroom gebruikt, start de back-up zodra het apparaat wordt aangesloten op een stroombron.

Niet starten bij verbinding met een datalimiet

Verhindert het maken van back-ups (met inbegrip van back-ups naar een lokale schijf) als het apparaat met internet is verbonden via een verbinding die is ingesteld als verbinding met een 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.

Als aanvullende maatregel om back-ups via mobiele hotspots te verhinderen, wordt automatisch de voorwaarde **Niet starten indien verbonden met de volgende wifinetwerken** ingeschakeld wanneer u de voorwaarde **Niet starten bij verbinding met een datalimiet** inschakelt. De volgende netwerknamen worden standaard opgegeven: 'android', 'telefoon', 'mobiel' en 'modem'. U kunt deze namen uit de lijst verwijderen door te klikken op de X.

Voorbeeld

Elke werkdag wordt er om 21:00 uur een back-up van de gegevens gemaakt. Als het apparaat met internet is verbonden via een verbinding met datalimiet (bijvoorbeeld wanneer de gebruiker op zakenreis is), 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 vrijdag Starten om: 21:00.
- Voorwaarde: **Niet starten bij verbinding met een datalimiet**.
- Startvoorwaarden voor back-up: **De geplande back-up overslaan**.

Het resultaat:

(1) Als het 21:00 is en het apparaat niet met internet is verbonden via een verbinding met datalimiet, start de back-up onmiddellijk.

(2) Als het 21:00 is en het apparaat met internet is verbonden via een verbinding met datalimiet, start de back-up op de volgende werkdag.

(3) Als het apparaat om 21:00 uur op werkdagen altijd met internet is verbonden via een verbinding met datalimiet, start de back-up nooit.

Niet starten indien verbonden met de volgende wifinetwerken

Verhindert het maken van back-ups (met inbegrip van back-ups naar een lokale schijf) als het apparaat is verbonden met een van de opgegeven draadloze netwerken. 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 substring bevatten in hun naam (niet hoofdlettergevoelig). Als u bijvoorbeeld 'telefoon' opgeeft als de netwerknaam, start de back-up niet wanneer het apparaat is verbonden met een van de volgende netwerken: 'Jans telefoon', 'telefoon_wifi" of "mijn_TELEFOON_wifi'

Deze voorwaarde is nuttig om te voorkomen dat back-ups worden gemaakt wanneer het apparaat met internet is verbonden via een mobiele telefoonhotspot.

Als aanvullende maatregel om back-ups via mobiele hotspots te verhinderen, wordt automatisch de voorwaarde **Niet starten indien verbonden met de volgende wifinetwerken** ingeschakeld wanneer u de voorwaarde **Niet starten bij verbinding met een datalimiet** inschakelt. De volgende netwerknamen worden standaard opgegeven: 'android', 'telefoon', 'mobiel' en 'modem'. U kunt deze namen uit de lijst verwijderen door te klikken op de X.

Voorbeeld

Elke werkdag wordt er om 21:00 uur een back-up van de gegevens gemaakt. Als het apparaat met internet is verbonden via een mobiele hotspot (bijvoorbeeld wanneer een laptop is verbonden in de tethering-modus), wilt u de back-up mogelijk overslaan en wacht u tot de geplande start op de volgende werkdag.

- Schema: Dagelijks, uitvoeren van maandag tot vrijdag Starten om: 21:00.
- 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:

(1) Als het 21:00 is en de machine niet is verbonden met het opgegeven netwerk, start de back-up onmiddellijk.

(2) Als het 21:00 is en de machine is verbonden met het opgegeven netwerk, start de back-up op de volgende werkdag.

(3) Als de machine om 21:00 uur op werkdagen altijd met het opgegeven netwerk is verbonden, start de back-up nooit.

IP-adres van apparaat controleren

Verhindert het maken van back-ups (met inbegrip van back-ups naar een lokale schijf) als een of meer IP-adressen van een apparaat ofwel binnen ofwel buiten het opgegeven IP-adresbereik zijn. 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.

Deze voorwaarde is nuttig om kosten voor grote gegevensoverdrachten te vermijden als een gebruiker in het buitenland is. Daarnaast wordt het maken van back-ups via een VPN-verbinding (Virtual Private Network) voorkomen.

Voorbeeld

Elke werkdag wordt er om 21:00 uur een back-up van de gegevens gemaakt. Als het apparaat is verbonden met het bedrijfsnetwerk via een VPN-tunnel (bijvoorbeeld wanneer de gebruiker thuis werkt), wilt u de back-up mogelijk overslaan en wachten totdat de gebruiker het apparaat naar kantoor brengt.

- Schema: Dagelijks, uitvoeren van maandag tot vrijdag Starten om: 21:00.
- Voorwaarde: **IP-adres van apparaat controleren**, **Starten indien buiten IP-bereik**, **Vanaf**: <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:

(1) Als het 21:00 is en het IP-adres van de machine niet in het opgegeven bereik is, start de back-up onmiddellijk.

(2) Als het 21:00 is en het IP-adres van de machine in het opgegeven bereik is, start de back-up zodra het apparaat een IP-adres ontvangt dat geen VPN is.

(3) Als het IP-adres van de machine altijd in het opgegeven bereik is op werkdagen om 21:00, start de back-up nooit.

14.7 Bewaarregels

1. Klik op **Bewaartijd**.
2. Kies bij **Opschonen** een van de volgende opties:
   - **Op leeftijd van de back-up** (standaard)

     Hier kunt u aangeven hoe lang de back-ups die door het beschermingsschema zijn gemaakt, moeten worden bewaard. De bewaarregels moeten standaard afzonderlijk voor elke back-upset[1] worden opgegeven. Als u één regel voor alle back-ups wilt gebruiken, klikt u op **Schakel over naar één regel voor alle back-upsets**.
   - **Op aantal back-ups**

     Hier kunt u opgeven hoeveel back-ups er maximaal worden bewaard.
   - **Op totale grootte van de back-ups**

     Hier kunt u de maximale totale grootte van de back-ups opgeven die worden bewaard.

     Deze instelling is niet beschikbaar voor het back-upschema **Altijd incrementeel (één bestand)** of wanneer u een back-up maakt naar de cloudopslag.
   - **Back-ups voor onbepaalde tijd bewaren**
3. Selecteren wanneer het opschonen start:
   - **Na een back-up** (standaard)

     De bewaarregels worden toegepast nadat een nieuwe back-up is gemaakt.
   - **Vóór een back-up**

     De bewaarregels worden toegepast voordat een nieuwe back-up is gemaakt.

     Deze instelling is niet beschikbaar wanneer een back-up wordt gemaakt van Microsoft SQL Server-clusters of Microsoft Exchange Server-clusters.

[1] 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.

14.7.1 Wat u verder moet weten

- De laatste back-up die is gemaakt door het beschermingsschema, wordt altijd bewaard, zelfs als een schending van een bewaarregel is gedetecteerd. Let op dat u niet de enige bestaande back-up verwijdert door de bewaarregels toe te passen vóór een back-up.
- Wanneer volgens het back-upschema en de back-upindeling elke back-up wordt opgeslagen als een afzonderlijke bestand, kan dit bestand niet worden verwijderd tot totdat de levensduur van alle daarvan afhankelijke (incrementele of differentiële) back-ups verloopt. Dit vereist extra ruimte voor de opslag van back-ups waarvan de verwijdering is uitgesteld. Daarnaast is het mogelijk dat de waarde voor de back-upleeftijd, het opgegeven aantal of de grootte van back-ups worden overschreden.

  Dit gedrag kan worden gewijzigd via de back-upoptie 'Back-up consolideren'.
- De bewaarregels zijn een onderdeel van een beschermingsschema. Ze werken niet meer voor back-ups van een machine zodra het beschermingsschema wordt ingetrokken of verwijderd voor de machine, of als de machine zelf wordt verwijderd van de Cyberbescherming-service. Als u de door het schema gemaakte back-ups niet meer nodig hebt, verwijdert u ze zoals beschreven in 'Back-ups verwijderen'.

14.8 Replicatie

U kunt back-upreplicatie inschakelen om elke back-up naar een tweede locatie te kopiëren onmiddellijk nadat de back-up is gemaakt in de primaire back-upbestemming. Als eerdere back-ups niet zijn gerepliceerd (bijvoorbeeld omdat de netwerkverbinding was verbroken), worden ook alle back-ups gerepliceerd die worden weergegeven na de laatst uitgevoerde replicatie. Als back-upreplicatie halverwege een proces wordt onderbroken, worden de al gerepliceerde gegevens bij de volgende replicatiestart niet opnieuw gerepliceerd, waardoor het tijdverlies kan worden beperkt.

Gerepliceerde back-ups zijn niet afhankelijk van de back-ups die in de originele locatie blijven en vice versa. U kunt gegevens herstellen vanaf elke back-up, zonder dat toegang tot andere locaties nodig is.

14.8.1 Voorbeelden van gebruik

- **Betrouwbaar noodherstel**

  Sla uw back-ups zowel op locatie (voor onmiddellijk herstel) als extern op (hiermee beveiligt u de back-ups tegen fouten in de lokale opslag of natuurrampen).
- **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 uit een snelle opslag te verwijderen, zodat u niet te veel beslag legt op dure opslagruimte.

14.8.2 Ondersteunde locaties

U kunt een back-up repliceren *vanaf* de volgende locaties:

- Een lokale map
- Een netwerkmap
- Secure Zone

U kunt een back-up repliceren *naar* de volgende locaties:

- Een lokale map
- Een netwerkmap
- De cloudopslag

Replicatie van back-ups mogelijk maken

1. Klik in de het gedeelte **Back-up** in het deelvenster voor het beschermingsschema op **Locatie toevoegen**.

   Opmerking
   Het besturingselement Locatie toevoegen is alleen beschikbaar als er ondersteuning is voor replicatie vanaf de laatst geselecteerde back-up- of replicatielocatie.

2. Selecteer in de lijst met beschikbare locaties de locatie waar de back-ups worden gerepliceerd. 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 beschikbare replicatieopties voor de locatie te bekijken.
   - **Prestatie- en back-upvenster**: stel het back-upvenster voor de gekozen locatie in, zoals beschreven in 'Prestatie- en back-upvenster'. Met deze instellingen worden de replicatieprestaties gedefinieerd.
   - **Locatie verwijderen**: verwijder de momenteel geselecteerde replicatielocatie.
   - [Alleen voor de cloudopslaglocatie] **Physical Data Shipping**: sla de initiële back-up op een verwisselbaar opslagapparaat op en verzend de back-up voor upload naar de cloud in plaats van replicatie 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. 239).

     Opmerking
     Deze optie wordt ondersteund met de Cyber Protect-agentversie vanaf release C21.06 of later.

4. [Optioneel] Configureer in de rij **Bewaartijd** de bewaarregels voor de gekozen locatie, zoals beschreven in 'Bewaarregels'.
5. [Optioneel] Herhaal stappen 1-4 als u locaties wilt toevoegen voor replicatie van de back-ups. U kunt maximaal vier replicatielocaties configureren, zolang replicatie vanaf de eerder geselecteerde back-up- of replicatielocatie wordt ondersteund.

14.9 Versleuteling

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.

Waarschuwing!
Er is geen manier om versleutelde back-ups te herstellen als u het wachtwoord verliest of vergeet.

14.9.1 Versleuteling in een beschermingsschema

Als u versleuteling wilt inschakelen, geeft u de versleutelingsinstellingen op wanneer u een beschermingsschema maakt. Wanneer een beschermingsschema is toegepast, kunnen de versleutelingsinstellingen niet meer worden gewijzigd. Maak een nieuw beschermingsschema om andere versleutelingsinstellingen te gebruiken.

U kunt geen versleutelingswachtwoord instellen in een beschermingsschema voor accounts in de modus Verbeterde beveiliging. U moet dit wachtwoord lokaal instellen op het beschermde apparaat.

Versleutelingsinstellingen opgeven in een beschermingsschema

1. Ga naar het deelvenster voor het beschermingsschema in de back-upmodule en schakel de optie **Versleuteling** in.
2. Geef het versleutelingswachtwoord op en bevestig dit.
3. Selecteer een van de volgende versleutelingsalgoritmen:
   - **AES 128** – de back-ups worden versleuteld met het AES-algoritme (Advanced Encryption Standard) met een 128-bits sleutel.
   - **AES 192** – de back-ups worden versleuteld met het AES-algoritme met een 192-bits sleutel.
   - **AES 256** – de back-ups worden versleuteld met het AES-algoritme met een 256-bits sleutel.
4. Klik op **OK**.

14.9.2 Versleuteling als machine-eigenschap

U kunt de versleuteling van back-ups afdwingen of een uniek versleutelingswachtwoord instellen voor een machine, ongeacht de instellingen in het beschermingsschema. De back-ups worden versleuteld met het AES-algoritme met een 256-bits sleutel.

Als u de versleutelingsinstellingen opslaat op een machine, heeft dit gevolgen voor de beschermingsschema's:

- **Beschermingsschema's die al worden toegepast op de machine.** Als de versleutelingsinstellingen in een beschermingsschema anders zijn, mislukken de back-ups.
- **Beschermingsschema's die later op de machine worden toegepast.** De versleutelingsinstellingen die zijn opgeslagen op een machine, overschrijven de versleutelingsinstellingen in een beschermingsschema. Back-ups worden versleuteld, zelfs als versleuteling is uitgeschakeld in de instellingen van het beschermingsschema.

Deze optie kan ook worden gebruikt op een machine met Agent voor VMware. Wees voorzichtig als er meer dan een Agent voor VMware is verbonden met dezelfde vCenter-server. U moet dezelfde versleutelingsinstellingen gebruiken voor alle agenten, want de taken worden verdeeld tussen de verschillende agenten.

Belangrijk
Wijzig de versleutelingsinstellingen op een machine alleen voordat er back-ups worden gemaakt voor het beschermingsschema. Als u de versleutelingsinstellingen later wijzigt, zal dit beschermingsschema mislukken en hebt u een nieuw beschermingsschema nodig om back-ups te blijven maken van deze machine.

Nadat de encryptie-instellingen zijn opgeslagen, kunnen ze worden gewijzigd of gereset zoals hieronder beschreven.

De versleutelingsinstellingen opslaan op een machine

1. Meld u aan als beheerder (in Windows) of rootgebruiker (in Linux).
2. Voer het volgende script uit:
   - In Windows: `<installatiepad>`**\PyShell\bin\acropsh.exe -m manage_creds --set-password** `<versleutelingswachtwoord>`

     `<installatiepad>` staat hier voor het installatiepad van de beveiligingsagent. Het standaardpad is **%ProgramFiles%\BackupClient**.
   - In Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<versleutelingswachtwoord>`

Versleutelingsinstellingen opnieuw instellen op een machine

1. Meld u aan als beheerder (in Windows) of rootgebruiker (in Linux).
2. Voer het volgende script uit:
   - In Windows: `<installatiepad>`**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     `<installatiepad>` staat hier voor het installatiepad van de beveiligingsagent. Het standaardpad is **%ProgramFiles%\BackupClient**.
   - In Linux: **/usr/sbin/acropsh -m manage_creds --reset**

De versleutelingsinstellingen wijzigen met Cyber Protect Monitor

1. Meld u aan als beheerder in Windows of macOS.
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. Voer een van de volgende handelingen uit:
   - Selecteer **Een specifiek wachtwoord instellen voor deze machine**. Geef het versleutelingswachtwoord op en bevestig dit.
   - Selecteer **Versleutelingsinstellingen gebruiken die zijn opgegeven in het beschermingsschema**.
6. Klik op **OK**.

14.9.3 Hoe versleuteling werkt

Het cryptografische AES-algoritme werkt in de CBC-modus (Cipher-block chaining) en gebruikt een willekeurig gegenereerde sleutel met een door de gebruiker gedefinieerd formaat van 128, 192 of 256 bits. Hoe groter het formaat van de sleutel is, hoe langer het duurt voordat het programma de back-ups versleutelt en hoe veiliger uw gegevens zijn.

De versleutelingssleutel wordt dan versleuteld met AES-256, waarbij een SHA-256 hash van het wachtwoord als sleutel wordt gebruikt. Het wachtwoord zelf wordt nergens op de schijf of in de back-ups opgeslagen: voor verificatie wordt de wachtwoordhash gebruikt. Met deze beveiliging op twee niveaus worden de back-upgegevens beschermd tegen niet-geautoriseerde toegang, maar een verloren wachtwoord kan niet worden hersteld.

14.10 Notarisatie

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

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

14.10.1 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.

14.10.2 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.

14.11 Handmatig een back-up starten

1. Selecteer een machine waarop minimaal één beschermingsschema wordt toegepast.
2. Klik op **Beschermen**.
3. Als er meerdere beschermingsschema's worden toegepast, selecteert u het gewenste beschermingsschema.
4. Voer een van de volgende handelingen uit:
   - Klik op **Nu uitvoeren**. Er wordt een incrementele back-up gemaakt.
   - Als het back-upschema verschillende back-upmethoden bevat, kunt u de methode kiezen die u wilt gebruiken. Klik op de pijl op de knop **Nu uitvoeren** om een **volledige, incrementele** of **differentiële** back-up uit te voeren.

De eerste back-up die wordt gemaakt met een beschermingsschema is altijd een volledige back-up.

De voortgang van de back-upbewerking voor de machine wordt weergegeven in de kolom **Status**.

14.12 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 serviceconsole.
   - Als u de standaardwaarde voor een eenheid wilt wijzigen, meldt u zich als beheerder van de eenheid aan bij de serviceconsole.
   - Als u de standaardwaarde voor uzelf wilt wijzigen, meldt u zich bij de serviceconsole 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**.

14.13 Back-upopties

Als u de back-upopties wilt wijzigen, klikt u op **Wijzigen** naast **Back-upopties** in de back-upmodule van het beschermingsschema.

14.13.1 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	+	+	-	+	+	-	-	-	-	-
Prestatie- en back-upvenster	+	+	+	+	+	+	+	+	+	+
Physical Data Shipping	+	+	+	+	+	+	+	+	+	-
Aangepaste opdrachten	+	+	+	+	+	+	+	+	+	+
Aangepaste opdrachten voor gegevensvastlegging	+	+	+	+	+	+	-	-	-	+
Plannen										
Starttijden binnen een tijdvenster distribueren	+	+	+	+	+	+	+	+	+	+
Gelijktijdig uitvoeren van aantal 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	+	-	-	+	-	-	+	+	-	+

14.13.2 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.

14.13.3 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.

14.13.4 Naam van back-upbestand

Met deze optie definieert u de namen van de back-upbestanden die zijn gemaakt door het beschermingsschema.

Deze namen kunnen worden bekeken in een bestandsmanager 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 (de 'naam van back-upbestand') opgeven wanneer u een beschermingsschema 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 wijzigt, zal de volgende back-up een volledige back-up zijn, tenzij u een bestandsnaam van een bestaande back-up van dezelfde machine opgeeft. Als dit laatste van toepassing is, wordt een volledige, incrementele of differentiële back-up gemaakt volgens het beschermingsschema.

Het is mogelijk namen van back-upbestanden in te stellen voor locaties die niet toegankelijk zijn voor bestandsbeheer (zoals de cloudopslag). Dat kan zinvol zijn als u de aangepaste namen wilt weergeven op het tabblad **Back-upopslag**.

Waar kan ik de namen van back-upbestanden zien?

Selecteer het tabblad **Back-upopslag** en vervolgens de groep back-ups.

- 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**.

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**).

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 `[Machinenaam]-[Schema-id]-[Unieke id]A`.

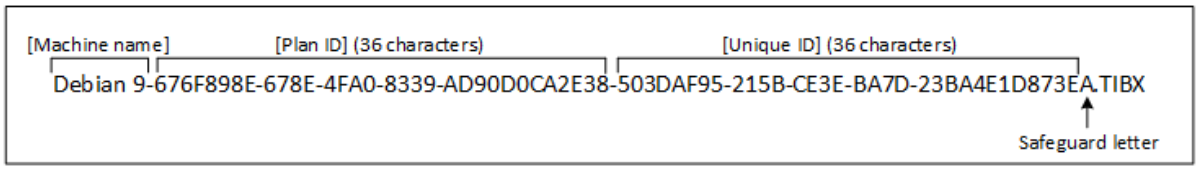
De standaardnaam voor back-ups van Exchange-postvakken en Microsoft 365-postvakken die door een lokale Agent voor Microsoft 365 zijn gemaakt, is `[Postvak-id]_postvak_[Schema-id]A`.

De standaardnaam voor back-ups van cloudtoepassingen die door cloudagenten worden gemaakt, is `[Resourcenaam]_[Resourcetype]_[Resource-id]_[Schema-id]A`.

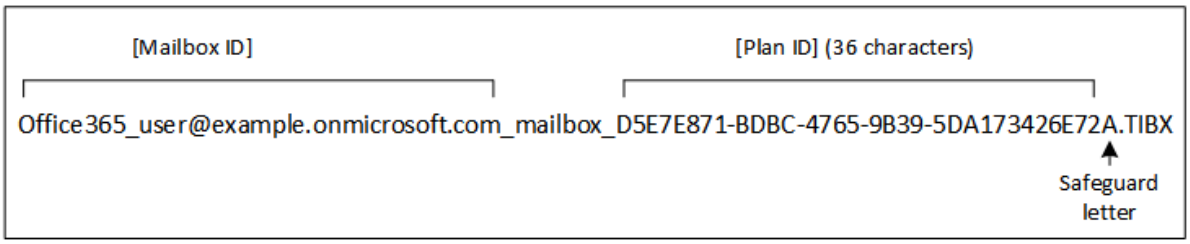
De standaardnaam bestaat uit de volgende variabelen:

- `[Machinenaam]` Deze variabele wordt vervangen door de naam van de machine (dezelfde naam als die wordt weergegeven in de serviceconsole).
- `[Schema-id, Schema-id]` Deze variabelen worden vervangen door de unieke id van het beschermingsschema. Deze waarde verandert niet als de naam van het schema wordt gewijzigd.
- `[Unieke 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.
- `[Postvak-id]` Deze variabele wordt vervangen door de principal-naam van de gebruiker van het postvak (UPN).
- `[Resourcenaam]` 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.
- `[Resourcetype]` Deze variabele wordt vervangen door het type van de cloudgegevensbron, zoals `postvak`, `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 `MijnBack-up`, 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 `[Schemanaam]`, die wordt vervangen door de naam van het beschermingsschema.
- De variabele `[Type virtualisatieserver]`, 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: `[Machinenaam]`, `[Unieke id`, `[Postvak-id]`, `[Resourcenaam]` of `[Resource-id]`.

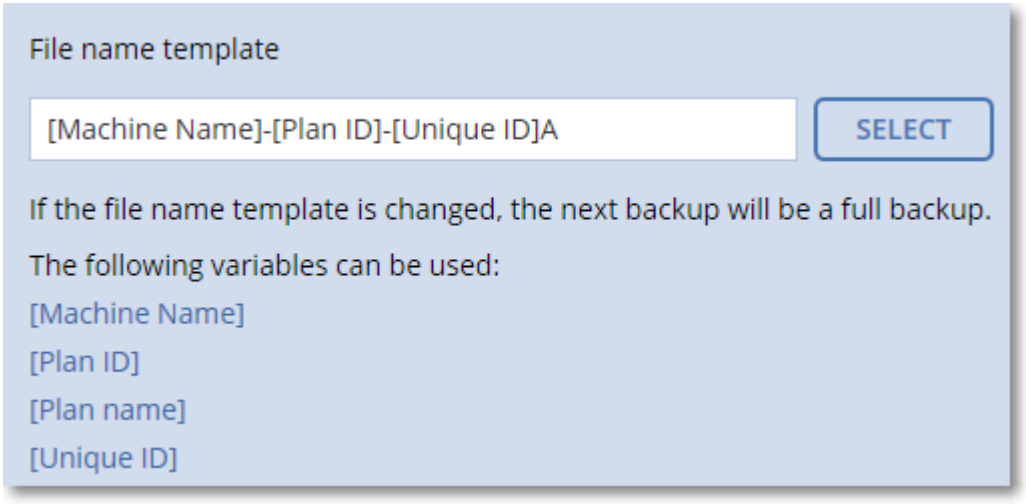
Voorbeelden van gebruik

- **Gebruiksvriendelijke bestandsnamen weergeven**

  U wilt eenvoudig onderscheid kunnen maken tussen back-ups wanneer u met bestandsbeheer door de back-uplocatie bladert.
- **Een bestaande reeks back-ups voortzetten**

  Stel dat een beschermingsschema wordt toegepast op één machine en dat u deze machine moet verwijderen uit de serviceconsole of dat u de agent met de bijbehorende configuratie-instellingen moet verwijderen. Wanneer de machine opnieuw is toegevoegd of de agent opnieuw is geïnstalleerd, kunt het beschermingsschema verder laten gaan bij dezelfde back-up of back-upreeks. Als u dit wilt doen, gaat u naar deze optie, klikt u op **Selecteren** en selecteert u de gewenste back-up.

  Met de knop **Selecteren** worden de back-ups weergegeven die te vinden zijn op de locatie die is geselecteerd in het gedeelte **Locatie van back-up** van het deelvenster voor het back-upschema. Het is niet mogelijk om buiten deze locatie te bladeren.



Opmerking
De knop **Selecteren** is alleen beschikbaar voor beschermingsschema's die zijn gemaakt voor en worden toegepast op een enkel apparaat.

14.13.5 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 voor snellere back-ups en herstel. 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 met 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.

14.13.6 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 volgens het

beschermingsschema, meteen gevalideerd. Deze bewerking wordt uitgevoerd door de beveiligingsagent.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

Bij validatie wordt een controlesom berekend voor elk gegevensblok dat kan worden hersteld vanuit de back-up. 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.

Het validatieproces vergt aanzienlijk wat tijd, zelfs voor incrementele en differentiële back-ups, die minder groot zijn. Dit komt omdat met de bewerking niet alleen de gegevens worden gecontroleerd die zich fysiek in de back-up bevinden, maar alle gegevens die kunnen worden hersteld wanneer de back-up wordt geselecteerd. Hiervoor is toegang nodig tot eerder gemaakte back-ups.

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. Als u een back-up maakt van het besturingssysteem, wordt aanbevolen om met de opstartmedia een test van het herstel uit te voeren naar een reserveschijf of om een virtuele machine uit te voeren vanaf de back-up in de ESXi- of Hyper-V-omgeving.

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.

14.13.7 Changed Block Tracking (CBT, Gewijzigde blokken bijhouden)

Deze optie is effectief voor back-ups op schijfniveau van virtuele machines en van fysieke machines met Windows. Deze optie is ook effectief voor back-ups van Microsoft SQL Server-databases en 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.

14.13.8 Clusterback-upmodus

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

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.

14.13.9 Compressieniveau

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**.

Een hoger compressieniveau houdt in dat het back-upproces langer duurt, 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.

14.13.10 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: 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 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.

Cloudopslag

Als de cloudopslag is geselecteerd als back-upbestemming, wordt de waarde van de optie automatisch ingesteld op **Ingeschakeld**. **Aantal pogingen: 300**. **Interval tussen pogingen: 30 seconden.**

In dit geval is het werkelijke aantal pogingen onbeperkt, maar de time-out vóór de mislukte back-up wordt als volgt berekend: (300 seconden + **Interval tussen pogingen**) * (**Aantal pogingen** + 1).

Voorbeelden:

- Met de standaardwaarden mislukt de back-up na (300 seconden + 30 seconden) * (300 + 1) = 99330 seconden ofwel ~ 27,6 uur.
- Als u **Aantal pogingen** instelt op 1 en **Interval tussen pogingen** op 1 seconde, mislukt de back-up na (300 seconden + 1 seconde) * (1 + 1) = 602 seconden ofwel ~ 10 minuten.

Als de berekende time-out langer is dan 30 minuten en de gegevensoverdracht nog niet is gestart, wordt de werkelijke time-out ingesteld op 30 minuten.

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.

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.

14.13.11 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.

14.13.12 Bestandsfilters

Met behulp van bestandsfilters wordt gedefinieerd welke bestanden en mappen tijdens het back-upproces worden overgeslagen.

Bestandsfilters zijn beschikbaar voor back-ups op schijfniveau en back-ups op bestandsniveau en voor back-ups van volledige machines, tenzij anders vermeld.

Bestandsfilters inschakelen

1. Selecteer de gegevens waarvan u een back-up wilt maken.
2. Klik op **Wijzigen** naast **Back-upopties**.
3. Selecteer **Bestandsfilters**.
4. Gebruik een van de hieronder beschreven opties.

Bestanden uitsluiten die aan specifieke criteria voldoen

Er zijn twee opties die omgekeerd werken.

- **Alleen back-up maken van bestanden die voldoen aan de volgende criteria**
  Voorbeeld: Als u een back-up van de hele machine maakt en in de filtercriteria **C:\File.exe** opgeeft, wordt er alleen een back-up van dit bestand gemaakt.

  Opmerking
  Dit filter werkt niet voor back-ups op bestandsniveau als **Versie 11** is geselecteerd in **Back-upindeling** en de back-upbestemming NIET de cloudopslag is.

- **Geen back-up maken van bestanden die voldoen aan de volgende criteria**
  Voorbeeld: Als u een back-up van de hele machine maakt en in de filtercriteria **C:\File.exe** opgeeft, wordt alleen dit bestand overgeslagen.

U kunt beide opties ook tegelijkertijd gebruiken. De laatste optie overschrijft de eerste. Oftewel, als u in beide velden **C:\File.exe** opgeeft, wordt dit bestand tijdens het back-upproces overgeslagen.

Criteria

- **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).
  Zowel in Windows als in Linux/macOS kunt u een slash in het bestands- of mappad gebruiken (zoals in **C:/Temp/File.tmp**). In Windows kunt u ook de traditionele backslash gebruiken (zoals in **C:\Temp\File.tmp**).
- **Naam**
  Geef de naam van het bestand of de map op, zoals **Document.txt**. Alle bestanden en mappen met die naam worden geselecteerd.

De criteria zijn *niet* hoofdlettergevoelig. Als u bijvoorbeeld **C:\Temp** opgeeft, selecteert u ook **C:\TEMP**, **C:\temp**, enzovoort.

U kunt een of meer jokertekens (*, ** en ?) in het criterium gebruiken. Deze tekens kunnen zowel in het volledige pad als de naam van het bestand of de map worden gebruikt.

Het sterretje (*) staat voor nul of meer tekens in een bestandsnaam. Het criterium **Doc*.txt** komt overeen met bestanden als **Doc.txt** en **Document.txt**.

[Alleen voor back-ups in de indeling **Versie 12**]Het dubbele sterretje (**) staat voor nul of meer tekens in een bestandsnaam en bestandspad, met inbegrip van de slash. Het criterium ****/Docs/**.txt** komt bijvoorbeeld overeen met alle txt-bestanden in alle submappen van alle mappen met de naam **Docs**.

Het vraagteken (?) staat voor één teken in een bestandsnaam. Het criterium **Doc?.txt** komt overeen met bestanden als **Doc1.txt** en **Docs.txt**, maar niet met de bestanden **Doc.txt** of **Doc11.txt**

Verborgen bestanden en mappen uitsluiten

Schakel dit selectievakje in om bestanden en mappen over te slaan die het kenmerk **Hidden** hebben (voor bestandssystemen die worden ondersteund door Windows) of die beginnen met een punt (.) (voor bestandssystemen in Linux, zoals Ext2 en Ext3). Als een map verborgen is, wordt alle inhoud (inclusief bestanden die niet verborgen zijn) uitgesloten.

Systeembestanden en -mappen uitsluiten

Deze optie is alleen effectief voor bestandssystemen die niet door Windows worden ondersteund. Schakel dit selectievakje in om bestanden en mappen met het kenmerk **System** over te slaan. Als een map het kenmerk **System** heeft, wordt alle inhoud (inclusief bestanden zonder het kenmerk **System**) uitgesloten.

Opmerking
U kunt de bestands- of mapkenmerken weergeven in de bestands-/mapeigenschappen of met de opdracht attrib. Raadpleeg de Help en ondersteuning in Windows voor meer informatie.

14.13.13 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.

14.13.14 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. Ga in de serviceconsole naar **Apparaten** > **Alle apparaten**. Indien gewenst, kunt u het beschermingsschema ook maken vanaf het tabblad **Schema's**.
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.

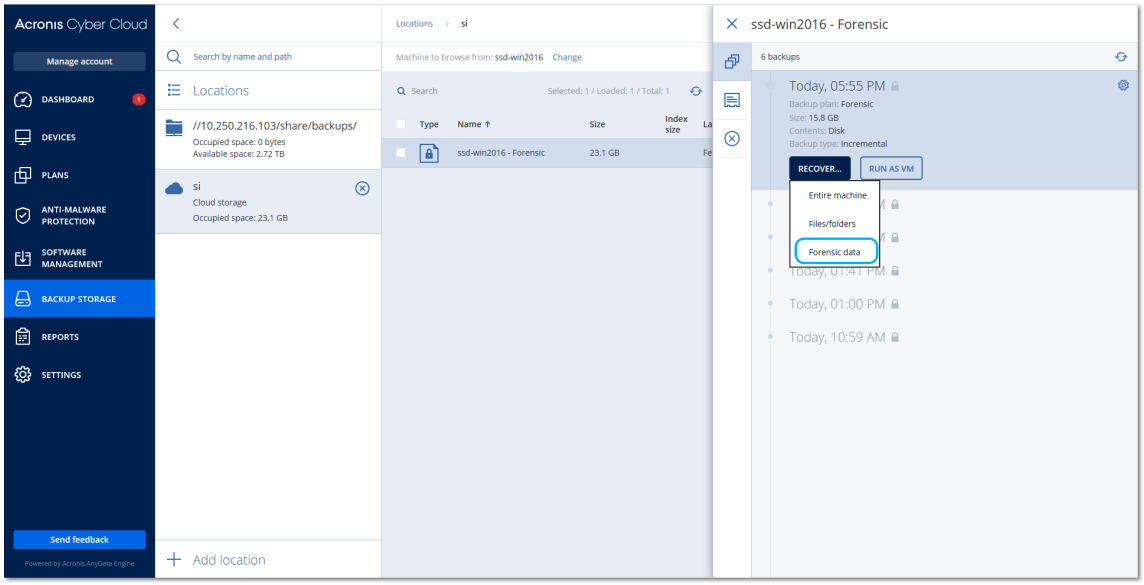
   Opmerking
   Volledige geheugendump kan gevoelige gegevens bevatten, zoals wachtwoorden.

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 **Dashboard** > **Activiteiten** en controleer of de back-up met forensische gegevens is gemaakt.

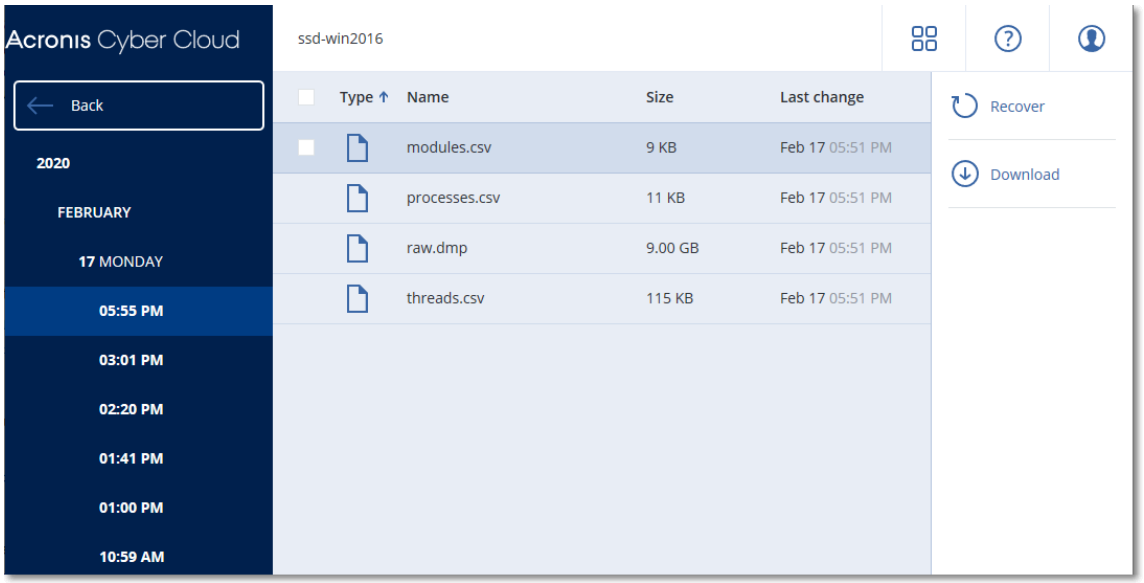
De back-ups zullen dan forensische gegevens bevatten en u kunt deze ophalen en analyseren. Back-ups met forensische gegevens worden gemarkeerd, zodat u hierop kunt filteren tussen andere back-ups in **Back-upopslag** > **Locaties** en de optie **Alleen met forensische gegevens**.

Hoe kan ik forensische gegevens ophalen uit een back-up?

1. Ga in de serviceconsole 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

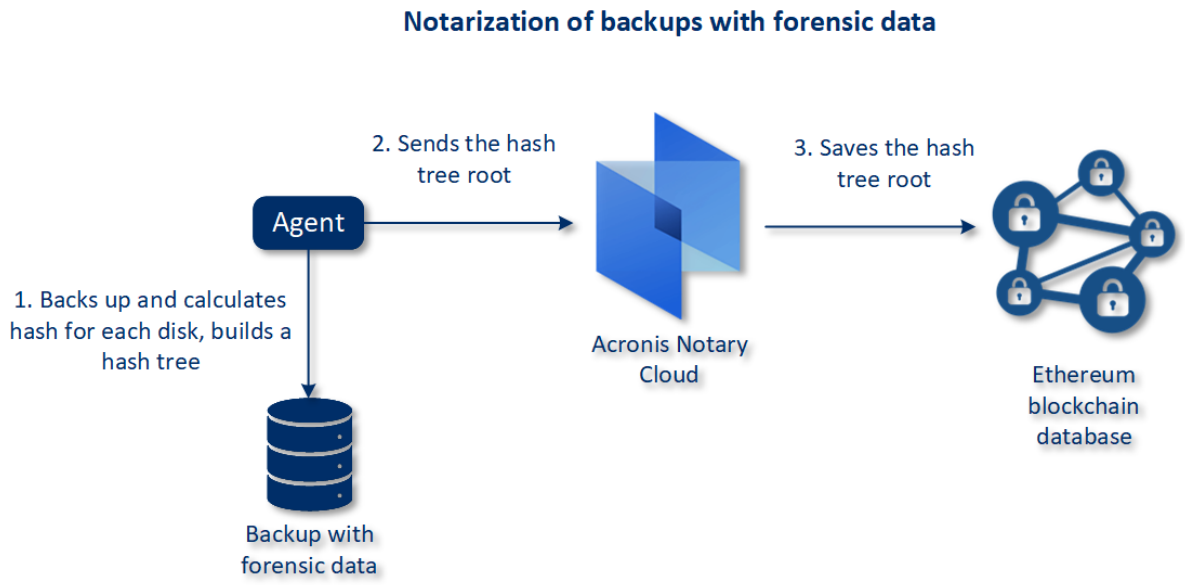
Met notarisatie kunt u bewijzen dat een schijf met forensische gegevens authentiek en ongewijzigd is sinds hiervan een back-up is gemaakt.

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 Cyberbescherming, `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 de SHA-256-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 webconsole. 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 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 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=WACHT	Een versleutelingswachtwoord voor uw back-up. Als de back-up niet is versleuteld, laat u deze waarde leeg.

WOORD	

--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%`

14.13.15 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.

14.13.16 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-back wordt sneller gemaakt en er is geen niet-toegewezen ruimte voor de volumegroep vereist. Het wordt daarom aangeraden 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.

14.13.17 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**.

14.13.18 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.

14.13.19 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.

U kunt deze optie afzonderlijk configureren voor elke locatie die is opgegeven in het beschermingsschema. Als u deze optie wilt configureren voor een replicatielocatie, klikt u op het tandwielpictogram naast de naam van de locatie en vervolgens op **Prestatie- en back-upvenster**.

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** (komt in Windows overeen met **Lager dan normaal**).
- Uitvoersnelheid: **Onbeperkt.**

Wanneer deze optie is ingeschakeld, worden geplande back-ups toegestaan of geblokkeerd op basis van de prestatieparameters die voor het huidige uur zijn opgegeven. Wanneer back-ups zijn geblokkeerd, wordt een back-upproces aan het begin van een uur automatisch gestopt en wordt een waarschuwing gegenereerd.

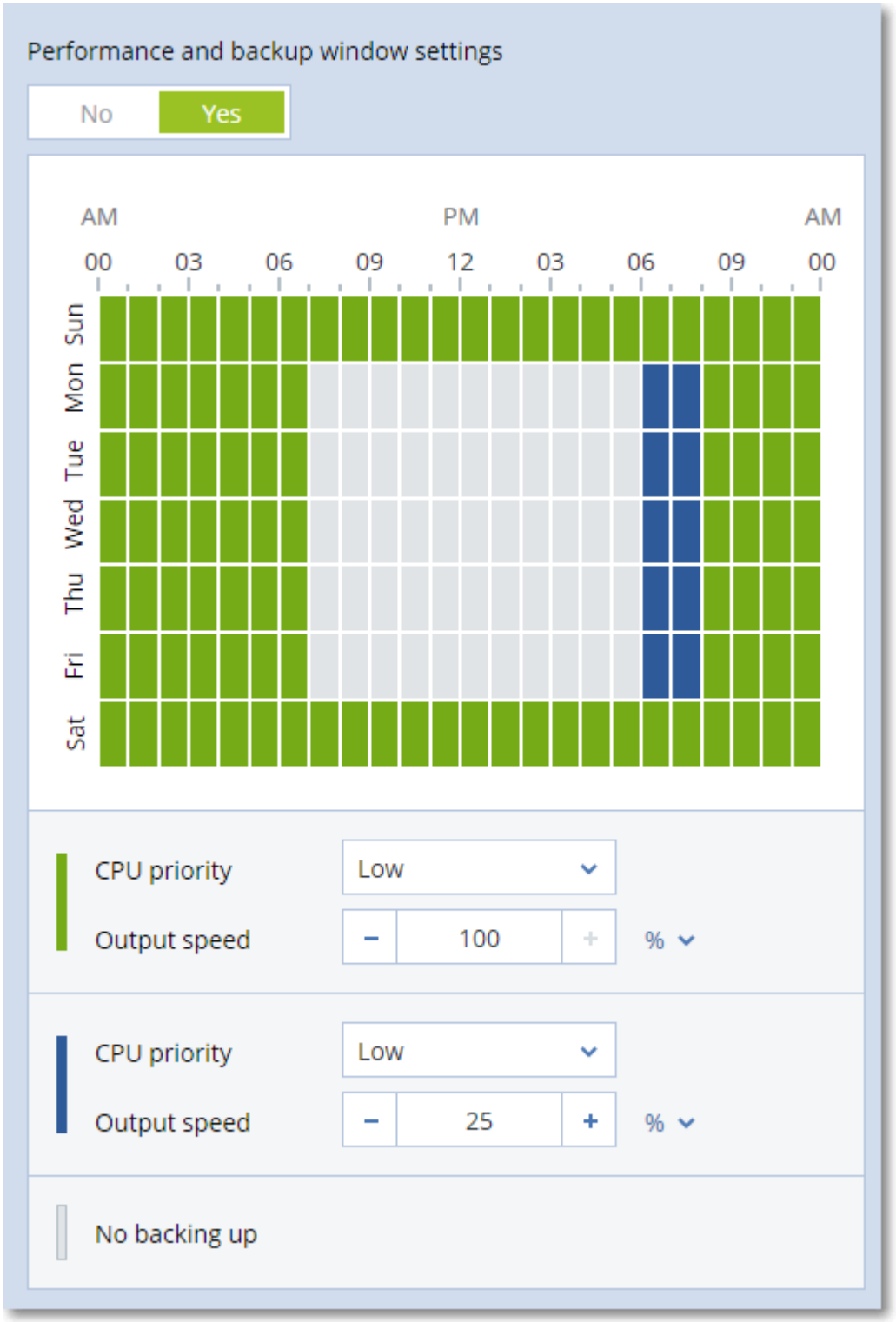
Zelfs als geplande back-ups zijn geblokkeerd, kan een back-up handmatig worden gestart. In dit geval worden de prestatieparameters gebruikt van het meest recente uur waarop back-ups waren toegestaan.

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.



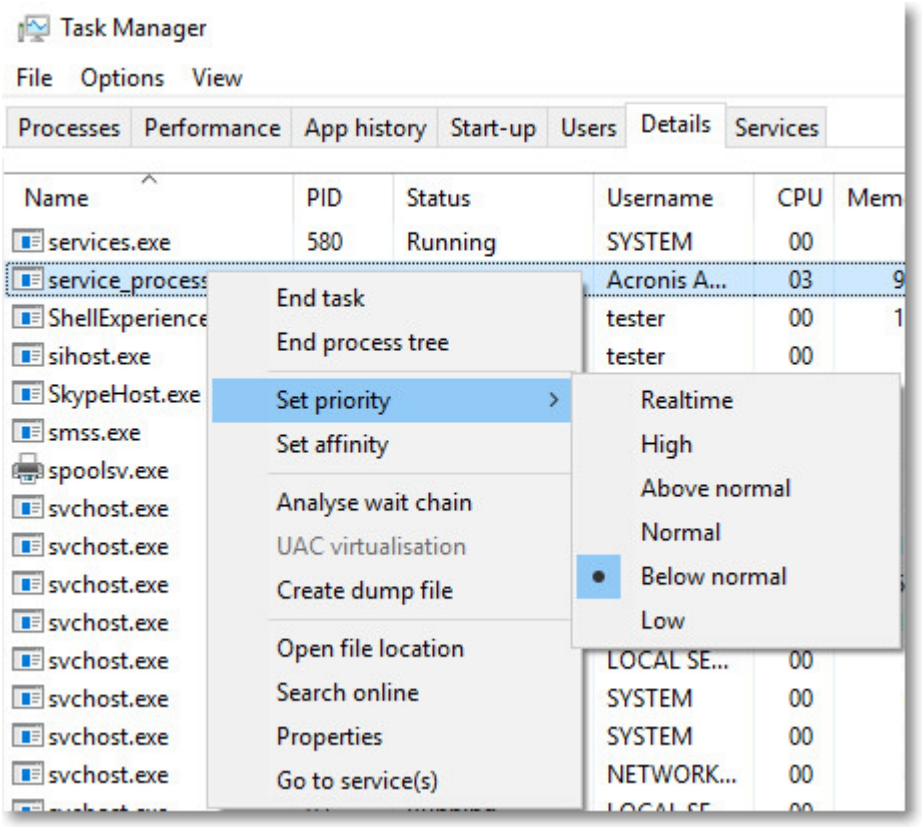
CPU-prioriteit

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 OS X instellen.



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).

14.13.20 Physical Data Shipping

Deze optie is beschikbaar als de back-up- of herstelbestemming 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 Cyber Protect-agentversie vanaf release C21.06 of later.

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.

14.13.21 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**.

14.13.22 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	Opdracht na back-up

Als de optie Volume Shadow Copy Service is ingeschakeld, worden de uitvoering van de opdrachten en de Microsoft VSS-acties in de volgende volgorde 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	Ingeschakeld	Ingeschakeld	Uitgeschakeld	Uitgeschakeld

opdracht volledig is uitgevoerd				
Resultaat				
	Vooraf ingesteld Leg de gegevens alleen vast wanneer de opdracht is uitgevoerd. Keur de back-up af als het uitvoeren van de opdracht mislukt.	Leg de gegevens vast wanneer de opdracht is uitgevoerd, ongeacht het resultaat van de uitvoering.	N.v.t.	Leg de gegevens vast gelijktijdig met 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 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	Ingeschakeld	Uitgeschakeld	Ingeschakeld	Uitgeschakeld

het uitvoeren van de opdracht mislukt*				
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.

14.13.23 Plannen

Met deze optie definieert u of back-ups volgens de planning worden gestart of met een vertraging, en van hoeveel virtuele machines gelijktijdig een back-up wordt gemaakt.

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**

  Deze optie is alleen beschikbaar wanneer een beschermingsschema wordt toegepast op meerdere virtuele machines. Met deze optie definieert u het aantal virtuele machines waarvan gelijktijdig een back-up kan worden gemaakt door een agent tijdens de uitvoering van het opgegeven beschermingsschema.

  Als een agent volgens het beschermingsschema moet beginnen met back-ups van meerdere machines tegelijk, worden er twee machines gekozen. (De back-upprestaties worden geoptimaliseerd doordat de agent probeert machines in verschillende opslaglocaties te vergelijken.) Zodra een van de twee back-ups is voltooid, kiest de agent de derde machine, enzovoort.

  U kunt wijzigen van hoeveel virtuele machines een agent gelijktijdig een back-up moet maken. De maximumwaarde is 10. Als de agent echter meerdere beschermingsschema's uitvoert die elkaar in de tijd overlappen, wordt de som berekend van de aantallen die zijn opgegeven in de betreffende opties. U kunt beperkingen instellen voor het totale aantal virtuele machines waarvan gelijktijdig een back-up kan worden gemaakt door een agent, ongeacht het aantal beschermingsschema's dat wordt uitgevoerd.

  Back-ups van fysieke machines beginnen exact zoals gepland.

