Cyber Disaster Recovery Cloud

21.10

Beheerdershandleiding

REVISIE:1-11-2021

Inhoudsopgave

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. 47).

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] 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.

2 Softwarevereisten

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.

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.

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.

3 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. 39) 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.

3.0.1 Volgende stappen

- U kunt de standaardconfiguratie van de herstelserver bewerken. Zie "Herstelservers instellen" (p. 47) voor meer informatie.
- U kunt de standaardnetwerkconfiguratie bewerken. Zie "Connectiviteit instellen" (p. 12) 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. 9) en "Cloudinfrastructuur" (p. 10) voor meer informatie.

3.1 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.

3.2 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. 32).
- 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. 23). 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**.

4 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.

4.1 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.

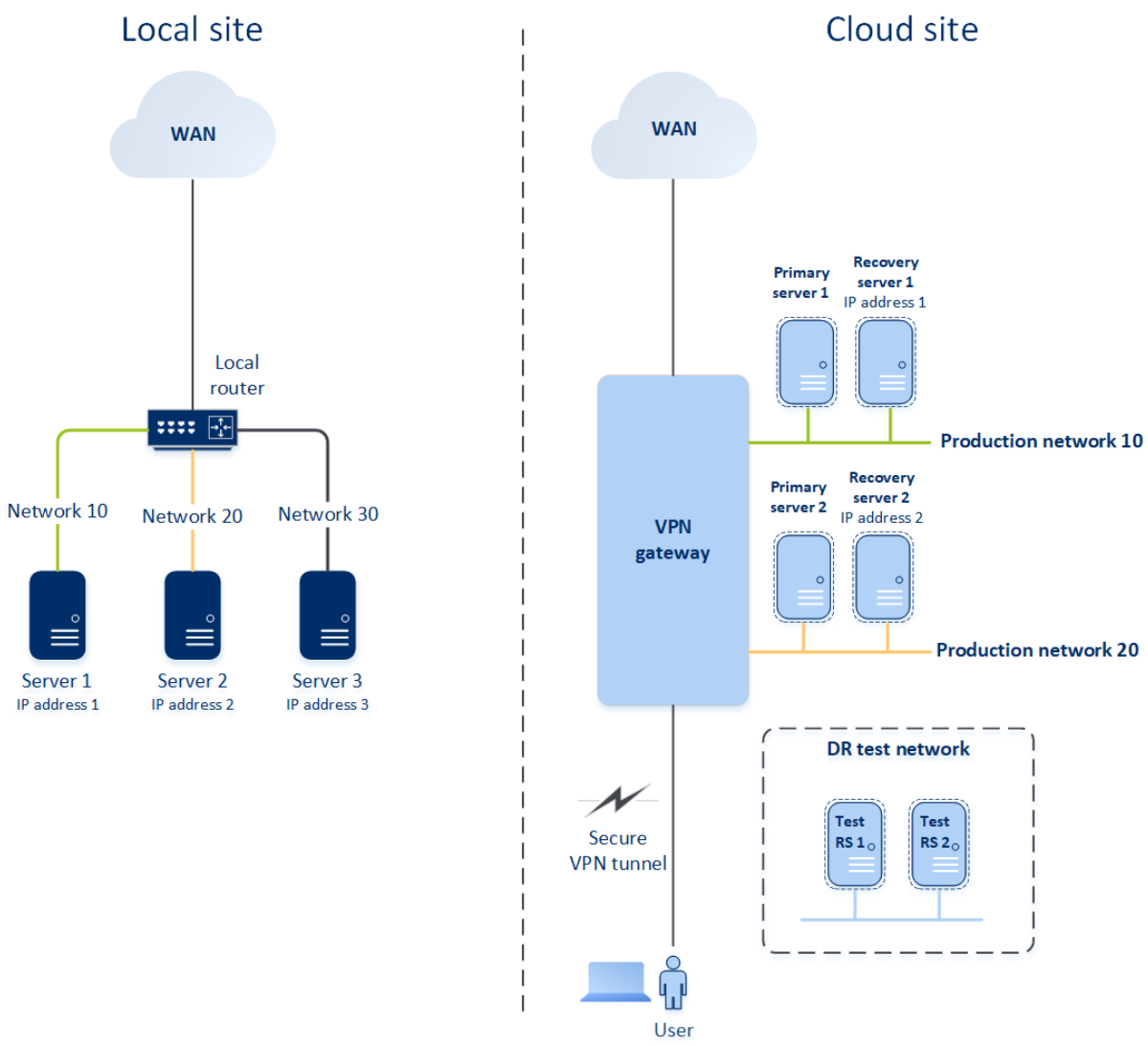
  Voor toegang tot een lokale site met dit type verbinding moet u een VPN-toepassing implementeren op de lokale site.