14.13.24 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.

14.13.25 Splitsen

Met deze optie selecteert u de methode voor het opsplitsen van grote back-ups in kleinere bestanden.

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.

14.13.26 Taakfout afhandelen

Deze optie bepaalt hoe het programma reageert wanneer een geplande uitvoering van een beschermingsschema mislukt. 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 eerste gebeurt.

De vooraf ingestelde waarde is: **Uitgeschakeld**.

14.13.27 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' voor meer informatie over 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.

14.13.28 Volume Shadow Copy Service (VSS)

Deze optie is alleen effectief voor Windows-besturingssystemen.

Met deze optie definieert u of een provider van VSS (Volume Shadow Copy Service) een melding moet versturen aan VSS-compatibele applicaties wanneer een back-up wordt gestart. Hiermee 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 vooraf ingestelde waarde is: **Ingeschakeld**. **Automatisch 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).

Schakel deze optie uit als uw database niet compatibel is met VSS. Momentopnamen worden sneller gemaakt, maar de gegevensconsistentie van applicaties met transacties die niet zijn voltooid wanneer een momentopname wordt gemaakt, kan niet worden gegarandeerd. U kunt Aangepaste opdrachten voor gegevensvastlegging gebruiken als u er zeker van wilt zijn dat 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
Als deze optie is ingeschakeld, wordt er 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.

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.

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.

14.13.29 Volume Shadow Copy Service (VSS) voor virtuele machines

Met deze optie definieert u of stilgelegde momentopnamen worden gemaakt van virtuele machines. 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.

De vooraf ingestelde waarde is: **Ingeschakeld**.

Als deze optie is ingeschakeld, worden de transacties van alle VSS-applicaties in een virtuele machine voltooid voordat de momentopname wordt gemaakt. Als een stilgelegde momentopname mislukt na het aantal pogingen dat is opgegeven in de optie 'Foutafhandeling' en applicatieback-up is uitgeschakeld, dan wordt een niet-stilgelegde momentopname gemaakt. Als applicatieback-up is ingeschakeld, mislukt de back-up.

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 die u mogelijk hebt gebruikt voor back-ups van de virtuele machine. Zie "Automatisch uitvoeren van scripts voorafgaand aan stilzetten en na afloop van reactivering" (p. 396) voor meer informatie over deze scripts.

Als deze optie is uitgeschakeld, wordt een niet-stilgelegde momentopname gemaakt. Er wordt een back-up gemaakt van de virtuele machine met een crashconsistente status.

Opmerking
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.

14.13.30 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**.

14.13.31 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**.

14.14 Herstel

14.14.1 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
Herstel via de webinterface is niet beschikbaar voor tenants in de modus Verbeterde beveiliging.

Te herstellen	Herstelmethode
Fysieke machine (Windows of Linux)	Webinterface Opstartmedia
Fysieke machine (Mac)	Opstartmedia
Virtuele machine (VMware, Hyper-V, Red Hat Virtualization (oVirt) of Scale Computing HC3)	Webinterface Opstartmedia
Virtuele machine of container (Virtuozzo, Virtuozzo Hybrid Server of Virtuozzo Hybrid Infrastructure)	Webinterface
ESXi-configuratie	Opstartmedia
Bestanden/mappen	Webinterface Bestanden downloaden uit de cloudopslag Opstartmedia Bestanden uitpakken vanuit lokale back-ups
Systeemstatus	Webinterface
SQL-databases	Webinterface
Exchange-databases	Webinterface
Exchange-postvakken	Webinterface
Websites	Webinterface
Microsoft 365	
Postvakken (lokale agent voor Microsoft 365)	Webinterface
Postvakken (cloudagent voor Microsoft 365)	Webinterface
Openbare mappen	Webinterface
OneDrive-bestanden	Webinterface
SharePoint Online-gegevens	Webinterface

Google Workspace	
Postvakken	Webinterface
Google Drive-bestanden	Webinterface
Gedeelde Drive-bestanden	Webinterface

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.

14.14.2 Veilig herstel

Een back-up van een OS-image kan malware bevatten die een machine na herstel opnieuw kan infecteren.

Met de functie voor veilig herstel kunt u herhaling van infecties voorkomen door gebruik te maken van de geïntegreerde antimalwarescan en malwareverwijdering tijdens het herstelproces.

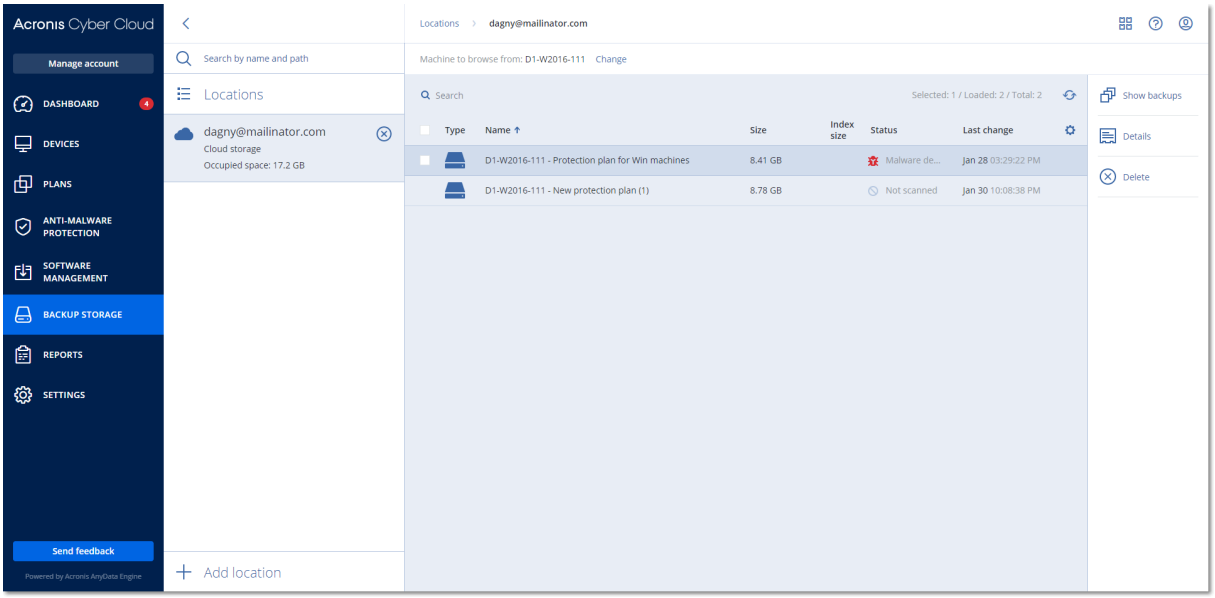
Beperkingen:

- Veilig herstel wordt alleen ondersteund voor fysieke of virtuele Windows-machines waarop Agent voor Windows is geïnstalleerd.
- U kunt kiezen uit de ondersteunde back-uptypen 'Volledige machine' of 'Schijven/volumes'.
- Veilig herstel wordt alleen ondersteund voor de volumes met NTFS-bestandssysteem. Niet-NTFS-partities worden hersteld zonder antimalwarescans.
- Veilig herstel wordt niet ondersteund voor CDP-back-ups. De machine wordt hersteld op basis van de meest recente reguliere back-up zonder de gegevens in de CDP-back-up. Als u de CDP-gegevens wilt herstellen, start u een herstelbewerking voor **Bestanden/mappen**.

Zo werkt het

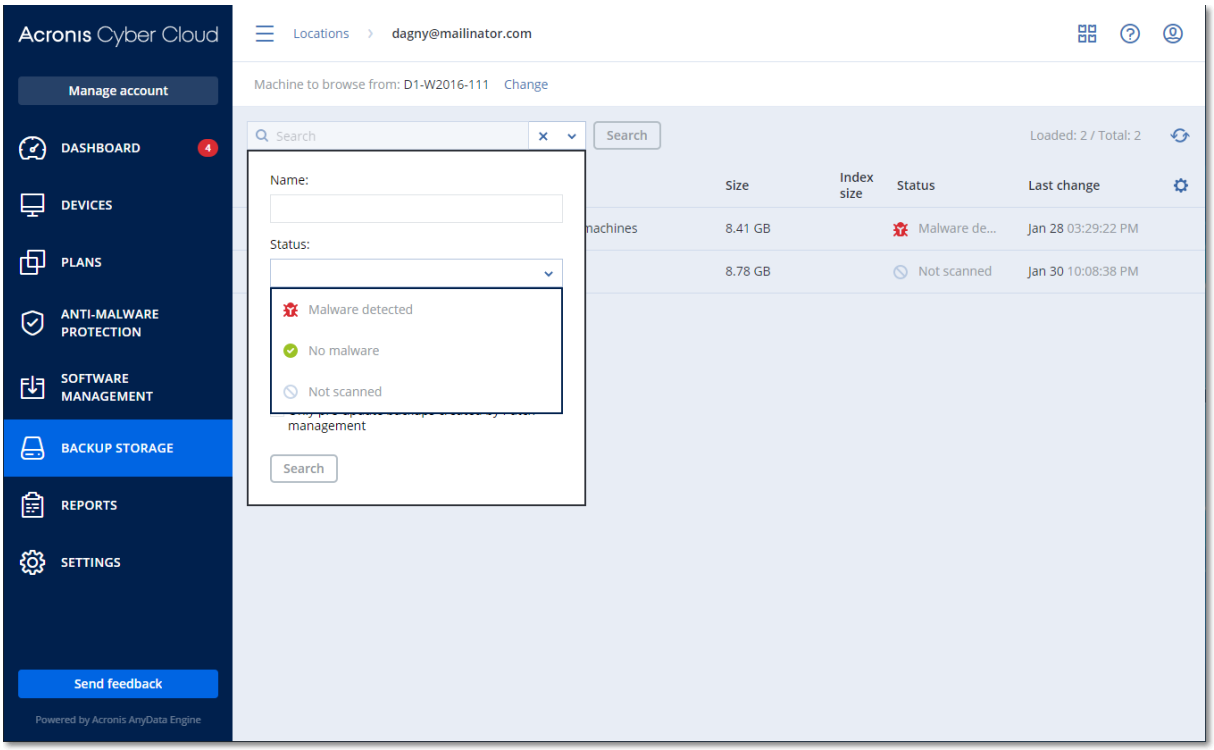
Als u de optie Veilig herstel inschakelt tijdens het herstelproces, worden de volgende bewerkingen uitgevoerd:

1. De systeemkopieback-up scannen op malware en de geïnfecteerde bestanden markeren. Een van de volgende statussen is toegewezen aan een back-up:
   - **Geen malware**: tijdens het scannen is geen malware gevonden in een back-up.
   - **Malware gedetecteerd**: tijdens het scannen is malware gevonden in een back-up.
   - **Niet gescand**: back-up is niet gescand op malware.



1. De back-up herstellen naar de geselecteerde machine.
2. De gedetecteerde malware verwijderen.

U kunt back-ups filteren met de parameter **Status**.



14.14.3 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 modus Verbeterde beveiliging
- 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:

Als u een besturingssysteem herstelt, moet u opnieuw opstarten. U kunt ervoor kiezen de machine automatisch opnieuw op te starten, maar u kunt ook de status **Interactie vereist** aan de machine toewijzen. Het herstelde besturingssysteem gaat automatisch online.

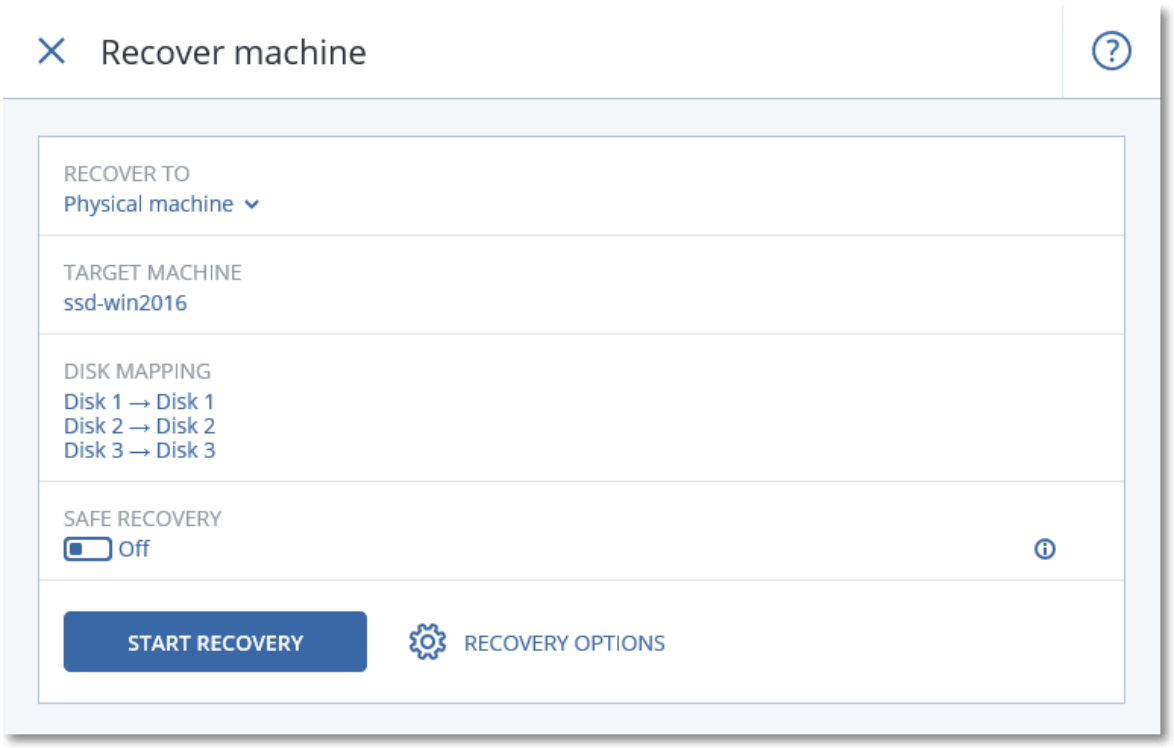
Een fysieke machine herstellen

1. Selecteer de machine waarvan een back-up is gemaakt.
2. Klik op **Herstellen**.
3. Selecteer een herstelpunt. Houd er rekening mee dat de herstelpunten worden gefilterd op locatie.

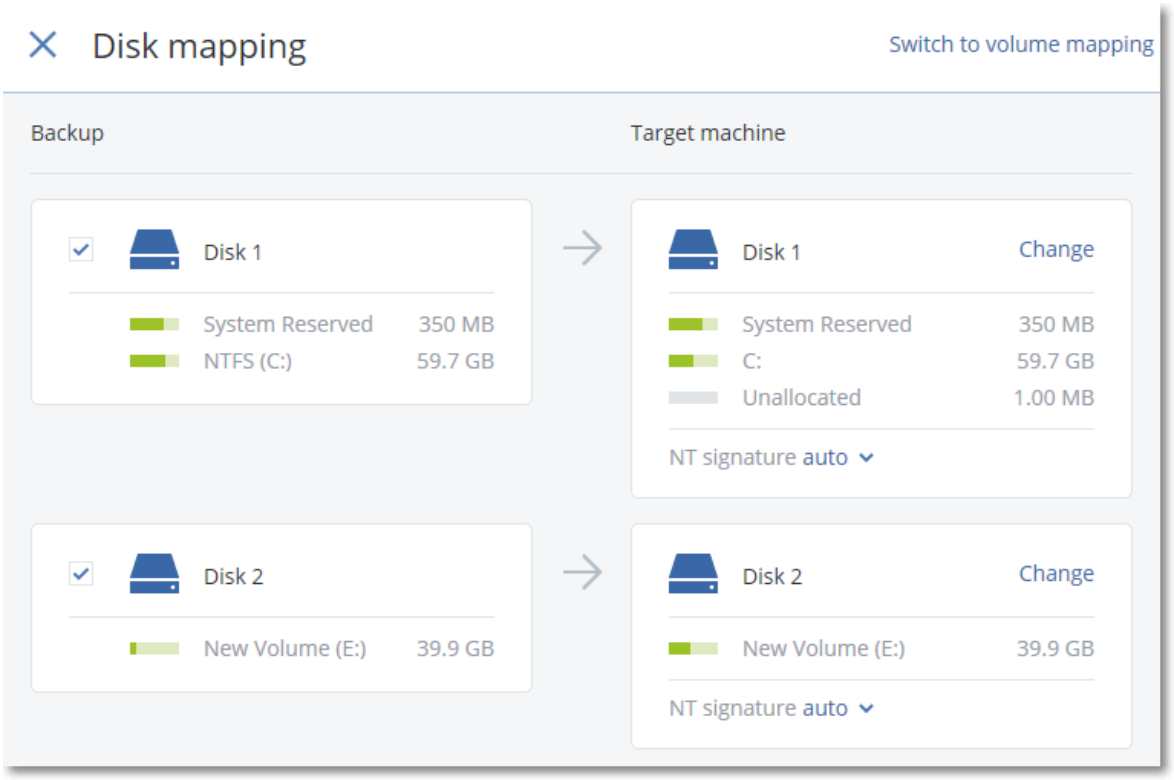
Als de machine offline is, worden de herstelpunten niet weergegeven. Voer een van de volgende handelingen uit:

- 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...** rechtsboven.



6. [Optioneel] Schakel **Veilig herstel** in om de back-up op malware te scannen. Als malware wordt gedetecteerd, wordt deze in de back-up gemarkeerd en verwijderd direct nadat het herstelproces is voltooid.
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 modus Verbeterde beveiliging.

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 **Herstellen**.
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.

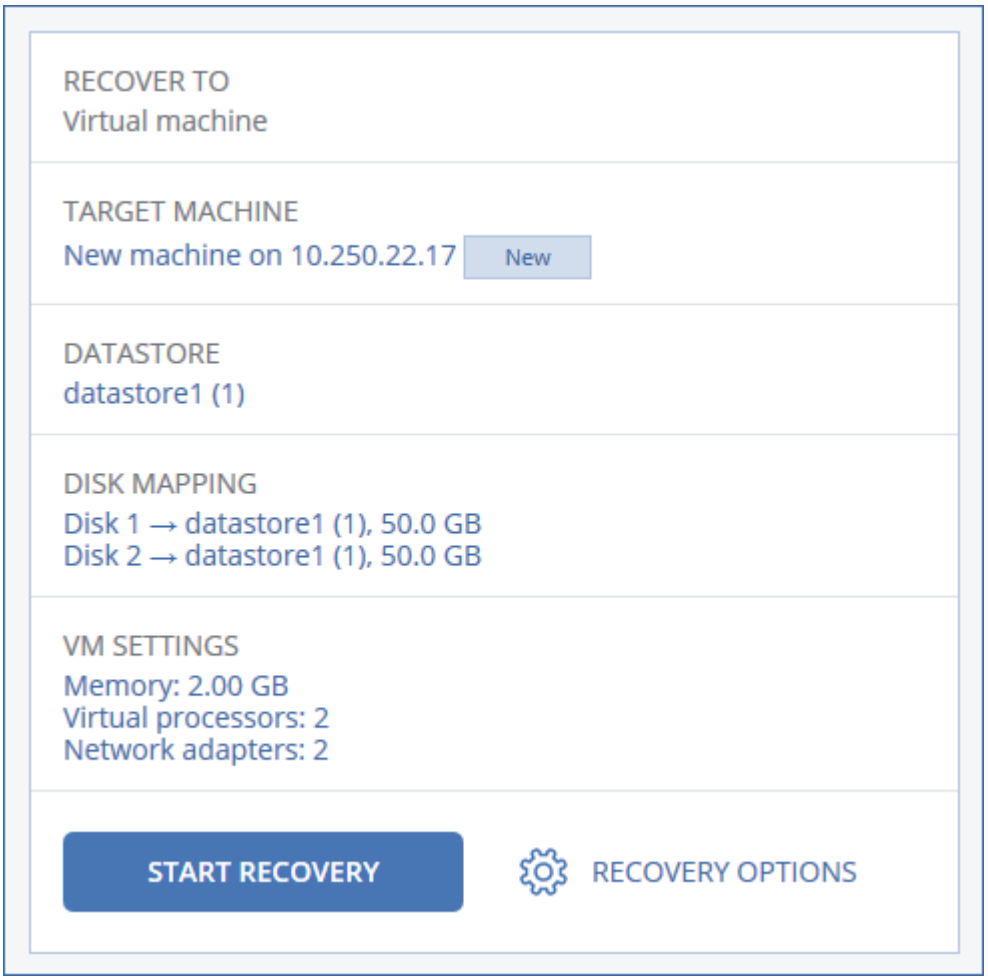
      Opmerking
      Er moet ten minste één agent voor die hypervisor zijn geïnstalleerd en geregistreerd in Acronis Management Server.

   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. Klik op **Herstel starten**.
10. 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
Herstel via de webinterface is niet beschikbaar voor tenants in de modus Verbeterde beveiliging.

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

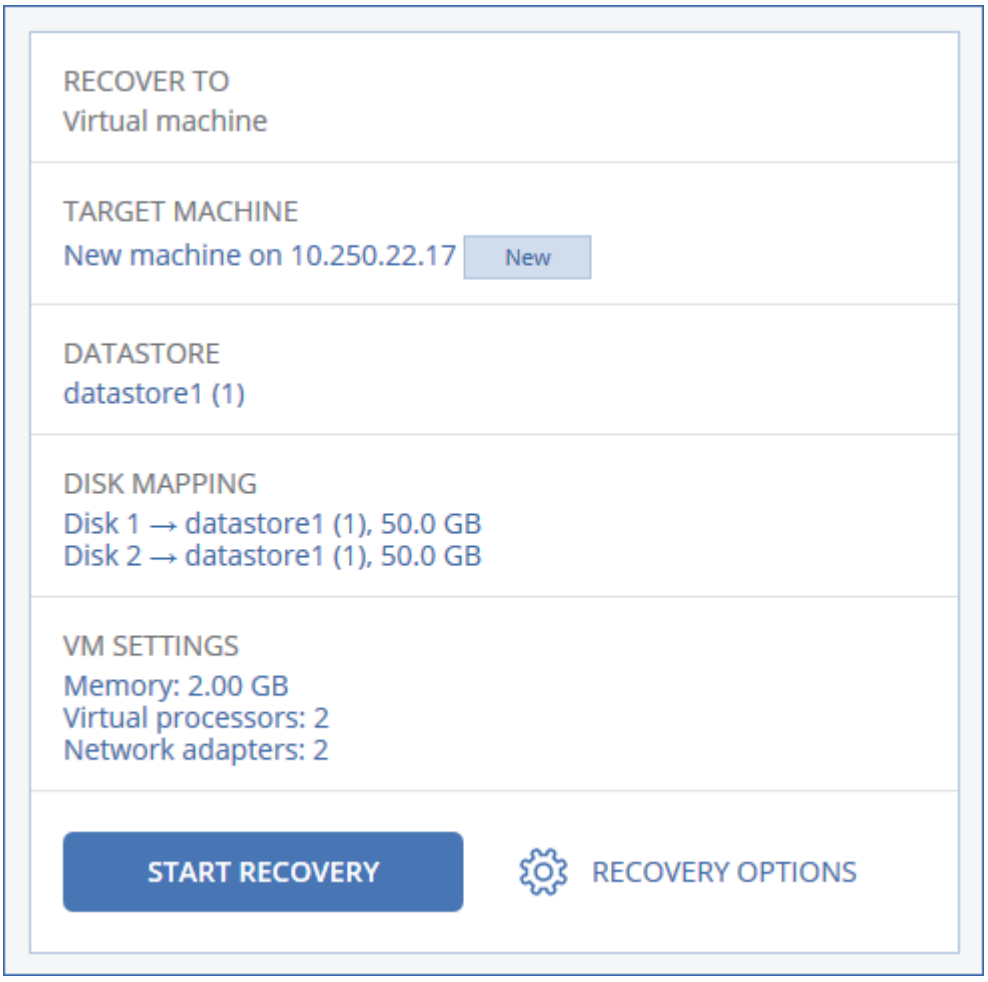
1. Voer een van de volgende handelingen uit:
   - Selecteer een machine waarvan een back-up is gemaakt, klik op **Herstellen** en selecteer vervolgens een herstelpunt.
   - Selecteer een herstelpunt op het tabblad Back-upopslag.
2. Klik op **Herstellen** > **Volledige machine**.
3. Als u wilt herstellen 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. Klik op **Herstel starten**.
7. 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**.

Schijven herstellen met opstartmedia

Zie "Fysieke opstartmedia maken" (p. 593) voor informatie over het maken van opstartmedia.

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 Cyberbescherming-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.

   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**.

14.14.4 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.

14.14.5 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.

14.14.6 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.

14.14.7 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.

14.14.8 Bestanden herstellen

Bestanden herstellen via de webinterface

Opmerking
Herstel via de webinterface is niet beschikbaar voor tenants in de modus Verbeterde beveiliging.

1. Selecteer de oorspronkelijke machine met de gegevens die u wilt herstellen.
2. Klik op **Herstellen**.

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. Voor meer informatie over jokers gaat u naar 'Bestandsfilters'.

   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.
8. Klik op **Herstellen**.

   In **Herstellen naar** ziet u een van de volgende items:

   - De machine die oorspronkelijk de bestanden bevatte die u wilt herstellen (als een agent is geïnstalleerd op deze machine).
   - De machine waarop Agent voor VMware, Agent voor Hyper-V, Agent voor Virtuozzo, Agent voor Scale Computing HC3 of Agent voor oVirt is geïnstalleerd (als de bestanden afkomstig zijn van een virtuele ESXi-, Hyper-V-, Virtuozzo-, Scale Computing HC3- of Red Hat Virtualization/oVirt-machine).

   Dit is de doelmachine voor het herstel. Indien nodig kunt u een andere machine selecteren.
9. Ga naar **Pad** en selecteer de herstelbestemming. U kunt een van de volgende opties selecteren:

   - De oorspronkelijke locatie (bij herstel naar de oorspronkelijke machine)
   - Een lokale map 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 dan**
    - **Bestaande bestanden niet overschrijven**

De voortgang van de herstelbewerking wordt weergegeven op het tabblad **Activiteiten**.

Bestanden downloaden uit de cloudopslag

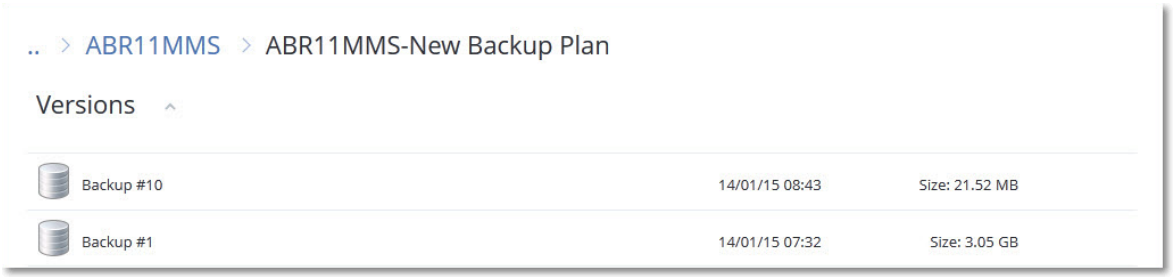
U kunt door de cloudopslag bladeren, de inhoud van de back-ups bekijken en de benodigde bestanden downloaden.

Beperkingen

- u kunt niet bladeren in back-ups van de systeemstatus, SQL-databases en Exchange-databases.
- U kunt niet downloaden als de totale grootte van de geselecteerde bestanden meer is dan 100 MB.

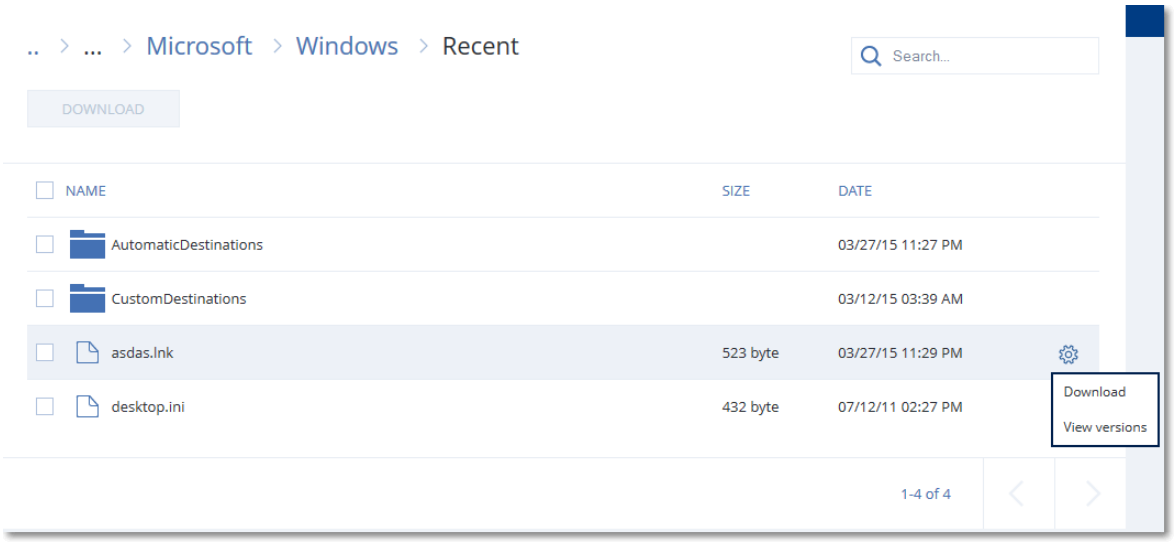
Bestanden downloaden uit de cloudopslag

1. Selecteer een machine waarvan een back-up is gemaakt.
2. Klik op **Herstellen** > **Meer herstelbewerkingen...** > **Bestanden downloaden**.
3. Geef de referenties op van het account waaraan de back-up van de machine is toegewezen.
4. [Wanneer u in back-ups op schijfniveau bladert] Klik bij **Versies** op de back-up waarvan u de bestanden wilt herstellen.



   [Wanneer u in back-ups op bestandsniveau bladert] U kunt bij de volgende stap de back-updatum en -tijd selecteren door op het tandwielpictogram rechts van het geselecteerde bestand te klikken. Standaard worden de bestanden van de laatste back-up hersteld.
5. Blader naar de vereiste map of gebruik de zoekbalk om de lijst met de vereiste bestanden op te halen.

   Zoekopdrachten zijn taalonafhankelijk.



6. Schakel de selectievakjes in voor de items die u wilt herstellen en klik vervolgens op **Downloaden**.

   Als u één bestand selecteert, wordt dit bestand als zodanig gedownload. In andere gevallen worden de geselecteerde gegevens gearchiveerd in een ZIP-bestand.
7. Selecteer de locatie waar u de gegevens wilt opslaan en klik vervolgens op **Opslaan**.

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
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

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 Cyberbescherming-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.

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.
- Er moet een beveiligingsagent zijn geïnstalleerd op de machine waar u bladert naar een back-up.
- 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+.
- 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.

14.14.9 Systeemstatus herstellen

Opmerking
Herstel via de webinterface is niet beschikbaar voor tenants in de modus Verbeterde beveiliging.

1. Selecteer de machine waarvan u de systeemstatus wilt herstellen.
2. Klik op **Herstellen**.
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**.

14.14.10 ESXi-configuratie herstellen

Als u een ESXi-configuratie wilt herstellen, hebt u Linux-opstartmedia nodig. Zie "Fysieke opstartmedia maken" (p. 593) 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.

14.14.11 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**.

Bij validatie wordt een controlesom berekend voor elk gegevensblok dat is opgeslagen in de back-up. 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.

Het validatieproces vergt aanzienlijk wat tijd, zelfs voor incrementele en differentiële back-ups, die minder groot zijn. Dit komt omdat met de bewerking niet alleen de gegevens worden gecontroleerd

die zich fysiek in de back-up bevinden, maar alle gegevens die kunnen worden hersteld wanneer de back-up wordt geselecteerd. Hiervoor is toegang nodig tot eerder gemaakte back-ups.

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 Vista SP1
  - 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	Ingeschakeld	Uitgeschakeld	Ingeschakeld	Uitgeschakeld

herstelbewerking afkeuren als het uitvoeren van de opdracht mislukt*				
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**.

14.15 Bewerkingen met back-ups

14.15.1 Het tabblad Back-upopslag

Het tabblad **Back-upopslag** biedt toegang tot alle back-ups, inclusief back-ups van offline machines, back-ups van machines die niet meer zijn geregistreerd in de Cyberbescherming-service en zwevende back-ups[1].

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.

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**.

[1] Een zwevende back-up is een back-up die niet meer is gekoppeld aan een beschermingsschema.

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 Cyberbescherming-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.

14.15.2 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.

14.15.3 Back-ups verwijderen

Waarschuwing!
Wanneer een back-up wordt verwijderd, worden alle gegevens permanent gewist. Verwijderde gegevens kunnen niet worden hersteld.

Back-ups verwijderen van een online machine in de serviceconsole

1. Ga naar het tabblad **Alle apparaten** en selecteer een machine waarvan u de back-ups wilt verwijderen.
2. Klik op **Herstellen**.
3. Selecteer de locatie waar u de back-ups wilt verwijderen.
4. Verwijder de gewenste back-ups. U kunt de hele back-upketen of een enkele back-up in de keten verwijderen.
   - Als u de hele back-upketen wilt verwijderen, klikt u op **Alles verwijderen**.
   - Als u een enkele back-up in de geselecteerde keten wilt verwijderen:
     a. Selecteer de back-up die u wilt verwijderen en klik vervolgens op het tandwielpictogram.
     b. Klik op **Verwijderen**.
5. Bevestig uw beslissing.

Back-ups verwijderen van een machine

1. Ga naar het tabblad **Back-upopslag** en selecteer de locatie waar u de back-ups wilt verwijderen.
   Alle back-ups die uw account mag bekijken in de geselecteerde locatie, worden weergegeven. De back-ups worden gecombineerd in back-upketens. De namen van de back-upketens zijn gebaseerd op de volgende sjabloon:
   - `<naam machine> – <naam beschermingsschema>`
   - `<gebruikersnaam>` of `<stationsnaam>` - `<cloudservice>` - `<naam van beschermingsschema>` - voor cloud-to-cloud back-ups
2. Selecteer een back-upketen.
3. Verwijder de gewenste back-ups. U kunt de hele back-upketen of een enkele back-up in de keten verwijderen.
   - Als u de hele back-upketen wilt verwijderen, klikt u op **Verwijderen**.
   - Als u een enkele back-up in de geselecteerde keten wilt verwijderen:
     a. Klik op **Back-ups weergeven**.
     b. Selecteer de back-up die u wilt verwijderen en klik vervolgens op het tandwielpictogram.
     c. Klik op **Verwijderen**.
4. Bevestig uw beslissing.

Back-ups rechtstreeks verwijderen uit de cloudopslag

1. Meld u aan bij de cloudopslag, zoals beschreven in 'Bestanden downloaden uit de cloudopslag'.
2. Klik op de naam van de machine waarvan u de back-ups wilt verwijderen.
   Het programma geeft een of meer back-upgroepen weer.
3. Klik op het tandwielpictogram voor de back-upgroep die u wilt verwijderen.

4. Klik op **Verwijderen**.
5. Bevestig de bewerking.

Wat te doen als u lokale back-ups hebt verwijderd met bestandsbeheer

We raden u aan om back-ups waar mogelijk te verwijderen met de serviceconsole. Als u lokale back-ups hebt verwijderd met bestandsbeheer, doet u het volgende:

1. Klik op het tabblad **Back-upopslag** op het tandwielpictogram naast de naam van de locatie.
2. Klik op **Vernieuwen**.

Op deze manier laat u de Cyberbescherming-service weten dat het lokale opslaggebruik is afgenomen.

14.16 Microsoft-toepassingen beschermen

14.16.1 Microsoft SQL Server en Microsoft Exchange Server beveiligen

Er zijn twee methoden om deze applicaties te beveiligen:

- **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 Web Services-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.

14.16.2 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.

14.16.3 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.

14.16.4 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	-	-	Volledige

SharePoint-front-endwebservers			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.

14.16.5 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 gebruikersaccountbeheer niet wilt uitschakelen, moet u de referenties van een ingebouwde domeinbeheerder (DOMAIN\Administrator) opgeven wanneer u de applicatieback-up inschakelt.

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 gebruikersaccountbeheer niet wilt uitschakelen, moet u de referenties van een ingebouwde domeinbeheerder (DOMAIN\Administrator) opgeven wanneer u de applicatieback-up inschakelt.
- 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**).

14.16.6 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', worden 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. Voor meer informatie over het maken van DAG's raadpleegt u 'Databasebeschikbaarheidsgroepen (DAG) beschermen'.

- 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', kunt u postvakken selecteren voor back-up.

4. Geef desgevraagd de referenties voor toegang tot de gegevens op.
5. Klik op **Beschermen**.

AlwaysOn-beschikbaarheidsgroepen (AAG) beschermen

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

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.

   Opmerking
   Nadat u de agent op een van de knooppunten hebt geïnstalleerd, worden de AAG en de bijbehorende knooppunten weergegeven onder **Apparaten** > **Microsoft SQL** > **Databases**. Als u Agent voor SQL wilt installeren op de rest van de knooppunten, selecteert u de AAG, klikt u op **Details** en klikt u vervolgens op **Agent installeren** naast elk knooppunt.

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
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

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

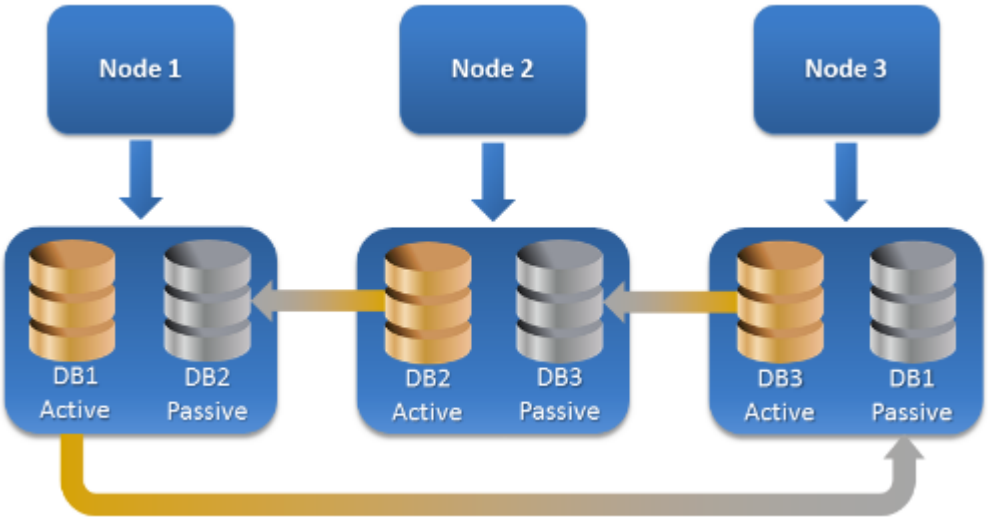
Met clustergerichte back-up maakt u een back-up van slechts één exemplaar van de geclusterde gegevens. Als de plaats van de gegevens binnen het cluster wordt gewijzigd (vanwege een switchover of failover), worden alle verplaatsingen van deze gegevens bijgehouden en wordt hiervan een veilige back-up gemaakt.

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 serviceconsole 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 wilt maken, selecteert u de DAG, zoals beschreven in 'Exchange Server-gegevens selecteren'.
2. Configureer de back-upoptie "Clusterback-upmodus".
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', 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.

14.16.7 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 **Toepassingsback-up** in voor extra bescherming van de gegevens van deze toepassingen.

Waarom applicatiegerichte back-up gebruiken?

Applicatiegerichte back-up biedt de volgende voordelen:

1. De back-ups van de applicaties worden gemaakt in een consistente status en deze zijn dus onmiddellijk beschikbaar nadat de machine is hersteld.
2. U kunt de SQL- en Exchange-databases, postvakken en postvakitems herstellen zonder de volledige machine te herstellen.
3. 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.
4. 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.

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.

Vereiste gebruikersrechten

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:
  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.
- 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 gebruikersaccountbeheer niet wilt uitschakelen, moet u de referenties van een ingebouwde domeinbeheerder (DOMAIN\Administrator) opgeven wanneer u de applicatieback-up inschakelt.

14.16.8 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.

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** > **Pastvakken**.

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.

14.16.9 SQL-databases herstellen

In dit gedeelte wordt beschreven hoe u herstelbewerkingen uitvoert vanaf databaseback-ups en applicatiegerichte back-ups.

U kunt SQL-databases herstellen naar een SQL Server-exemplaar als Agent voor SQL is geïnstalleerd op de machine waarop het exemplaar wordt uitgevoerd.

Als u Windows-verificatie gebruikt, 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.

U kunt de databases eventueel ook herstellen als bestanden. Dit kan handig zijn wanneer u gegevens moet uitpakken voor gegevensanalyse, controledoeleinden of verdere verwerking door hulpprogramma's van derden. U kunt de SQL-databasebestanden koppelen aan een SQL Server-exemplaar, zoals beschreven in 'SQL Server-databases 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.

Systeemdatabases worden in principe op dezelfde manier hersteld als gebruikersdatabases. De eigenaardigheden met betrekking tot het herstellen van systeemdatabases worden beschreven in 'Systeemdatabases herstellen'.

SQL-databases herstellen naar een SQL Server-exemplaar

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 SQL** en selecteert u vervolgens de databases die u wilt herstellen.
2. Klik op **Herstellen**.
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 agents hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een online machine met Agent voor SQL 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 SQL-databases.
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 exemplaar**.
5. De databases worden standaard hersteld naar de oorspronkelijke databases. Als de oorspronkelijke database niet bestaat, wordt deze opnieuw gemaakt. U kunt ook een ander SQL Server-exemplaar (op dezelfde machine) selecteren waarnaar u de databases herstelt.

   Een database als een andere database naar hetzelfde exemplaar herstellen:

   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. [Optioneel] [Niet beschikbaar voor een database die als nieuwe database is hersteld naar het oorspronkelijke exemplaar] Als u de status van de database na de herstelbewerking wilt wijzigen,

klikt u op de naam van de database en kiest u een van de volgende statusopties:

- **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.

7. Klik op **Herstel starten**.

De voortgang van de herstelbewerking wordt weergegeven op het tabblad Activiteiten.

SQL-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 SQL** en selecteert u vervolgens de databases die u wilt herstellen.
2. Klik op **Herstellen**.
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 agents hier toegang toe hebben), klikt u op **Machine selecteren**, selecteert u een online machine met Agent voor SQL 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 SQL-databases.

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 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.

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**.

14.16.10 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 **Herstellen**.
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 **Herstellen**.
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

14.16.11 Exchange-postvakken en postvakitems herstellen

In dit onderdeel wordt beschreven hoe u Exchange-postvakken en -postvakitems kunt herstellen vanaf databaseback-ups, applicatiegerichte back-ups en postvakback-ups. De postvakken of postvakitems kunnen worden hersteld naar een live Exchange-server of naar Microsoft 365.

De volgende items kunnen worden hersteld:

- Postvakken (behalve archiefpostvakken)
- Openbare mappen

Opmerking
Alleen beschikbaar in databaseback-ups. Zie "Exchange Server-gegevens selecteren" (p. 292).

- Items uit openbare mappen
- E-mailmappen
- E-mailberichten
- Agendagebeurtenissen
- Taken
- Contacten
- Logboekvermeldingen
- Notities

U kunt een zoekopdracht gebruiken om de items te vinden.

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-postvakken beschermen' voor meer informatie over het herstellen 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).

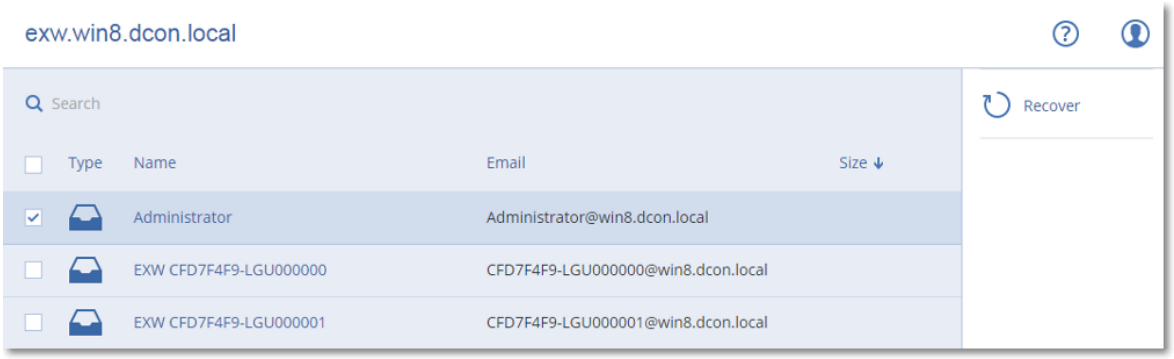
- Als u Agent voor Microsoft 365 al hebt in uw organisatie, kopieert u bibliotheken van de machine waarvan een back-up is gemaakt (of van een andere machine met dezelfde Microsoft Exchange Server-versie), naar de machine met Agent voor Microsoft 365, zoals beschreven in 'Microsoft Exchange-bibliotheken 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 **Herstellen**.
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 **Herstellen**.
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.

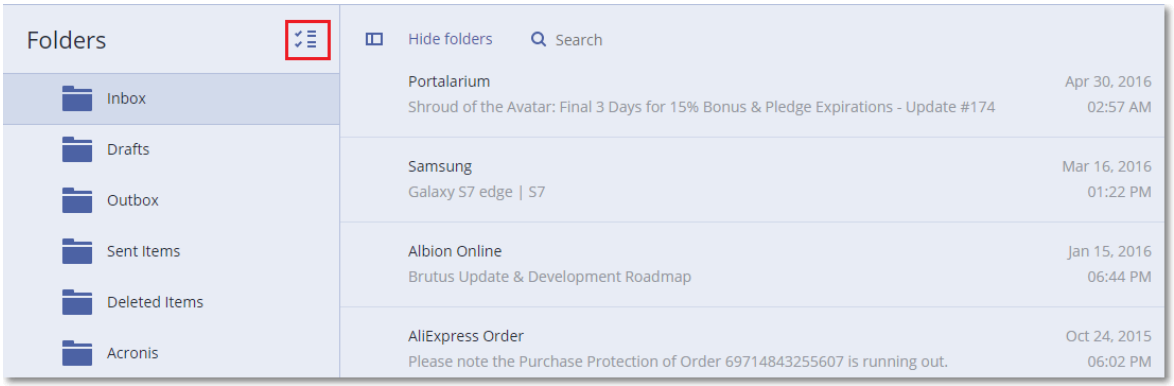
   De herstelbewerking wordt uitgevoerd door de machine die u kiest voor het bladeren bij een van de genoemde acties, en niet door de oorspronkelijke machine die offline is.
5. Klik op **Herstellen** > **Exchange-postvakken**.
6. Klik op het postvak dat oorspronkelijk de items bevatte die u wilt herstellen.
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,	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange`

2019		`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.

14.16.12 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**.

14.17 Mobiele apparaten beschermen

Met de Cyber Protect-app kunt u een back-up van uw mobiele gegevens maken naar de cloudopslag en de gegevens vervolgens herstellen in geval van verlies of beschadiging. Let op: voor back-up naar de cloudopslag hebt u een account en het cloudabonnement nodig.

14.17.1 Ondersteunde mobiele apparaten

U kunt de Cyber Protect-app installeren op een mobiel apparaat met een van de volgende besturingssystemen:

- iOS 12.0 en later (iPhone, iPod en iPad)
- Android 7.0 en later

14.17.2 Van welke items kunt u een back-up maken

- Contacten
- Foto's
- Video's
- Kalenders
- Herinneringen (alleen op iOS-apparaten)

14.17.3 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:
  - Voor Android 7.0 of hoger: nieuwe gegevens worden direct gedetecteerd door de Cyber Protect-app en automatisch geüpload naar de cloud,
  - Voor Android 6: er wordt elke drie uur gecontroleerd of er wijzigingen zijn. U kunt continue back-up uitschakelen in de app-instellingen.
- 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**. Deze functie 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**. Deze 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. Deze optie is beschikbaar voor Android 8 of hoger.
- 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 serviceconsole.

- 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 versies van de gegevens herstellen. Als u wilt herstellen vanaf een specifieke back-upversie, gebruikt u de serviceconsole op een tablet of een computer.
- 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.

14.17.4 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.

14.17.5 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.

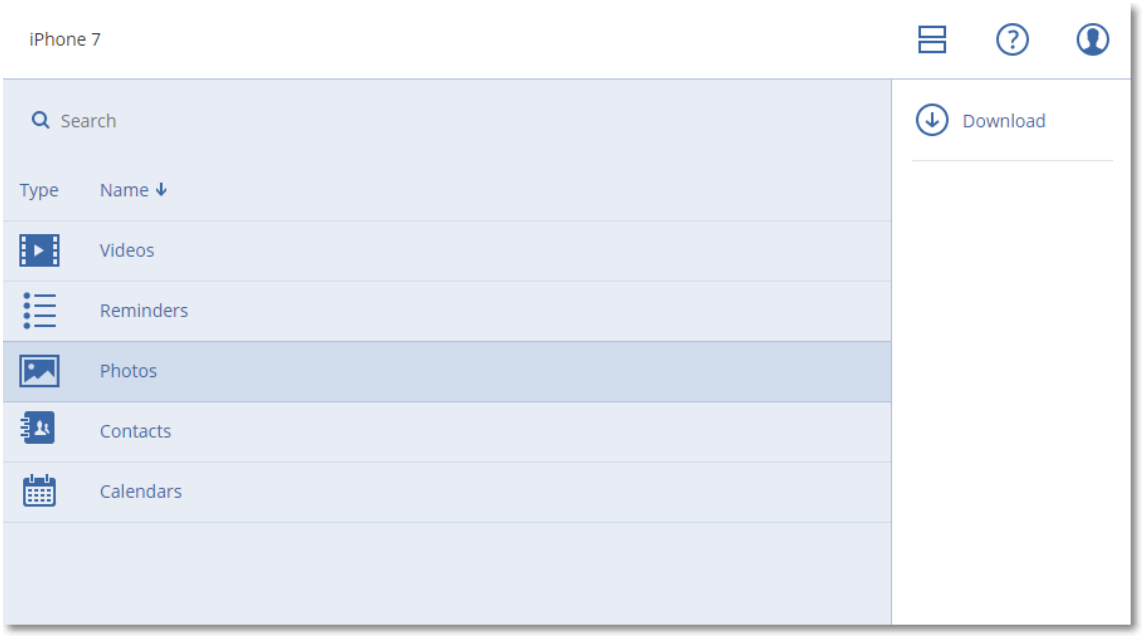
De back-up begint.

14.17.6 Hoe kunt u gegevens herstellen naar een mobiel apparaat

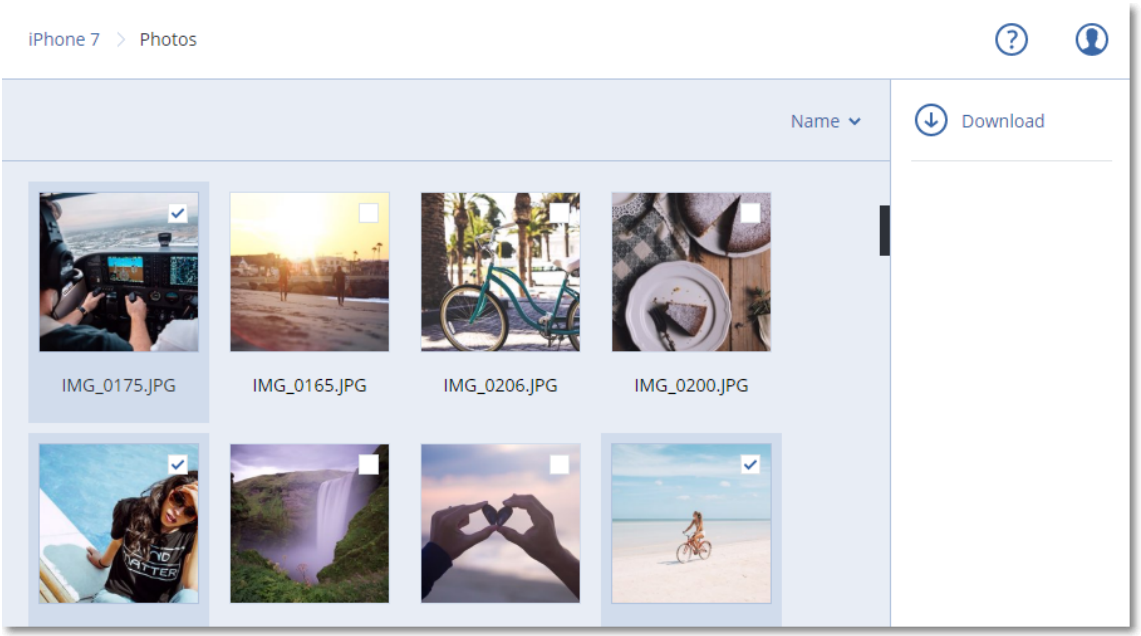
1. Open de Cyber Protect-app.
2. Tik op **Bekijken**.
3. Tik op de naam van het apparaat:
4. Voer een van de volgende handelingen uit:
   - Als u alle gegevens wilt herstellen waarvan een back-up is gemaakt, tikt u op **Alles herstellen**. U hoeft geen verdere actie te ondernemen.
   - Als u een of meer 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**.

14.17.7 Gegevens bekijken via de serviceconsole

1. Open een browser op een computer en typ de URL van de serviceconsole.
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.

14.18 Gehoste Exchange-gegevens beschermen

14.18.1 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.

14.18.2 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.

14.18.3 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 Cyberbescherming-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**.

14.18.4 Postvakken en postvakitems herstellen

Postvakken herstellen

1. Klik op **Apparaten > Gehoste Exchange**.
2. Als meerdere Gehoste Exchange-organisaties zijn toegevoegd aan de Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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.

14.19 Microsoft 365-gegevens beschermen

14.19.1 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.

14.19.2 Agent voor Microsoft 365

U kunt kiezen of u Agent voor Microsoft 365 lokaal wilt installeren, de in de cloud geïnstalleerde agent wilt gebruiken, of allebei, afhankelijk van de gewenste functionaliteit. De volgende tabel bevat een overzicht van de functies van de lokale agent en de cloudagent.

	Lokale agent voor Microsoft 365	**Cloudagent voor Microsoft 365**
Gegevensitems waarvan een back-up kan worden gemaakt	**Exchange Online**: gebruikers- en gedeelde postvakken	• **Exchange Online**: gebruikers-, gedeelde en groepspostvakken; openbare mappen • **OneDrive**: gebruikersbestanden en -mappen • **SharePoint Online**: klassieke siteverzamelingen, groeps(team)sites, communicatiesites, individuele gegevensitems • **Microsoft 365 Teams**: volledige teams, teamkanalen, kanaalbestanden, teampostvakken, bestanden en e-mailberichten in teampostvakken, vergaderingen, teamsites
Back-up van archiefpostvakken (**in-place archief**)	Nee	Ja
Back-upschema	Door gebruiker gedefinieerd	Kan niet worden gewijzigd. Elk beschermingsschema wordt dagelijks op hetzelfde tijdstip uitgevoerd.*
Back-uplocaties	Cloudopslag, lokale map, netwerkmap	Alleen cloudopslag
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	Ja	Ja

binnen één organisatie		
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

*Aangezien een 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.

Opmerking
Het beschermingsschema kan worden beïnvloed door de werking van externe services, bijvoorbeeld de toegankelijkheid van Microsoft Office 365-servers, beperkingsinstellingen op de Microsoft-servers, enzovoort. Zie ook https://docs.microsoft.com/en-us/graph/throttling.

**Het wordt aanbevolen 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.

14.19.3 Beperkingen

- Alleen gebruikers met een toegewezen Microsoft 365-licentie kunnen een back-up laten maken van hun postvakken en OneDrives.

- 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.

14.19.4 Vereiste gebruikersrechten

In de Cyberbescherming-service

De lokale agent voor Microsoft 365 moet zijn geregistreerd onder een bedrijfbeheerdersaccount en worden gebruikt op klanttenantniveau. Bedrijfbeheerders die werken op eenheidniveau, eenheidbeheerders en gebruikers kunnen geen back-up- en herstelbewerkingen uitvoeren voor Microsoft 365-gegevens.

De cloudagent voor Microsoft 365 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. 330) voor meer informatie over deze niveaus en de respectievelijke beheerders.

In Microsoft 365

Aan uw account moet de rol van globale beheerder in Microsoft Office 365 zijn toegewezen.

Als u een 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 dit account wilt wijzigen, werkt u het wachtwoord in de serviceconsole bij, zoals beschreven in 'De Microsoft 365-toegangsreferenties wijzigen'.
- De cloudagent meldt zich niet aan bij Microsoft 365. De agent krijgt de nodige machtigingen rechtstreeks vanuit Microsoft 365. U hoeft slechts één keer te bevestigen dat u deze machtigingen toekent, wanneer u bent aangemeld als globale beheerder. De agent slaat uw accountreferenties niet op en gebruikt deze niet om back-up of herstel uit te voeren. Als u het wachtwoord van dit account wijzigt of dit account uitschakelt of verwijdert in Microsoft 365, heeft dit geen invloed op de werking van de agent.

14.19.5 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 Cyberbescherming-serviceconsole.
2. Klik op het accountpictogram in de rechterbovenhoek.
3. Klik op **Rapport Licenties voor Microsoft 365-seats**.

14.19.6 Lokale Agent voor Office 365 gebruiken

Een Microsoft 365-organisatie toevoegen

Een Microsoft 365-organisatie toevoegen

1. Meld u als bedrijfbeheerder aan bij de serviceconsole.
2. Klik op het accountpictogram in de rechterbovenhoek en vervolgens op **Downloads** > **Agent voor Office 365**.
3. Download en installeer de agent op een machine met Windows en een verbinding met internet.
4. Wanneer de installatie is voltooid, klikt u op **Apparaten** > **Microsoft Office 365** en voert u de referenties van de globale beheerder van Microsoft 365 in.

Belangrijk
Er mag slechts één lokaal geïnstalleerde Agent voor Microsoft 365 in een organisatie (bedrijfsgroep) zijn.

Hierdoor worden de gegevensitems van uw organisatie weergegeven in de serviceconsole op de **Microsoft Office 365**-pagina.

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.

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**.
2. Meld u, als daarom wordt gevraagd, aan als globale beheerder bij Microsoft 365.
3. Selecteer de postvakken waarvan u een back-up wilt maken.
4. Klik op **Back-up**.

Postvakken en postvakitems herstellen

Postvakken herstellen

1. Klik op **Microsoft Office 365**.
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**.
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 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**.
2. Klik op **Referenties opgeven**.
3. Voer de referenties van de globale beheerder van Microsoft 365 in en klik op **OK**.
   De 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.

14.19.7 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 serviceconsole 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 Cyberbescherming-service.

Uw Microsoft 365-organisatie wordt dan weergegeven op het tabblad **Apparaten** in de serviceconsole.

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 Cyberbescherming-service. Als u een gebruiker, groep of site toevoegt of verwijdert, ziet u deze wijziging niet onmiddellijk in de serviceconsole. Als u de wijziging onmiddellijk wilt synchroniseren, selecteert u de organisatie op

de pagina **Microsoft 365** en klikt u op **Vernieuwen**.

- 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 niet actief (grijs weergegeven) in de serviceconsole en worden hiervan geen back-ups gemaakt. Wanneer het verwijderde item niet meer beschikbaar is via de API, verdwijnt het uit de serviceconsole. 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 Office 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 verwijderen van een machine" (p. 286) voor meer informatie over het verwijderen van back-ups.

Een Microsoft Office 365-organisatie verwijderen

1. Meld u aan bij de serviceconsole 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.

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 archiefpostvakken (**in-place archief**) van de geselecteerde postvakken.

Vanaf versie 8.0 van de Cyberbescherming-service kunt u een back-up maken van openbare mappen. Als uw organisatie vóór de release van versie 8.0 aan de Cyberbescherming-service is

toegevoegd, moet u de organisatie opnieuw toevoegen om deze functionaliteit te verkrijgen. Verwijder de organisatie niet, maar herhaal de stappen beschreven in 'Een Microsoft 365-organisatie toevoegen'. Als gevolg hiervan krijgt de Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 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 Microsoft 365-organisatie en vervolgens de wijziging laten synchroniseren door de cloudagent. De cloudagent wordt om de 24 uur automatisch gesynchroniseerd met Microsoft 365. Als u de wijziging onmiddellijk wilt synchroniseren, gaat u naar de serviceconsole, selecteert u de organisatie op de pagina **Microsoft 365** 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 **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyberbescherming-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.
   - 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 Microsoft 365-organisaties zijn toegevoegd aan de Cyberbescherming-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 Cyberbescherming-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.

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 serviceconsole, 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 Office 365-organisaties zijn toegevoegd aan de Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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.
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:
    - **Bestaande items overschrijven**
    - **Bestaande items niet overschrijven**
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.

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.

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 Cyberbescherming-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.

OneDrive- en OneDrive-bestanden herstellen

Een volledige OneDrive herstellen

1. Klik op **Microsoft 365**.

2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-service, moet u de doelorganisatie opgeven.
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:
    - **Bestaande bestanden overschrijven**
    - **Een bestaand bestand overschrijven als dit ouder is dan**
    - **Bestaande bestanden niet overschrijven**
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 Cyberbescherming-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.
   De zoekfunctie is niet beschikbaar als de back-up is versleuteld.
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 Cyberbescherming-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 Cyberbescherming-service, moet u de doelorganisatie opgeven.
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:
    - **Bestaande bestanden overschrijven**
    - **Een bestaand bestand overschrijven als dit ouder is dan**
    - **Bestaande bestanden niet overschrijven**
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.

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.
- OneNote-bestanden (vanwege beperkingen van de SharePoint Online API).
- 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 Cyberbescherming-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.

SharePoint Online-gegevens herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyberbescherming-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.
   De zoekfunctie is niet beschikbaar als de back-up is versleuteld.
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. Als u een item wilt downloaden, selecteert u het item, klikt u op **Downloaden**, selecteert u de locatie waar u het item 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 Cyberbescherming-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 Cyberbescherming-service, moet u de doelorganisatie opgeven.
11. In **Herstellen naar site** kunt u de doelsite weergeven, wijzigen of opgeven.
    Standaard is de oorspronkelijke site geselecteerd. Als deze site niet bestaat of als een niet-oorspronkelijke organisatie is geselecteerd, moet u de doelsite 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 bestanden overschrijven**
    - **Een bestaand bestand overschrijven als dit ouder is dan**
    - **Bestaande bestanden niet overschrijven**
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.

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.
- Privégesprekken – één-op-één chats en groepschats.
- Stickers en lof.

Back-up en herstel worden ondersteund voor de volgende kanaaltabs:

- Word
- Excel
- PowerPoint
- PDF
- Documentbibliotheek

Er wordt een back-up gemaakt van bestanden die worden gedeeld in privékanalen, maar ze worden niet hersteld vanwege een beperking van de API.

Opmerking
Deze bestanden worden opgeslagen op specifieke locaties, apart van de bestanden die worden gedeeld in openbare kanalen.

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 Cyberbescherming-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.

Een volledig team herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-service, moet u de doelorganisatie opgeven.

6. 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.
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**
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 Cyberbescherming-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.

7. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyberbescherming-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 Cyberbescherming-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**
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 Cyberbescherming-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. Selecteer de items die u wilt herstellen en klik vervolgens op **Herstellen**
8. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyberbescherming-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 Cyberbescherming-service, moet u de doelorganisatie opgeven.
9. 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.
10. In **Herstellen naar kanaal** kunt u het doelkanaal weergeven, wijzigen of 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**
14. 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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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.

E-mailberichten en vergaderingen herstellen

1. Klik op **Microsoft 365**.
2. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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.
   De zoekfunctie is niet beschikbaar als de back-up is versleuteld.
7. Selecteer de items die u wilt herstellen en klik vervolgens op **Herstellen**.

8. Als meerdere Microsoft 365-organisaties zijn toegevoegd aan de Cyberbescherming-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 Cyberbescherming-service, moet u de doelorganisatie opgeven.
9. 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.
10. Selecteer of u de machtigingen voor delen voor de herstelde items wilt herstellen.
11. Klik op **Herstel starten**.
12. Selecteer een van de opties voor overschrijven:
    - **Bestaande inhoud overschrijven als deze ouder is**
    - **Bestaande inhoud overschrijven**
    - **Bestaande inhoud niet overschrijven**
13. Klik op **Doorgaan** om uw beslissing te bevestigen.

De cloudagent upgraden

In dit gedeelte wordt beschreven hoe u kunt upgraden naar de huidige versie van de back-upoplossing voor Microsoft 365. Deze versie ondersteunt back-ups van OneDrive en SharePoint Online en biedt verbeterde prestaties voor back-up en herstel. Vanaf versie 8.0 van de Cyberbescherming-service wordt de volgende functionaliteit niet meer ondersteund door de oude oplossing: beschermingsschema bewerken, verwijderen, toepassen en intrekken.

De beschikbaarheid van de upgrade hangt af van de gereedheid van het datacentrum en de instellingen van uw serviceprovider. Als de upgrade beschikbaar is, ziet u een melding van de serviceconsole bovenaan het tabblad **Microsoft Office 365 (v1)**.

Het upgradeproces

Tijdens de upgrade worden gebruikers van uw Microsoft 365-organisatie toegevoegd aan de nieuwe back-upoplossing. De beschermingsschema's worden gemigreerd en toegepast op de juiste gebruikers.

De eerder gemaakte back-ups worden gekopieerd naar een andere locatie in de cloud. Op het tabblad **Back-upopslag** worden de gekopieerde back-ups weergegeven in een afzonderlijk gedeelte met de naam **Back-ups van cloudtoepassingen**, maar de oorspronkelijke back-ups blijven in de **cloudopslaglocatie**. Wanneer het upgradeproces is voltooid, worden de oorspronkelijke back-ups verwijderd uit de **cloudopslaglocatie**.

De upgrade kan enkele uren of zelfs dagen duren, afhankelijk van het aantal gebruikers in de organisatie, het aantal back-ups en de toegangssnelheid tot Microsoft 365. Tijdens de upgrade is herstel van de eerder gemaakte back-ups mogelijk. Back-ups en beschermingsschema's die tijdens de upgrade zijn gemaakt, gaan echter verloren.

In het onwaarschijnlijke geval dat de upgrade mislukt, blijft de back-upoplossing volledig operationeel en kan de upgrade opnieuw worden gestart vanaf het storingspunt.

Het upgradeproces starten

1. Klik op **Microsoft Office 365 (v1)**.
2. Klik op **Upgrade** in de melding bovenaan het scherm.
3. Bevestig dat u het upgradeproces wilt starten.
4. Selecteer het Microsoft-datacentrum dat door uw organisatie wordt gebruikt.
   U wordt automatisch doorgestuurd naar de aanmeldingspagina van Microsoft 365.
5. 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.
6. Bevestig dat u deze machtigingen toekent aan de Cyberbescherming-service.
   U wordt doorgestuurd naar de serviceconsole en het upgradeproces begint. De voortgang van de upgrade wordt weergegeven in het deelvenster **Microsoft 365** > **Activiteiten**.

14.20 Google Workspace-gegevens beveiligen

14.20.1 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.

14.20.2 Vereiste gebruikersrechten

In de Cyberbescherming-service

In de Cyberbescherming-service moet u een bedrijfbeheerder zijn die werkt op klanttenantniveau. Bedrijfbeheerders die op eenheidniveau werken, eenheidbeheerders en gebruikers kunnen geen back-up- en herstelbewerkingen uitvoeren voor Google Workspace-gegevens.

In Google Workspace

Als u uw Google Workspace-organisatie wilt toevoegen aan de Cyberbescherming-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 Cyberbescherming-service.

Als de superbeheerder die de G-Suite-organisatie heeft toegevoegd, wordt verwijderd uit de G-Suite of een rol krijgt met minder rechten, mislukken de back-ups met een foutmelding zoals 'toegang geweigerd'. Herhaal in dit geval de procedure 'Een Google Workspace-organisatie toevoegen' en geef geldige referenties voor de superbeheerder op. Als u deze situatie wilt voorkomen, raden wij u aan een speciale gebruiker met superbeheerdersrechten te maken voor back-ups en herstel.

14.20.3 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.

14.20.4 Beperkingen

- Alleen gebruikers met een toegewezen Google Workspace-licentie kunnen een back-up laten maken van hun postvakken en Google Drives.
- De zoekfunctie in versleutelde back-ups wordt niet ondersteund.
- De back-ups van documenten in de native Google-indelingen worden gemaakt als generieke Office-documenten en worden in de serviceconsole 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.

14.20.5 Een Google Workspace-organisatie toevoegen

Als u een Google Workspace-organisatie wilt toevoegen aan de Cyberbescherming-service, hebt u een speciaal persoonlijk Google Cloud-project nodig. Zie "Een persoonlijk Google Cloud project maken" (p. 356) 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 serviceconsole.
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 serviceconsole.

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 Cyberbescherming-service. Als u een gebruiker of gedeelde Drive toevoegt of verwijdert, ziet u deze wijziging niet onmiddellijk in de serviceconsole. Als u de wijziging onmiddellijk wilt synchroniseren, selecteert u de organisatie op de pagina **Google Workspace** en klikt u op **Vernieuwen**.
- 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 Google-beleid blijft een gebruiker of gedeelde Drive die is verwijderd uit de gebruikersinterface van Google Workspace, nog een paar dagen beschikbaar via een API. Tijdens deze periode is het verwijderde item niet actief (grijs weergegeven) in de serviceconsole en worden hiervan geen back-ups gemaakt. Wanneer het verwijderde item niet meer beschikbaar is via de API, verdwijnt het uit de serviceconsole. Eventuele back-ups vindt u in **Back-upopslag** > **Back-ups van cloudtoepassingen**.

14.20.6 Een persoonlijk Google Cloud project maken

Als u uw Google Workspace-organisatie wilt toevoegen aan de Cyberbescherming-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 Cyberbescherming-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 **Een project selecteren** > **Nieuw project**.
3. Geef een naam op voor uw nieuwe project.
4. 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 de optie **API's en services** > **Dashboard**.
3. Schakel één voor één alle API's uit die standaard zijn ingeschakeld in dit project:
   a. Schuif omlaag op de pagina **Dashboard** en klik op de naam van een ingeschakelde API. De pagina **Overzicht** van de geselecteerde API wordt geopend.
   b. Klik op **API uitschakelen** en vervolgens op **Uitschakelen** om uw keuze te bevestigen.
   c. Ga terug naar **API's en services** > **Dashboard** 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:
   - Gmail-API
   - Google Drive-API
   - Admin SDK
   - Google Agenda-API
   - Personen-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 **Samenvatting** en klik vervolgens op **Terug naar dashboard**.

Het serviceaccount voor de Cyberbescherming-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. Geef een beschrijving op voor het serviceaccount.
5. Klik op **Maken**.
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 op de pagina **Serviceaccounts** het nieuwe serviceaccount en klik vervolgens onder **Acties** op **Bewerken**.
9. Vouw het gedeelte **Domeinbrede machtiging weergeven** uit en schakel vervolgens het selectievakje **Google Workspace-domeinbrede machtiging inschakelen** in.
10. Klik onder **Sleutels** op **Sleutel toevoegen** > **Nieuwe sleutel maken** en selecteer vervolgens het sleuteltype **JSON**.
11. 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 Cyberbescherming-service.

Het nieuwe project toegang verlenen tot uw Google Workspace-account

1. Selecteer in het navigatiemenu in het Google Cloud Platform de optie **API's en services** > **Referenties**.
2. Kopieer in het gedeelte **OAuth 2.0-client-id's**, onder **Client-id**, de client-id van uw serviceaccountclient.
3. Meld u aan bij de Google-beheerconsole (admin.google.com) als superbeheerder.
4. Selecteer in het navigatiemenu **Beveiliging** > **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. In het veld **OAuth-scopes** voegt u de volgende scopes één voor één toe:
   - 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 Cyberbescherming-service koppelen. Zie "Een Google Workspace-organisatie toevoegen via een speciaal persoonlijk Google Cloud-project" (p. 355) 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 Cyberbescherming-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 **Beveiliging** > **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 Cyberbescherming-service hebben dan geen toegang meer tot uw Google Workspace-account en kunnen geen back-ups maken van de gegevens in uw account.

14.20.7 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 een zoekopdracht gebruiken om items te vinden in een back-up, tenzij de back-up is versleuteld. De zoekfunctie in versleutelde back-ups wordt niet ondersteund.

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

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 Cyberbescherming-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**.

Zoekopdracht in volledige tekst

Met deze optie bepaalt u of de inhoud van de e-mailberichten wordt geïndexeerd door de cloudagent.

De vooraf ingestelde waarde is: **Ingeschakeld**.

Als deze optie is ingeschakeld, wordt de inhoud van de berichten geïndexeerd en kunt u berichten zoeken op inhoud. Anders is alleen zoeken op onderwerp, afzender, ontvanger of datum beschikbaar.

Opmerking
De zoekfunctie in versleutelde back-ups wordt niet ondersteund.

Het indexeringsproces heeft geen invloed op de prestaties van de back-up omdat het door een ander softwareonderdeel wordt uitgevoerd. Het indexeren van de eerste (volledige) back-up kan enige tijd in beslag nemen, waardoor er een vertraging kan optreden tussen de voltooiing van de back-up en de inhoud die in de zoekresultaten wordt weergegeven.

De index neemt 10-30 procent van de opslagruimte voor de postvakback-ups in beslag. Als u de exacte waarde wilt weten, klikt u op **Back-upopslag** > **Back-ups van cloudtoepassingen** en bekijkt u de kolom **Indexgrootte**. U kunt het zoeken in volledige tekst uitschakelen als u ruimte wilt besparen. De waarde in de kolom **Indexgrootte** zal na de volgende back-up dalen tot enkele megabytes. Deze minimale hoeveelheid metagegevens is nodig om een zoekopdracht uit te voeren op onderwerp, afzender, ontvanger of datum.

Wanneer u het zoeken in volledige tekst weer mogelijk maakt, indexeert de software alle back-ups die eerder zijn gemaakt door het beschermingsschema. Dit neemt ook enige tijd in beslag.

Postvakken en postvakitems herstellen

Postvakken herstellen

1. Klik op **Google Workspace**.
2. Als meerdere Google Workspace-organisaties zijn toegevoegd aan de Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 serviceconsole, 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 Cyberbescherming-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. De laatste twee opties leveren alleen resultaten op als de optie **Zoekopdracht in volledige tekst** is ingeschakeld tijdens de back-up. De taal van het berichtfragment dat wordt doorzocht, kan als aanvullende parameter worden opgegeven.
   - 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 Cyberbescherming-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 Cyberbescherming-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.

14.20.8 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. U kunt er ook voor kiezen een back-up te maken van bestanden die zijn gedeeld met de Google Drive-gebruiker.

Bij het maken van een back-up van bestanden, wordt ook een back-up gemaakt van de machtigingen voor delen van die bestanden.

De volgende items worden *overgeslagen* tijdens een back-up:

- Een gedeeld bestand, als de gebruiker als commentator of lezer toegang heeft tot het bestand en de bestandseigenaar de opties voor downloaden, afdrukken en kopiëren heeft uitgeschakeld voor commentatoren en lezers.
- De map **Computers** (gemaakt door de back-up en synchronisatieclient)

Beperkingen

- Specifieke Google-bestandsindelingen: er worden alleen back-ups gemaakt van Google Documenten, Google Spreadsheets, Google Presentaties en Google Tekeningen.

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 een zoekopdracht gebruiken om items te vinden in een back-up, tenzij de back-up is versleuteld. De zoekfunctie in versleutelde back-ups wordt niet ondersteund.

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 Cyberbescherming-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 een back-up wilt maken van de bestanden die met de geselecteerde gebruikers worden gedeeld, schakelt u de optie **Gedeelde bestanden opnemen** in.
   - 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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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:
    - **Bestaande bestanden overschrijven**
    - **Een bestaand bestand overschrijven als dit ouder is dan**
    - **Bestaande bestanden niet overschrijven**
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 Cyberbescherming-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.
   De zoekfunctie is niet beschikbaar als de back-up is versleuteld.
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 Cyberbescherming-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 Cyberbescherming-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:
    - **Bestaande bestanden overschrijven**
    - **Een bestaand bestand overschrijven als dit ouder is dan**
    - **Bestaande bestanden niet overschrijven**
16. Klik op **Doorgaan** om uw beslissing te bevestigen.

14.20.9 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.

Beperkingen

- Er kan geen back-up worden gemaakt van een Shared drive zonder leden vanwege beperkingen van de Google Drive-API.
- Specifieke Google-bestandsindelingen: er worden alleen back-ups gemaakt van Google Documenten, Google Spreadsheets, Google Presentaties en Google Tekeningen.

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 een zoekopdracht gebruiken om items te vinden in een back-up, tenzij de back-up is versleuteld. De zoekfunctie in versleutelde back-ups wordt niet ondersteund.

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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-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:
    - **Bestaande bestanden overschrijven**
    - **Een bestaand bestand overschrijven als dit ouder is dan**
    - **Bestaande bestanden niet overschrijven**
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 Cyberbescherming-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.

   De zoekfunctie is niet beschikbaar als de back-up is versleuteld.
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 Cyberbescherming-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 Cyberbescherming-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:
    - **Bestaande bestanden overschrijven**
    - **Een bestaand bestand overschrijven als dit ouder is dan**
    - **Bestaande bestanden niet overschrijven**
16. Klik op **Doorgaan** om uw beslissing te bevestigen.

14.20.10 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.

14.21 Oracle Database beschermen

Hoe u Oracle Database kunt beveiligen wordt beschreven in een afzonderlijk document: https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper.pdf

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

14.22 SAP HANA beveiligen

De beveiliging van SAP HANA wordt beschreven in een afzonderlijk document dat beschikbaar is op https://dl.managed-protection.com/u/pdf/SAP%20HANA_backup_whitepaper.pdf

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

14.23 Websites en hostingservers beveiligen

14.23.1 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 **Schema's** > **Bescherming**.

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 serviceconsole.
   - 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 serviceconsole 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.

14.23.2 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.

Integratie voor Plesk en cPanel

Webhostingbeheerders die de Plesk- of cPanel-platforms gebruiken, kunnen deze platforms integreren met de Cyberbescherming-service.

Met de integratie kan een beheerder het volgende doen:

- Een back-up van een volledige Plesk- of cPanel-server maken naar de cloudopslag, met back-up op schijfniveau
- De volledige server herstellen, inclusief alle websites
- Voor Plesk: granulair herstel van websites, individuele bestanden, postvakken of databases uitvoeren
- Voor cPanel: granulair herstel van websites, individuele bestanden, postvakken, filters en doorstuurfuncties voor e-mail, databases en accounts uitvoeren
- Selfserviceherstel inschakelen voor klanten van Plesk en cPanel

De integratie wordt uitgevoerd met een Cyberbescherming-service-extensie. Als u de extensie voor Plesk of cPanel nodig hebt, neemt u contact op met de provider van de Cyberbescherming-service.

Ondersteunde versies van Plesk en cPanel

- Plesk voor Linux 17.0 en hoger
- Elke versie van cPanel met PHP 5.6 en later

14.24 Speciale bewerkingen met virtuele machines

14.24.1 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 aan deze tijdelijke virtuele machine 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.

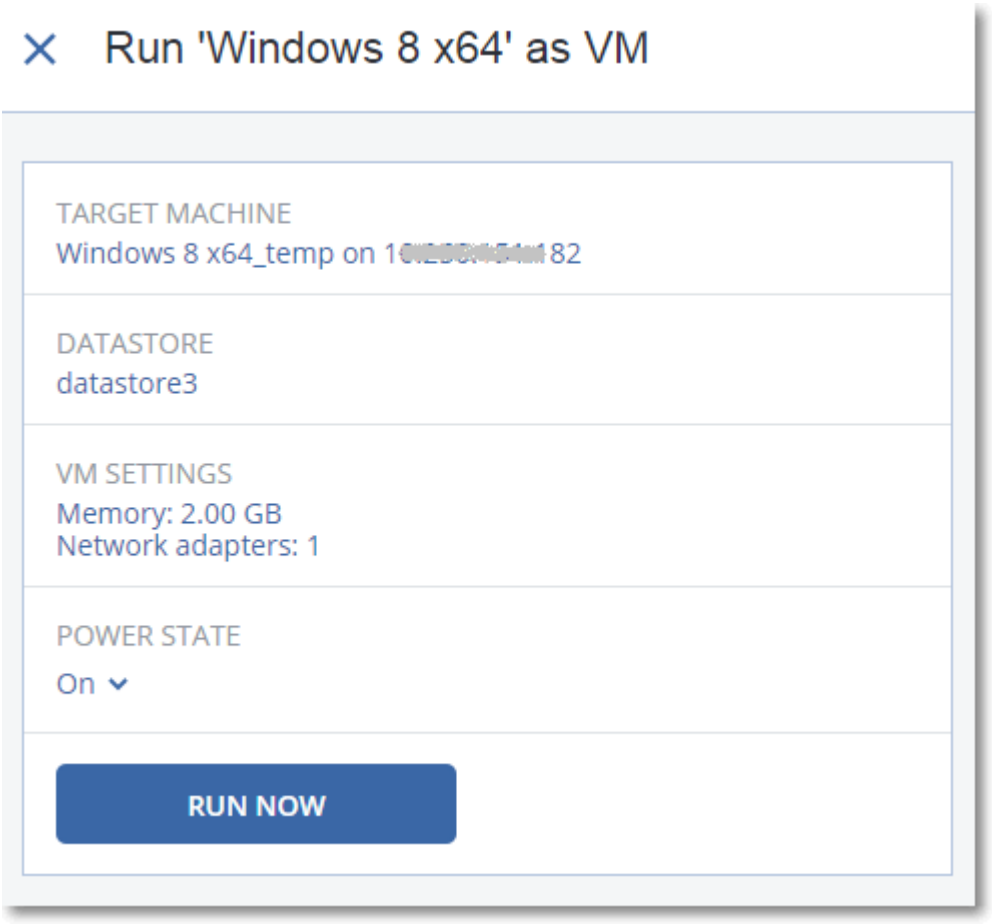
Vereisten

- Er moet ten minste één Agent voor VMware of Agent voor Hyper-V zijn geregistreerd in de Cyberbescherming-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 **Herstellen** 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.

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.

14.24.2 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.

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.

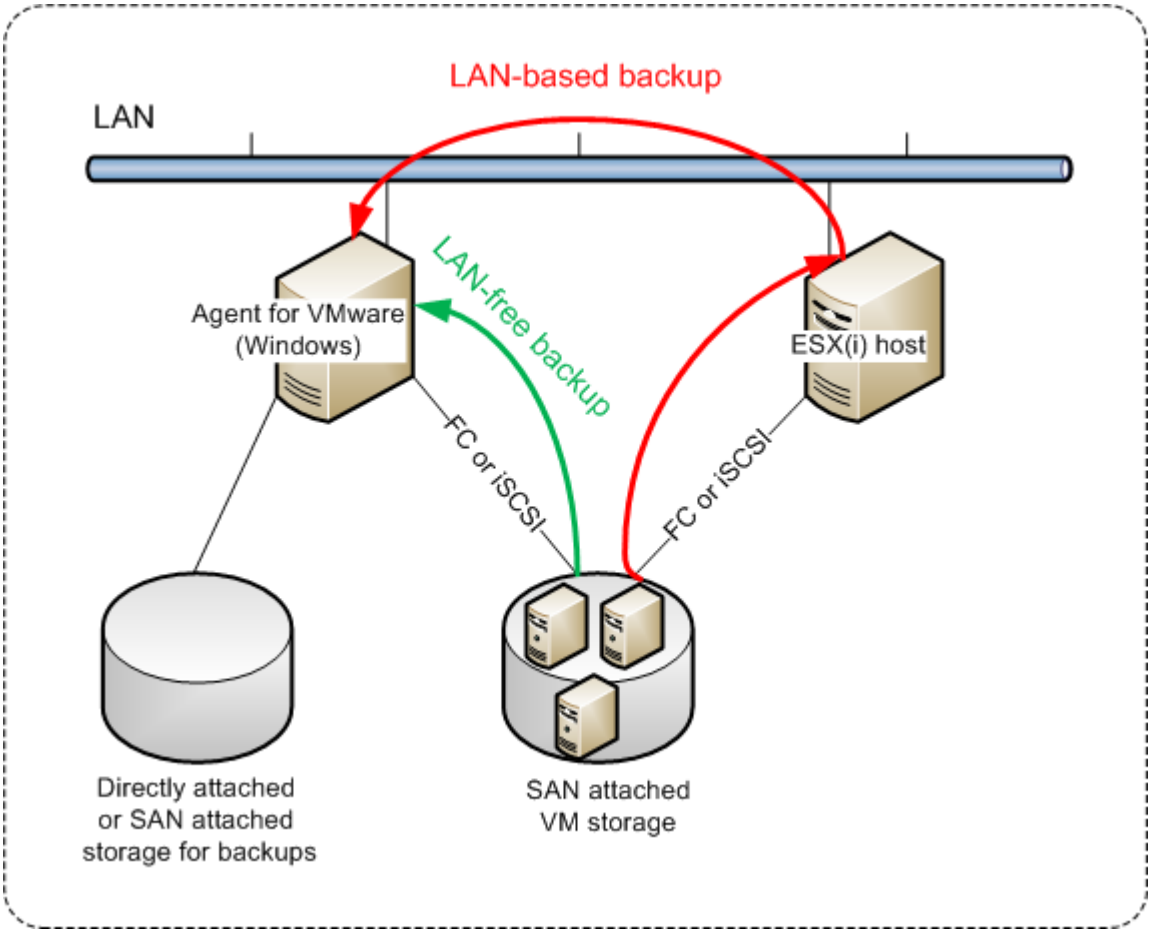
7. Bewerk het replicatieschema dat u hebt gemaakt in stap 2. Selecteer bij **Doelmachine** de optie **Bestaande replica** en selecteer vervolgens de geïmporteerde replica.

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

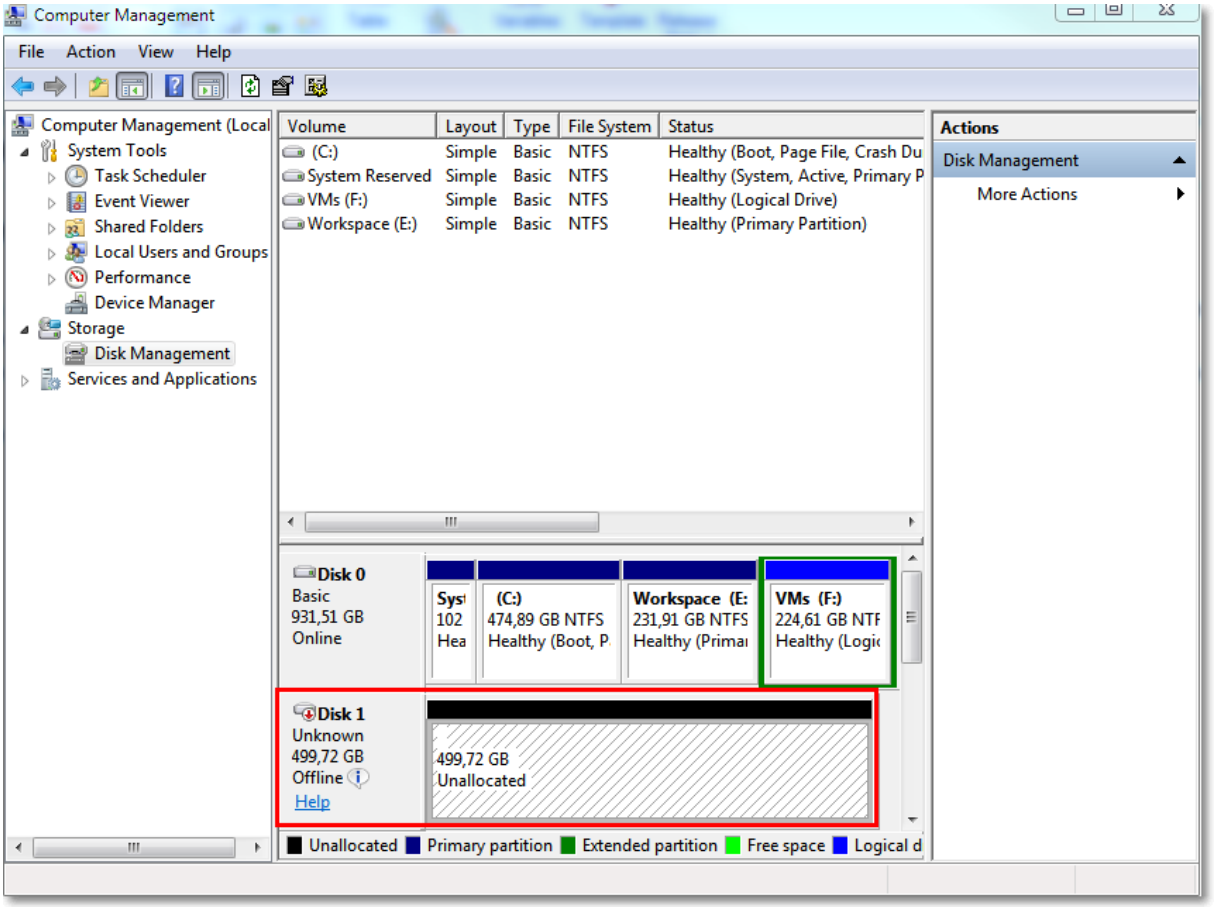
1. Ga naar **Configuratiescherm** > **Systeembeheer** > **iSCSI-initiator**.

   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:**.

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 Cyberbescherming-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 Cyberbescherming-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 Cyberbescherming-service toegewezen aan de nieuwe agent. De belasting van de oude agents wordt minder.

Wanneer u een agent uit de Cyberbescherming-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.

Virtualisatieomgevingen beheren

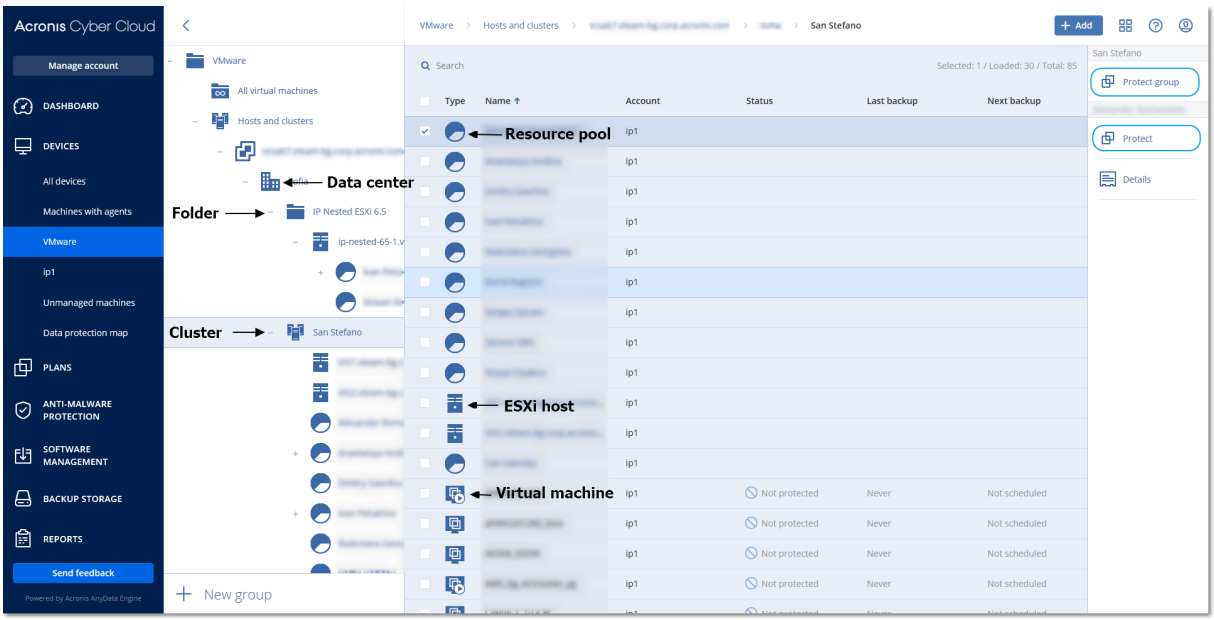
U kunt de vSphere-, Hyper-V- en Virtuozzo-omgevingen weergeven in hun eigen presentatie. Wanneer de betreffende agent is geïnstalleerd en geregistreerd, wordt het tabblad **VMware**, **Hyper-V** of **Virtuozzo** weergegeven onder **Apparaten**.

Op het tabblad **VMware** kunt u een back-up maken van de volgende vSphere-infrastructuurobjecten:

- Datacenter
- Map
- Cluster
- ESXi-host
- Resourcegroep

Elk van deze infrastructuurobjecten werkt als een groepsobject voor virtuele machines. Wanneer u een beschermingsschema toepast op een van deze groepsobjecten, wordt er een back-up gemaakt van alle virtuele machines die hierin zijn opgenomen. Klik op **Beschermen** om een back-up te maken van de geselecteerde groepsmachines of klik op **Groep beschermen** om een back-up te maken van de bovenliggende groepsmachines waarin de geselecteerde groep is opgenomen.

U hebt bijvoorbeeld het San Stefano-cluster geselecteerd en vervolgens de resourcegroep hierin geselecteerd. Als u op **Beschermen** klikt, wordt er een back-up gemaakt van alle virtuele machines in de geselecteerde resourcegroep. Als u op **Groep beschermen** klikt, wordt er een back-up gemaakt van alle virtuele machines in het San Stefano-cluster.



Op het tabblad **VMware** kunt u de toegangsreferenties voor de vCenter-server of stand-alone ESXi-host wijzigen zonder dat u de agent opnieuw hoeft te installeren.

De toegangsreferenties voor vCenter-server of ESXi-host wijzigen

1. Klik onder **Apparaten** op **VMware**.
2. Klik op **Hosts en clusters**.

3. Ga naar de lijst **Hosts en clusters** (rechts van de boomstructuur **Hosts en clusters**) en selecteer de vCenter-server of stand-alone ESXi-host die is opgegeven tijdens de installatie van Agent voor VMware.
4. Klik op **Details**.
5. Klik onder **Referenties** op de gebruikersnaam.
6. Geef de nieuwe toegangsreferenties op en klik vervolgens op **OK**.

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 (**Summary** (Samenvatting) > **Custom attributes**/**Annotations**/**Notes** (Aangepaste kenmerken/Aantekeningen/Opmerkingen), afhankelijk van het type client en de vSphere-versie). U kunt ook de kolommen **Last backup** (Laatste back-up) en **Backup status** (Back-upstatus) op het tabblad **Virtual Machines** (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**

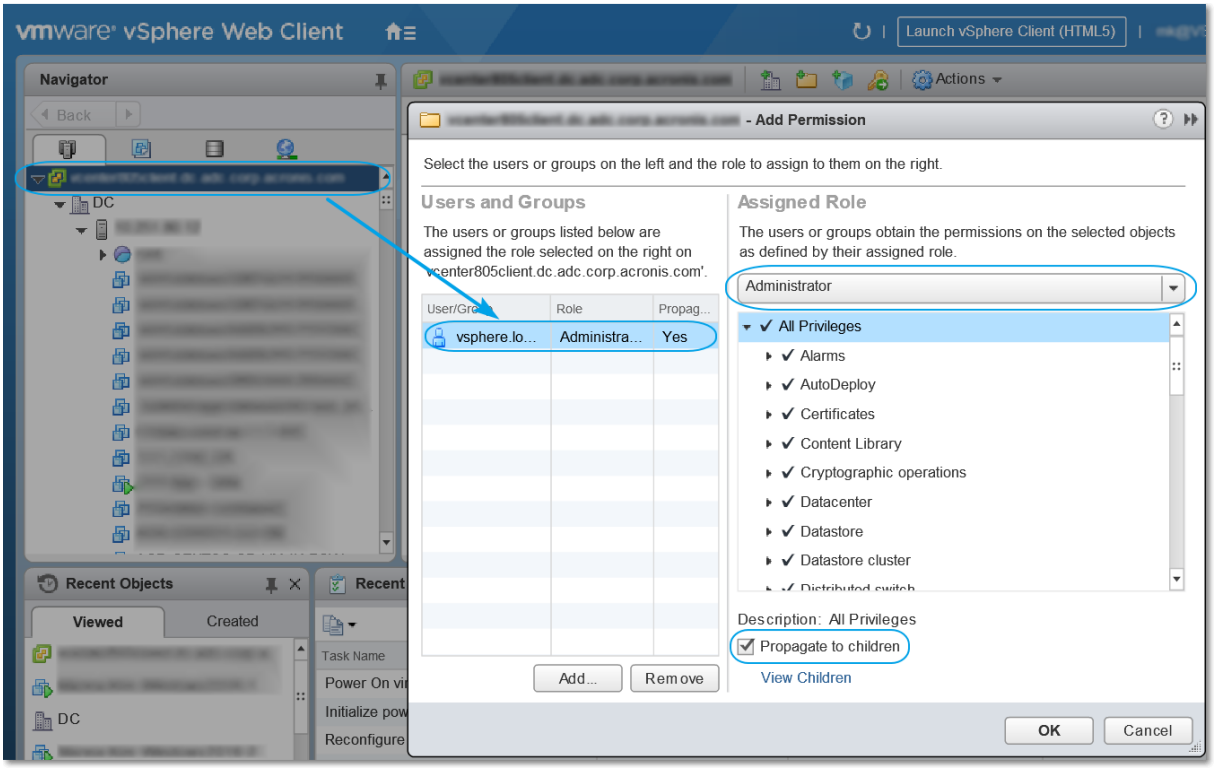
Agent voor VMware – vereiste rechten

Als u bewerkingen wilt uitvoeren met vCenter-objecten, zoals virtuele machines, ESXi-hosts, clusters, vCenter en meer, dan gebruikt Agent voor VMware de door een gebruiker opgegeven vSphere-referenties voor verificatie op vCenter of de ESXi-host. Het vSphere-account dat door Agent voor VMware wordt gebruikt voor verbinding met vSphere, moet de vereiste rechten hebben op alle niveaus van de vSphere-infrastructuur vanaf het vCenter-niveau.

Geef het vSphere-account met de nodige rechten op tijdens de installatie of configuratie van Agent voor VMware. Raadpleeg het gedeelte 'Virtualisatieomgevingen beheren' als u het account later moet wijzigen.

Ga als volgt te werk om de machtigingen toe te wijzen aan een vSphere-gebruiker op vCenter-niveau:

1. Meld u aan bij de vSphere-webclient.
2. Klik met de rechtermuisknop op vCenter en klik vervolgens op **Machtiging toevoegen**.
3. Selecteer of voeg een nieuwe gebruiker toe met de vereiste rol (de rol moet alle vereiste machtigingen uit de onderstaande tabel bevatten).
4. Selecteer de optie **Doorgeven aan onderliggende items**.



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	**Licenties**	+	+	+	+
	Methoden uitschakelen	+	+	+	
	Methoden inschakelen	+	+	+	

	Aangepaste kenmerken beheren	+	+	+	
	Aangepast kenmerk instellen	+	+	+	
Host > **Configuratie**	**Opslagpartitie configureren**				+
Host > **Lokale bewerkingen**	**VM maken**				+
	VM verwijderen				+
	VM opnieuw configureren				+
Netwerk	**Netwerk toewijzen**		+	+	+
Resource	**VM toewijzen aan resourcegroep**		+	+	+
Virtuele machine > **Configuratie**	**Bestaande schijf toevoegen**	+	+		+
	Nieuwe schijf toevoegen		+	+	+
	Apparaat toevoegen of verwijderen		+		+
	Geavanceerd	+	+	+	
	Aantal CPU's wijzigen		+		
	Schijfwijziging bijhouden	+		+	
	Schijf leasen	+		+	
	Geheugen		+		
	Schijf verwijderen	+	+	+	+
	Naam wijzigen		+		
	Aantekening instellen				+
	Instellingen		+	+	+
Virtuele machine > **Gastbewerkingen**	**Uitvoering van het programma voor gastbewerkingen**	+**			
	Query's voor gastbewerkingen	+**			

	Wijzigingen voor gastbewerkingen	+**			
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 > **Inrichting**	**Schijftoegang toestaan**		+	+	+
	Schijftoegang met alleen-lezen toestaan	+		+	
	Download van virtuele machine toestaan	+	+	+	+
Virtuele machine > **Status**	**Momentopname maken**	+		+	+
	Momentopname verwijderen	+		+	+
vApp	**Virtuele machine toevoegen**				+

* Dit recht is alleen vereist voor back-ups van versleutelde machines.

** Dit recht is alleen vereist voor applicatiegerichte back-ups.

14.24.3 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 Cyberbescherming-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**.

14.24.4 Beperkingen instellen voor het totale aantal virtuele machines waarvan gelijktijdig een back-up kan worden gemaakt

Met de back-upoptie **Plannen** definieert u het aantal virtuele machines waarvan gelijktijdig een back-up kan worden gemaakt door een agent tijdens de uitvoering van het opgegeven beschermingsschema.

Wanneer meerdere beschermingsschema's elkaar in de tijd overlappen, wordt de som berekend van de aantallen die zijn opgegeven in de betreffende back-upopties. Hoewel het resulterende totale aantal in de software is beperkt tot 10, kunnen overlappende plannen van invloed zijn op de back-upprestaties en zowel de opslag van de host als van de virtuele machine overbelasten.

U kunt verdere beperkingen instellen voor het totale aantal virtuele machines waarvan gelijktijdig een back-up kan worden gemaakt door Agent voor VMware of Agent voor Hyper-V.

Beperkingen instellen voor het totale aantal virtuele machines waarvan een back-up kan worden gemaakt door Agent voor VMware (Windows) of Agent voor Hyper-V

1. Maak een nieuw tekstdocument op de machine waarop de agent wordt uitgevoerd, en open het in een teksteditor, zoals Kladblok.

2. Kopieer en plak de volgende regels in het bestand:

```
Windows Register-editor versie 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. Ga als volgt te werk om de agent opnieuw op te starten:
   a. Klik in het menu **Start** op **Uitvoeren** en typ: **cmd**
   b. Klik op **OK**.
   c. Voer de volgende opdrachten uit:

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

Beperkingen instellen voor het totale aantal virtuele machines waarvan een back-up kan worden gemaakt door Agent voor VMware (Virtual Appliance)

1. Als u de opdrachtshell wilt starten, drukt u op CTRL+SHIFT+F2 in de gebruikersinterface van de virtuele toepassing.
2. Open het bestand **/etc/Acronis/MMS.config** in een teksteditor, zoals **vi**.
3. Zoek het volgende gedeelte:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Vervang `10` door de decimale waarde van de limiet die u wilt instellen.
5. Sla het bestand op.
6. Voer de opdracht `reboot` uit om de agent opnieuw te starten.

14.24.5 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	Virtuele Virtuozzo-machine	Virtuozzo-container	Virtuele Virtuozzo Hybrid Infrastructure-machine	Virtuele Scale Computing HC3-machine	Virtuele RHV/oVirt-machine
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	+	+	+	-	-	+	-	+

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.

Voor instructies over het uitvoeren van een migratie raadpleegt u de volgende gedeelten:

- Physical-to-virtual (P2V) - 'Fysieke machine naar virtueel'
- Virtual-to-virtual (V2V) - 'Virtuele machine'
- Virtual-to-physical (V2P) - 'Virtuele machine' of 'Schijven herstellen met opstartmedia'

U kunt een V2P-migratie uitvoeren in de webinterface, maar in bepaalde gevallen raden we aan om opstartmedia te gebruiken. U kunt soms de media voor migratie naar ESXi of Hyper-V gebruiken.

Met de media kunt u het volgende doen:

- P2V-migratie of V2P-migratie of V2V-migratie vanuit Virtuozzo uitvoeren van een Linux-machine die logische volumes (LVM) bevat. Agent voor Linux of opstartmedia gebruiken om de back-up- en opstartmedia voor herstel te maken.
- Stuurprogramma's opgeven voor specifieke hardware die essentieel is voor de opstartbaarheid van het systeem.

14.24.6 Virtuele Windows Azure- en Amazon EC2-machines

Als u een back-up wilt maken van een virtuele Windows 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 Windows Azure- en Amazon EC2-machines niet kunnen worden opgestart vanaf opstartmedia. Als u wilt herstellen naar een nieuwe virtuele Windows Azure- of Amazon EC2-machine, volgt u de volgende procedure.

Een machine herstellen als virtuele Windows Azure- of Amazon EC2-machine

1. Maak een nieuwe virtuele machine vanaf een image/sjabloon in Windows 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.

15 Noodherstel

Opmerking
Deze functionaliteit is alleen beschikbaar met de Disaster Recovery-add-on van de Cyberbescherming-service.

15.1 Over Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) – een deel van Cyberbescherming 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. 448).

15.1.1 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 vijf 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.

15.2 Softwarevereisten

15.2.1 Ondersteunde besturingssystemen

Beveiliging met een herstelserver is getest voor de volgende besturingssystemen:

- CentOS 6.6, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Debian 9
- Ubuntu 16.04, 18.04
- 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

Besturingssystemen voor Windows-desktop worden niet ondersteund vanwege Microsoft-productvoorwaarden.

De software werkt mogelijk met andere Windows-besturingssystemen en Linux-distributies, maar dit is niet gegarandeerd.

15.2.2 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
- 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
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Kernel-based Virtual Machines (KVM)
- 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
- 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.

15.2.3 Beperkingen

De volgende platforms en configuraties worden niet ondersteund in Cyber Disaster Recovery Cloud:

1. Niet-ondersteunde platforms:
   - Agent voor Virtuozzo
   - macOS
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
   - Fysieke en virtuele Linux-machines die logische volumes (LVM) hebben en waarvan back-ups worden gemaakt met een agent
   - Fysieke en virtuele Linux-machines met volumes die zijn geformatteerd met het XFS-bestandssysteem
   - Bestandssysteem zonder een partitietabel
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.

15.3 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 "Failback uitvoeren naar een virtuele machine" (p. 457) en "Failback uitvoeren naar een fysieke machine" (p. 461) voor meer informatie over het failbackproces.

15.4 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 bij het maken van een nieuw beschermingsschema. Wanneer u de functionaliteit voor noodherstel hebt ingeschakeld en het

schema hebt toegepast op uw machines, wordt voor elke beschermde machine 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 de beschermde machine. 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

- We raden u aan om noodherstel vooraf te configureren. U kunt de test- of productiefailover dan uitvoeren vanaf een van de herstelpunten die zijn gegenereerd nadat de herstelserver is gemaakt voor het apparaat. Herstelpunten die zijn gegenereerd toen een apparaat niet was beschermd met noodherstel (er is bijvoorbeeld geen herstelserver 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 agenten 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. 441) voor meer informatie.

Een beschermingsschema voor noodherstel maken

1. Ga in de serviceconsole 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. 448) voor meer informatie.
- U kunt de standaardnetwerkconfiguratie bewerken. Zie "Connectiviteit instellen" (p. 414) 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. 412) en "Cloudinfrastructuur" (p. 413) voor meer informatie.

15.4.1 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.

15.4.2 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. 434).
- 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. 425). 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**.

15.5 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.

15.5.1 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 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.

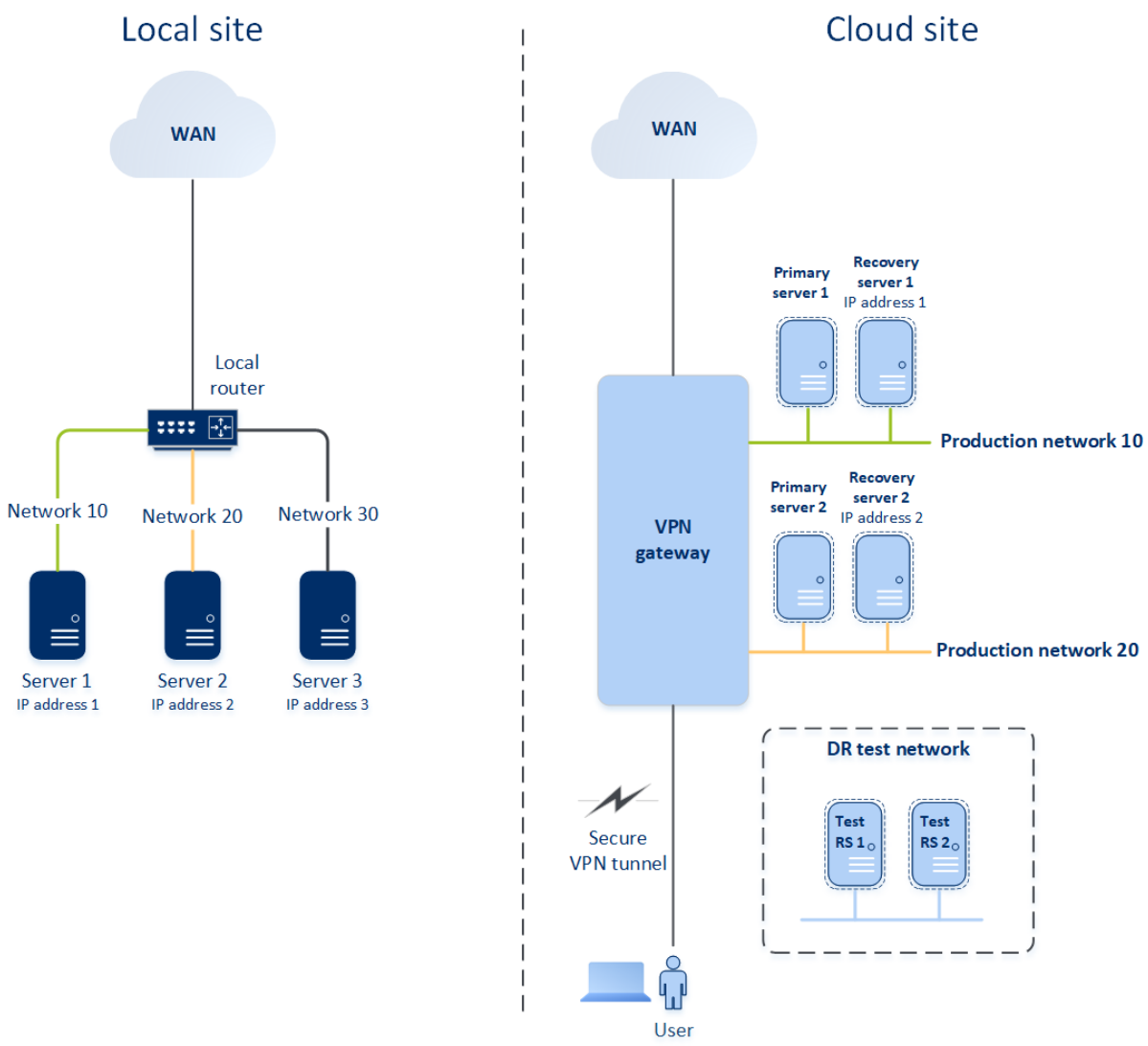
  Voor toegang tot een lokale site met dit type verbinding moet u een VPN-toepassing implementeren op de lokale site.

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.

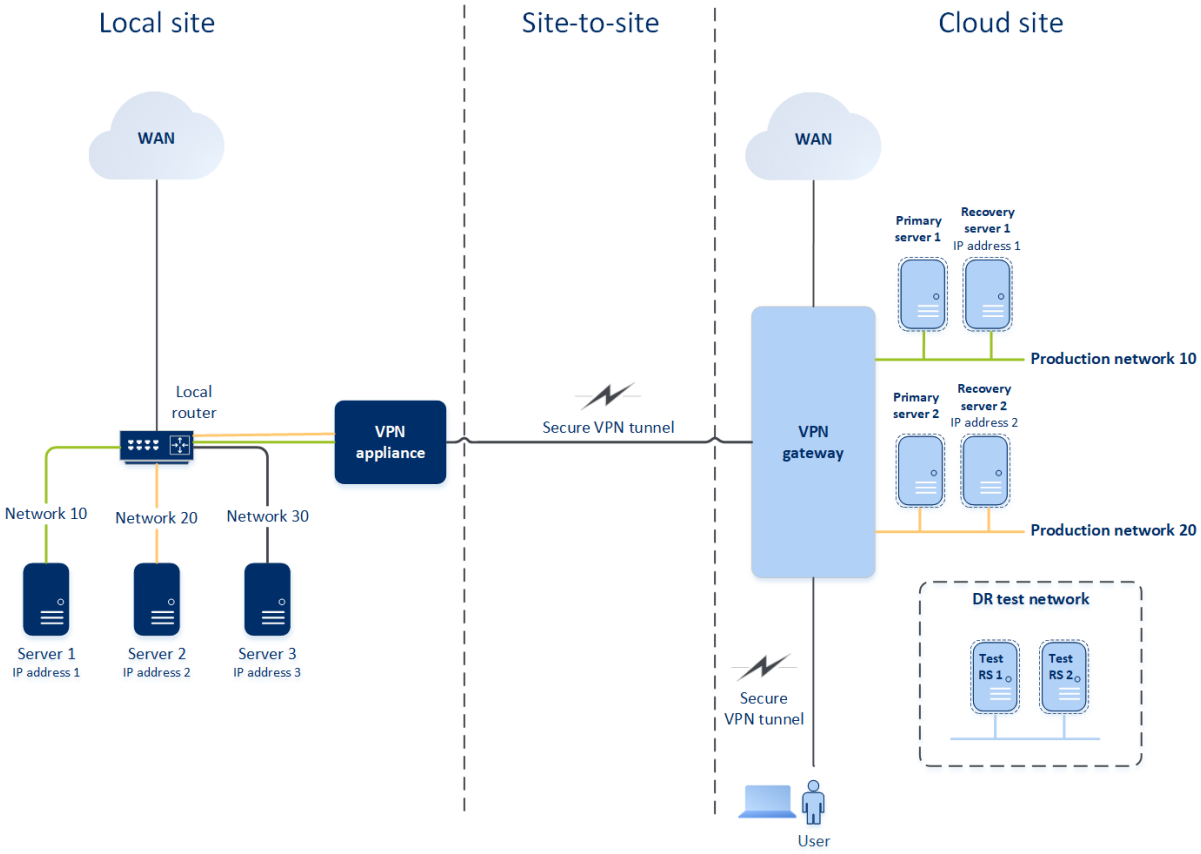


Site-to-site OpenVPN-verbinding

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 vijf 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 serviceconsole, 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

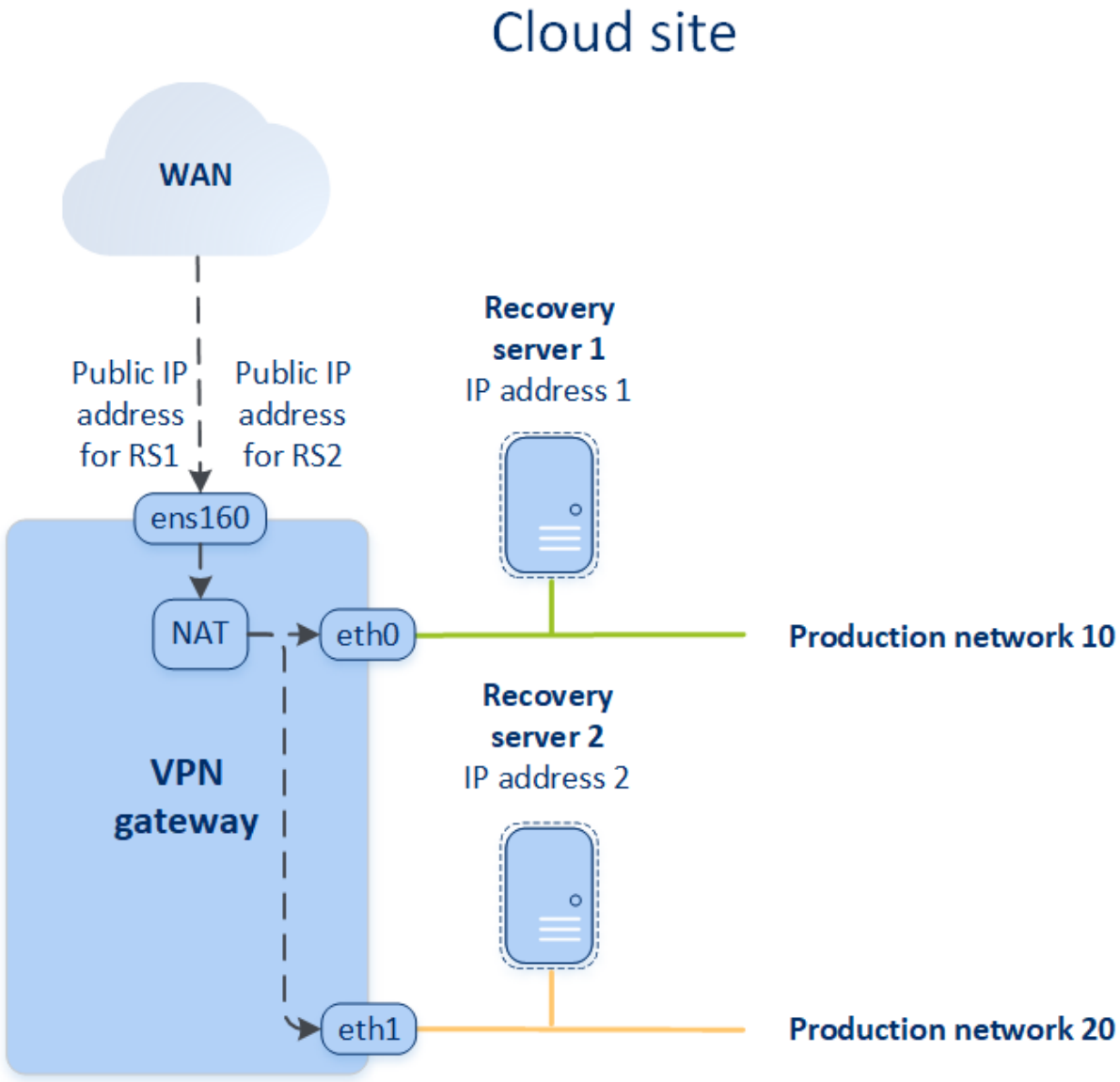
Een **herstelserver**: een replica van de oorspronkelijke machine op basis van de beveiligde serverback-ups die in de cloud zijn opgeslagen. Herstelservers worden gebruikt om workloads vanaf de oorspronkelijke servers te verplaatsen in het geval van een ramp.

Bij het maken van een herstelserver moet u de volgende netwerkparameters opgeven:

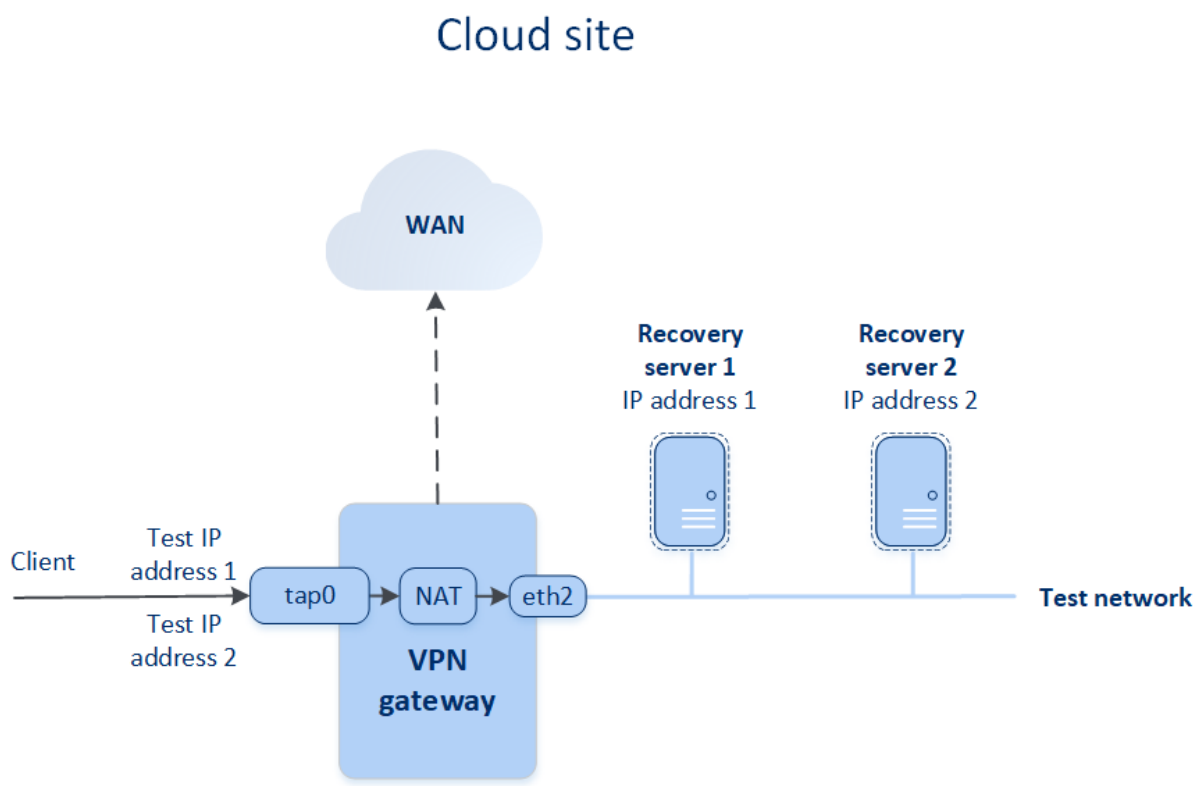
- **Cloudnetwerk** (verplicht): een cloudnetwerk gebruikt voor verbinding met een herstelserver.
- **IP-adres in productienetwerk** (verplicht): een IP-adres waarmee een virtuele machine voor een herstelserver wordt gestart. Dit adres wordt zowel in productie- als in testnetwerken gebruikt. Voor de start 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 "Bijlage A. Site-naar-site Open VPN - Aanvullende informatie" (p. 639) 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 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 serviceconsole, 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. 442) 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.

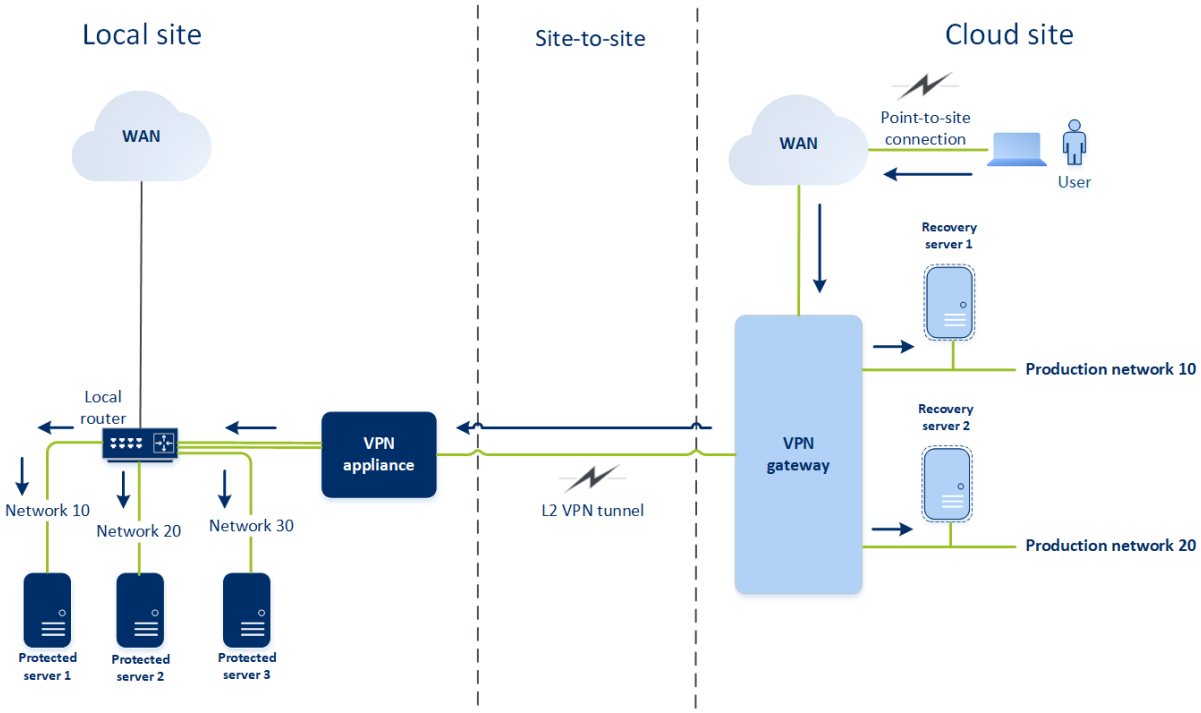
De point-to-site-verbinding is een veilige externe VPN-verbinding naar uw cloudsite en lokale site via uw eindpuntapparaten (zoals computer of laptop). Deze is beschikbaar nadat u een site-to-site OpenVPN-verbinding met de Cyber Disaster Recovery Cloud-site tot stand hebt gebracht. Dit type verbinding 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 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.

15.5.2 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 serviceconsole 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 serviceconsole 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 Cyberbescherming-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 serviceconsole 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 serviceconsole 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 serviceconsole 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 serviceconsole 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**.

15.5.3 Vereisten

- Een geconfigureerde multi-site IPsec VPN-connectiviteit. Zie "Multi-site IPsec VPN configureren" (p. 427) voor meer informatie over het configureren van de multi-site IPsec VPN-connectiviteit.
- Openbaar IP-adres van elke lokale IPsec VPN-gateway.
- Plan uw cloudnetwerk zo dat er voldoende IP-adressen zijn 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, moet u de volgende IP-protocollen en UDP-poorten toestaan op de lokale sites: IP Protocol ID 50 (ESP), UDP-poort 500 (IKE) en UDP-poort 4500.

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**.
   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. 429) 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. 430) 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.
- Let op: 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 **Starten** als u wilt dat de cloudsite de verbinding initieert, of in **Routeren** als u wilt dat beide kanten de verbinding kunnen initiëren (geschikt voor firewalls die de optie Routeren 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.
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

Parameter	Beschrijving
	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. 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.

Parameter	Beschrijving
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. **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. 442) 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. 442) 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

- Er is een multi-site IPsec VPN-connectiviteit geconfigureerd.
- De VPN-toepassing is geïnstalleerd op de lokale site.

De point-to-site-verbinding met de lokale site configureren

1. Ga in de serviceconsole 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 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 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/.
   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 OpenVPN.
   e. Meld u aan bij de OpenVPN-client met de Cyber 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 Cloud om tweeledige verificatie in te stellen voor hun accounts.

Als gevolg hiervan kan uw gebruiker verbinding maken met machines op de lokale site.

15.5.4 Netwerkbeheer

In dit gedeelte worden scenario's voor netwerkbeheer beschreven.

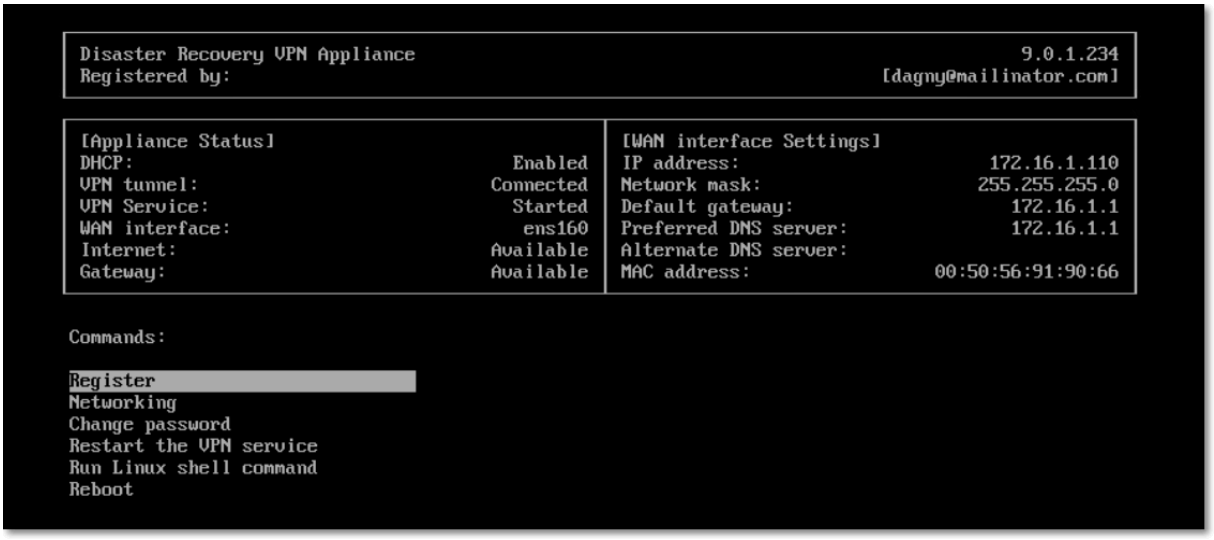
Netwerken beheren

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 serviceconsole worden de interfaces weergegeven, gebaseerd op de informatie van de VPN-toepassing.

Een netwerk verwijderen dat is uitgebreid naar de cloud

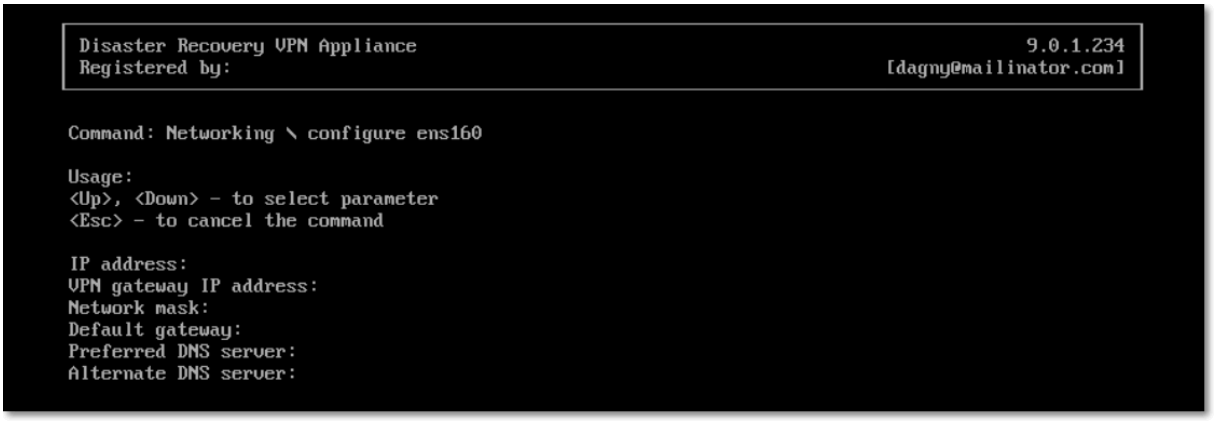
1. Meld u aan bij de VPN-toepassingsconsole.
2. Selecteer in het gedeelte **Netwerken** de interface die u wilt verwijderen en klik vervolgens op **Netwerkinstellingen wissen**.
3. Bevestig de bewerking.

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 vijf 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 serviceconsole (**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 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 serviceconsole 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 serviceconsole 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
   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 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 serviceconsole 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 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 serviceconsole 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

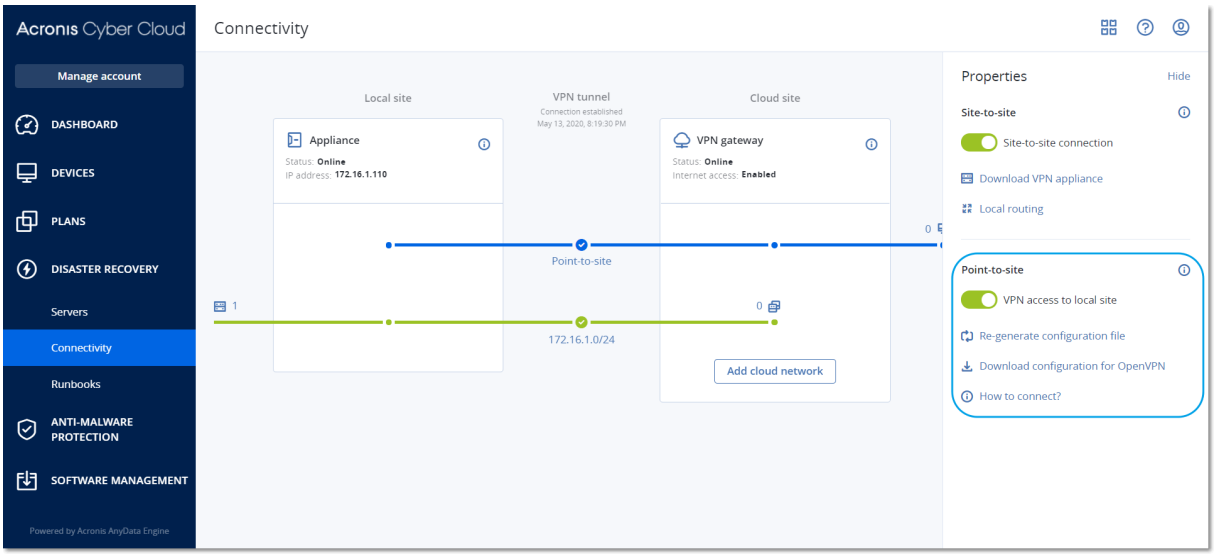
1. Ga naar **Noodherstel** > **Connectiviteit**.
2. Klik op **Eigenschappen weergeven** en klik vervolgens op **Lokale routering**.
3. Geef de lokale netwerken op in de CIDR-indeling.
4. Klik op **Opslaan**.

De servers van de opgegeven lokale netwerken kunnen dan communiceren met de cloudservers.

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 serviceconsole 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:

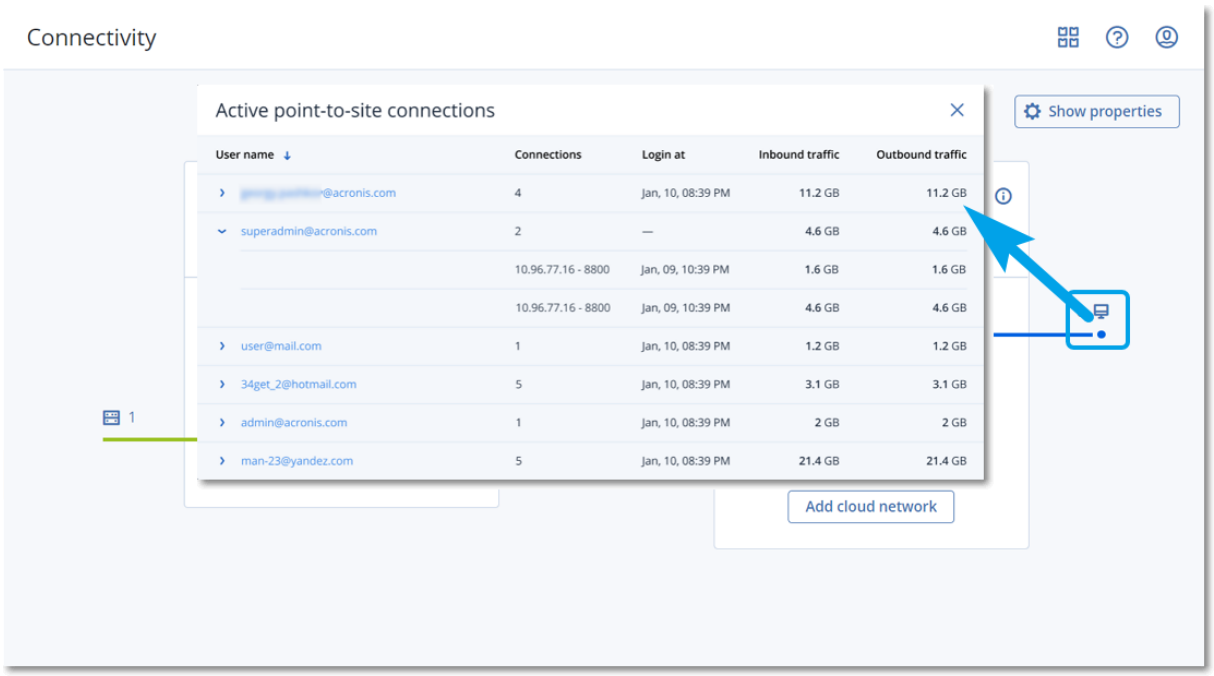
- Als u vermoedt dat het configuratiebestand is beschadigd.
- Als tweeledige verificatie is ingeschakeld voor uw account.

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.



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**	Klik op **Opnieuw proberen** en controleer of er een

Probleem	Mogelijke oplossing
de IKE fase 1-onderhandeling. Controleer de IPsec IKE-instellingen in de cloud en op de lokale sites.	specifiekere foutmelding wordt weergegeven. Een meer specifieke foutmelding kan bijvoorbeeld een foutmelding zijn over algoritmen die niet overeenkomen of een onjuiste vooraf gedeelde sleutel. **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

Probleem	Mogelijke oplossing
	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**.
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.

15.5.5 Vereisten

Multi-site IPsec VPN-connectiviteit is geconfigureerd.

Het .zip-archief met de logbestanden downloaden

1. Ga in de serviceconsole naar **Noodherstel** > **Connectiviteit**.
2. Klik op het tandwielpictogram naast de VPN-gateway van de cloudsite.
3. Klik op **Logbestand downloaden**.

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 geeft meer informatie over de IPsec VPN-logbestanden die deel uitmaken van 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.

15.6 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.

15.6.1 Herstelserver maken

U kunt de onderstaande instructies volgen of de videoles bekijken.

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.

   Let op de compute-punten naast elke optie. Het aantal compute-punten geeft de kosten per uur weer voor het uitvoeren van de herstelserver.
4. Geef het cloudnetwerk op waarmee de server wordt verbonden.
5. 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.
6. [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.
7. [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.
8. [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.
9. [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.

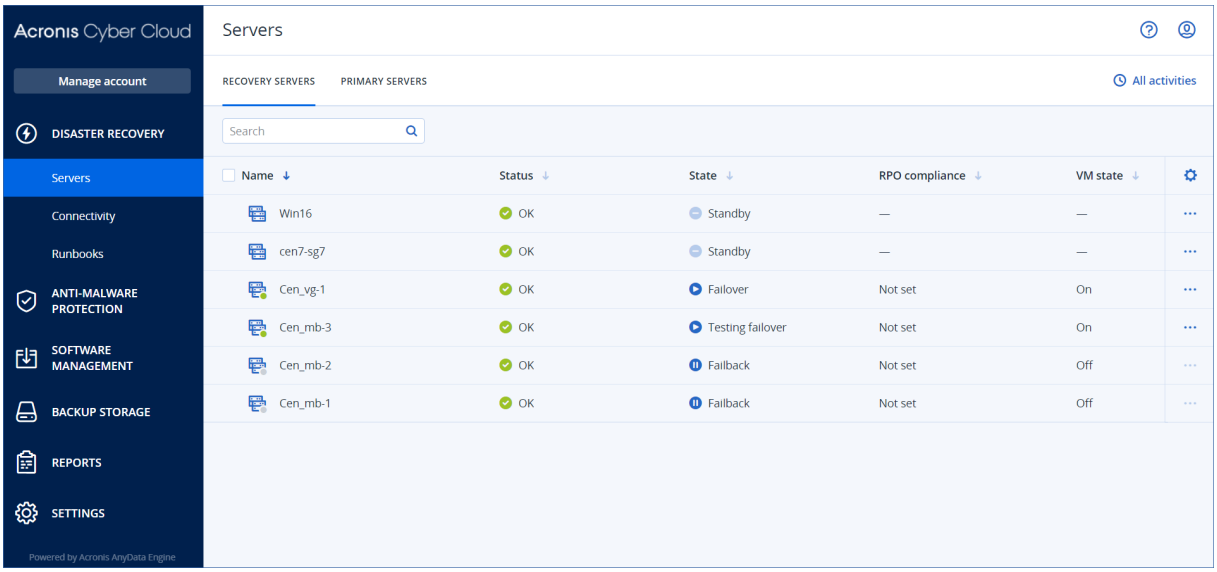
   Voor de optie **Openbaar IP-adres gebruiken** moet de optie **Internettoegang** zijn ingeschakeld.

   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.
10. [Optioneel] Als de back-ups voor de geselecteerde machine zijn versleuteld, kunt u het wachtwoord opgeven dat automatisch wordt gebruikt wanneer een virtuele machine voor de herstelserver wordt gemaakt vanaf de versleutelde back-up. Klik op **Opgeven** en geef de

gebruikersnaam en het wachtwoord op. Standaard ziet u de meest recente back-up in de lijst. Als u alle back-ups wilt bekijken, selecteert u **Alle back-ups weergeven**.

11. [Optioneel] Wijzig de naam van de herstelserver.
12. [Optioneel] Typ een beschrijving voor de herstelserver.
13. [Optioneel] Klik op het tabblad **Cloudfirewallregels** om de standaardfirewallregels te bewerken. Zie "Firewallregels instellen voor cloudservers" (p. 466) voor meer informatie.
14. Klik op **Maken**.

De herstelserver wordt weergegeven op het tabblad **Noodherstel** > **Servers** > **Herstelservers** van de serviceconsole. U kunt de instellingen ook zien als u de oorspronkelijke machine selecteert en op **Noodherstel** klikt.



15.6.2 Hoe failover werkt

Productiefailover

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

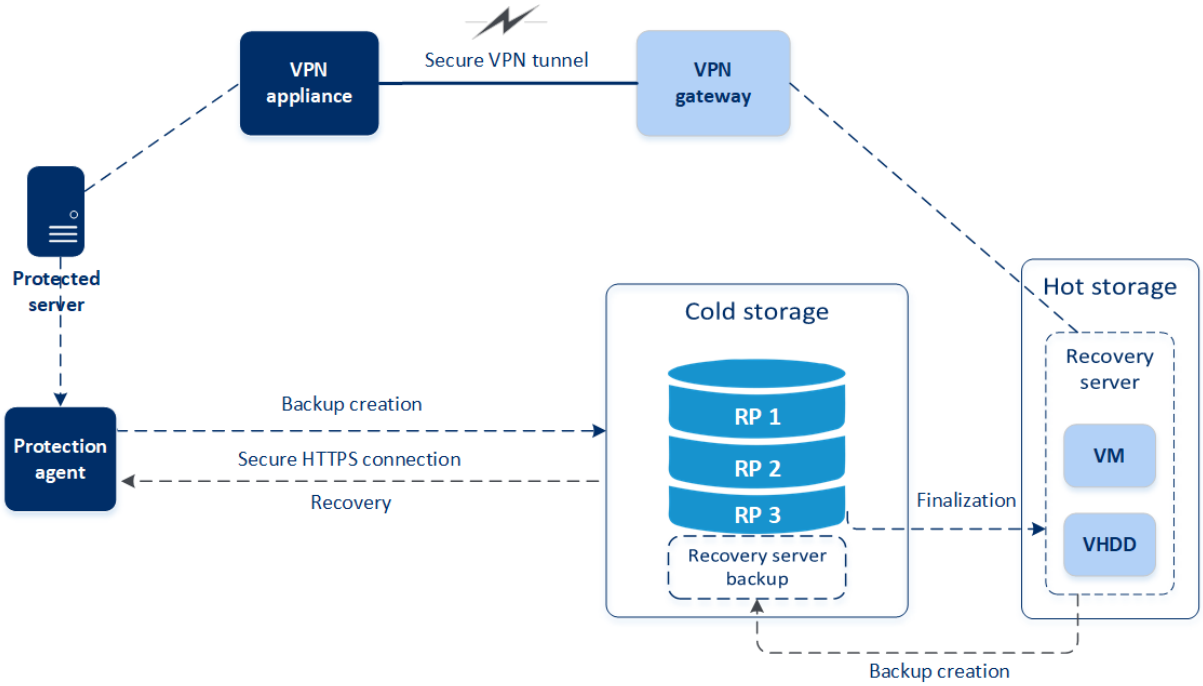
Wanneer u een herstelserver maakt, blijft deze de status **Stand-by** behouden. De overeenkomstige virtuele machine bestaat pas als u de failover start. Voordat u het failoverproces start, moet u ten minste één back-up van een schijfimage (met opstartvolume) van uw oorspronkelijke machine maken.

Bij het starten van het failoverproces selecteert u het herstelpunt 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 ('cold storage') naar de noodherstelopslag ('hot storage'). Tijdens het voltooien is de server toegankelijk en bruikbaar, maar de prestaties zijn minder dan normaal. Na het voltooien zijn de serverprestaties weer als normaal. De serverstatus verandert in **Failover**. De workload is nu verplaatst van de oorspronkelijke machine naar de herstelserver in 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 **testfailover** wordt de virtuele machine niet voltooid. De agent leest de inhoud van de virtuele schijven dan rechtstreeks uit de back-up (dat wil zeggen voert willekeurige toegang tot verschillende delen van de back-up uit). Zie "Een testfailover uitvoeren" (p. 451) voor meer informatie over het proces van een testfailover.

Een testfailover uitvoeren

Bij het testen van een failover wordt een herstelserver gestart in een test-VLAN dat is geïsoleerd van uw productienetwerk. U kunt meerdere herstelservers tegelijkertijd testen om de interactie te 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 machines in uw lokale netwerk.

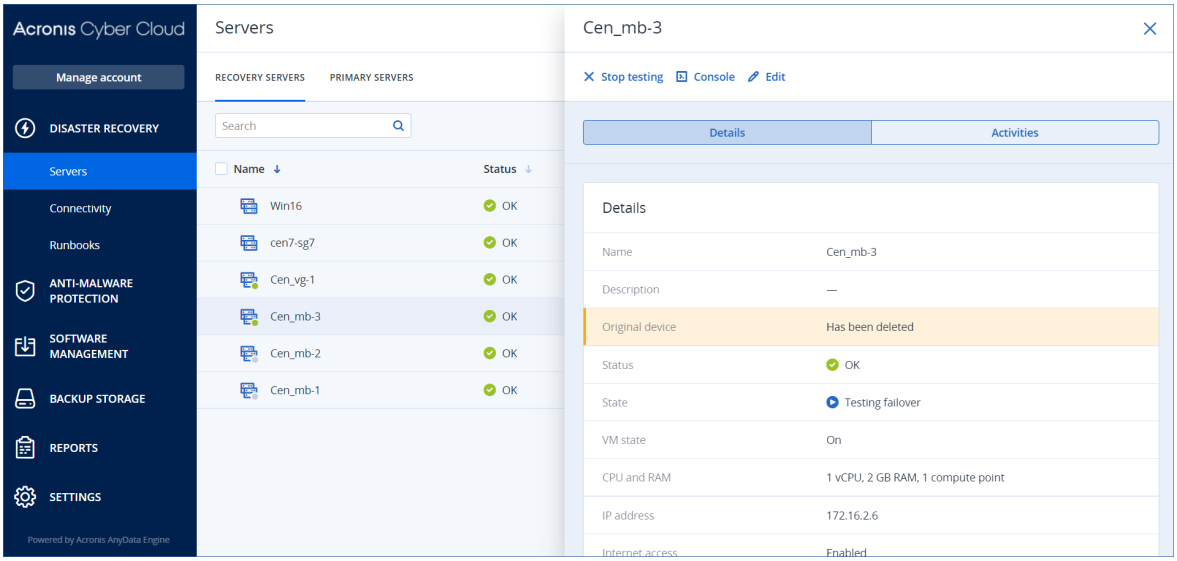
Hoewel het testen van een failover optioneel is, raden we u aan om dit regelmatig te doen. Maak een afweging van kosten en veiligheid en kies een frequentie die geschikt voor u is. Het is verstandig

gebruik te maken van een runbook: een set instructies die beschrijven hoe de productieomgeving in de cloud bedrijfsklaar kan worden gemaakt.

Het wordt aanbevolen om van te voren een herstelserver te maken om uw apparaten te beschermen tegen een noodgeval. U kunt de testfailover dan uitvoeren vanaf een van de herstelpunten die zijn gegenereerd nadat de herstelserver is gemaakt voor het apparaat.

Een test-failover 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 en klik vervolgens op **Failover testen**.
   Wanneer de herstelserver start, wordt de status gewijzigd in **Failover testen**.



6. 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.
7. 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.

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 initieert, start de herstelserver in het productienetwerk. Alle beschermingsschema's worden ingetrokken van de oorspronkelijke machine. Automatisch wordt een nieuw beschermingsschema gemaakt en toegepast op de herstelserver.

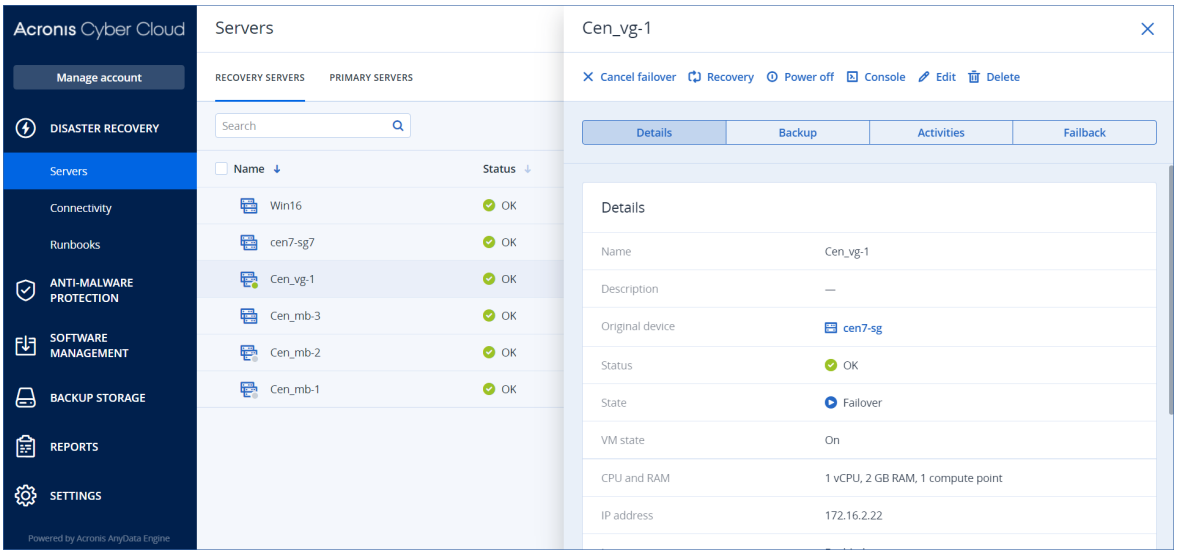
Er moet ten minste één herstelpunt worden gemaakt voordat er wordt overgeschakeld naar een herstelserver.

Het is verstandig om van te voren een herstelserver te maken om uw apparaten te beschermen tegen een noodgeval. U kunt de productiefailover dan uitvoeren vanaf een van de herstelpunten die zijn gegenereerd nadat de herstelserver is gemaakt voor het apparaat.

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 serviceconsole naar **Noodherstel** > **Servers** > **Herstelservers** en selecteer de herstelserver.
3. Klik op **Failover**.
4. Selecteer het type failover **Productiefailover**.
5. Selecteer het herstelpunt en klik vervolgens op **Productiefailover starten**.
   Wanneer de herstelserver start, verandert de status ervan in **Voltooien** en na verloop van tijd in **Failover.** Belangrijk: hoewel de voortgangsindicator draait, is de server in beide statussen wel beschikbaar. Zie "Hoe failover werkt" (p. 450) voor meer informatie.



6. Controleer in de console of de herstelserver is gestart. Klik op **Noodherstel** > **Servers**, selecteer de herstelserver en klik vervolgens op **Console**.
7. 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 kiest voor failback uitvoeren, dan 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.

15.6.3 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 de server blijven gebruiken op uw lokale site.

Tijdens het failbackproces naar een virtuele doelmachine 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 serviceconsole). U kunt deze informatie bekijken en gebruiken om uw activiteiten te plannen en, indien nodig, uw klanten te waarschuwen voor een komende downtimeperiode.

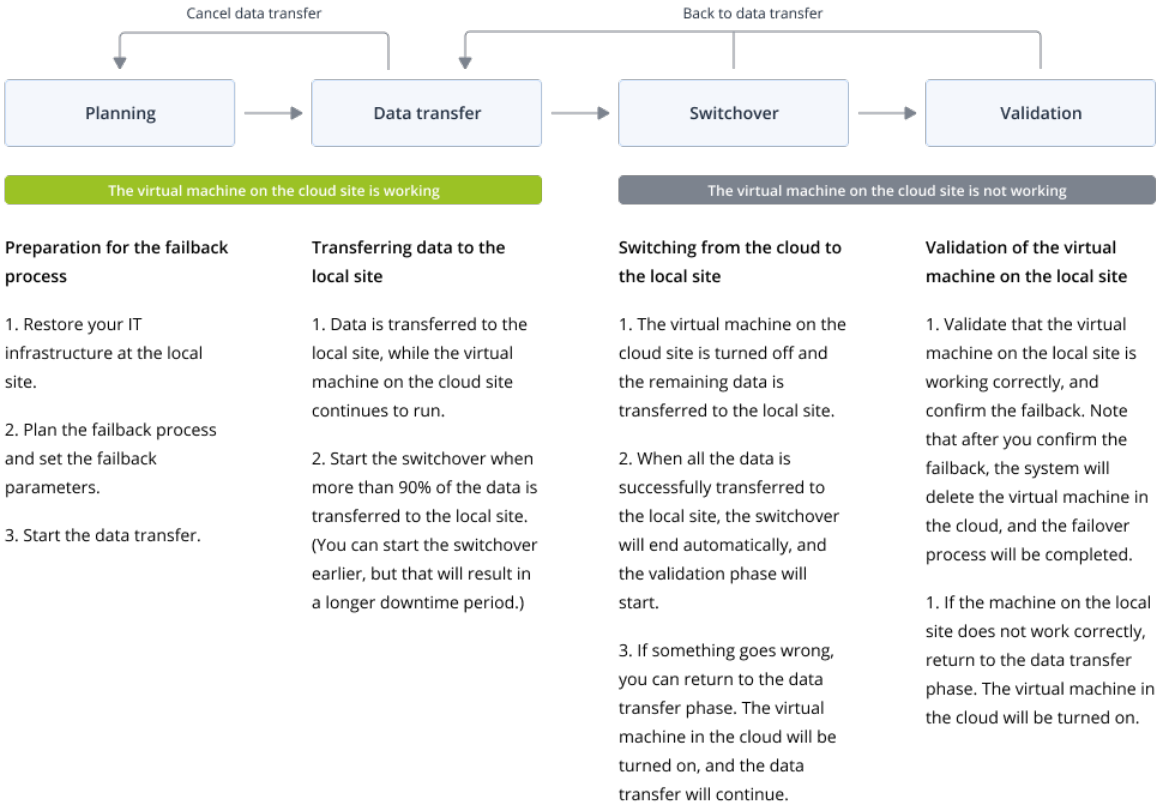
Er is een verschil tussen het failbackproces naar virtuele doelmachines en het failbackproces naar fysieke doelmachines. Zie "Failback naar een virtuele doelmachine" (p. 455) en "Failback naar een fysieke doelmachine" (p. 460) voor meer informatie over de fasen van het failbackproces.

Opmerking
Runbookbewerkingen ondersteunen alleen de failback naar een fysieke machine. 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 het instellen van 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 starten op elk moment 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 fase van **switchover**.

Als u de downtime tot een minimum wilt beperken, start u de fase van **switchover** nadat meer dan 90% van de gegevens zijn 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 fase van **switchover** 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, inclusief de laatste incrementele back-up, overgedragen naar de lokale site. Let op: Wanneer de fase van **switchover** is voltooid, worden alle gegevens overgedragen naar de lokale site. Er gaan geen gegevens verloren en de virtuele machine op de lokale site is een exacte kopie van de virtuele machine in de cloud. U kunt de geschatte tijd tot voltooiing (downtimeperiode) van deze fase bekijken in de serviceconsole. Wanneer alle gegevens naar de lokale site zijn overgedragen, wordt de virtuele machine op de lokale site hersteld en wordt de fase van **Validatie** automatisch gestart.
4. **Validatie**. Tijdens deze fase is de virtuele machine op de lokale site klaar en kunt u deze inschakelen. 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 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.

Een failback uitvoeren naar een virtuele machine

1. Ga in de serviceconsole 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
Back-upgrootte	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 **back-upgrootte** 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 **back-upgrootte** (omdat wij aanbevelen de fase van **switchover** 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 uitgevoerd.
Instellingen van doelmachine	Instellingen van virtuele machine: • **Virtuele processors**. Selecteer het aantal virtuele processors.

Parameter	Beschrijving
	• **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). • **Thick**.
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**.
   De fase van **gegevensoverdracht** start. In de console wordt de volgende informatie weergegeven:
   - **Voortgang**. De parameter geeft aan hoeveel gegevens al zijn overgedragen naar de lokale site en de totale hoeveelheid gegevens die nog moet worden overgedragen. Let op: 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**. De parameter geeft aan hoelang de virtuele machine niet beschikbaar zal zijn als u nu de fase van **Switchover** start. De waarde wordt berekend op basis van de waarden van **Voortgang** en daalt in de loop van de tijd.

6. Klik op **Switchover** en vervolgens in het bevestigingsvenster nogmaals op **Switchover**.
   De fase van **Switchover** start. In de console wordt de volgende informatie weergegeven:
   - **Voortgang**. De parameter toont de voortgang van het herstel van de virtuele machine op de lokale site.
   - **Geschatte tijd om te voltooien**. De parameter geeft bij benadering het tijdstip aan waarop de fase van **Switchover** zal zijn voltooid en u de virtuele machine op de lokale site kunt inschakelen.
7. Nadat de fase van **Switchover** is voltooid, controleert u of de virtuele machine op uw lokale site 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**.

Failback naar een fysieke doelmachine

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Er is een verschil tussen het failbackproces naar een fysieke doelmachine en het failbackproces naar een virtuele doelmachine. De gegevensoverdracht van de back-up in de cloud naar de lokale site maakt geen deel uit van de geautomatiseerde workflow en wordt handmatig uitgevoerd nadat de virtuele machine in de cloud is uitgeschakeld. Daarom moet u rekening houden met een langere downtimeperiode bij het uitvoeren van een failback naar een fysieke machine.

Het failbackproces naar een fysieke doelmachine bestaat uit 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. 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 machine 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**.

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 uitvoeren naar een fysieke doelmachine op uw lokale site.

Een failback uitvoeren naar een fysieke machine

1. Ga in de serviceconsole naar **Noodherstel** > **Servers**.
2. Selecteer de herstelserver die de status **Failover** heeft.
3. Klik op het tabblad **Failback**.
4. Selecteer in het veld **Doel selecteren** de optie **Fysieke machine**.
5. [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.

6. Klik op **Switchover** en vervolgens in het bevestigingsvenster nogmaals op **Switchover**.
   De virtuele machine op de cloudsite wordt uitgeschakeld.
7. Herstel de server vanaf een back-up naar de fysieke machine op uw lokale site.
   - Volg bij het gebruik van opstartmedia de procedure zoals beschreven in 'Schijven herstellen met opstartmedia' in de Gebruikershandleiding voor Cyber Protection. Zorg ervoor dat u zich aanmeldt bij de cloud met het account waarvoor de server is geregistreerd en controleer of u de meest recente back-up hebt geselecteerd.
   - Als de doelmachine online is, kunt u de serviceconsole gebruiken. Ga naar het tabblad **Back-upopslag** en selecteer de cloudopslag. Ga naar **Machine waarmee u wilt bladeren** en selecteer de fysieke doelmachine. De geselecteerde machine moet zijn geregistreerd voor hetzelfde account als waarvoor de server is geregistreerd. Zoek de meest recente back-up van de server, klik op **Volledige machine herstellen** en stel vervolgens de andere herstelparameters in. Ga voor gedetailleerde instructies naar 'Een machine herstellen' in de Gebruikershandleiding voor Cyber Protection.
8. Controleer of het herstelproces volledig is uitgevoerd en of de herstelde machine goed werkt. Klik vervolgens op **Machine is hersteld**.
9. 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.

15.6.4 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.

15.7 Primaire servers instellen

In dit gedeelte wordt beschreven hoe u uw primaire servers kunt maken en beheren.

15.7.1 Primaire server maken

Vereisten

- Een van de typen connectiviteit met de cloudsite moet worden ingesteld.

Een primaire server maken

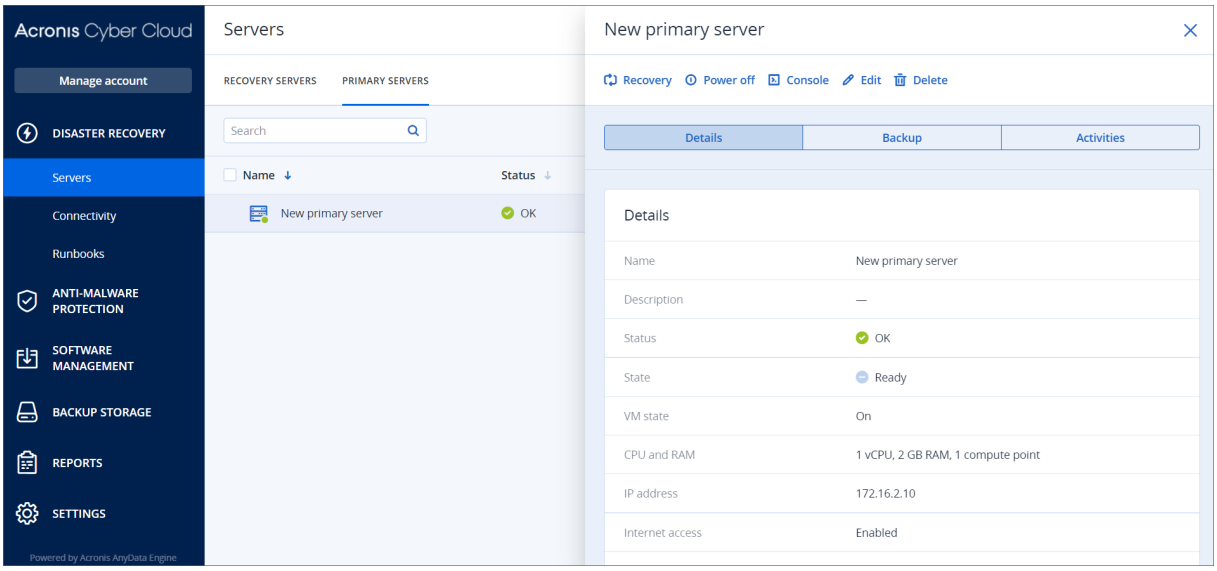
1. Ga naar **Noodherstel** > **Servers** > tabblad **Primaire servers**.
2. Klik op **Maken**.
3. Selecteer een sjabloon voor de nieuwe virtuele machine.
4. Selecteer het aantal virtuele kernen en de grootte van het RAM.
   Let op de compute-punten naast elke optie. Het aantal compute-punten geeft de kosten per uur weer voor het uitvoeren van de primaire server.

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. 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.

8. [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.
9. [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.
10. [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.
11. Definieer de naam van de primaire server.
12. [Optioneel] Typ een beschrijving voor de primaire server.
13. [Optioneel] Klik op het tabblad **Cloudfirewallregels** om de standaardfirewallregels te bewerken. Zie "Firewallregels instellen voor cloudservers" (p. 466) voor meer informatie.
14. 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.



15.7.2 Bewerkingen met een primaire server

De herstelserver wordt weergegeven in **Noodherstel** > **Servers** > tabblad **Primaire servers** van de serviceconsole.

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.

15.8 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

15.9 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

15.9.1 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 serviceconsole 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**.

15.9.2 De activiteiten van de cloudfirewall controleren

Wanneer de configuratie van de firewallregels van een cloudserver is bijgewerkt, is een logboek van de updateactiviteit beschikbaar in de serviceconsole. 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 serviceconsole op **Dashboard**> **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.

15.10 Back-up maken van de cloudservers

Back-ups van primaire en herstelservers worden gemaakt door Agent voor VMware. Deze is geïnstalleerd op de cloudsite. In de eerste release heeft deze back-up enigszins beperkte functionaliteit in vergelijking met een back-up die wordt uitgevoerd door lokale agenten. Deze beperkingen zijn tijdelijk en zullen in toekomstige releases worden verwijderd.

- De enig mogelijke back-uplocatie is de cloudopslag.
- Een beschermingsschema kan niet worden toegepast op meerdere servers. Elke server moet een eigen beschermingsschema hebben, zelfs als alle beschermingsschema's dezelfde instellingen hebben.
- Er kan slechts één beschermingsschema 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 beschermingsschema's voor cloudservers worden uitgevoerd op UTC-tijd.

15.11 Orchestration (runbooks)

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

Een runbook is een set instructies om te beschrijven hoe de productieomgeving in de cloud bedrijfsklaar kan worden gemaakt. U kunt runbooks maken in de serviceconsole. Als u het tabblad **Runbooks** wilt openen, selecteert u **Noodherstel** > **Runbooks**.

15.11.1 Waarom runbooks gebruiken?

Met runbooks kunt u het volgende doen:

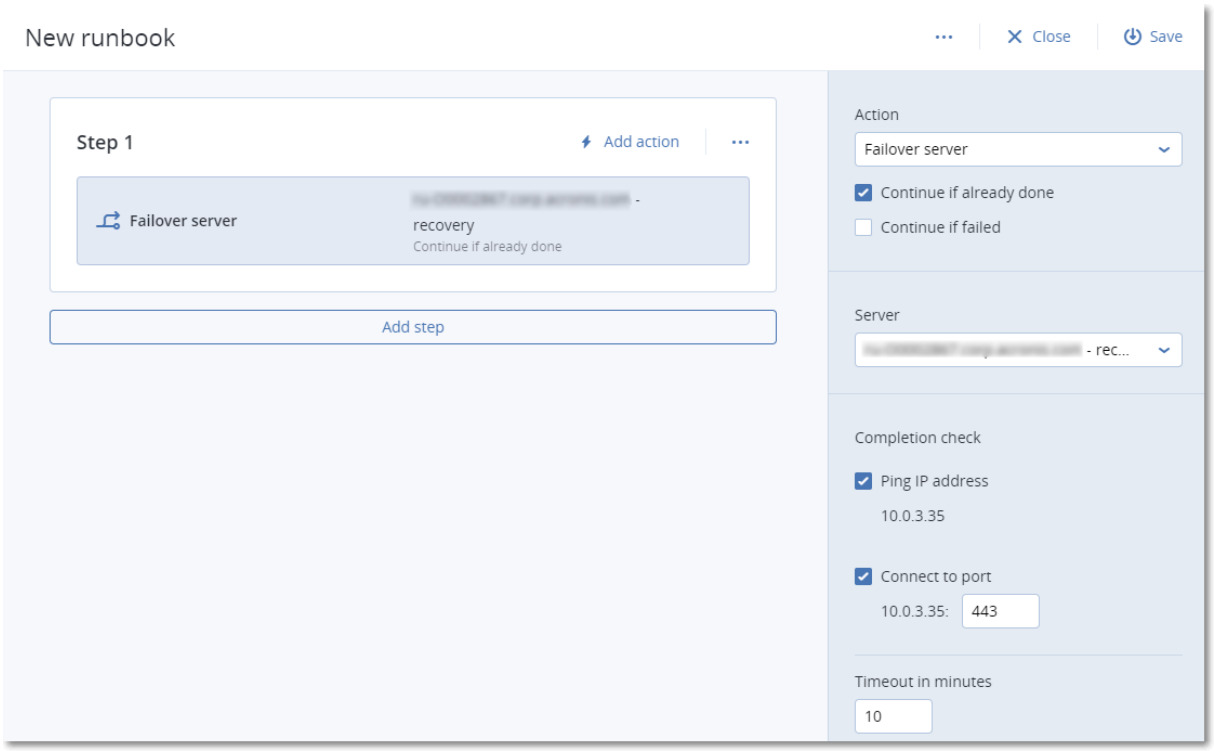
- Een failover van een of meerdere servers automatiseren
- Het failoverresultaat automatisch laten controleren door het IP-adres van de server te pingen en de verbinding met de door u opgegeven poort te controleren
- De volgorde van bewerkingen instellen voor servers met gedistribueerde toepassingen
- Handmatige bewerkingen toevoegen aan de workflow
- Verifieer de integriteit van uw noodhersteloplossing door runbooks uit te voeren in de testmodus.

15.11.2 Runbook maken

U kunt de onderstaande instructie volgen of de videoles bekijken.

Als u een runbook wilt maken, klikt u op **Runbook maken** > **Stap toevoegen** > **Actie toevoegen**. U kunt acties en stappen ook verplaatsen met slepen en neerzetten. Vergeet niet om het runbook een

duidelijke naam te geven. Klik tijdens het maken van een lang runbook regelmatig op **Opslaan**. Wanneer u klaar bent, klikt u op **Sluiten**.



Stappen en acties

Een runbook bestaat uit stappen die achtereenvolgens worden uitgevoerd. Een stap bestaat uit acties die tegelijkertijd starten. Een actie kan bestaan uit:

- Een bewerking die moet worden uitgevoerd met een cloudserver (**failover uitvoeren voor server**, **server starten**, **server stoppen**, **failback uitvoeren voor server**). Als u deze bewerking wilt definiëren, moet u de bewerking, de cloudserver en de bewerkingsparameters kiezen.
- Een handmatige bewerking die u in woorden moet omschrijven. Wanneer de bewerking is voltooid, moet een gebruiker op de knop voor bevestiging klikken om het runbook voort te zetten.
- De uitvoering van een ander runbook. Als u deze bewerking wilt definiëren, moet u het runbook 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.

Opmerking
In deze productversie moet een gebruiker een failback handmatig uitvoeren. Een runbook toont de prompt wanneer deze verplicht is.

Actieparameters

Alle bewerkingen met cloudservers hebben de volgende parameters:

- **Doorgaan indien al gereed** (standaard ingeschakeld)
  Deze parameter definieert het runbookgedrag wanneer de vereiste bewerking al is voltooid (er is bijvoorbeeld al een failover uitgevoerd of een server is al actief). Wanneer dit is ingeschakeld, geeft het runbook een waarschuwing weer en gaat dan verder. Wanneer dit is uitgeschakeld, mislukt de bewerking en mislukt het runbook.
- **Doorgaan indien mislukt** (standaard uitgeschakeld)
  Deze parameter definieert het runbookgedrag wanneer de vereiste bewerking mislukt. Wanneer dit is ingeschakeld, geeft het runbook een waarschuwing weer en gaat dan verder. Wanneer dit is uitgeschakeld, mislukt de bewerking en mislukt het runbook.

Voltooiingscontrole

U kunt voltooiingscontroles toevoegen aan de acties **failover uitvoeren voor server** en **server starten** om te waarborgen dat de server beschikbaar is en de nodige services levert. Als een van de controles mislukt, wordt de actie als mislukt beschouwd.

- **IP-adres pingen**
  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)
  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.

De standaardtime-out is 10 minuten. Indien gewenst, kunt u deze waarde wijzigen.

15.11.3 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**

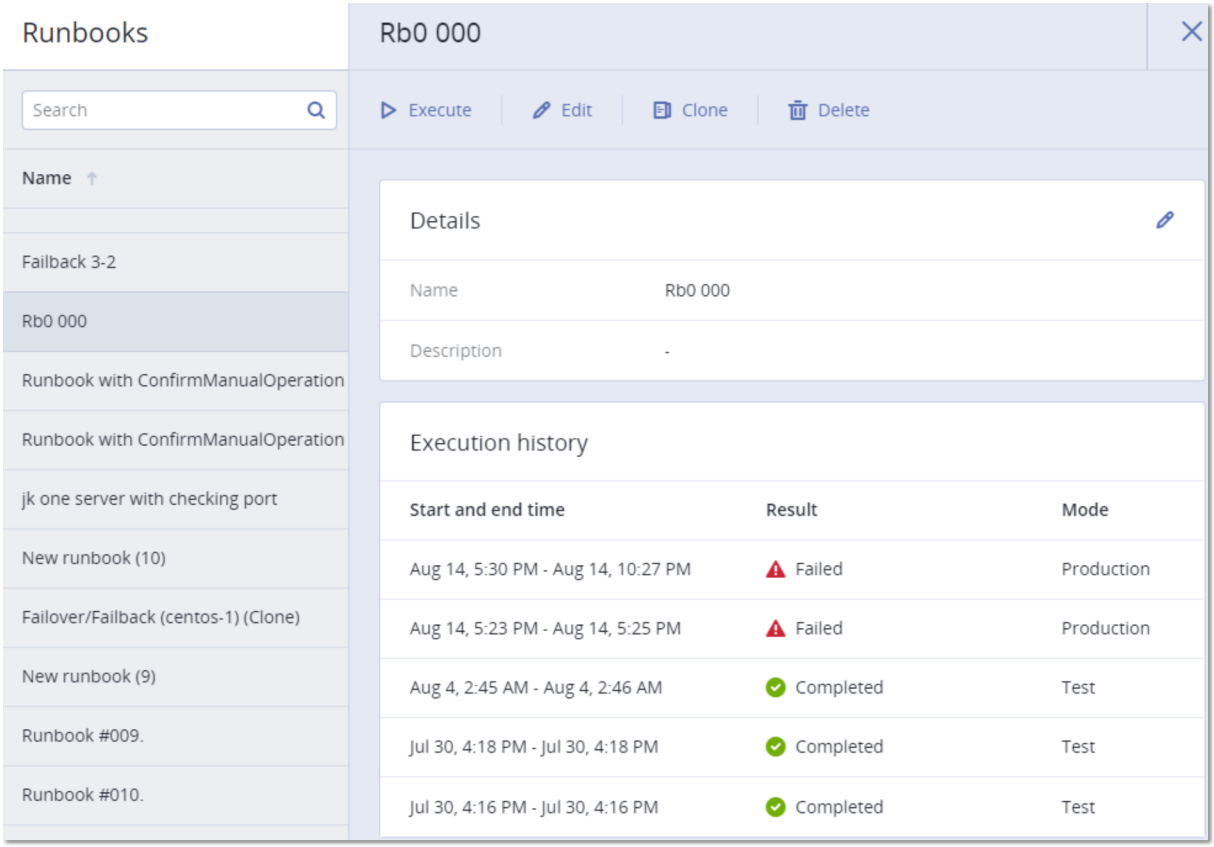
  Kies het meest recente herstelpunt (standaard) of selecteer een tijdstip in het verleden. In dit laatste geval worden de herstelpunten die zich het dichtst bij de opgegeven datum en tijd bevinden, voor elke server geselecteerd.

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.


Runbooks
Search
Name
Failback 3-2
Rb0 000
Runbook with ConfirmManualOperation
Runbook with ConfirmManualOperation
jk one server with checking port
New runbook (10)
Failover/Failback (centos-1) (Clone)
New runbook (9)
Runbook #009.
Runbook #010.
Rb0 000
Execute
Edit
Clone
Delete
Details
Name
Rb0 000
Description
-
Execution history
Start and end time
Result
Mode
Aug 14, 5:30 PM - Aug 14, 10:27 PM
Failed
Production
Aug 14, 5:23 PM - Aug 14, 5:25 PM
Failed
Production
Aug 4, 2:45 AM - Aug 4, 2:46 AM
Completed
Test
Jul 30, 4:18 PM - Jul 30, 4:18 PM
Completed
Test
Jul 30, 4:16 PM - Jul 30, 4:16 PM
Completed
Test

16 Antimalwarebeveiliging en webbeveiliging

Opmerking
Voor de functies voor antimalwarebeveiliging en URL-filtering op Windows-machines moet Agent voor antimalwarebeveiliging en URL-filtering zijn geïnstalleerd. Deze wordt automatisch geïnstalleerd voor beschermde workloads als de module **Antivirus- en antimalwarebeveiliging** of de module **URL-filtering** is ingeschakeld in de betreffende beschermingsschema's.

Antimalwarebeveiliging in Cyberbescherming 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.

16.1 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: Ondersteunde functies per besturingssysteem.

Antivirus- en antimalwarebeveiliging wordt ondersteund en geregistreerd in Windows Security Center.

16.1.1 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

16.1.2 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.

- Met **Snelle scan** worden alleen de systeembestanden van de machine gecontroleerd.
- Met een **volledige scan** worden alle bestanden op uw machine gecontroleerd.

U kunt de resultaten van de antimalwarescan controleren in **Dashboard** > **Overzicht** > de widget Onlangs beïnvloed.

16.1.3 Instellingen voor Antivirus- en antimalwarebeveiliging

Voor meer informatie over het maken van een beschermingsschema met de module **Antivirus- en antimalwarebeveiliging** raadpleegt u 'Een beschermingsschema maken'.

De volgende functies kunnen worden geconfigureerd voor de module **Antivirus- en antimalwarebeveiliging**.

Opmerking
In dit gedeelte worden de beschikbare instellingen voor alle ondersteunde besturingssystemen beschreven. Raadpleeg de tabel met ondersteunde Cyber Protect-functies per besturingssysteem voor informatie over de functies die van toepassing zijn op uw workloads: "Ondersteunde Cyber Protect-functies per besturingssysteem" (p. 19).
Voor sommige functies zijn mogelijk extra licenties vereist, afhankelijk van het toegepaste licentiemodel.

Active Protection

Active Protection beschermt een systeem tegen ransomware en cryptocurrency mining-malware. Met ransomware worden bestanden versleuteld, waarna om losgeld wordt gevraagd voor de versleutelingssleutel. Met cryptomining-malware worden op de achtergrond wiskundige berekeningen uitgevoerd, zodat rekenkracht en netwerkverkeer worden gestolen.

Standaardinstelling: **Ingeschakeld**.

Onder Windows is Active Protection beschikbaar voor machines met de volgende besturingssystemen:

- Besturingssystemen van desktop: Windows 7 Service Pack 1 en later
  Controleer op machines met Windows 7 of Update voor Windows 7 (KB2533623) is geïnstalleerd.
  Controleer voor agentversies 21.07 en later of de volgende KB-updates voor Windows 7 zijn geïnstalleerd:
  - Update van ondersteuning voor handtekening bij SHA-2-programmacode voor Windows Server 2008 R2, Windows 7 en Windows Server 2008 (KB4474419)

  - Update van servicestack voor Windows 7 SP1 en Windows Server 2008 R2 SP1 (KB4490628)
- Besturingssystemen van server: Windows Server 2008 R2 en later

Agent voor Windows moet zijn geïnstalleerd op de beschermde machine. De versie van de agent moet 12.0.4290 (uitgebracht in oktober 2017) of later zijn. Zie "Agenten bijwerken" (p. 119) voor meer informatie over het bijwerken van een agent.

Onder Linux is Active Protection beschikbaar voor machines met:

- CentOS 6.10, 7.8 en latere secundaire versies
- CloudLinux 6.10, 7.8 en latere secundaire versies
- Ubuntu 16.04.7 en latere secundaire versies

Agent voor Linux moet zijn geïnstalleerd op de beschermde machine. De versie van de agent moet 15.0.26077 (uitgebracht in december 2020) of later zijn. Voor een lijst met ondersteunde Linux-kernelversies raadpleegt u Active Protection voor Linux: Ondersteunde kernelversies (67747).

Instellingen voor Active Protection

Selecteer in **Actie bij detectie** de actie die de software moet uitvoeren bij het detecteren van een ransomware-activiteit en klik vervolgens op **Gereed** .

U kunt een van de volgende opties selecteren:

- **Alleen melden**
  De software genereert een waarschuwing over het proces.
- **Het proces stoppen**
  De software genereert een waarschuwing en stopt het proces.
- **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**.

Geavanceerde antimalware

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Met de schakelaar **Geavanceerde antimalware** kunt u een lokale engine op basis van handtekeningen inschakelen. Deze engine gebruikt een verbeterde database van virushandtekeningen om de efficiëntie van antimalwaredetectie te verbeteren voor zowel snelle als volledige scans.

Realtime bescherming is alleen beschikbaar voor de lokale engine op basis van handtekeningen.

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 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`. 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: **Ingeschakeld**.

Bescherming op server

Met deze instelling bepaalt u of Active Protection ook door u gedeelde netwerkmappen beschermt tegen de externe inkomende verbindingen van andere servers in het netwerk die mogelijk bedreigingen kunnen veroorzaken.

Standaardinstelling: **Uitgeschakeld**.

Opmerking
Bescherming op server wordt niet ondersteund voor Linux.

Vertrouwde en geblokkeerde verbindingen instellen

Een vertrouwde of geblokkeerde verbinding configureren:

1. Selecteer een tabblad in het dialoogvenster Bescherming op server:
   - Selecteer het tabblad **Vertrouwd** om de verbindingen op te geven waarmee gegevens mogen worden gewijzigd.
   - Selecteer het tabblad **Geblokkeerd** om de verbindingen op te geven waarmee geen gegevens mogen worden gewijzigd.
2. Voer de volgende gegevens in:
   - Computernaam en account van de machine waarop de beveiligingsagent is geïnstalleerd. Bijvoorbeeld: `MijnComputer\Testgebruiker`.
   - Hostnaam van de machine die verbinding mag maken met de machine met de agent.
3. Klik op het vinkje rechts om de verbindingsdefinitie op te slaan.
4. Als u meer verbindingen wilt toevoegen, klikt u op de knop **Toevoegen**.

Zelfbescherming

Zelfbescherming voorkomt ongeautoriseerde wijzigingen in softwareprocessen, registerrecords, uitvoerbare bestanden, configuratiebestanden en back-ups in lokale mappen. We raden u niet aan deze functie uit te schakelen.

Standaardinstelling: **Ingeschakeld**.

Opmerking
Zelfbescherming wordt niet ondersteund voor Linux.

Wachtwoordbescherming

Wachtwoordbescherming voorkomt 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 Cyberbescherming-webconsole
- De installatie herstellen

Standaardinstelling: **Uitgeschakeld**

Zie Voorkomen van niet-geautoriseerde verwijdering of wijziging van agenten voor meer informatie over het inschakelen van wachtwoordbescherming.

Detectie van cryptomining-processen

Met deze instelling bepaalt u of Active Protection potentiële cryptomining-malware detecteert.

Cryptomining-malware kan leiden tot mindere prestaties van nuttige toepassingen, een hogere elektriciteitsrekening, systeemcrashes en zelfs schade aan de hardware als gevolg van misbruik. Als u uw workloads wilt beschermen, raden we u aan om cryptomining-malware toe te voegen aan de lijst met **Schadelijke processen**.

Standaardinstelling: **Ingeschakeld**.

Opmerking
Detectie van cryptomining-processen wordt niet ondersteund voor Linux.

Instellingen voor detectie van cryptomining-processen

Selecteer in **Actie bij detectie** de actie die de software moet uitvoeren bij het detecteren van een cryptomining-proces en klik vervolgens op **Gereed**.

U kunt een van de volgende opties selecteren:

- **Alleen melden**
  Er wordt een waarschuwing gegenereerd over het proces dat wordt verdacht van cryptomining-activiteiten.
- **Het proces stoppen**
  Er wordt een waarschuwing gegenereerd en het proces dat wordt verdacht van cryptomining-activiteiten, wordt gestopt.

Standaardinstelling: **Het proces stoppen**.

Quarantaine

Quarantaine is een map om verdachte (waarschijnlijk geïnfecteerde) of potentieel gevaarlijke bestanden te isoleren.

Bestanden in quarantaine verwijderen na: hiermee definieert u de periode in dagen waarna de bestanden in quarantaine worden verwijderd.

Standaardinstelling: **30 dagen**.

Zie Quarantaine voor meer informatie over deze functie.

Gedragengine

Acronis Cyberbescherming beschermt uw systeem door schadelijke processen te identificeren met behulp van gedragsheuristiek: de reeks acties in een proces worden vergeleken met de actiereeksen die zijn opgenomen in de database van schadelijke gedragspatronen. Op die manier wordt nieuwe malware gedetecteerd door het typische gedrag van die malware.

Standaardinstelling: **Ingeschakeld**.

Opmerking
Gedragengine wordt niet ondersteund voor Linux.

Voor macOS wordt de gedragengine niet ondersteund op Apple Silicon-processors, zoals Apple M1.

Instellingen voor de gedragengine

Selecteer in **Actie bij detectie** de actie die de software moet uitvoeren bij het detecteren van een malwareactiviteit en klik vervolgens op **Gereed**.

U kunt een van de volgende opties selecteren:

- **Alleen melden**
  De software genereert een waarschuwing over het proces dat wordt verdacht van malwareactiviteit.
- **Het proces stoppen**

De software genereert een waarschuwing en stopt het proces dat wordt verdacht van malwareactiviteit.

- **Quarantaine**
  De software genereert een waarschuwing, stopt het proces en verplaatst het uitvoerbare bestand naar de quarantainemap.

Standaardinstelling: **Quarantaine**.

Preventie tegen aanvallen

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 Windows-systemen. 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.

Instellingen voor Preventie tegen aanvallen

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.

Selecteer onder **Ingeschakelde actie bij detectie** welke actie moet worden ondernomen wanneer er een aanval wordt gedetecteerd en klik vervolgens op **Gereed**.

- **Alleen melden**
  De software genereert een waarschuwing over het proces dat wordt verdacht van malwareactiviteit.
- **Het proces stoppen**
  De software genereert een waarschuwing en stopt het proces dat wordt verdacht van malwareactiviteit.

Standaardinstelling: **Het proces stoppen**

Schakel onder **Ingeschakelde technieken voor preventie tegen aanvallen** de methoden die u wilt toepassen, in of uit en klik vervolgens op **Gereed**.

U kunt een van de volgende opties selecteren:

- **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 van de ROP-aanvalstechniek waarbij een aanvaller code kan uitvoeren ondanks de beveiligingen, zoals bescherming van uitvoerbare ruimte en handtekening bij programmacode. De aanvaller krijgt de controle over de aanroepstack en kaapt vervolgens de controlestroom van het programma en voert schadelijke code uit.
- **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.

Standaardinstelling: **Alle methoden zijn ingeschakeld**.

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.

Realtime bescherming zorgt ervoor dat uw systeem voortdurend wordt gecontroleerd op virussen en andere bedreigingen gedurende de hele tijd dat uw systeem is ingeschakeld.

Standaardinstelling: **Ingeschakeld**.

Belangrijk
Realtime bescherming is alleen beschikbaar wanneer de lokale engine op basis van handtekeningen is ingeschakeld. Voor realtime bescherming moet u zowel de schakelaar **Realtime bescherming** als de schakelaar **Geavanceerde antimalware** inschakelen.

De actie bij detectie configureren voor realtime bescherming

Selecteer in **Actie bij detectie** de actie die de software moet uitvoeren bij het detecteren van een virus of andere bedreigingen en klik vervolgens op **Gereed**.

U kunt een van de volgende opties selecteren:

- **Blokkeren en melden**
  Het proces wordt geblokkeerd en er wordt een waarschuwing gegenereerd over het proces dat wordt verdacht van malwareactiviteit.
- **Quarantaine**
  Er wordt een waarschuwing gegenereerd, het proces wordt gestopt en het uitvoerbare bestand wordt verplaatst naar de quarantainemap.

Standaardinstelling: **Quarantaine**.

De scanmodus configureren voor realtime bescherming

Selecteer in **Scanmodus** de actie die de software moet uitvoeren bij het detecteren van een virus of andere bedreigingen en klik vervolgens op **Gereed**.

U kunt een van de volgende opties selecteren:

- **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 schoon zijn en geen schade aan uw computer of gegevens kunnen veroorzaken.

Standaardinstelling: **Smart bij toegang**.

Scan plannen

Als u de instelling **Scan plannen** inschakelt, kunt u een schema definiëren op basis waarvan uw machine wordt gecontroleerd op malware.

Actie bij detectie:

- **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.

Standaardinstelling: **Quarantaine**.

Scanmodus:

- **Volledig**
  De volledige scan duurt veel langer dan de snelle scan omdat elk bestand wordt gecontroleerd.
- **Snel**
  Met de snelle scan worden alleen de gemeenschappelijke gebieden gescand waar malware zich doorgaans op de machine bevindt.

U kunt zowel **Quick scan** als **Full scan** plannen in één beschermingsschema.

Standaardinstelling: **Quick scan** en **Full scan** zijn gepland.

De taakuitvoering plannen met de volgende gebeurtenissen:

- **Schema op tijd**: 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.

- **Bij het opstarten van het systeem**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt gestart.

- **Bij het afsluiten van het systeem**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt afgesloten.

Standaardinstelling: **Planning op tijd**.

Type schema:

- **Maandelijks**: selecteer de maanden en de weken of dagen van de maand wanneer de taak zal worden uitgevoerd.
- **Dagelijks**: selecteer de dagen van de week wanneer de taak zal worden uitgevoerd.
- **Elk uur**: selecteer de dagen van de week, het aantal herhalingen en het tijdinterval waarin de taak wordt uitgevoerd.

Standaardinstelling: **Dagelijks**.

Starten om: selecteer het exacte tijdstip waarop de taak wordt uitgevoerd.

Uitvoeren binnen een datumbereik: stel een bereik in waarin het geconfigureerde schema van kracht is.

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.
- **Als niet aan de startvoorwaarden wordt voldaan, de taak daarna toch uitvoeren**: geef aan na hoeveel tijd de taak wordt uitgevoerd, ongeacht de andere startvoorwaarden.

Opmerking
Startvoorwaarden worden niet ondersteund voor Linux.

Alleen nieuwe en gewijzigde bestanden scannen: alleen nieuw gemaakte en gewijzigde bestanden worden gescand.

Standaardinstelling: **Ingeschakeld**.

Bij het plannen van een **Full scan** hebt u twee extra opties:

Archiefbestanden scannen

Standaardinstelling: **Ingeschakeld**.

- **Max. recursiediepte**
  Hoeveel niveaus van ingesloten archieven kunnen worden gescand. Bijvoorbeeld MIME-document > ZIP-archief > Office-archief > documentinhoud.
  Standaardinstelling: **16**.
- **Maximale grootte**
  Maximale grootte van een te scannen archiefbestand.
  Standaardinstelling: **Onbeperkt**.

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

Als u de resources die door de heuristische analyse worden gebruikt, wilt minimaliseren en zogenaamde 'fout-positieven' wilt voorkomen, kunt u de volgende instellingen definiëren wanneer een vertrouwd programma wordt beschouwd als ransomware of andere malware:

Op het tabblad **Vertrouwd** kunt u het volgende opgeven:

- Processen die nooit als malware worden beschouwd. Processen ondertekend door Microsoft worden altijd vertrouwd.
- Mappen waarin bestandswijzigingen niet worden gecontroleerd.
- Bestanden en mappen waarvoor de geplande scan niet wordt uitgevoerd.

Op het tabblad **Geblokkeerd** kunt u het volgende opgeven:

- Processen die altijd worden geblokkeerd. Deze processen kunnen niet worden gestart wanneer Active Protection of Antimalwarebeveiliging is ingeschakeld op de machine.
- Mappen waarin processen worden geblokkeerd.

Standaardinstelling: Standaard worden geen uitsluitingen gedefinieerd.

U kunt een jokerteken (*) gebruiken om items toe te voegen aan de uitsluitingslijsten.

U kunt variabelen ook gebruiken om items toe te voegen aan de uitsluitingslijsten. Let op 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\ *

16.2 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 antimalwarebeveiliging.

Standaardinstelling: **Ingeschakeld**.

Onder Windows is Active Protection beschikbaar voor machines met de volgende besturingssystemen:

- Besturingssystemen van desktop: Windows 7 Service Pack 1 en later
  Controleer op machines met Windows 7 of Update voor Windows 7 (KB2533623) is geïnstalleerd.
  Controleer voor agentversies 21.07 en later of de volgende KB-updates voor Windows 7 zijn geïnstalleerd:
  - Update van ondersteuning voor handtekening bij SHA-2-programmacode voor Windows Server 2008 R2, Windows 7 en Windows Server 2008 (KB4474419)
  - Update van servicestack voor Windows 7 SP1 en Windows Server 2008 R2 SP1 (KB4490628)
- Besturingssystemen van server: Windows Server 2008 R2 en later

Agent voor Windows moet zijn geïnstalleerd op de beschermde machine. De versie van de agent moet 12.0.4290 (uitgebracht in oktober 2017) of later zijn. Zie "Agenten bijwerken" (p. 119) voor meer informatie over het bijwerken van een agent.

Onder Linux is Active Protection beschikbaar voor machines met:

- CentOS 6.10, 7.8 en latere secundaire versies
- CloudLinux 6.10, 7.8 en latere secundaire versies
- Ubuntu 16.04.7 en latere secundaire versies

Agent voor Linux moet zijn geïnstalleerd op de beschermde machine. De versie van de agent moet 15.0.26077 (uitgebracht in december 2020) of later zijn. Voor een lijst met ondersteunde Linux-kernelversies raadpleegt u Active Protection voor Linux: Ondersteunde kernelversies (67747).

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.

16.2.1 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

Selecteer in **Actie bij detectie** de actie die de software moet uitvoeren bij het detecteren van een ransomware-activiteit en klik vervolgens op **Gereed** .

U kunt een van de volgende opties selecteren:

- **Alleen melden**
  De software genereert een waarschuwing over het proces.

- **Het proces stoppen**
  De software genereert een waarschuwing en stopt het proces.
- **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**.

Zelfbescherming

Zelfbescherming voorkomt ongeautoriseerde wijzigingen in softwareprocessen, registerrecords, uitvoerbare bestanden, configuratiebestanden en back-ups in lokale mappen. We raden u niet aan deze functie uit te schakelen.

Standaardinstelling: **Ingeschakeld**.

Opmerking
Zelfbescherming wordt niet ondersteund voor Linux.

Wachtwoordbescherming

Wachtwoordbescherming voorkomt 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 Cyberbescherming-webconsole
- De installatie herstellen

Standaardinstelling: **Uitgeschakeld**

Zie Voorkomen van niet-geautoriseerde verwijdering of wijziging van agenten voor meer informatie over het inschakelen van wachtwoordbescherming.

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`. 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: **Ingeschakeld**.

Bescherming op server

Met deze instelling bepaalt u of Active Protection ook door u gedeelde netwerkmappen beschermt tegen de externe inkomende verbindingen van andere servers in het netwerk die mogelijk bedreigingen kunnen veroorzaken.

Standaardinstelling: **Uitgeschakeld**.

Opmerking
Bescherming op server wordt niet ondersteund voor Linux.

Vertrouwde en geblokkeerde verbindingen instellen

Een vertrouwde of geblokkeerde verbinding configureren:

1. Selecteer een tabblad in het dialoogvenster Bescherming op server:
   - Selecteer het tabblad **Vertrouwd** om de verbindingen op te geven waarmee gegevens mogen worden gewijzigd.
   - Selecteer het tabblad **Geblokkeerd** om de verbindingen op te geven waarmee geen gegevens mogen worden gewijzigd.
2. Voer de volgende gegevens in:
   - Computernaam en account van de machine waarop de beveiligingsagent is geïnstalleerd. Bijvoorbeeld: `MijnComputer\Testgebruiker`.
   - Hostnaam van de machine die verbinding mag maken met de machine met de agent.
3. Klik op het vinkje rechts om de verbindingsdefinitie op te slaan.
4. Als u meer verbindingen wilt toevoegen, klikt u op de knop **Toevoegen**.

Detectie van cryptomining-processen

Met deze instelling bepaalt u of Active Protection potentiële cryptomining-malware detecteert.

Cryptomining-malware kan leiden tot mindere prestaties van nuttige toepassingen, een hogere elektriciteitsrekening, systeemcrashes en zelfs schade aan de hardware als gevolg van misbruik. Als u uw workloads wilt beschermen, raden we u aan om cryptomining-malware toe te voegen aan de lijst met **Schadelijke processen**.

Standaardinstelling: **Ingeschakeld**.

Opmerking
Detectie van cryptomining-processen wordt niet ondersteund voor Linux.

Instellingen voor detectie van cryptomining-processen

Selecteer in **Actie bij detectie** de actie die de software moet uitvoeren bij het detecteren van een cryptomining-proces en klik vervolgens op **Gereed**.

U kunt een van de volgende opties selecteren:

- **Alleen melden**
  Er wordt een waarschuwing gegenereerd over het proces dat wordt verdacht van cryptomining-activiteiten.
- **Het proces stoppen**
  Er wordt een waarschuwing gegenereerd en het proces dat wordt verdacht van cryptomining-activiteiten, wordt gestopt.

Standaardinstelling: **Het proces stoppen**.

Uitsluitingen

Als u de resources die door de heuristische analyse worden gebruikt, wilt minimaliseren en zogenaamde 'fout-positieven' wilt voorkomen, kunt u de volgende instellingen definiëren wanneer een vertrouwd programma wordt beschouwd als ransomware of andere malware:

Op het tabblad **Vertrouwd** kunt u het volgende opgeven:

- Processen die nooit als malware worden beschouwd. Processen ondertekend door Microsoft worden altijd vertrouwd.
- Mappen waarin bestandswijzigingen niet worden gecontroleerd.
- Bestanden en mappen waarvoor de geplande scan niet wordt uitgevoerd.

Op het tabblad **Geblokkeerd** kunt u het volgende opgeven:

- Processen die altijd worden geblokkeerd. Deze processen kunnen niet worden gestart wanneer Active Protection of Antimalwarebeveiliging is ingeschakeld op de machine.
- Mappen waarin processen worden geblokkeerd.

Standaardinstelling: Standaard worden geen uitsluitingen gedefinieerd.

U kunt een jokerteken (*) gebruiken om items toe te voegen aan de uitsluitingslijsten.

U kunt variabelen ook gebruiken om items toe te voegen aan de uitsluitingslijsten. Let op 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\ *

16.3 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. De database voor URL-filtering bevat ook gegevens over websites met omstreden informatie over COVID-19, oplichting en phishing-URL's. Dergelijke websites worden automatisch geblokkeerd wanneer een gebruiker ze probeert te openen.

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.

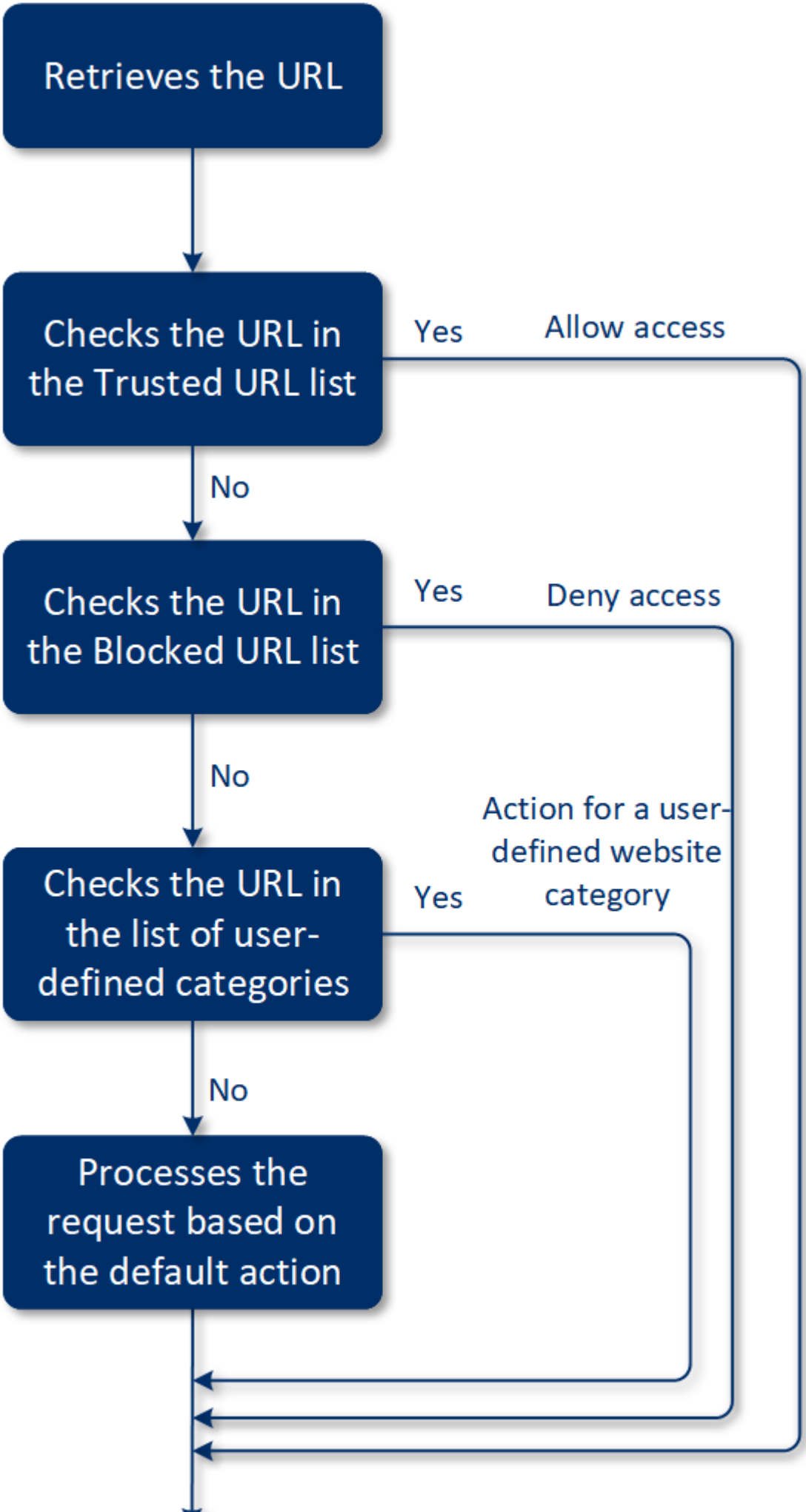
De functie URL-filtering werkt alleen als er een internetverbinding is.

Opmerking
Mogelijke compatibiliteitsproblemen met builds 15.0.26692 (release C21.03 HF1) en eerder van Cyber Protection-agent worden voorkomen doordat de functionaliteit voor URL-filtering automatisch wordt uitgeschakeld als een andere antivirusoplossing wordt gedetecteerd, of als de Windows Beveiligingscentrum-service niet aanwezig is op het systeem.
Bij latere Cyber Protection-agenten zijn de compatibiliteitsproblemen opgelost, zodat URL-filtering altijd is ingeschakeld volgens het beleid.

16.3.1 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.

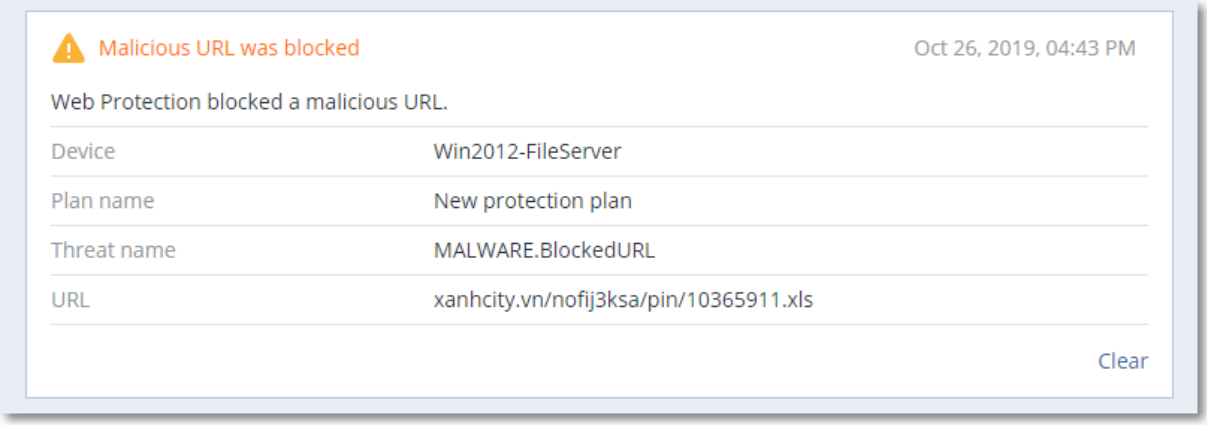

Retrieves the URL
Checks the URL in the Trusted URL list
Yes
Allow access
No
Checks the URL in the Blocked URL list
Yes
Deny access
No
Checks the URL in the list of user-defined categories
Yes
Action for a user-defined website category
No
Processes the request based on the default action

16.3.2 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 **Dashboard** > **Waarschuwingen**.



16.3.3 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:

- **Blokkeren**: de toegang tot de schadelijke website blokkeren. De gebruiker heeft geen toegang tot de website en er wordt een waarschuwing gegenereerd.
- **Altijd vragen aan gebruiker**: de gebruiker vragen om toch door te gaan naar de website of terug te 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 Narcotica.
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. Het wordt aanbevolen 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

URL's

Domeinnamen of IP-adressen die bekend staan als veilig, kunnen worden toegevoegd aan de lijst met vertrouwde URL's. Domeinnamen of IP-adressen die een bedreiging vormen, kunnen worden toegevoegd aan de lijst met geblokkeerde URL's.

Als u een host wilt toevoegen aan de vertrouwde URL's, klikt u op **Toevoegen** op het tabblad **Vertrouwd** en geeft u de specifieke domeinnaam of het specifieke IP-adres op.

Als u een host wilt toevoegen aan de geblokkeerde URL's, klikt u op **Toevoegen** op het tabblad **Geblokkeerd** en geeft u de specifieke domeinnaam of het specifieke IP-adres op.

Opmerking
Alle adressen van het domein dat u hebt ingevoerd, worden verwerkt als vertrouwd of geblokkeerd. Als u bijvoorbeeld xyz.com hebt ingevoerd als vertrouwd domein, worden alle paden of subdomeinen onder xyz.com behandeld als vertrouwd.

Voeg niet het voorvoegsel 'www.' toe wanneer u de domeinnaam invoert.

Processen

Processen die nooit als malware worden beschouwd, kunnen worden toegevoegd aan de lijst met vertrouwde processen. Processen ondertekend door Microsoft worden altijd vertrouwd.

URL-filtering ondersteunt alleen uitsluitingen voor vertrouwde processen. U kunt geen processen toevoegen aan de blokkeringslijst.

Standaardinstelling: Standaard worden geen uitsluitingen gedefinieerd.

U kunt een jokerteken (*) gebruiken om items toe te voegen aan de lijst met vertrouwde processen. Let op: jokertekens worden niet ondersteund aan het begin van het pad, maar alleen aan het einde.

U kunt ook variabelen gebruiken om items toe te voegen aan de lijsten met procesuitsluitingen. Let op de volgende beperkingen:

- Voor Windows worden alleen SYSTEM-variabelen ondersteund. Gebruikersspecifieke variabelen, bijvoorbeeld %USERNAME% of %APPDATA% worden niet ondersteund. Variabelen met {username} worden niet ondersteund. Zie https://ss64.com/nt/syntax-variables.html voor meer informatie.
- Netwerkpaden worden niet ondersteund.
- Omgevingsvariabelen worden niet ondersteund voor macOS.
- Omgevingsvariabelen worden niet ondersteund voor Linux.

Voorbeelden van ondersteunde indelingen:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\ *

16.4 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 Cyberbescherming-serviceconsole.

Deze module is van toepassing op de machines 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 Cyberbescherming-serviceconsole.

Deze module is van toepassing op de machines 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 Cyberbescherming-serviceconsole.

16.4.1 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

16.4.2 Standaardacties

Definieer de standaardacties die moeten worden uitgevoerd voor de gedetecteerde bedreigingen van verschillende ernstniveaus:

- **Opschonen**: de gedetecteerde malware op een machine opschonen.
- **In quarantaine plaatsen**: de gedetecteerde malware in de quarantainemap plaatsen maar niet verwijderen.
- **Verwijderen**: de gedetecteerde malware verwijderen van een machine.
- **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

16.4.3 Realtime bescherming

Realtime bescherming: schakel dit in om te detecteren of en te voorkomen dat malware wordt geïnstalleerd of op machines wordt uitgevoerd.

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

16.4.4 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 Cyberbescherming-serviceconsole.
- **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

16.4.5 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

16.5 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.

16.5.1 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.

16.5.2 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.

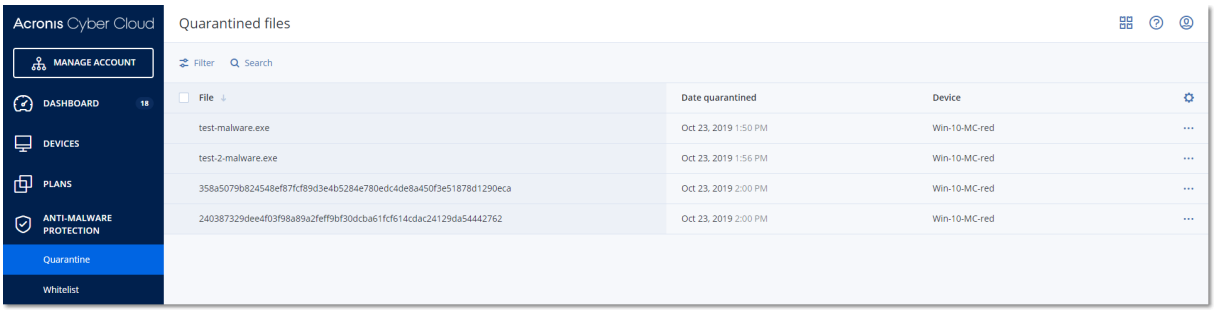
Naam	Beschrijving
Bestand	De bestandsnaam.
In quarantaine geplaatst op	De datum en tijd waarop het bestand in quarantaine is geplaatst.
Apparaat	Het apparaat waarop het geïnfecteerde bestand is gevonden.
Naam van bedreiging	De naam van de bedreiging.
Beschermingsschema	Het beschermingsschema dat is toegepast 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.

- **Herstellen**: een in quarantaine geplaatst bestand zonder wijzigingen herstellen naar de oorspronkelijke locatie. Als er een bestand met dezelfde naam bestaat op de oorspronkelijke locatie, wordt dit overschreven door het herstelde bestand. Let op: Het herstelde bestand wordt toegevoegd aan de witte lijst en wordt overgeslagen tijdens verdere antimalwarescans.



16.5.3 Quarantainelocatie op machines

De standaardlocatie voor in quarantaine geplaatste bestanden is:

Voor een Windows-machine: `%ProgramData%\%product_name%\Quarantine`

Voor een Mac/Linux-machine: `/usr/local/share/%product_name%/quarantine`

De quarantaineopslag valt onder de zelfverdedigingsbescherming van de serviceprovider.

16.6 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.

Met Cyberbescherming 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 worden ook verbeterd door de witte lijst van de hele organisatie.

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 Cyberbescherming-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.

16.6.1 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.

16.6.2 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 serviceconsole naar **Antimalwarebeveiliging** > **Witte lijst**.
2. Klik op **Bestand toevoegen**.
3. Geef het pad naar het bestand op en klik vervolgens op **Toevoegen**.

16.6.3 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 serviceconsole naar **Antimalwarebeveiliging** > **Quarantaine**.
2. Selecteer een bestand dat in quarantaine is geplaatst en klik vervolgens op **Toevoegen aan witte lijst**.

16.6.4 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.

16.6.5 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.

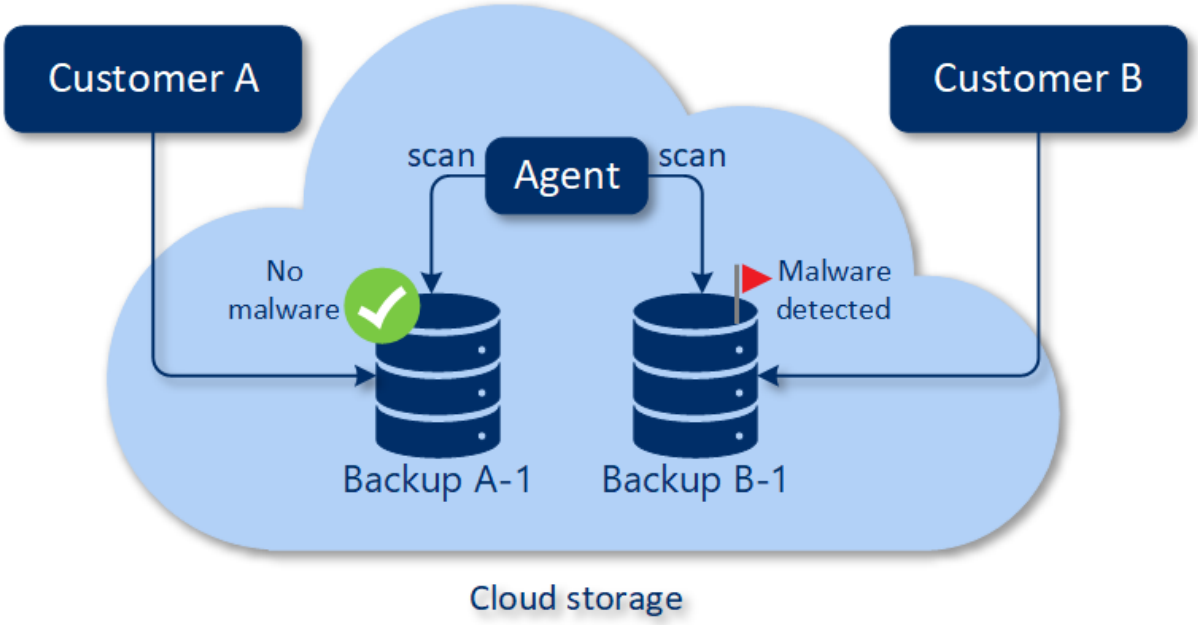
16.7 Antimalwarescan van back-ups

Met de back-upscanfunctie kunt u voorkomen dat geïnfecteerde bestanden worden hersteld vanuit back-ups. Door deze functie te gebruiken kunt u controleren of uw back-ups schoon zijn (niet geïnfecteerd door malware). De back-upscanfunctie wordt alleen ondersteund voor Windows-besturingssystemen.

Back-upscans worden door de cloudagent uitgevoerd in de omgeving buiten een eindgebruikersmachine, namelijk in de Acronis-cloud. Voor elk nieuw back-upscanschema wordt een nieuwe scantaak gemaakt. De taak wordt in de gemeenschappelijke wachtrij voor het huidige datacentrum geplaatst en verwerkt volgens de volgorde in de wachtrij. De tijd die nodig is voor de scan, hangt af van de grootte van een back-up. Mogelijk kan er dus wat vertraging zijn tussen de tijd dat u een back-upscanschema hebt gemaakt en de uitvoering ervan.

Als geen back-upscans zijn uitgevoerd, behouden de back-ups de status **Niet gescand**. Wanneer de back-upscans zijn uitgevoerd, krijgen de back-ups een van de volgende statussen:

- **Geen malware**
- **Malware gedetecteerd**



De back-upscan kan worden geconfigureerd met een back-upscanschema.

16.7.1 Back-upscans in de cloud configureren

Let op het volgende:

- U kunt kiezen uit de ondersteunde back-uptypen 'Volledige machine' of 'Schijven/volumes'.
- Alleen volumes met het NTFS-bestandssysteem met GPT- en MBR-partities worden gescand.
- De ondersteunde back-uplocatie is cloudopslag (momenteel alleen gehost in Acronis).
- De back-ups met CDP-herstelpunten kunnen worden geselecteerd voor scans, maar alleen reguliere herstelpunten (dus geen CDP-herstelpunten) worden gescand.
- Wanneer de CDP-back-up is geselecteerd voor veilig herstel van een volledige machine, wordt de machine veilig hersteld zonder de gegevens in het CDP-herstelpunt. Als u de CDP-gegevens wilt herstellen, start u de herstelactiviteit Bestanden/mappen.

Als u een back-upscan in de cloud wilt configureren, maakt u een back-upscanschema.

De resultaten van back-upscans zijn te vinden op het dashboard in de widget 'Back-upscangegevens'.

17 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 Cyberbescherming-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. Een beschermingsschema toepassen: meld u aan bij de serviceconsole 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

18 Evaluatie van beveiligingsproblemen en patchbeheer

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. 514) voor meer informatie.
- macOS. Zie "Ondersteunde producten van Apple en derden" (p. 515) voor meer informatie.
- Linux-machines (CentOS 7/Virtuozzo/Acronis Cyber Infrastucture). Zie "Ondersteunde Linux-producten" (p. 516) voor meer informatie.

Gebruik de functionaliteit **Patchbeheer** (PM) 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. 514) voor meer informatie.

18.1 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 **Dashboard** > **Overzicht** > widgets **Beveiligingsproblemen/Bestaande beveiligingsproblemen**.

18.1.1 Ondersteunde producten van Microsoft en derden

De volgende Microsoft-producten en producten van derden voor Windows-besturingssystemen worden ondersteund voor evaluatie van beveiligingsproblemen:

Ondersteunde Microsoft-producten

Windows OS

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

Windows Server OS

- 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 2016

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 Cyberbescherming-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.

18.1.2 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 10.14.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

18.1.3 Ondersteunde Linux-producten

De volgende Linux-distributies en -versies worden ondersteund voor evaluatie van beveiligingsproblemen:

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10 (320)
- Virtuozzo 7.0.9 (539)
- Virtuozzo 7.0.8 (524)
- CentOS 7.x
- Acronis Cyber Infrastructure 3.x
- Acronis Storage 2.4.0
- Acronis Storage 2.2.0

18.1.4 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:

De taakuitvoering plannen met de volgende gebeurtenissen:

- **Schema op tijd**: 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.

- **Bij het opstarten van het systeem**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt gestart.
- **Bij het afsluiten van het systeem**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt afgesloten.

Standaardinstelling: **Planning op tijd**.

Type schema:

- **Maandelijks**: selecteer de maanden en de weken of dagen van de maand wanneer de taak zal worden uitgevoerd.

- **Dagelijks**: selecteer de dagen van de week wanneer de taak zal worden uitgevoerd.
- **Elk uur**: selecteer de dagen van de week, het aantal herhalingen en het tijdinterval waarin de taak wordt uitgevoerd.

Standaardinstelling: **Dagelijks**.

Starten om: selecteer het exacte tijdstip waarop de taak wordt uitgevoerd.

Uitvoeren binnen een datumbereik: stel een bereik in waarin het geconfigureerde schema van kracht is.

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.
- **Als niet aan de startvoorwaarden wordt voldaan, de taak daarna toch uitvoeren**: geef aan na hoeveel tijd de taak wordt uitgevoerd, ongeacht de andere startvoorwaarden.

Opmerking
Startvoorwaarden worden niet ondersteund voor Linux.

18.1.5 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 serviceconsole 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 **Schema** raadpleegt u "Instellingen voor evaluatie van beveiligingsproblemen" (p. 516).

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 **Dashboard** > **Overzicht** > widgets **Beveiligingsproblemen/Bestaande beveiligingsproblemen** als u de resultaten van de evaluatie van beveiligingsproblemen wilt controleren.

18.1.6 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 serviceconsole 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 **Schema** raadpleegt u "Instellingen voor evaluatie van beveiligingsproblemen" (p. 516).
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 **Dashboard** > **Overzicht** > widgets **Beveiligingsproblemen/Bestaande beveiligingsproblemen** als u de resultaten van de evaluatie van beveiligingsproblemen wilt controleren.

18.1.7 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 serviceconsole 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 **Schema** raadpleegt u "Instellingen voor evaluatie van beveiligingsproblemen" (p. 516).

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.

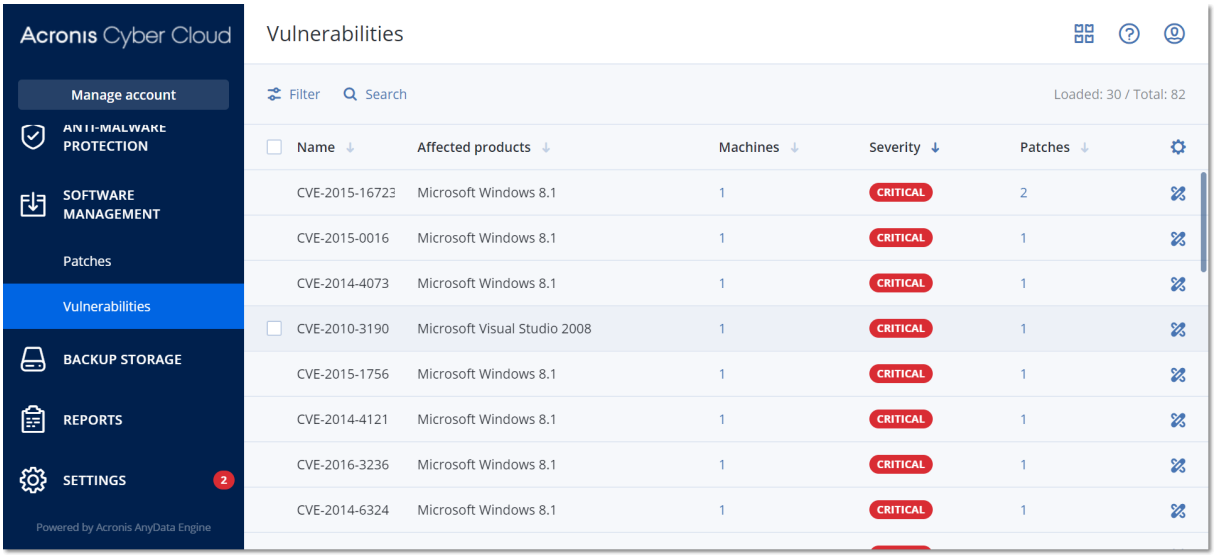
Ga naar **Dashboard** > **Overzicht** > widgets **Beveiligingsproblemen/Bestaande beveiligingsproblemen** als u de resultaten van de evaluatie van beveiligingsproblemen wilt controleren.

18.1.8 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 serviceconsole naar **Softwarebeheer** > **Beveiligingsproblemen**.
2. Selecteer het beveiligingsprobleem in de lijst en klik op **Patches installeren**. De wizard voor het herstellen van beveiligingsproblemen wordt geopend.
3. Selecteer de patches die op de geselecteerde machines moeten worden geïnstalleerd. Klik op **Volgende**.
4. Selecteer de machines waarvoor u patches wilt installeren.
5. Selecteer of de machine opnieuw moet worden opgestart na installatie van de patch:
   - **Nee**: na installatie van de update wordt er nooit opnieuw opgestart.
   - **Indien nodig**: opnieuw opstarten wordt alleen uitgevoerd als dit is vereist voor het toepassen van de updates.
   - **Ja**: na de updates wordt altijd opnieuw opgestart. U kunt altijd een vertraging voor opnieuw opstarten opgeven.

   Niet opnieuw opstarten tot de back-up is voltooid. Als het back-upproces wordt uitgevoerd, wordt de machine pas opnieuw opgestart wanneer de back-up is voltooid.

   Klik wanneer u klaar bent op **Patches installeren**.

Hierdoor worden de geselecteerde patches op de geselecteerde machines geïnstalleerd.

18.2 Patchbeheer

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

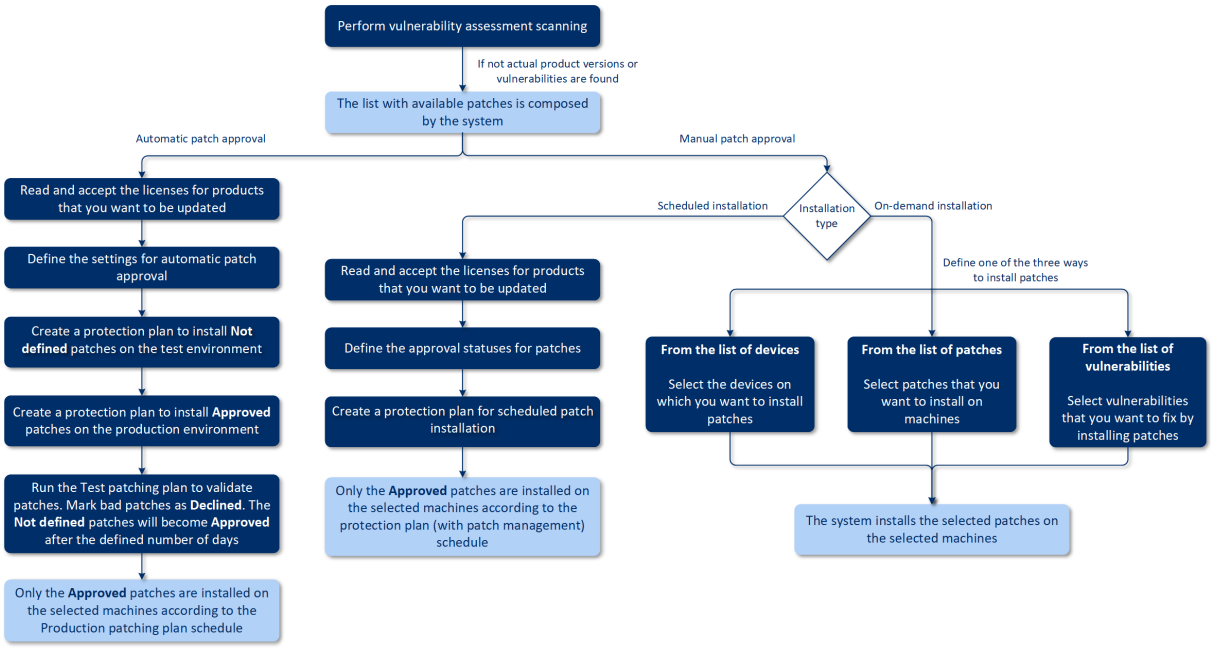
Gebruik de functie voor patchbeheer voor het volgende:

- 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

Cyberbescherming 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.

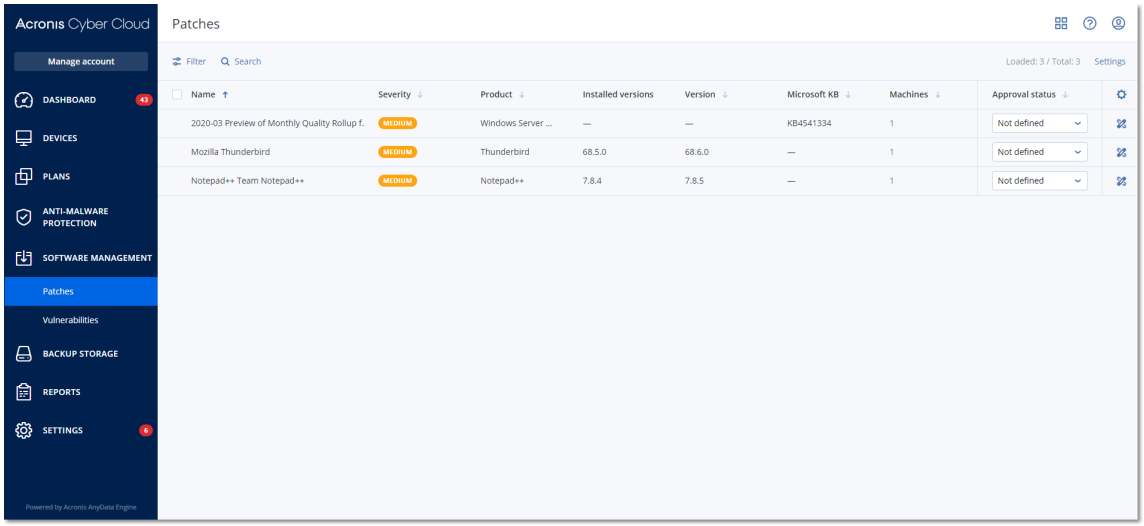
18.2.1 Zo werkt het

U kunt automatische of handmatige patchgoedkeuring configureren. In het onderstaande schema ziet u de automatische en handmatige workflows voor patchgoedkeuring.



1. Eerst moet u ten minste één VA-scan uitvoeren met het beschermingsschema terwijl de module **Evaluatie van beveiligingsproblemen** is ingeschakeld. Nadat de scan is uitgevoerd, worden de lijsten met gevonden beveiligingsproblemen en beschikbare patches gegenereerd door het systeem.
2. Vervolgens kunt u automatische patchgoedkeuring configureren of handmatige patchgoedkeuring gebruiken.
3. Bepaal hoe u patches wilt installeren: volgens een schema of op aanvraag. Er zijn drie verschillende manieren om patches op aanvraag te installeren:

- Ga naar de lijst met patches (**Softwarebeheer** > **Patches**) en installeer de nodige patches.



- Ga naar de lijst met beveiligingsproblemen (**Softwarebeheer** > **Beveiligingsproblemen**) en start het herstelproces dat ook patchinstallatie omvat.
- Ga naar de lijst met apparaten (**Apparaten** > **Alle apparaten**), selecteer de specifieke machines die u wilt bijwerken en installeer de patches daarop.

U kunt de resultaten van de evaluatie van beveiligingsproblemen controleren in **Dashboard** > **Overzicht** > widget **Geschiedenis van patchinstallatie**.

18.2.2 Instellingen voor patchbeheer

Raadpleeg 'Een beschermingsschema maken' voor meer informatie over het maken van een beschermingsschema met de module voor patchbeheer. Via het beschermingsschema kunt u opgeven welke updates voor Microsoft en Windows OS-producten van derden automatisch moeten worden geïnstalleerd op de gedefinieerde machines.

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

De volgende instellingen kunnen worden opgegeven voor de module voor patchbeheer.

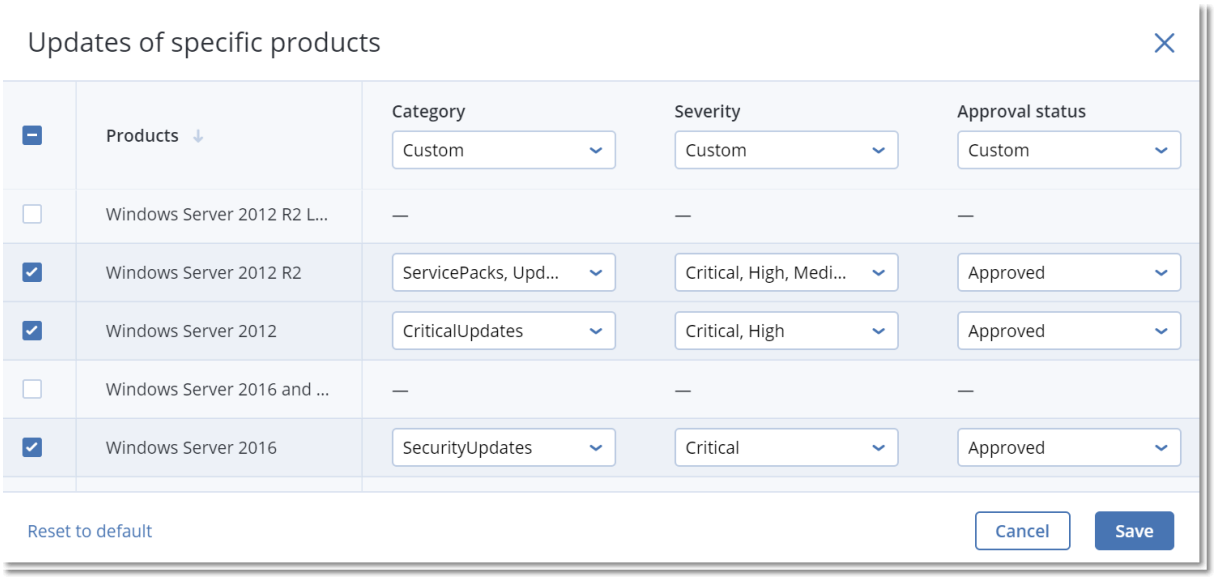
Microsoft-producten

Als u de Microsoft-updates wilt installeren op de geselecteerde machines, schakelt u de optie **Microsoft-producten bijwerken** in.

Selecteer welke updates u wilt installeren:

- **Alle updates**
- **Alleen beveiligings- en kritieke updates**
- **Updates van specifieke producten**: u kunt aangepaste instellingen definiëren voor verschillende producten. Als u specifieke producten wilt bijwerken, kunt u voor elk product

definiëren welke updates moeten worden geïnstalleerd per categorie, ernst of goedkeuringsstatus.

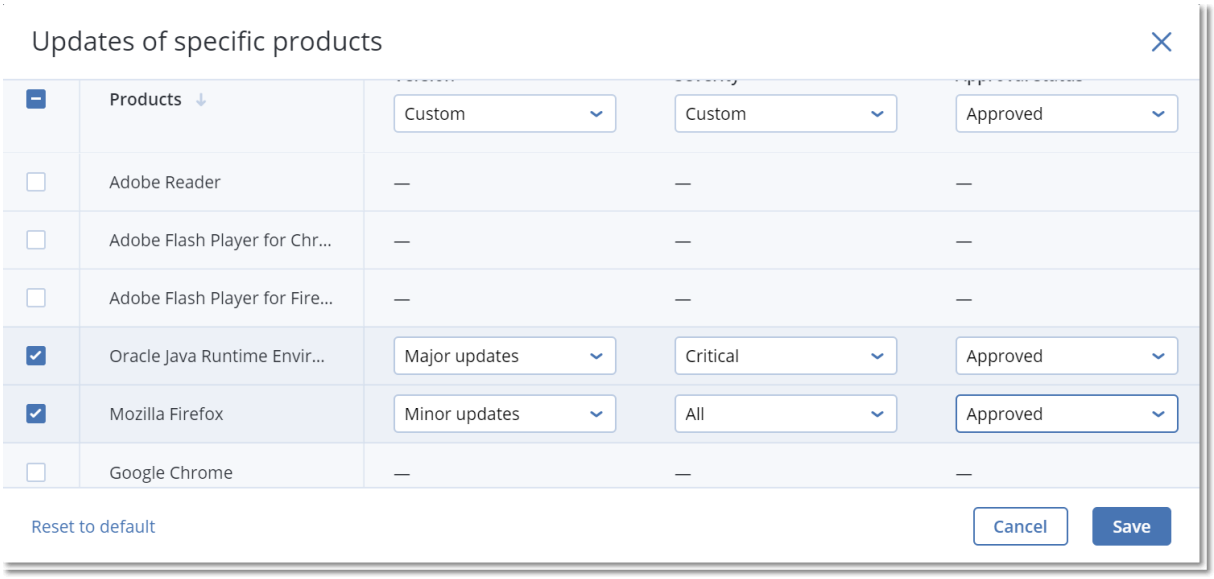


Windows-producten van derden

Als u updates van derden voor Windows OS wilt installeren op de geselecteerde machines, schakelt u de optie **Windows-producten van derden** in.

Selecteer welke updates u wilt installeren:

- **Alleen laatste belangrijke updates**: hiermee kunt u de meest recente beschikbare versie van de update installeren.
- **Alleen laatste kleine updates** kunt u de secundaire versie van de update installeren.
- **Updates van specifieke producten**: u kunt aangepaste instellingen definiëren voor verschillende producten. Als u specifieke producten wilt bijwerken, kunt u voor elk product definiëren welke updates moeten worden geïnstalleerd per categorie, ernst of goedkeuringsstatus.



Planning

Definieer het schema op basis waarvan de updates worden geïnstalleerd op de geselecteerde machines.

De taakuitvoering plannen met de volgende gebeurtenissen:

- **Schema op tijd**: 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.

- **Bij het opstarten van het systeem**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt gestart.
- **Bij het afsluiten van het systeem**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt afgesloten.

Standaardinstelling: **Planning op tijd**.

Type schema:

- **Maandelijks**: selecteer de maanden en de weken of dagen van de maand wanneer de taak zal worden uitgevoerd.
- **Dagelijks**: selecteer de dagen van de week wanneer de taak zal worden uitgevoerd.

- **Elk uur**: selecteer de dagen van de week, het aantal herhalingen en het tijdinterval waarin de taak wordt uitgevoerd.

Standaardinstelling: **Dagelijks**.

Starten om: selecteer het exacte tijdstip waarop de taak wordt uitgevoerd.

Uitvoeren binnen een datumbereik: stel een bereik in waarin het geconfigureerde schema van kracht is.

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.
- **Als niet aan de startvoorwaarden wordt voldaan, de taak daarna toch uitvoeren**: geef aan na hoeveel tijd de taak wordt uitgevoerd, ongeacht de andere startvoorwaarden.

Opmerking
Startvoorwaarden worden niet ondersteund voor Linux.

Opnieuw opstarten na update: definieer of opnieuw opstarten wordt geïnitieerd na de installatie van updates:

- **Nooit**: er wordt nooit opnieuw opgestart na de updates.
- **Indien nodig**: opnieuw opstarten wordt alleen uitgevoerd als dit is vereist voor het toepassen van de updates.
- **Altijd**: er wordt altijd opnieuw opgestart na de updates. U kunt altijd een vertraging voor opnieuw opstarten opgeven.

Niet opnieuw opstarten tot de back-up is voltooid. Als het back-upproces wordt uitgevoerd, wordt de machine pas opnieuw opgestart wanneer 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.

18.2.3 Lijst met patches beheren

Nadat de VA-scan is voltooid, vindt u de beschikbare patches in **Softwarebeheer** > **Patches**.

Naam	Beschrijving
Naam	De naam van de patch
Ernstgraad	De ernst van de patch: • **Kritiek** • **Hoog** • **Medium** • **Laag** • **Geen**
Verkoper	De verkoper van de patch
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.
Microsoft KB	Als de patch is bedoeld voor Microsoft-producten, wordt de id van het KB-artikel opgegeven
Releasedatum	De datum waarop de patch is uitgebracht
Machines	Aantal betroffen machines
Goedkeuringsstatus	De goedkeuringsstatus is voornamelijk nodig voor automatisch goedkeuringen en om in het beschermingsschema te kunnen definiëren welke updates moeten worden geïnstalleerd per status. 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 • **Niet gedefinieerd**: de patchstatus is onduidelijk en moet worden gevalideerd
Licentieovereenkomst	• Lezen en accepteren • Niet mee eens. Als u het niet eens bent met de licentieovereenkomst, wordt de patchstatus de waarde **Afgewezen** en wordt deze niet geïnstalleerd
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

18.2.4 Automatische patchgoedkeuring

Met automatische patchgoedkeuring kunt u updates eenvoudiger installeren op machines. Laten we een voorbeeld bekijken van hoe het werkt.

Zo werkt het

U hebt twee omgevingen nodig: een test- en productieomgeving. De testomgeving wordt gebruikt om de patchinstallatie te testen en ervoor te zorgen dat alles goed verloopt. Wanneer u patchinstallatie hebt getest in de testomgeving, kunt u deze veilige patches automatisch in de productieomgeving installeren.

Automatische patchgoedkeuring configureren

Automatische patchgoedkeuring configureren

1. Lees en accepteer de licentieovereenkomsten voor elke leverancier voor wie u de producten wilt bijwerken. Anders is automatische patchinstallatie niet mogelijk.
2. Configureer de instellingen voor automatische goedkeuring.
3. Maak het beschermingsschema (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 **Niet-gedefinieerd** zijn. Deze stap is nodig om de patches te valideren en te controleren of de machines goed werken na de patchinstallatie.
4. Maak het beschermingsschema (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.
5. Voer het schema Testpatch uit en controleer de resultaten. De goedkeuringsstatus voor die machines die geen problemen hebben, kan worden bewaard als **Niet gedefinieerd** terwijl de status voor machines die niet goed werken, moet worden ingesteld op **Afgewezen**.
6. Afhankelijk van het aantal dagen dat is ingesteld in de optie **Automatische goedkeuring**, krijgen de patches die **Niet gedefinieerd** zijn, nu de status **Goedgekeurd**.
7. Wanneer het schema Productiepatch wordt gestart, worden alleen de patches met de status **Goedgekeurd** geïnstalleerd op de productiemachines.

De handmatige stappen worden hieronder vermeld.

Stap 1. De licentieovereenkomsten voor de producten die u wilt bijwerken, lezen en accepteren

1. Ga in de serviceconsole naar **Softwarebeheer** > **Patches**.
2. Selecteer de patch en lees en accepteer de licentieovereenkomst.

Stap 2. De instellingen voor automatische goedkeuring configureren

1. Ga in de serviceconsole naar **Softwarebeheer** > **Patches**.
2. Klik op **Instellingen**.
3. Schakel de optie **Automatische goedkeuring** in en geef het aantal dagen op. De patches met de status **Niet gedefinieerd** worden dan automatisch ingesteld op **Akkoord** na opgegeven aantal dagen sinds de eerste poging tot patchinstallatie.
   U hebt bijvoorbeeld 10 dagen opgegeven. U hebt het schema Testpatch voor testmachines uitgevoerd en patches geïnstalleerd. Die patches die fouten hebben veroorzaakt op machines, hebt u gemarkeerd als **Afgewezen** en de rest van de patches behoudt de status **Niet**

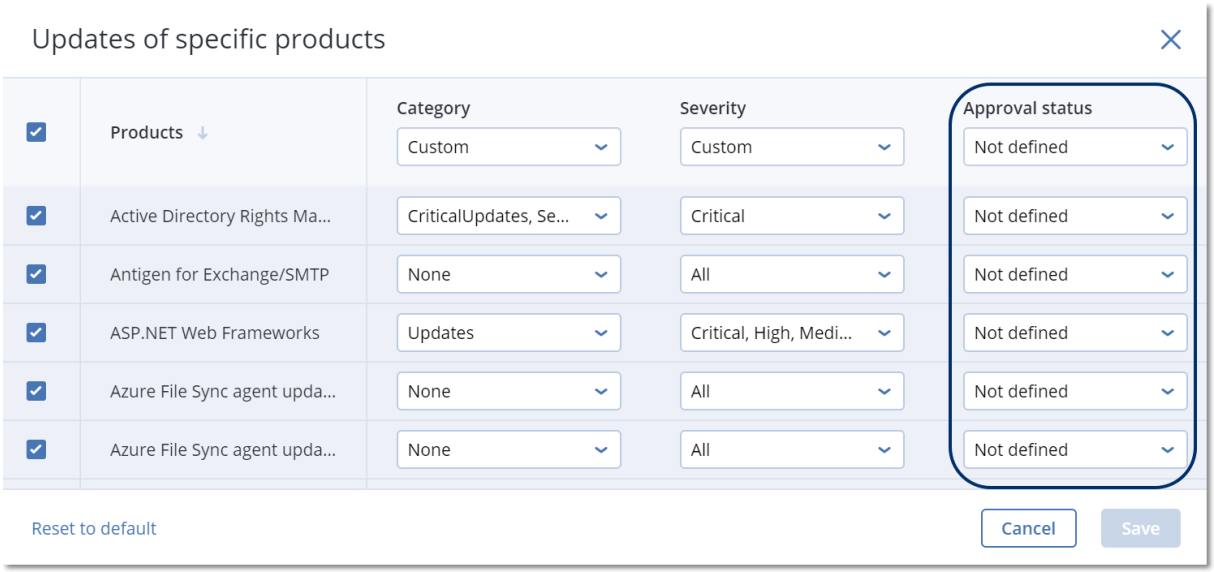
gedefinieerd. Nadat 10 dagen zijn verstreken, krijgen de patches met de status **Niet gedefinieerd** automatisch de status **Goedgekeurd**.

4. Schakel de optie **Licentieovereenkomsten automatisch accepteren** in. Dit is nodig voor automatische acceptatie van licenties tijdens de patchinstallatie. Er is geen bevestiging vereist van een gebruiker.

Stap 3. Het beschermingsschema Testpatch voorbereiden

1. Ga in de serviceconsole naar **Schema's** > **Bescherming**.
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. Raadpleeg 'Instellingen voor patchbeheer' voor meer informatie over deze instellingen.

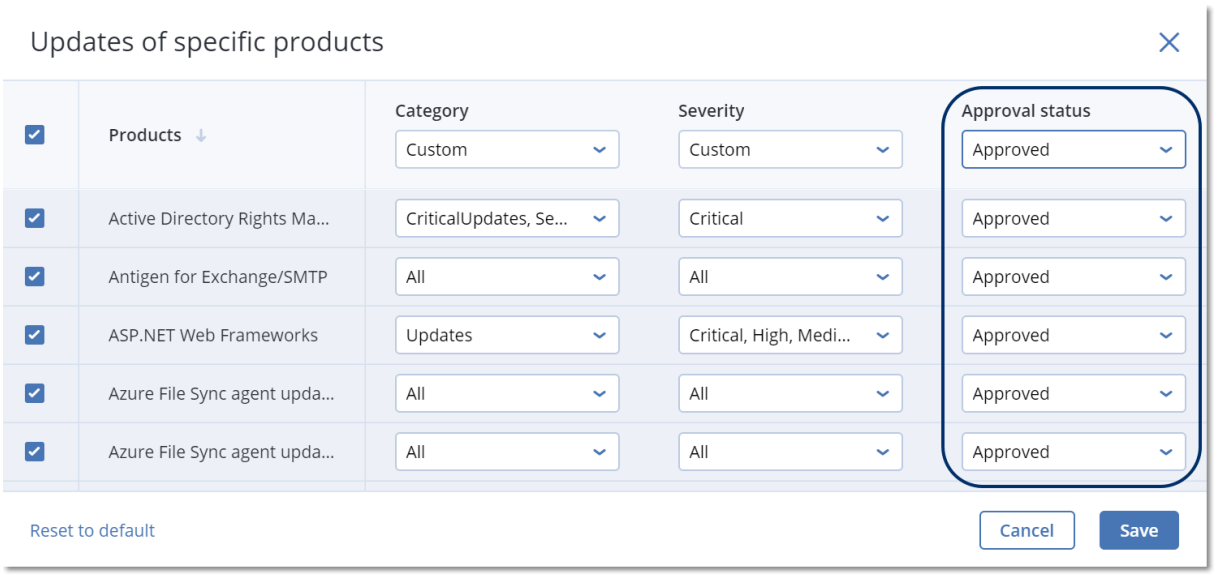
Belangrijk
Voor alle producten die moeten worden bijgewerkt, stelt u de **Goedkeuringsstatus** in als **Niet gedefinieerd**. Wanneer het tijd is om bij te werken, installeert de agent alleen patches met de status **Niet gedefinieerd** op de geselecteerde machines in de testomgeving.



Stap 4. Het beschermingsschema Productiepatch voorbereiden

1. Ga in de serviceconsole naar **Schema's** > **Bescherming**.
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. Raadpleeg 'Instellingen voor patchbeheer' voor meer informatie over deze instellingen.

Belangrijk
Voor alle producten die moeten worden bijgewerkt, stelt u de **Goedkeuringsstatus** in als **Goedgekeurd**. Wanneer het tijd is om bij te werken, installeert de agent alleen patches met de status **Goedgekeurd** op de geselecteerde machines in de productieomgeving.



Stap 5. Voer het beschermingsschema Testpatch uit en controleer de resultaten

1. Voer het beschermingsschema Testpatch (volgens schema of op aanvraag) uit.
2. Controleer daarna welke van de geïnstalleerde patches veilig zijn en welke niet.
3. Ga naar **Softwarebeheer** > **Patches** en stel de **Goedkeuringsstatus** in als **Afgewezen** voor de patches die niet veilig zijn.

18.2.5 Handmatige patchgoedkeuring

Het proces voor handmatige patchgoedkeuring is als volgt:

1. Ga in de serviceconsole naar **Softwarebeheer** > **Patches**.
2. Selecteer de patches die u wilt installeren en lees en accepteer de licentieovereenkomsten.
3. Stel **Goedkeuringsstatus** in op **Goedgekeurd** voor de patches die u goedkeurt voor installatie.
4. Maak een beschermingsschema terwijl de module Patchbeheer is ingeschakeld. U kunt het schema configureren of het schema op aanvraag starten door te klikken op **Nu uitvoeren** in de instellingen van de patchbeheermodule.

Hierdoor worden alleen de goedgekeurde patches op de geselecteerde machines geïnstalleerd.

18.2.6 Patchinstallatie op aanvraag

Patchinstallatie op aanvraag kan op drie manieren worden uitgevoerd, al naargelang wat u het beste uitkomt:

- Ga naar de lijst met patches (**Softwarebeheer** > **Patches**) en installeer de nodige patches.
- Ga naar de lijst met beveiligingsproblemen (**Softwarebeheer** > **Beveiligingsproblemen**) en start het herstelproces dat ook patchinstallatie omvat.
- Ga naar de lijst met apparaten (**Apparaten** > **Alle apparaten**), selecteer de specifieke machines die u wilt bijwerken en installeer de patches daarop.

Laten we de patchinstallatie doen aan de hand van de lijst met patches:

1. Ga in de serviceconsole naar **Softwarebeheer** > **Patches**.
2. Accepteer de licentieovereenkomsten voor de patches die u wilt installeren.
3. Selecteer de patches die u wilt installeren en klik op **Installeren**.
4. Selecteer de machines waarop patches moeten worden geïnstalleerd.
5. Bepaal of opnieuw opstarten wordt geïnitieerd na de installatie van patches:
   - **Nooit**: er wordt nooit opnieuw opgestart na de patches.
   - **Indien nodig**: opnieuw opstarten wordt alleen uitgevoerd als dit is vereist voor het toepassen van de patches.
   - **Altijd**: na de patches wordt altijd opnieuw opgestart. U kunt altijd een vertraging voor opnieuw opstarten opgeven.

   Niet opnieuw opstarten tot de back-up is voltooid. Als het back-upproces wordt uitgevoerd, wordt de machine pas opnieuw opgestart wanneer de back-up is voltooid.
6. Klik op **Patches installeren**.

De geselecteerde patches worden geïnstalleerd op de geselecteerde machines.

18.2.7 Levensduur in lijst voor patches

Als u de lijst met patches actueel wilt houden, gaat u naar **Softwarebeheer** > **Patches** > **Instellingen** en geeft u de optie **Levensduur in lijst** op.

De optie **Levensduur in lijst** bepaalt hoe lang de gedetecteerde beschikbare patch in de lijst met patches wordt bewaard. Over het algemeen wordt de patch uit de lijst verwijderd als de patch is geïnstalleerd op alle machines waarop de afwezigheid wordt gedetecteerd of de gedefinieerde tijd verstrijkt.

- **Voor altijd**: de patch blijft altijd in de lijst.
- **7 dagen**: de patch wordt verwijderd als er zeven dagen zijn verstreken na de eerste installatie. U hebt bijvoorbeeld twee machines 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 uit de lijst met patches verwijderd, zelfs als deze niet op de tweede machine is geïnstalleerd omdat deze offline was.

- **30 dagen**: de patch wordt verwijderd als er dertig dagen zijn verstreken na de eerste installatie.

19 Software-inventaris

Met de functie voor software-inventaris kunt u alle softwaretoepassingen bekijken die beschikbaar zijn op alle Windows- en macOS-apparaten met Cyber Protect-licenties (Essentials, Standard of Advanced).

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.

19.1 De software-inventarisscans inschakelen

Wanneer software-inventarisscan is ingeschakeld op apparaten met een toegewezen Cyber Protect-licentie en servicequota, worden de softwaregegevens automatisch om de 12 uur verzameld.

De functie voor software-inventarisscans is standaard ingeschakeld, 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 serviceconsole 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 serviceconsole 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.

19.2 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 een Cyber Protect-licentie.

Een software-inventarisscan uitvoeren vanaf het scherm Software-inventaris

1. Ga in de serviceconsole 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 serviceconsole naar **Apparaten**.
2. Klik op het apparaat dat u wilt scannen en klik op **Inventaris**.
3. Klik op het tabblad **Software** op **Nu scannen**.

19.3 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 een Cyber Protect-licentie.
- 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 serviceconsole 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**.
Verkoper	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 **Toepassingen**.
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.
Verkoper	Leverancier van de toepassing. Meervoudige selectie is mogelijk. Gebruik dit filter als u alle toepassingen van een specifieke leverancier op specifieke apparaten of op

Filter	Beschrijving
	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.

19.4 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 een Cyber Protect-licentie.
- Software-inventarisscan op het apparaat is voltooid.

De software-inventaris van een bepaald apparaat bekijken vanaf het scherm Software-inventaris

1. Ga in de serviceconsole 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 serviceconsole naar **Apparaten**.
2. Klik op het apparaat dat u wilt bekijken en klik op **Inventaris**.
3. Klik op het tabblad **Software**.

20 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. 31) 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.

20.1 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 serviceconsole 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 serviceconsole 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.

20.2 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 overeenkomen met de huidige datum en tijd in UTC. Zorg ervoor dat 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-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 virtuele machines) De machine wordt uitgevoerd op een van de ondersteunde virtualisatieplatforms. Zie "Hardware-inventaris" (p. 539) voor meer informatie.

Een hardware-inventarisscan uitvoeren voor een bepaald apparaat

1. Ga in de serviceconsole naar **Apparaten**.
2. Klik op het apparaat dat u wilt scannen en klik op **Inventaris**.
3. Klik op het tabblad **Hardware** op **Nu scannen**.

20.3 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. 539) voor meer informatie.

Alle hardwareonderdelen bekijken die beschikbaar zijn op de Windows- en macOS-apparaten van het bedrijf

1. Ga in de serviceconsole 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.

Kolom	Beschrijving
	• **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.

20.4 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. 539) voor meer informatie.

De gedetailleerde informatie bekijken over de hardware van een specifiek apparaat

1. Ga in de serviceconsole 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**.

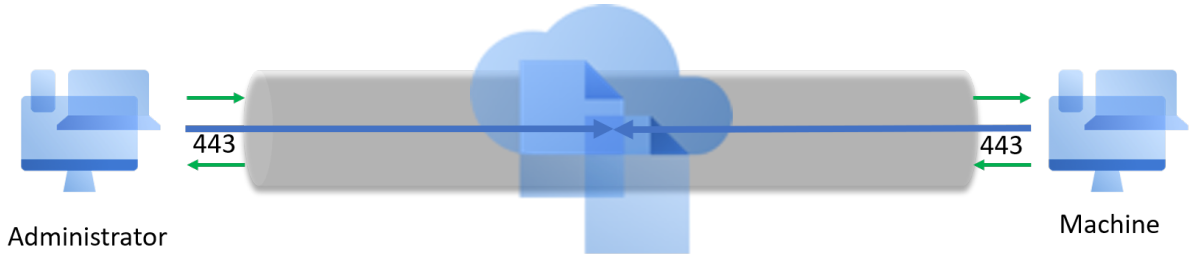
4. Klik op de rij waar het apparaat wordt vermeld en klik op **Inventaris**.
5. Klik op het tabblad **Hardware**.
   De volgende hardwaregegevens zijn beschikbaar.

Hardwareonderdeel	Weergegeven informatie
Moederbord	Naam, fabrikant, model en serienummer van het moederbord van het apparaat.
Processors	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.

21 Toegang tot extern bureaublad

21.1 Externe toegang (RDP- en HTML5-clients)

Cyberbescherming biedt een functie voor externe toegang. U kunt verbinding maken en uw machines voor eindgebruikers beheren via een externe verbinding. U kunt tekst kopiëren en plakken van en naar de externe machine met de HTML5-client. Met de RDP-client kunt u zowel tekst als bestanden kopiëren en plakken. Zo kunt u uw eindgebruikers gemakkelijk helpen bij het oplossen van problemen op hun machines.

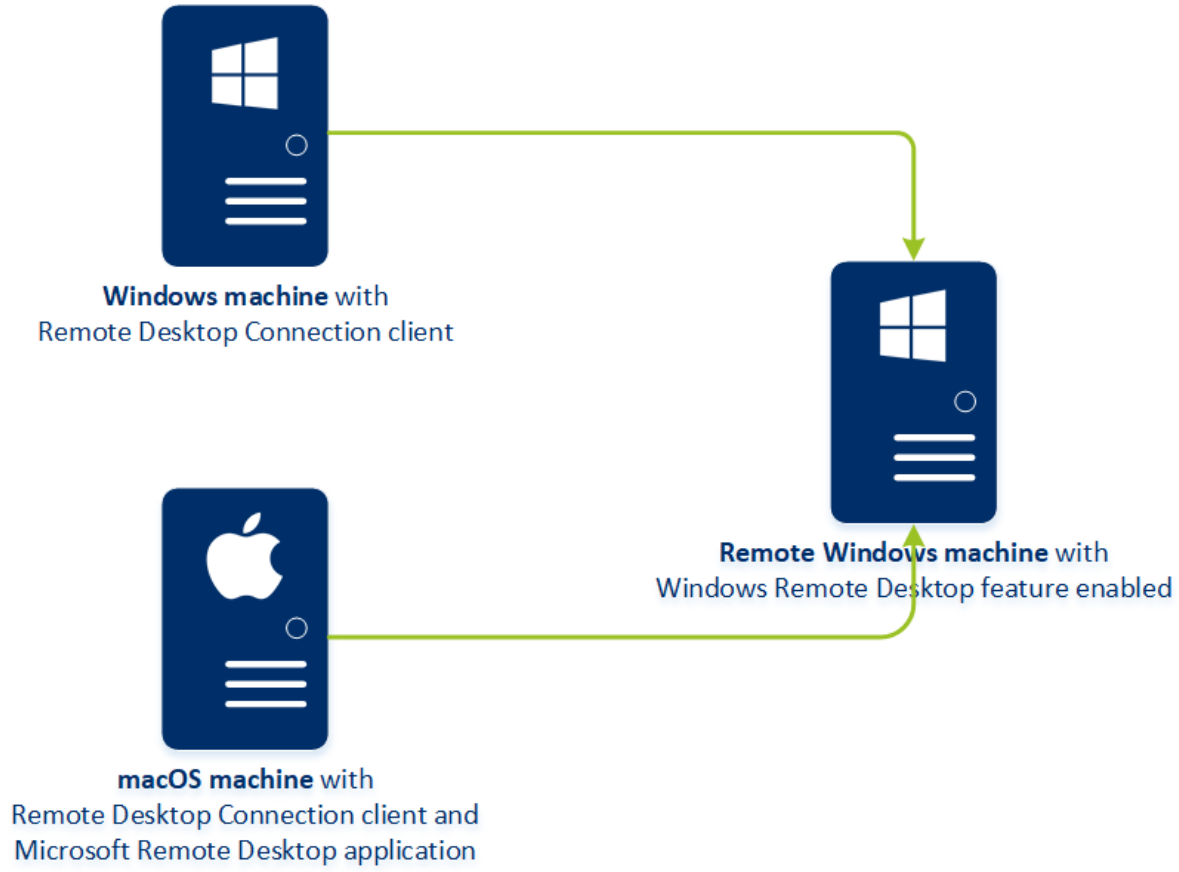


Cloud Connection broker

Vereisten:

- Een externe machine is geregistreerd in Cyberbescherming en de beveiligingsagent is geïnstalleerd.
- De Cyber Protect-quota bestaat of is al opgehaald voor een machine.
- De client voor verbinding met extern bureaublad voor RDP-verbindingen is geïnstalleerd op een machine vanwaaruit de verbinding wordt gestart.

Een RDP-sessie kan tot stand worden gebracht vanaf zowel Windows- als macOS-machines. Een HTML5-sessie voor externe verbinding kan tot stand worden gebracht met elke browser die HTML5 ondersteunt.



De functionaliteit voor externe toegang kan worden gebruikt voor verbindingen met Windows-machines waarop de functie Windows Extern bureaublad beschikbaar is. Externe toegang kan dus bijvoorbeeld niet worden gebruikt voor een verbinding met Windows 10 Home en macOS-systemen.

Als u een macOS-machine en een externe machine wilt verbinden, moeten de volgende toepassingen zijn geïnstalleerd op de macOS-machine:

- De client voor verbinding met extern bureaublad
- De toepassing Microsoft Extern bureaublad

21.1.1 Zo werkt het

Wanneer u probeert verbinding te maken met een externe machine, wordt eerst gecontroleerd of deze machine een Cyber Protect-quota heeft. Als de nodige servicequota voor de externe RDP-functionaliteit bestaat voor de klanttenant, maar niet is opgehaald voor de machine, wordt u gevraagd om deze servicequota handmatig op te halen. Vervolgens controleert het systeem of verbinding via de HTML5- of RDP-client mogelijk is. U start een verbinding via de RDP- of HTML5-client. Het systeem maakt een tunnel naar de externe machine en controleert of de verbindingen voor extern bureaublad zijn ingeschakeld op de externe machine. Vervolgens voert u de referenties in en krijgt u toegang tot de machine als de validatie lukt.

21.1.2 Verbinding maken met een externe machine

Ga als volgt te werk om verbinding te maken met een externe machine:

1. Ga in de serviceconsole naar **Apparaten** > **Alle apparaten**.
2. Klik op de machine waarmee u een externe verbinding wilt maken en klik vervolgens op **Cyber Protection Desktop** > **Verbinden via RDP-client** / **Verbinden via HTML5-client**.
   Er wordt automatisch gecontroleerd of deze machine een Cyber Protect-quota heeft. Als de nodige servicequota voor de externe RDP-functionaliteit bestaat voor de klanttenant, maar niet is opgehaald voor de machine, wordt u gevraagd om deze servicequota handmatig op te halen.
3. Selecteer, indien daarom wordt gevraagd, een van de aanbevolen servicequota's en klik op **Wijzigen en verbinden**.
4. [Optioneel, alleen voor verbinding via RDP-client] Download en installeer de client voor Verbinding met extern bureaublad. Breng de verbinding met de externe machine tot stand.
5. Geef de gebruikersnaam en het wachtwoord op voor toegang tot de machine te krijgen en klik op **Verbinden**.

U bent dan verbonden met de externe machine en u kunt deze beheren.

21.1.3 Een sessie voor hulp op afstand uitvoeren

Hulp op afstand maakt gelijktijdige toegang tot dezelfde extern-bureaubladsessie mogelijk. Wanneer u bijvoorbeeld een probleem op een computer van een externe gebruiker moet oplossen, kunt u verbinding maken met die computer via hulp op afstand. De gebruiker en de externe beheerder delen één sessie, zodat de gebruiker een probleem kan delen en reproduceren.

1. Ga in de serviceconsole naar **Apparaten** > **Alle apparaten**.
2. Klik op de machine waarmee u een verbinding op afstand wilt maken en klik vervolgens op **Cyber Protection Desktop** > **Hulp op afstand uitvoeren**.
   Er wordt automatisch gecontroleerd of deze machine een Cyber Protect-quota heeft. Als de nodige servicequota voor de externe RDP-functionaliteit bestaat voor de klanttenant, maar niet is opgehaald voor de machine, wordt u gevraagd om deze servicequota handmatig op te halen.
3. Selecteer, indien daarom wordt gevraagd, een van de aanbevolen servicequota's en klik op **Wijzigen en verbinden**.
4. Kopieer het wachtwoord voor de sessie van hulp op afstand en klik op **Verbinden**. Als de sessie niet start, download en installeer dan de connectiviteitsagent op uw machine en probeer opnieuw verbinding te maken.
5. Als er al interactieve sessies zijn, klik dan op **Verbinding maken met sessie**.
6. Voer het wachtwoord voor de sessie van hulp op afstand in.

U krijgt dan toegang tot de externe machine via het externe bureaublad, zodat u de gebruiker kunt helpen.

21.2 Een externe verbinding delen met gebruikers

Gebruikers die op afstand werken en toegang moeten hebben tot een externe machine, hebben toegang tot de machine zonder een geconfigureerd VPN of andere tools voor een externe verbinding.

Met de Cyberbescherming-service kunt u een RDP-link delen met eindgebruikers, zodat ze extern toegang krijgen tot hun machines.

1. De functionaliteit voor externe verbindingen inschakelen
   a. Ga in de serviceconsole naar **Instellingen** > **Bescherming** > **Externe verbinding**.
   b. Schakel **Verbinding met extern bureaublad delen** in.

   Wanneer u een apparaat selecteert, wordt de nieuwe optie **Externe verbinding delen** weergegeven in het rechtermenu.
2. Genereer de link om de externe verbinding te delen.
   a. Ga in de serviceconsole naar **Apparaten** > **Alle apparaten** en selecteer het apparaat waarmee u een externe verbinding wilt laten maken.
   b. Klik op **Cyber Protection Desktop** > **Externe verbinding delen**.
   c. Klik op **Link ophalen**. Kopieer de gegenereerde link in het geopende venster.

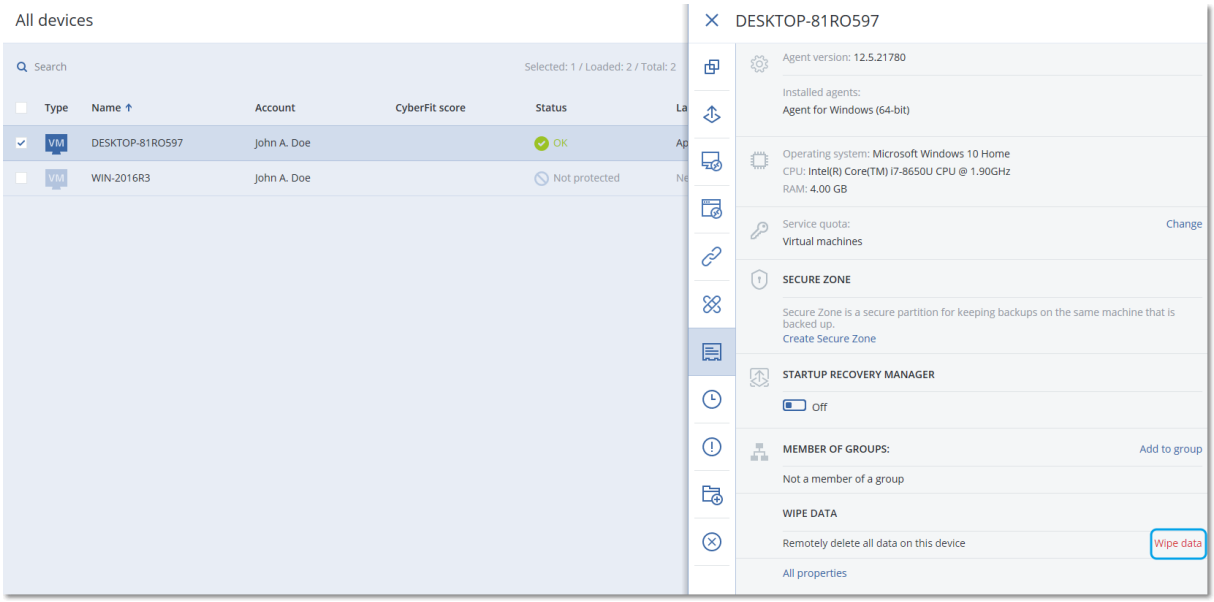
   De link is 10 uur geldig.
3. Deel de link met de gebruiker.

   Via deze link wordt de gebruiker doorgeleid naar een pagina waar het verbindingstype moet worden geselecteerd:
   - Maak verbinding via RDP-client. U wordt gevraagd of u de client voor de externe verbinding wilt downloaden en installeren.
   - Maak verbinding via HTML5-client. Voor deze verbinding is geen installatie van een RDP-client op de machine van de gebruiker vereist. Een aanmeldingsscherm wordt geopend waar de gebruiker de referenties voor de externe machine moet invoeren.

22 Extern wissen

Beheerders van de Cyberbescherming-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 10. De machine moet zijn ingeschakeld en verbinding hebben met internet om de opdracht voor wissen te kunnen ontvangen.



Gegevens van een machine wissen

1. Ga in de serviceconsole 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
   Tip U kunt de details over het wissen bekijken en zien wie de bewerking heeft gestart, via **Dashboard** > **Activiteiten**.

23 Slimme bescherming

23.1 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.

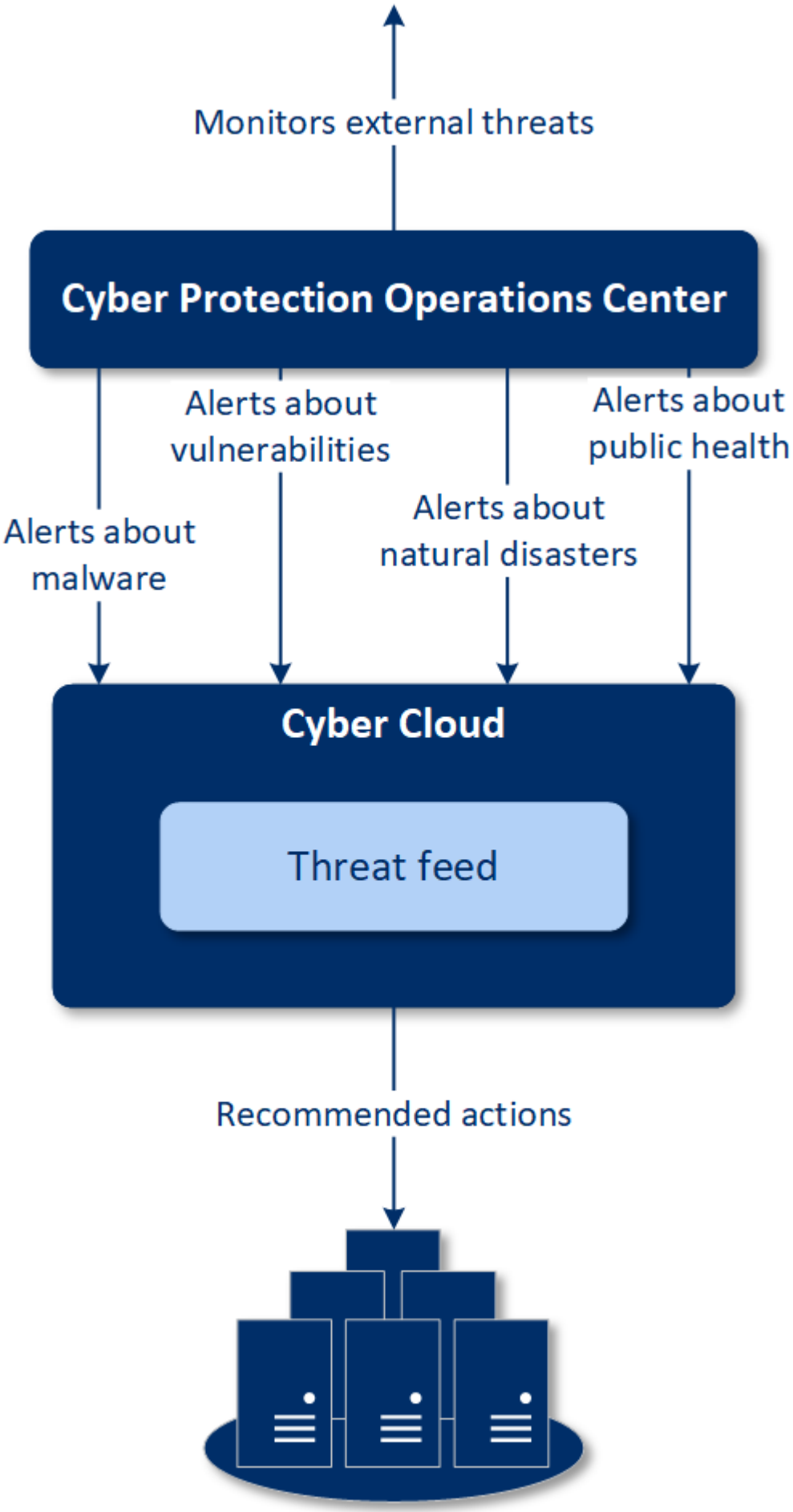
Sommige beveiligingswaarschuwingen kunnen worden opgelost met een set specifieke acties die worden opgegeven door de beveiligingsexperts. Andere beveiligingswaarschuwingen geven u alleen informatie over komende bedreigingen, maar er zijn geen aanbevolen acties beschikbaar.

Opmerking
Malwarewaarschuwingen worden alleen gegenereerd voor machines waarop de agent voor Antimalwarebeveiliging is geïnstalleerd.

23.1.1 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 serviceconsole 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.


Monitors external threats
Cyber Protection Operations Center
Alerts about malware
Alerts about vulnerabilities
Alerts about natural disasters
Alerts about public health
Cyber Cloud
Threat feed
Recommended actions
Machines

Als u de aanbevolen acties wilt starten voor ontvangen waarschuwingen van Acronis Cyber Protection Operations Center, gaat u als volgt te werk:

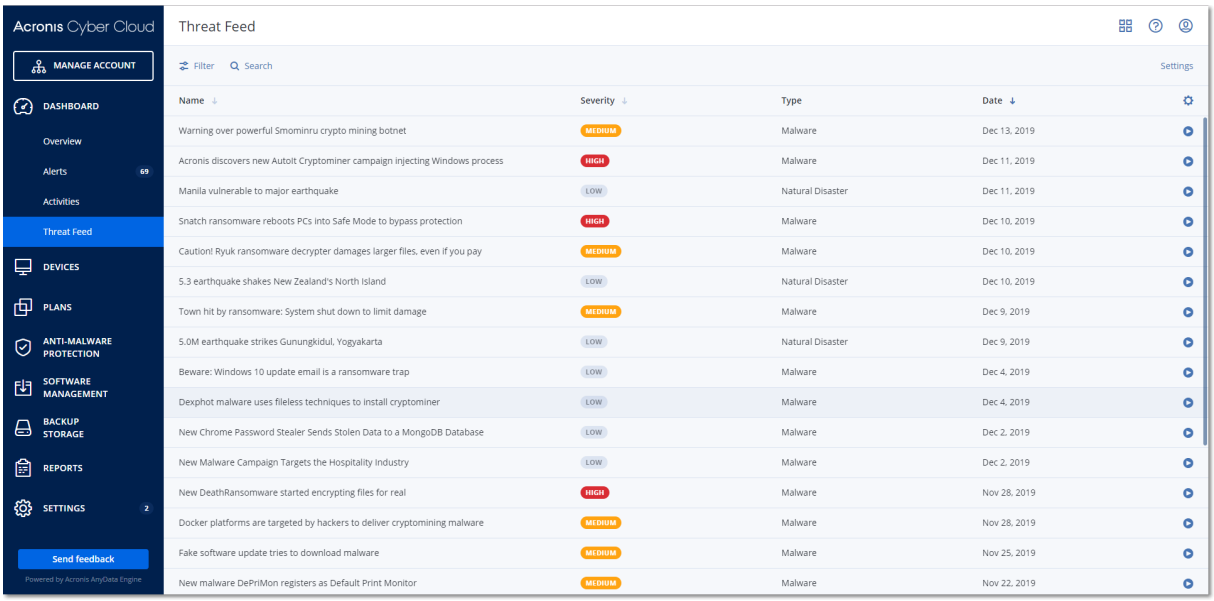
1. Ga in de serviceconsole naar **Dashboard** > **Bedreigingsfeed** om te controleren of er bestaande beveiligingsmeldingen zijn.
2. Selecteer een waarschuwing in de lijst en bekijk de opgegeven details.
3. Klik op **Starten** om de wizard te starten.
4. Schakel de acties in die u wilt uitvoeren en de 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 werkblad, maakt het systeem een volledige back-up met de volgende naamnotatie:

     `%workload_name%-Remediation`

     Als er al een back-up bestaat, maakt het systeem een incrementele back-up in het bestaande archief.
5. Klik op **Starten**.
6. Controleer op de pagina **Activiteiten** of de activiteit is uitgevoerd.



23.1.2 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

23.2 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.

23.2.1 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.

23.2.2 Gedetecteerde onbeschermde bestanden beheren

Ga als volgt te werk om de belangrijke bestanden te beschermen die zijn gedetecteerd als onbeschermd:

1. Ga in de serviceconsole 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.

23.2.3 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.

De taakuitvoering plannen met de volgende gebeurtenissen:

- **Schema op tijd**: 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.

- **Bij het opstarten van het systeem**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt gestart.
- **Bij het afsluiten van het systeem**: de taak wordt uitgevoerd wanneer het besturingssysteem wordt afgesloten.

Standaardinstelling: **Planning op tijd**.

Type schema:

- **Maandelijks**: selecteer de maanden en de weken of dagen van de maand wanneer de taak zal worden uitgevoerd.
- **Dagelijks**: selecteer de dagen van de week wanneer de taak zal worden uitgevoerd.
- **Elk uur**: selecteer de dagen van de week, het aantal herhalingen en het tijdinterval waarin de taak wordt uitgevoerd.

Standaardinstelling: **Dagelijks**.

Starten om: selecteer het exacte tijdstip waarop de taak wordt uitgevoerd.

Uitvoeren binnen een datumbereik: stel een bereik in waarin het geconfigureerde schema van kracht is.

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.
- **Als niet aan de startvoorwaarden wordt voldaan, de taak daarna toch uitvoeren**: 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.

24 Modus Verbeterde beveiliging

De modus Verbeterde beveiliging biedt speciale instellingen voor klanten met verhoogde beveiligingseisen. In deze modus is versleuteling van alle back-ups vereist en zijn alleen lokaal ingestelde versleutelingswachtwoorden toegestaan.

Met de modus Verbeterde beveiliging 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 kunnen de versleutelingswachtwoorden niet instellen in de beschermingsschema's.

Cloudservices hebben geen toegang tot de versleutelingswachtwoorden. Als gevolg van deze beperking zijn de volgende functies niet beschikbaar voor tenants in de modus Verbeterde beveiliging:

- Herstel via de serviceconsole
- Bladeren door back-ups op bestandsniveau via de serviceconsole
- 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

24.1 Beperkingen

- De modus Verbeterde beveiliging is alleen compatibel met agenten met versie 15.0.26390 of hoger.
- De modus Verbeterde beveiliging is niet beschikbaar voor apparaten waarop Red Hat Enterprise Linux 4.x of 5.x en afgeleiden daarvan worden uitgevoerd.

24.2 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.

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 "De versleutelingsinstellingen opslaan op een machine" (p. 204).
3. In Cyber Protect Monitor (voor Windows en macOS).

Waarschuwing!
Er is geen manier om versleutelde back-ups te herstellen als u het wachtwoord verliest of vergeet.

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**.

24.3 Versleutelingswachtwoord wijzigen

U kunt het versleutelingswachtwoord wijzigen voordat er back-ups worden gemaakt voor een beschermingsschema.

Het wordt niet aanbevolen 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. 211) 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 "De versleutelingsinstellingen opslaan op een machine" (p. 204).

24.4 Back-ups herstellen

Met de modus Verbeterde beveiliging kunt u geen back-ups herstellen via de serviceconsole.

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.

25 Apparaatbesturing

De apparaatbeheermodule[1], die deel uitmaakt van de beschermingsschema's van de Cyberbescherming-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 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

[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.

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:

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

Opmerking
Agent voor preventie van gegevensverlies voor macOS ondersteunt alleen x64-processors (ARM64 wordt niet ondersteund).

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 weergeven dat Agent voor preventie van gegevensverlies op de computer is geïnstalleerd, maar de functie voor apparaatbeheer zal niet werken. De functie voor apparaatbeheer werkt alleen op macOS-systemen die worden ondersteund door Agent voor preventie van gegevensverlies.

25.0.1 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 serviceconsole. 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.

25.1 Apparaatbeheer gebruiken

Dit gedeelte bevat stapsgewijze instructies voor basistaken bij het gebruik van de apparaatbeheermodule.

25.1.1 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. Ga in de serviceconsole 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 klik om de optie **Apparaatbeheer** in of uit te schakelen.
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 **Bewerken**.

Indien gewenst, kunt u het deelvenster voor het beschermingsschema ook openen vanaf het tabblad Schema's. Deze mogelijkheid is echter niet beschikbaar in alle edities van de Cyberbescherming-service.

25.1.2 Het gebruik van de apparaatbeheermodule inschakelen op macOS

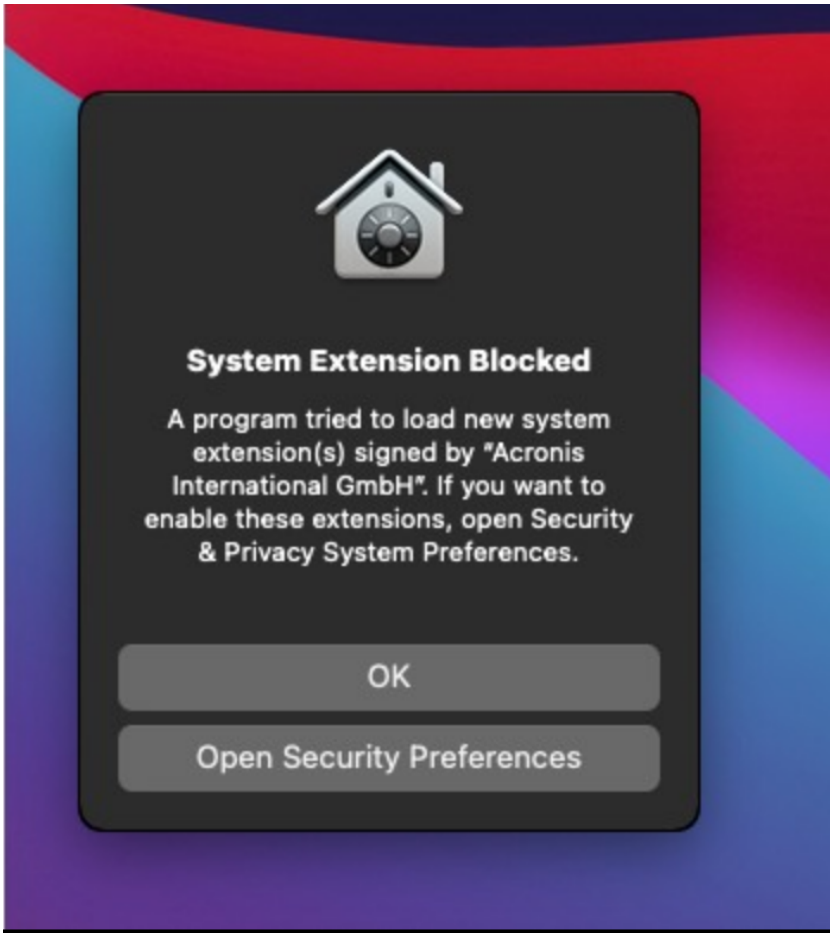
De instellingen voor apparaatbeheer van een beschermingsschema worden pas van kracht nadat het stuurprogramma voor apparaatbeheer op de beschermde workload is geladen. In dit gedeelte wordt beschreven hoe het stuurprogramma voor apparaatbeheer moet worden geladen om het gebruik van de apparaatbeheermodule op macOS mogelijk te maken. Dit is een eenmalige operatie waarvoor beheerdersrechten op de eindpuntmachine zijn vereist.

Ondersteunde macOS-versies:

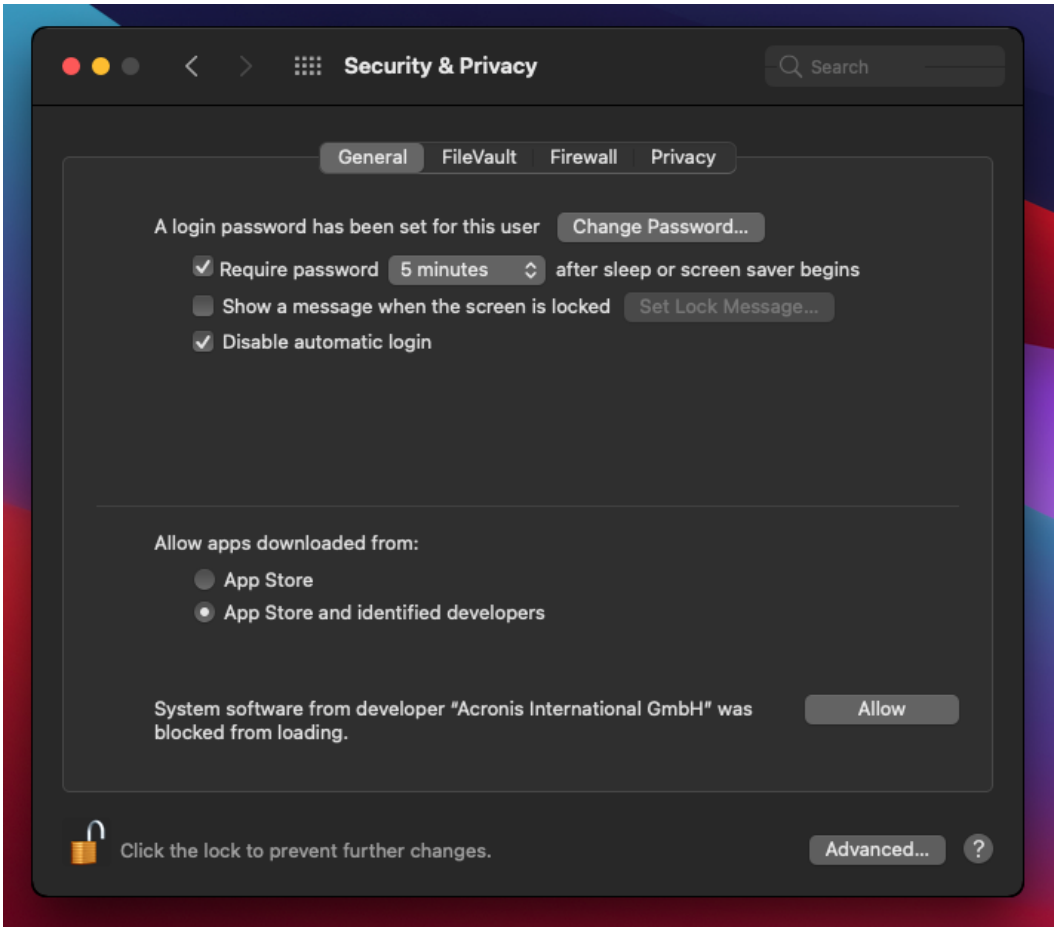
- macOS 10.15 (Catalina) en later
- macOS 11.2.3 (Big Sur) en later

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.

25.1.3 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.

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.

25.1.4 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.

25.1.5 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. Ga in de serviceconsole 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 serviceconsole naar **Dashboard** > **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. 581).

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.

25.1.6 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 serviceconsole naar **Dashboard** > **Waarschuwingen**.
2. Zoek waarschuwingen met de volgende status: 'Toegang tot randapparaat is geblokkeerd'.

Zie Waarschuwingen van apparaatbeheer voor meer informatie.

25.2 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.

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.

25.2.1 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 serviceconsole. 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.

25.3 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).

25.4 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 het is raadzaam dit selectievakje voor dergelijke apparaten (muis, toetsenbord) in te schakelen. Het is ook raadzaam 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.

25.4.1 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).
- Voeg een apparaat toe op het tabblad USB-apparaten van het deelvenster Inventaris van een computer in de serviceconsole (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 gebruikersinterface van de serviceconsole, 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 serviceconsole 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 serviceconsole 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**.

25.5 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 **Uitzonderingen**.
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 **Uitzonderingen**.
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 **Uitzonderingen**.
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.

25.6 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 serviceconsole. 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 serviceconsole, gaat u naar **Dashboard** > **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 waarop de gebeurtenis zich heeft voorgedaan.
- **Apparaat**: De naam van de computer waarop de gebeurtenis zich heeft voorgedaan.
- **[Schemanaam]**: De naam van het beschermingsschema waardoor de gebeurtenis is gegenereerd.
- **Bron**: Het apparaattype of de poort waarvoor de gebeurtenis zich heeft voorgedaan. 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 geïnitieerd.
- **Proces**: U moet een volledig gekwalificeerd pad definiëren 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.

25.6.1 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.
- **Afbeelding 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 (afbeelding) 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, afbeelding) 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 (afbeelding, bestand) kopiëren**: Gebruik Rich Text Format om een afbeelding met een bestand te kopiëren/plakken via het lokale klembord.
- **RTF-gegevens (tekst, afbeelding, 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 (afbeelding)**: 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, afbeelding)**: 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 (afbeelding, 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, afbeelding, 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 (afbeelding)**: 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, afbeelding)**: 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 (afbeelding, 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, afbeelding, 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).

26 Het tabblad Schema's

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

Op het tabblad **Schema's** kunt u beschermingsschema's en andere beschikbare schema's bewaken en beheren, zoals schema's voor back-upscans, schema's voor cloudtoepassingen en VM-replicatieschema's.

Elk van de subsecties van het tabblad **Schema's** bevat een specifiek type schema:

- **Bescherming**
- **Back-upscan**
- **Back-up van cloudtoepassingen**
- **VM-replicatie**

Voor beschermingsschema's en VM-replicatieschema's is een klikbare statusbalk beschikbaar. Hierop worden de statussen weergegeven met kleurcodes:

- OK (groen)
- Waarschuwing (oranje)
- Fout (rood)
- Het schema is actief (blauw)
- Het schema is uitgeschakeld (grijs)

Als u op de statusbalk klikt, kunt u zien welke status een schema heeft en op hoeveel machines. Elke status in deze lijst kan ook worden aangeklikt.

26.1 Beschermingsschema

Een beschermingsschema maken

1. Ga in de serviceconsole naar **Schema's** > **Bescherming**.
2. Klik op **Schema maken**.
3. Selecteer de machines die u wilt beschermen.
4. Klik op **Beschermen**. U ziet het beschermingsschema met de standaardinstellingen.
5. [Optioneel] Klik op het potloodpictogram naast de naam om de naam van het beschermingsschema te wijzigen.
6. [Optioneel] Klik op de optie naast de modulenaam om de schemamodule in of uit te schakelen.
7. [Optioneel] Als u de parameters van de module wilt wijzigen, klikt u op het desbetreffende gedeelte van het beschermingsschema.

8. Klik op **Apparaten toevoegen** om de machines te selecteren waarop u het schema wilt toepassen.
9. Wanneer u klaar bent, klikt u op **Maken**.

De geselecteerde apparaten zijn dan beveiligd met het beschermingsschema.

U kunt de volgende bewerkingen uitvoeren met beschermingsschema's:

- Een beschermingsschema maken, bekijken, bewerken, klonen, uitschakelen, inschakelen en verwijderen
- Activiteiten voor elk beschermingsschema bekijken
- Waarschuwingen voor elk beschermingsschema bekijken
- Een schema exporteren naar een bestand
- Een eerder geëxporteerd schema importeren

26.2 Schema voor back-upscans

Als u back-ups op malware wilt scannen, kunt u een back-upscanschema maken.

Let op het volgende:

- De back-ups met CDP-herstelpunten kunnen worden geselecteerd voor scans, maar alleen reguliere herstelpunten (dus geen CDP-herstelpunten) worden gescand.
- Wanneer de CDP-back-up is geselecteerd voor veilig herstel van een volledige machine, wordt de machine veilig hersteld zonder de gegevens in het CDP-herstelpunt. Als u de CDP-gegevens wilt herstellen, start u de herstelactiviteit Bestanden/mappen.

Een back-upscanschema maken

1. Ga in de serviceconsole naar **Schema's** > **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 opnieuw worden gedefinieerd. De back-ups worden door de cloudagent in het clouddatacentrum gescand. Het systeem selecteert automatisch de cloudagent waarmee de scan wordt uitgevoerd.
   - **Back-ups om te scannen**:
     - **Locaties**: selecteer locaties met back-ups die u wilt scannen.
     - **Back-ups**: selecteer back-ups die u wilt scannen.
   - **Scannen op**:
     - **Malware**: deze optie kan niet opnieuw worden gedefinieerd. Hiermee worden back-ups gecontroleerd op de aanwezigheid van malware.

- **Versleuteling**: geef een wachtwoord op om versleutelde back-ups te scannen. Als een kluis of meerdere back-ups zijn geselecteerd, kunt u één wachtwoord opgeven voor alle back-ups. Als het wachtwoord niet geschikt is voor een back-up, wordt een waarschuwing gegenereerd.
- **Schema** : deze optie kan niet opnieuw worden gedefinieerd. De scanactiviteit wordt automatisch gestart in de cloudopslag.

4. Wanneer u klaar bent, klikt u op **Maken**.

Het back-upscanschema wordt dan gemaakt. De opgegeven locaties of back-ups worden automatisch gescand door de cloudagent.

26.3 Back-upschema's voor cloudtoepassingen

In het gedeelte **Schema's** > **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 Cyberbescherming-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.

27 Opstartmedia

Een opstartmedium is een cd, dvd, USB-flashstation of een ander verwisselbaar medium waarmee u de Cyberbescherming-agent kunt uitvoeren in een Linux-omgeving of een Windows Preinstallation Environment/Windows Recovery Environment (WinPE/WinRE), zonder de hulp 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.

27.1 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.

27.2 Op Linux of op WinPE/WinRE gebaseerde opstartmedia?

27.2.1 Op Linux gebaseerd

Op Linux gebaseerde opstartmedia bevatten een Cyberbescherming-agent, 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.

27.2.2 Op WinPE/WinRE gebaseerd

Op WinPE gebaseerde opstartmedia bevatten een minimaal Windows-systeem, de zogenaamde Windows Preinstallation Environment (WinPE), en een Cyberbescherming-plug-in voor WinPE, dat wil zeggen een aangepaste Cyberbescherming-agent 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 Cyberbescherming 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 Cyberbescherming-agent 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).

27.3 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 Cyberbescherming-agent.

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. 594) om een aangepast ISO-bestand te maken.

   Als u het kant-en-klare ISO-bestand wilt downloaden, selecteert u een machine in de Cyberbescherming-serviceconsole en klikt u vervolgens op **Herstellen** > **Meer herstelbewerkingen...** > **ISO-image downloaden**.
2. [Optioneel] Genereer een registratietoken in de Cyberbescherming-serviceconsole. 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 **Toepassingen** > **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.

27.4 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 Cyberbescherming-agent is geïnstalleerd.

27.4.1 Waarom Bootable Media Builder gebruiken?

Het kant-en-klare opstartmedium dat kan worden gedownload in de serviceconsole, is 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.

27.4.2 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.

27.4.3 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. 595) 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 Cyberbescherming-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. 598) voor meer informatie over de scripts.
10. [Optioneel] Selecteer hoe de opstartmedia worden geregistreerd in de Cyberbescherming-service bij het opstarten. Zie "De opstartmedia registreren" (p. 607) 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 Cyberbescherming-serviceconsole 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.

27.4.4 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).

27.4.5 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` `tekenreeks`,	Nee	De standaardwaarde voor het besturingselement. Als het paar niet wordt opgegeven, is de standaardwaarde

	`multiString`, `wachtwoord` of `enum` number voor het `type` `getal`, `spinner` of `selectievakje`		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 `spinner`)	number	Nee	De stapwaarde van het kringveld in een draaivak. Als het paar niet wordt opgegeven, is de waarde `1`.
`items` (alleen voor `enum`)	reeks van tekenreeksen	Ja	De waarden voor een vervolgkeuzelijst.
`required` (voor `tekenreeks`, `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.

27.4.6 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
        }
    }
}
```

27.4.7 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, 8.1, 10 (32 bits en 64 bits)
- Windows Server 2012, 2016, 2019 (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)
- Vensters 10 (PE voor Windows 10)

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 Cyberbescherming met WinPE en WinRE:

- Een geheel nieuw ISO-bestand maken met de Cyberbescherming-plug-in.
- De Cyberbescherming-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 Cyberbescherming-agent 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 Cyberbescherming-service bij het opstarten. Zie "De opstartmedia registreren" (p. 607) 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 installatiekopieën van PE 2.x of 3.x wilt maken of wijzigen, installeert u Bootable Media Builder op een machine waarop een pakket voor automatische Windows-installaties (Windows Automated Installation Kit, AIK) is geïnstalleerd. Als u geen machine met AIK hebt, gaat u als volgt te werk.

Een machine met AIK voorbereiden

1. Download en installeer Windows Automated Installation Kit.
   Automated Installation Kit (AIK) voor Windows Vista (PE 2.0):
   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en
   Automated Installation Kit (AIK) voor Windows Vista SP1 en Windows Server 2008 (PE 2.1):
   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=en
   Automated Installation Kit (AIK) voor Windows 7 (PE 3.0):
   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en
   Automated Installation Kit (AIK), aanvulling voor Windows 7 SP1 (PE 3.1):
   http://www.microsoft.com/download/en/details.aspx?id=5188
   U kunt de systeemvereisten voor installatie vinden via de hier vermelde links.
2. [Optioneel] Brand de WAIK op dvd of kopieer deze naar een flashstation.
3. Installeer Microsoft .NET Framework vanuit dit pakket (NETFXx86 of NETFXx64, afhankelijk van uw hardware).
4. Installeer Microsoft Core XML (MSXML) Parser 5.0 of 6.0 vanuit dit pakket.
5. Installeer Windows AIK vanuit dit pakket.
6. Installeer Bootable Media Builder op dezelfde machine.

Voorbereiding: WinPE 4.0 en later

Als u installatiekopieën van PE 4 of later wilt maken of wijzigen, installeert u Bootable Media Builder op een machine waarop Windows Assessment and Deployment Kit (ADK) is geïnstalleerd. Als u geen machine met ADK hebt, gaat u als volgt te werk.

Een machine met ADK voorbereiden

1. Download het installatieprogramma van Assessment and Deployment Kit.

   Assessment and Deployment Kit (ADK) voor Windows 8 (PE 4.0): http://www.microsoft.com/en-us/download/details.aspx?id=30652.

   Assessment and Deployment Kit (ADK) voor Windows 8.1 (PE 5.0): http://www.microsoft.com/en-US/download/details.aspx?id=39982.

   Assessment and Deployment Kit (ADK) voor Windows 10 (PE voor Windows 10): https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx.

   U kunt de systeemvereisten voor installatie vinden via de hier vermelde links.
2. Installeer Assessment and Deployment Kit op de machine.
3. Installeer Bootable Media Builder op dezelfde machine.

27.4.8 De opstartmedia registreren

Door de opstartmedia te registreren in de Cyberbescherming-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 Cyberbescherming-service

1. Ga in Bootable Media Builder naar **Registratie van opstartmedia**.
2. Geef in **Service-URL** het serviceadres van Cyberbescherming op.
3. [Optioneel] Geef bij **Weergavenaam** een naam op voor de opgestarte machine.
4. Als u de automatische registratie in de Cyberbescherming-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 Cyberbescherming op.
4. Voer bij **Registratietoken** het registratietoken in.
5. Klik op **Registreren**.

27.4.9 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.

27.5 Een machine registreren die is opgestart vanaf opstartmedia

27.5.1 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.

27.5.2 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**.

27.6 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.

27.6.1 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**.

27.6.2 Herstel

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**.

27.7 Startup Recovery Manager

Startup Recovery Manager is een opstartbaar onderdeel dat zich op de Windows-systeemschijf of in de Linux /boot-partitie bevindt. Met Startup Recovery Manager kunt u het opstartbare herstelprogramma starten zonder afzonderlijke opstartmedia te gebruiken.

Startup Recovery Manager is vooral handig voor gebruikers die op reis zijn. Als er een fout optreedt, start u de machine opnieuw op, wacht u tot de prompt **Druk op F11 voor Acronis Startup Recovery Manager** wordt weergegeven en drukt u vervolgens op F11. Het programma start en u kunt het herstel uitvoeren. Op machines waarop de GRUB-opstartlader is geïnstalleerd, selecteert u Startup Recovery Manager in het opstartmenu in plaats van op F11 te drukken tijdens het opnieuw opstarten.

Als u Startup Recovery Manager wilt gebruiken, moet u het eerst activeren. Op die manier wordt de opstartprompt **Druk op F11 voor Acronis Startup Recovery Manager** ingeschakeld (of wordt het item **Startup Recovery Manager** toegevoegd aan het GRUB-menu (als u GRUB gebruikt)).

Opmerking
Als u Startup Recovery Manager wilt activeren, moet u minstens 100 MB vrije schijfruimte hebben op de Windows-systeemschijf of in de Linux /boot-partitie.

Door de activering van Startup Recovery Manager wordt de MBR overschreven met een eigen opstartcode, tenzij u de GRUB-opstartlader gebruikt en deze in de Master Boot Record (MBR) is geïnstalleerd. Als er opstartladers van derden zijn geïnstalleerd, moeten deze mogelijk opnieuw worden geactiveerd.

Wanneer u in Linux een andere opstartlader dan GRUB (zoals LILO) gebruikt, kunt u overwegen deze te installeren op een Linux root- (of boot-)partitie in plaats van de MBR voordat u Startup Recovery Manager activeert. Installeer de opstartlader anders handmatig na de activering.

Startup Recovery Manager activeren op een machine met Agent voor Windows of Agent voor Linux

1. Selecteer in de Cyberbescherming-serviceconsole de machine waarop u Startup Recovery Manager wilt activeren.
2. Klik op **Details**.
3. Schakel de optie **Startup Recovery Manager** in.
4. Wacht totdat Startup Recovery Manager is geactiveerd door de software.

Startup Recovery Manager activeren op een machine zonder agent

1. Start de machine op vanaf de opstartmedia.
2. Klik op **Hulpmiddelen** > **Startup Recovery Manager activeren**.
3. Wacht totdat Startup Recovery Manager is geactiveerd door de software.

Als u Startup Recovery Manager wilt deactiveren, herhaalt u de activeringsprocedure en selecteert u de respectievelijke tegengestelde acties. Als u deactiveert, wordt de opstartprompt **Druk op F11 voor Acronis Startup Recovery Manager** (of het menu-item in GRUB) uitgeschakeld.

28 Controle

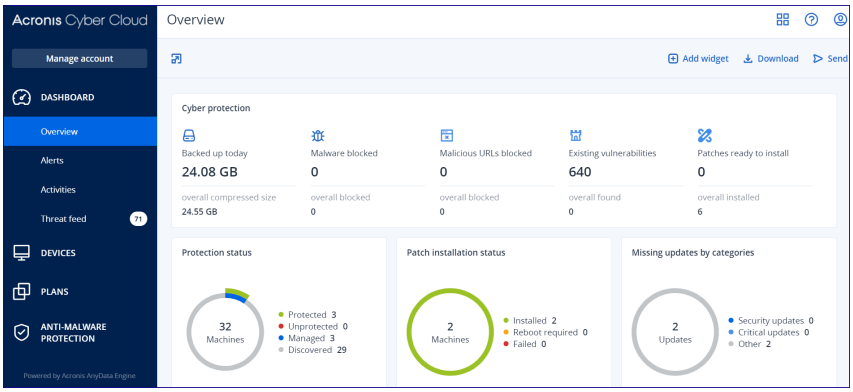
28.1 Het dashboard Overzicht

Het dashboard **Overzicht** bevat enkele aanpasbare widgets die een overzicht bieden van de bewerkingen voor de Cyberbescherming-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 **Dashboard** > **Overzicht** zijn niet beschikbaar in de Standard-edities van de Cyberbescherming-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.

28.2 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.

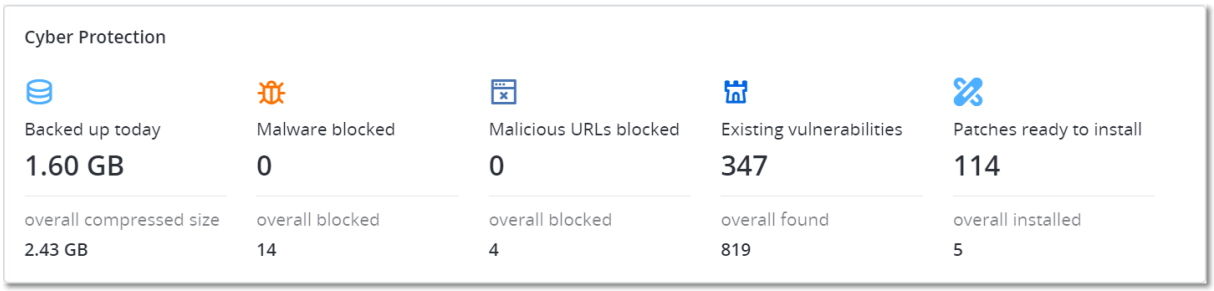
U kunt de activiteiten ook filteren op de volgende eigenschappen:

- **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 op het Developer Network Portal voor meer informatie over de beschikbare eigenschappen.

28.3 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 beveiligingsproblemen**: het aantal momenteel bestaande beveiligingsproblemen
- **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

28.4 Beveiligingsstatus

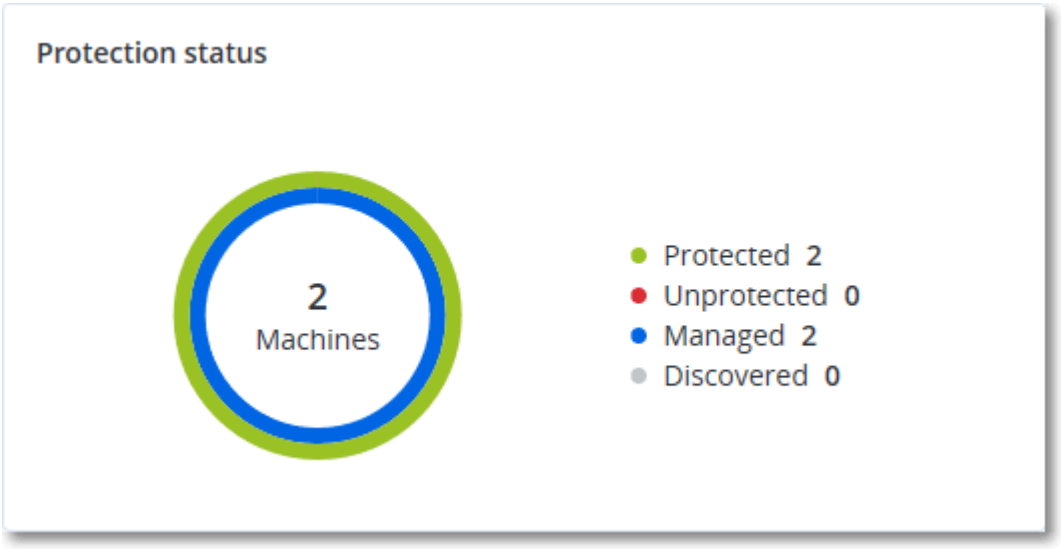
28.4.1 Beveiligingsstatus

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.



28.4.2 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

28.5 #CyberFit-score per machine

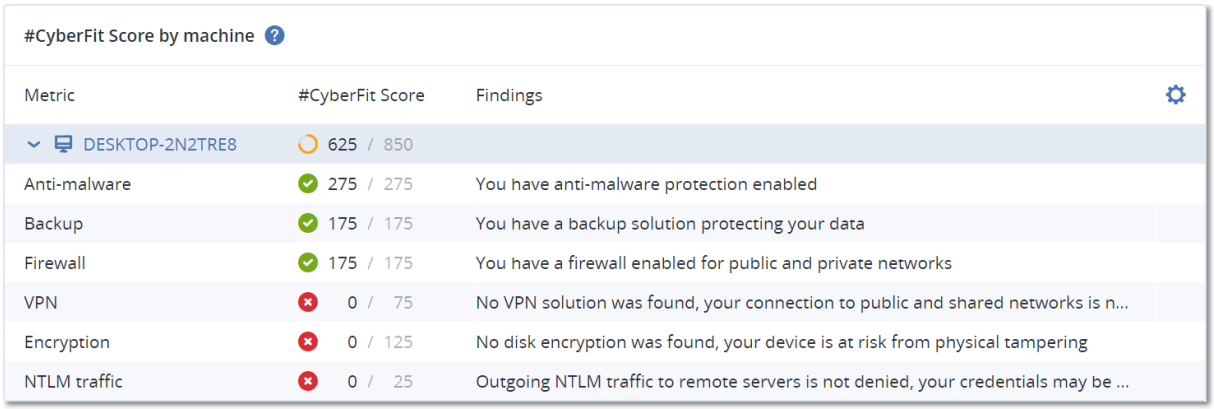
In deze widget ziet u voor elke machine de totale #CyberFit-score, de samengestelde scores en de bevindingen voor elk van de beoordeelde metrieken:

- 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.



28.6 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.
- Op NVMe-stations wordt schijfintegriteitscontrole alleen ondersteund voor stations die de SMART-gegevens via de Windows-API communiceren. Schijfintegriteitscontrole wordt niet ondersteund voor NVMe-stations waarop de SMART-gegevens rechtstreeks van het station moeten worden gelezen.

Schijfintegriteit kan een van de volgende statussen hebben:

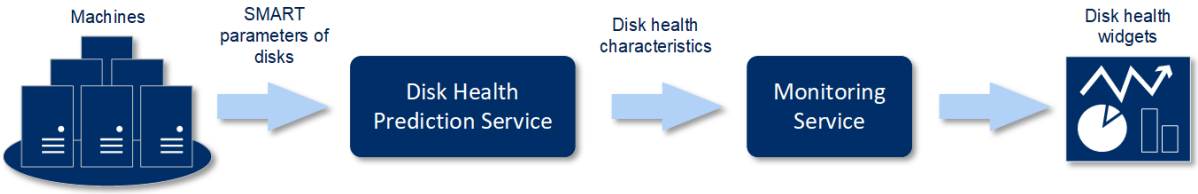
- **OK**
  : de schijfintegriteit is tussen de 70 en 100%.
- **Waarschuwing**
  : de schijfintegriteit is tussen de 30 en 70%.
- **Kritiek**
  : de schijfintegriteit is tussen de 0 en 30%.
- **Schijfgegevens berekenen**
  : de huidige schijfstatus en -prognose worden berekend.

28.6.1 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 serviceconsole.



28.6.2 Widgets voor schijfintegriteit

De resultaten van de schijfintegriteitscontrole worden weergegeven in de volgende widgets die beschikbaar zijn in de serviceconsole.

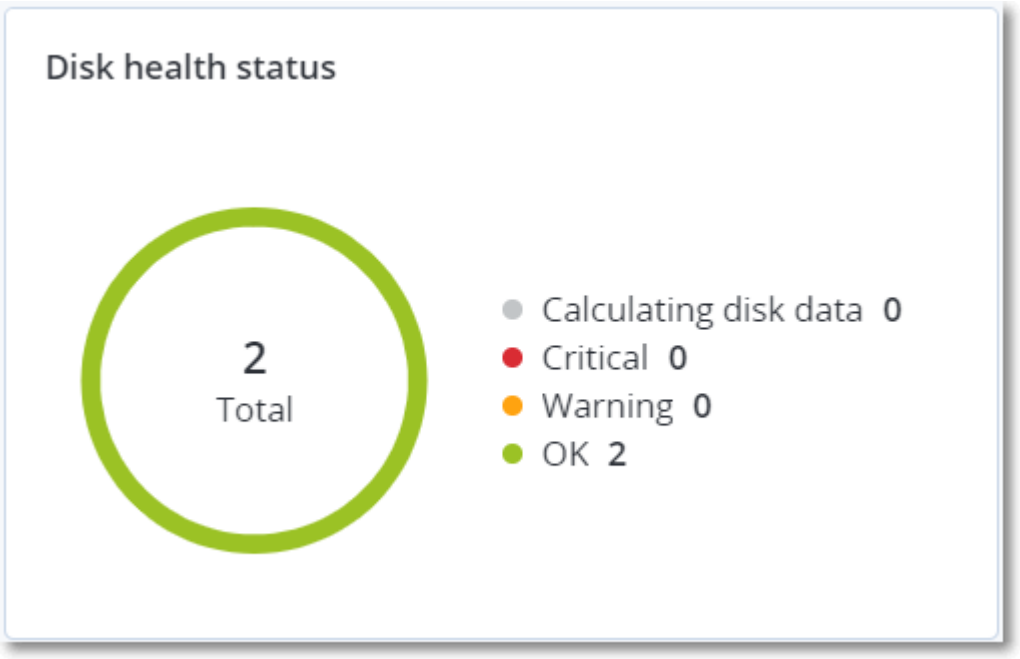
- **Overzicht van schijfintegriteit**: een widget met een structuurkaart op twee detailniveaus waartussen kan worden geschakeld.
  - Machineniveau
    : Geeft samengevatte informatie weer over de status van de schijfintegriteit van de geselecteerde klantmachines. Alleen de meest kritieke schijfstatus 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.



28.6.3 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. Een imageback-up van deze schijf wordt op dit moment niet aanbevolen, 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.

28.7 Overzicht van gegevensbescherming

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.

Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

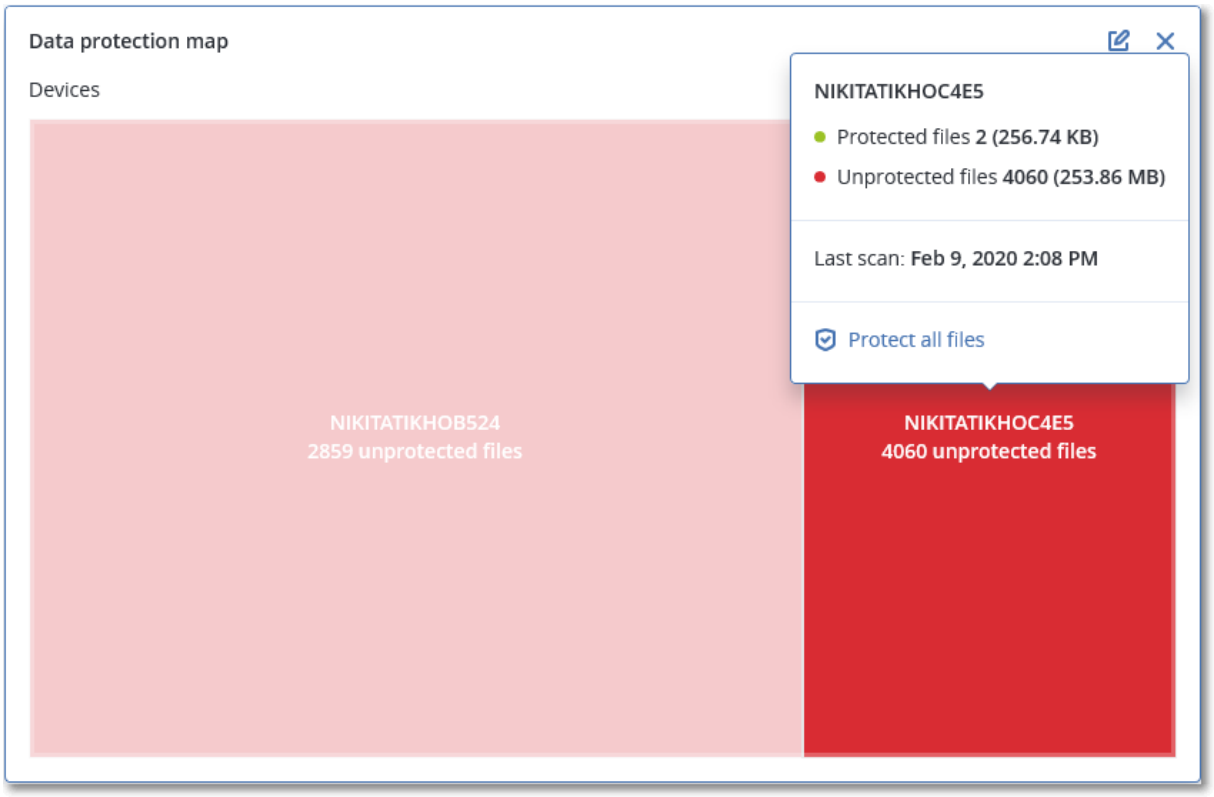
Bestanden kunnen een van de volgende beveiligingsstatussen hebben:

- **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 oor 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 oor 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 dashboard in de widget Overzicht van gegevensbescherming, een widget met een structuurkaart waarin de detailniveaus 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.

28.8 Widgets voor evaluatie van beveiligingsproblemen

28.8.1 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

28.8.2 Bestaande kwetsbaarheden

Deze widget geeft de momenteel bestaande beveiligingsproblemen op machines weer. De widget **Bestaande beveiligingsproblemen** 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

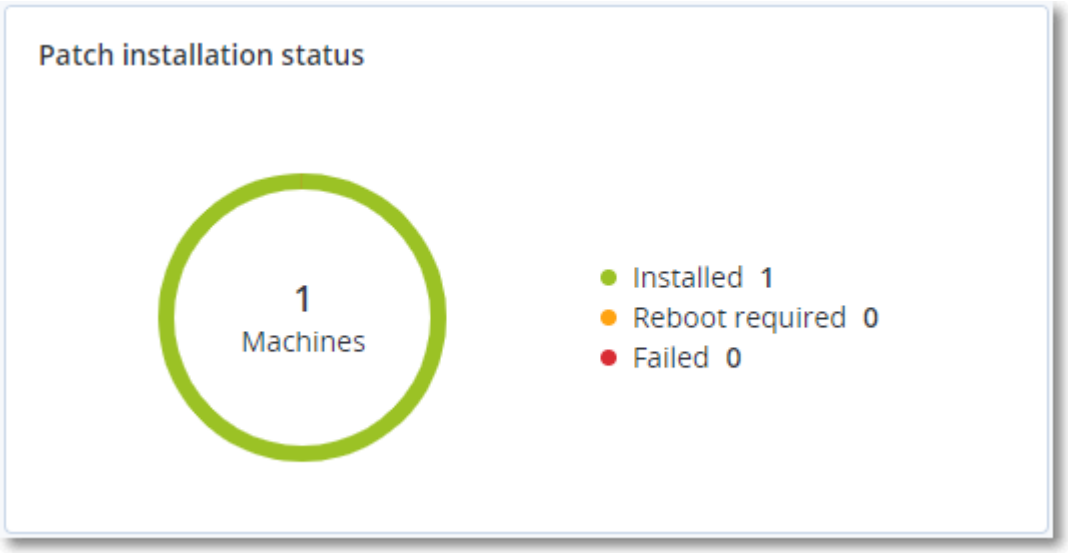
28.9 Widgets voor patchinstallatie

Er zijn vier widgets gerelateerd aan de functionaliteit voor patchbeheer.

28.9.1 Status van patchinstallatie

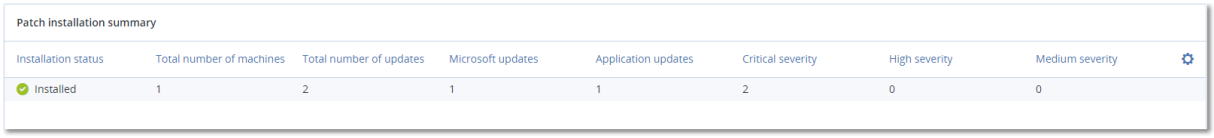
Deze widget geeft het aantal machines weer, gegroepeerd op status van de patchinstallatie.

- **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



28.9.2 Overzicht van patchinstallatie

Deze widget geeft een overzicht van de patches op machines weer, gesorteerd op de status van de patchinstallatie.



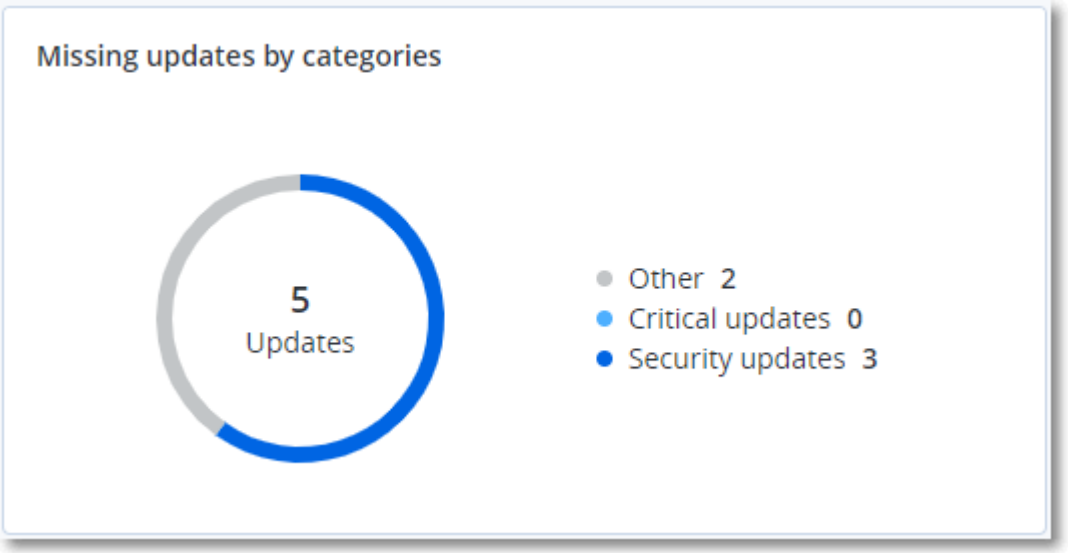
28.9.3 Geschiedenis van patchinstallatie

Deze widget geeft gedetailleerde informatie over patches op machines weer.

28.9.4 Ontbrekende updates per categorie

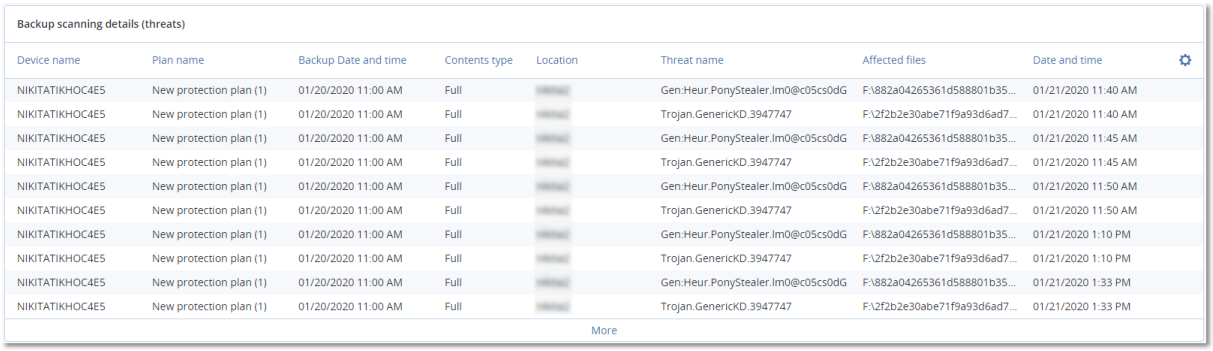
Deze widget geeft het aantal ontbrekende updates per categorie weer. De volgende categorieën worden weergegeven:

- Beveiligingsupdates
- Kritieke updates
- Anders



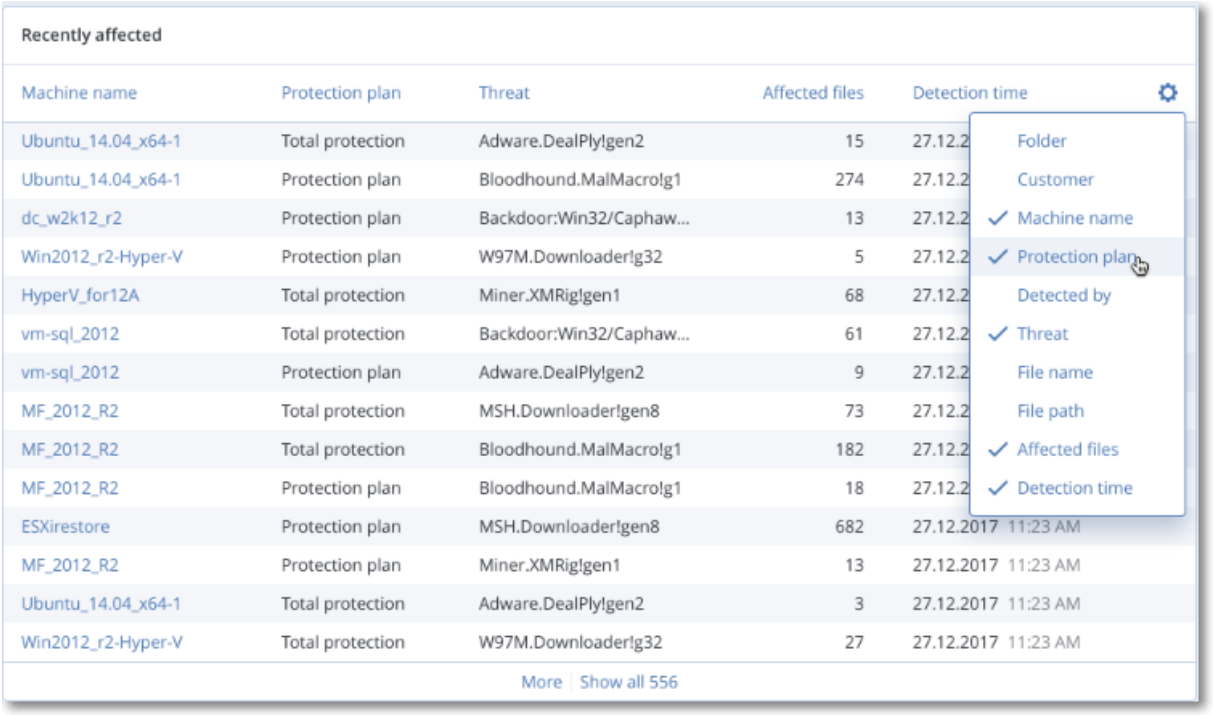
28.10 Gegevens van back-upscan

Deze widget geeft gedetailleerde informatie over de gedetecteerde bedreigingen in back-ups weer.



28.11 Onlangs beïnvloed

Deze widget geeft gedetailleerde informatie over recent geïnfecteerde machines weer. U kunt informatie vinden over welke bedreiging is gedetecteerd en hoeveel bestanden zijn geïnfecteerd.

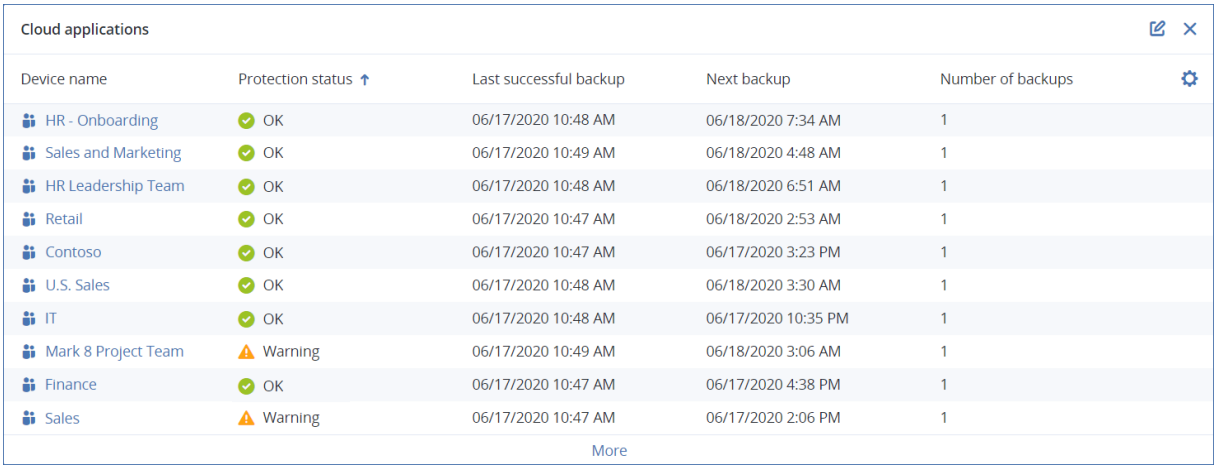


28.12 Cloudtoepassingen

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

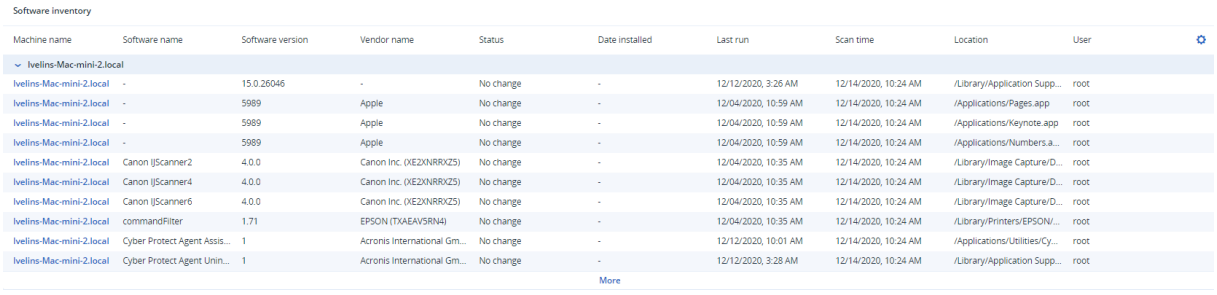


Aanvullende informatie over cloud-to-cloud-resources is ook beschikbaar in de volgende widgets:

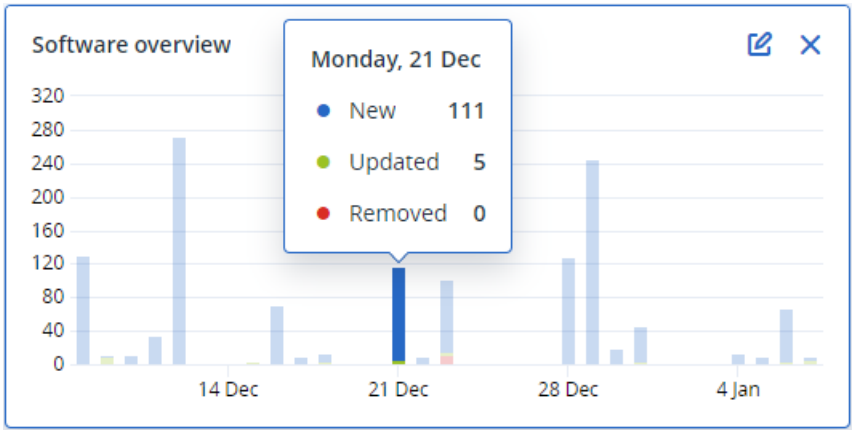
- Activiteiten
- Activiteitenlijst
- 5 meest recente waarschuwingen
- Geschiedenis van waarschuwingen
- Overzicht van waarschuwingen activeren
- Overzicht van historische waarschuwingen
- Gegevens van actieve waarschuwingen
- Locatieoverzicht

28.13 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.

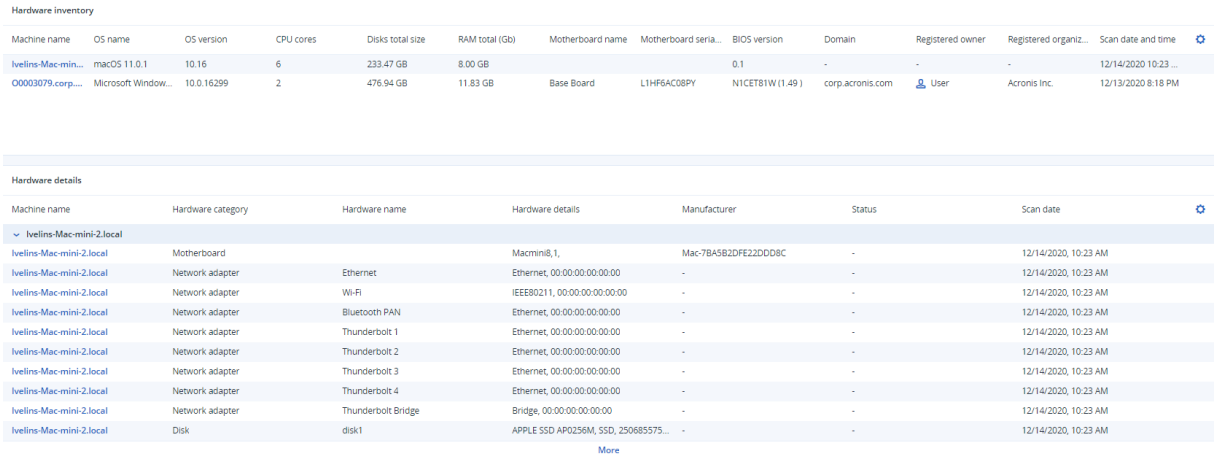
Bijgewerkt: het aantal bijgewerkte toepassingen.

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.

28.14 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.



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

29 Rapporten

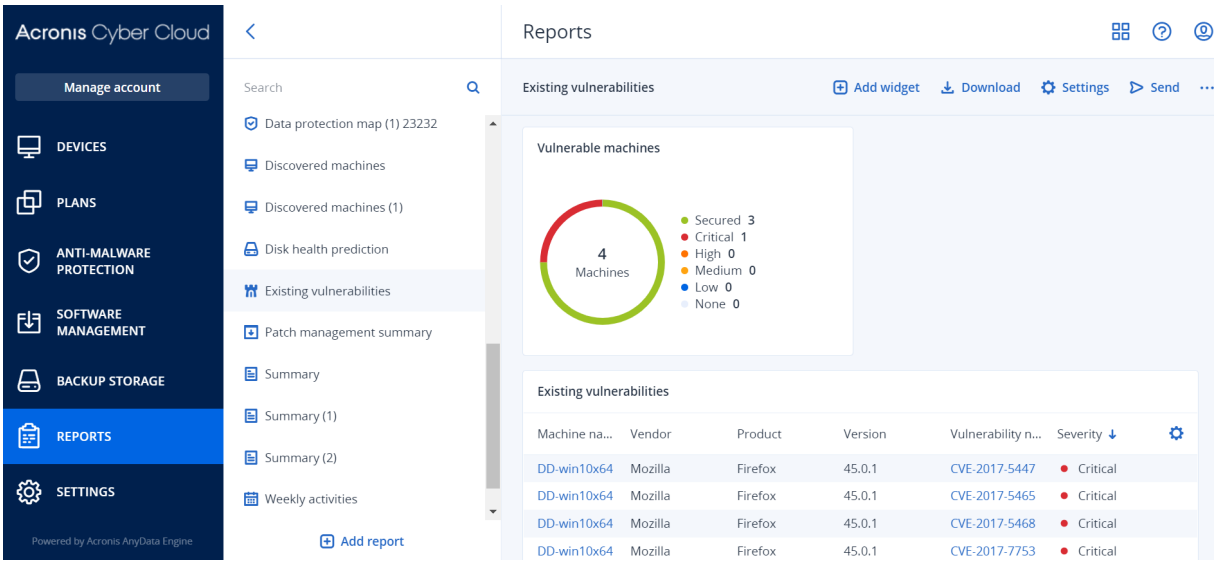
Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

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. 635).

Alle historische widgets tonen gegevens voor hetzelfde tijdbereik. U kunt dit bereik wijzigen in de rapportinstellingen.

U kunt de standaardrapporten gebruiken of een aangepast rapport maken.



De set standaardrapporten hangt af van de Cyberbescherming-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.

Als u een rapport wilt bekijken, klikt u op de naam ervan.

Als u bewerkingen met een rapport wilt openen, klikt u op het ellipspictogram op de rapportregel. Dezelfde bewerkingen zijn beschikbaar vanuit het rapport.

29.0.1 Rapport toevoegen

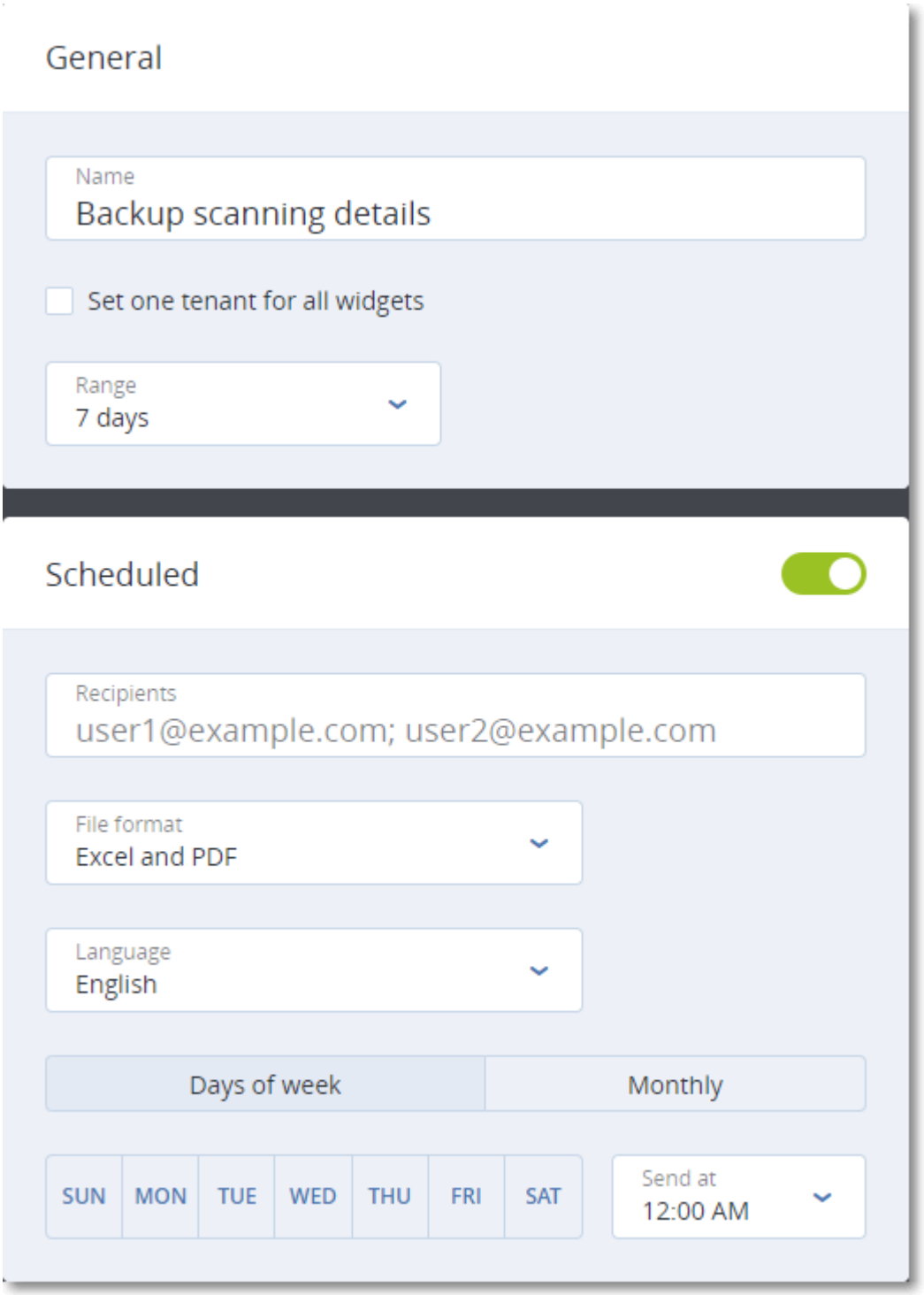
1. Klik op **Rapport toevoegen**.
2. Voer een van de volgende handelingen uit:
   - Als u een vooraf gedefinieerd rapport wilt toevoegen, klikt u op de naam ervan.
   - Als u een aangepast rapport wilt toevoegen, klikt u op **Aanpassen**, klikt u op de naam van het rapport (de standaard toegewezen namen zien eruit als **Aangepast (1)**) en vervolgens voegt u widgets toe aan het rapport.

3. [Optioneel] Versleep de widgets om ze opnieuw te rangschikken.
4. [Optioneel] Bewerk het rapport zoals hieronder beschreven.

29.0.2 Rapport bewerken

Als u een rapport wilt bewerken, klikt u op de naam ervan en vervolgens klikt u op **Instellingen**. Wanneer u een rapport bewerkt, kunt u het volgende doen:

- De naam van het rapport wijzigen
- Het tijdbereik voor alle widgets in het rapport wijzigen
- Plannen om het rapport in PDF- en/of XLSX-indeling via e-mail te verzenden



29.0.3 Een rapport plannen

1. Klik op de naam van het rapport en klik vervolgens op **Instellingen**.
2. Schakel de switch **Gepland** in.
3. Geef de e-mailadressen van de ontvangers op.
4. Selecteer het rapportformaat: .pdf, .xlsx of beide.

5. Selecteer de dagen en het tijdstip waarop het rapport wordt verzonden.
6. Klik op **Opslaan** in de rechterbovenhoek.

Opmerking
Het maximale aantal geëxporteerde items is 1000 voor een .pdf-bestand en 10.000 voor een .xlsx-bestand.

29.0.4 De rapportstructuur exporteren en importeren

U kunt de rapportstructuur exporteren en importeren (de serie widgets en de rapportinstellingen) naar een JSON-bestand.

Als u de rapportstructuur wilt exporteren, klikt u op de naam van het rapport, klikt u op het ellipspictogram in de rechterbovenhoek en klikt u vervolgens op **Exporteren**.

Als u de rapportstructuur wilt importeren, klikt u op **Rapport toevoegen** en vervolgens op **Importeren**.

29.0.5 Een rapport downloaden

U kunt een rapport downloaden. Klik op **Downloaden** en selecteer de gewenste indelingen:

- Excel en PDF
- Excel
- PDF

29.0.6 Een dump maken van de rapportgegevens

U kunt een dump van de rapportgegevens in een CSV-bestand via e-mail verzenden. De dump bevat alle rapportgegevens (zonder dat deze gefilterd zijn) voor een aangepast tijdbereik. De tijdstempels in CSV-rapporten hebben de UTC-indeling, terwijl de tijdstempels in Excel- en PDF-rapporten de huidige tijdzone van het systeem weergeven.

De software genereert de gegevensdump binnen een mum van tijd. Als u een lange tijdsduur opgeeft, kan deze actie lang duren.

Een dump maken van de rapportgegevens

1. Klik op de naam van het rapport.
2. Klik op het ellipspictogram in de rechterbovenhoek en klik vervolgens op **Dumpgegevens**.
3. Geef de e-mailadressen van de ontvangers op.
4. Geef in **Tijdbereik** het tijdbereik op.
5. Klik op **Verzenden**.

Opmerking
In een .csv-bestand kunnen maximaal 150.000 items worden geëxporteerd.

29.1 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
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

Cyberbescherming	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
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
Software-inventaris	Actueel
Softwareoverzicht	Historisch
Machines met beveiligingsproblemen	Actueel

30 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.

31 Problemen oplossen

In dit gedeelte wordt beschreven hoe u een logboek van de agent opslaat naar een ZIP-bestand. Als een back-up om onduidelijke redenen mislukt, kan het technische ondersteuningspersoneel dit bestand gebruiken om het probleem te identificeren.

Logboekbestanden verzamelen

1. Selecteer de machines waarvan u de logbestanden wilt verzamelen.
2. Klik op **Activiteiten**.
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.

32 Bijlage A. Site-naar-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**.

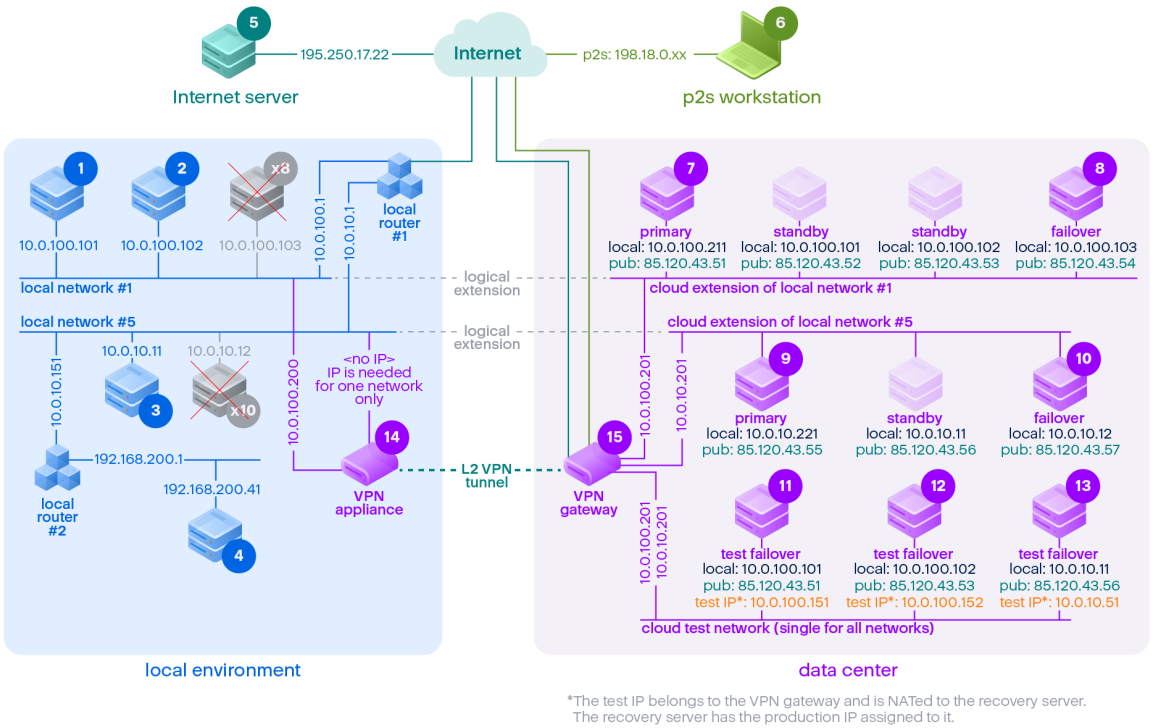
Wanneer u een testfailover uitvoert, kunt u de testserver alleen bereiken via het **Test-IP-adres**, dat alleen zichtbaar is in de configuratie van de herstelserver.

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 Disaster Recovery 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 Disaster Recovery (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 Disaster Recovery.
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	

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 uit bekende apparaten in de serviceconsole.

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

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

E

F

G

N

O

P

S