4.1.1 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.

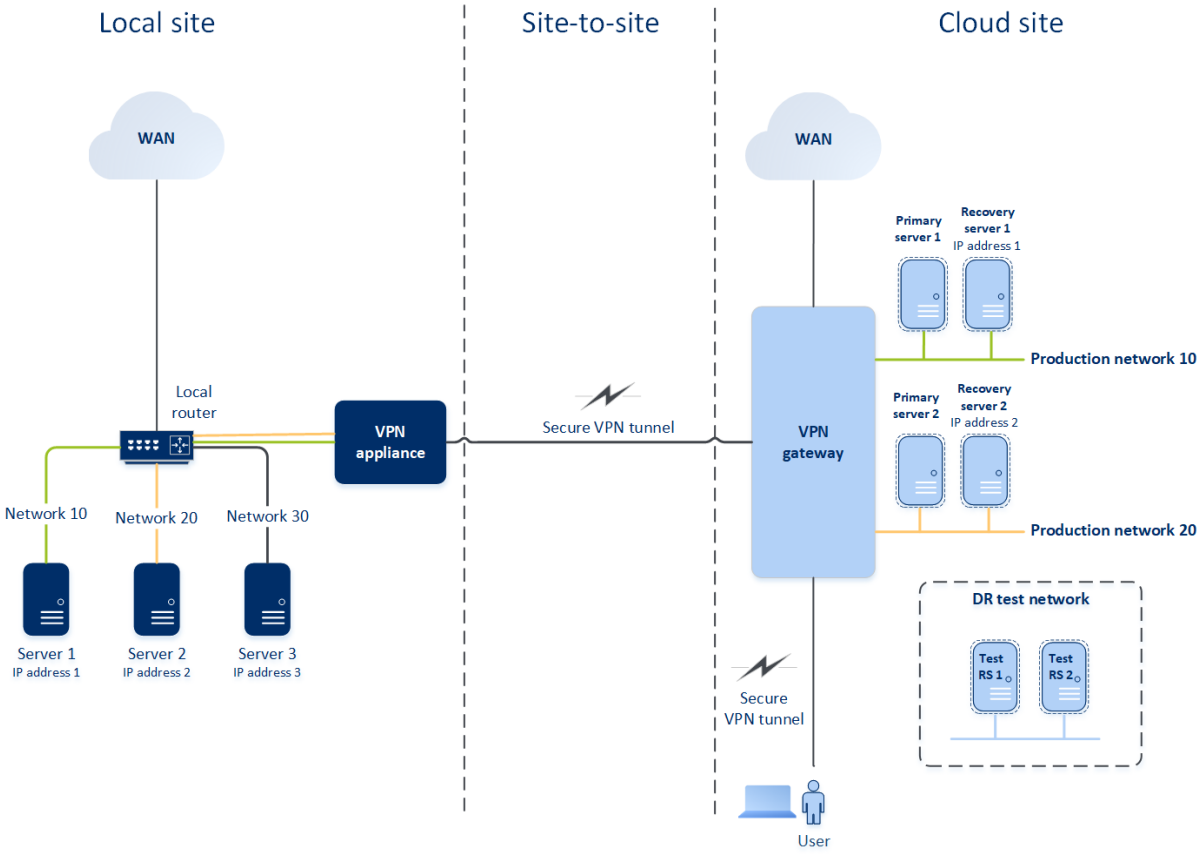


4.1.2 Site-to-site OpenVPN-verbinding

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

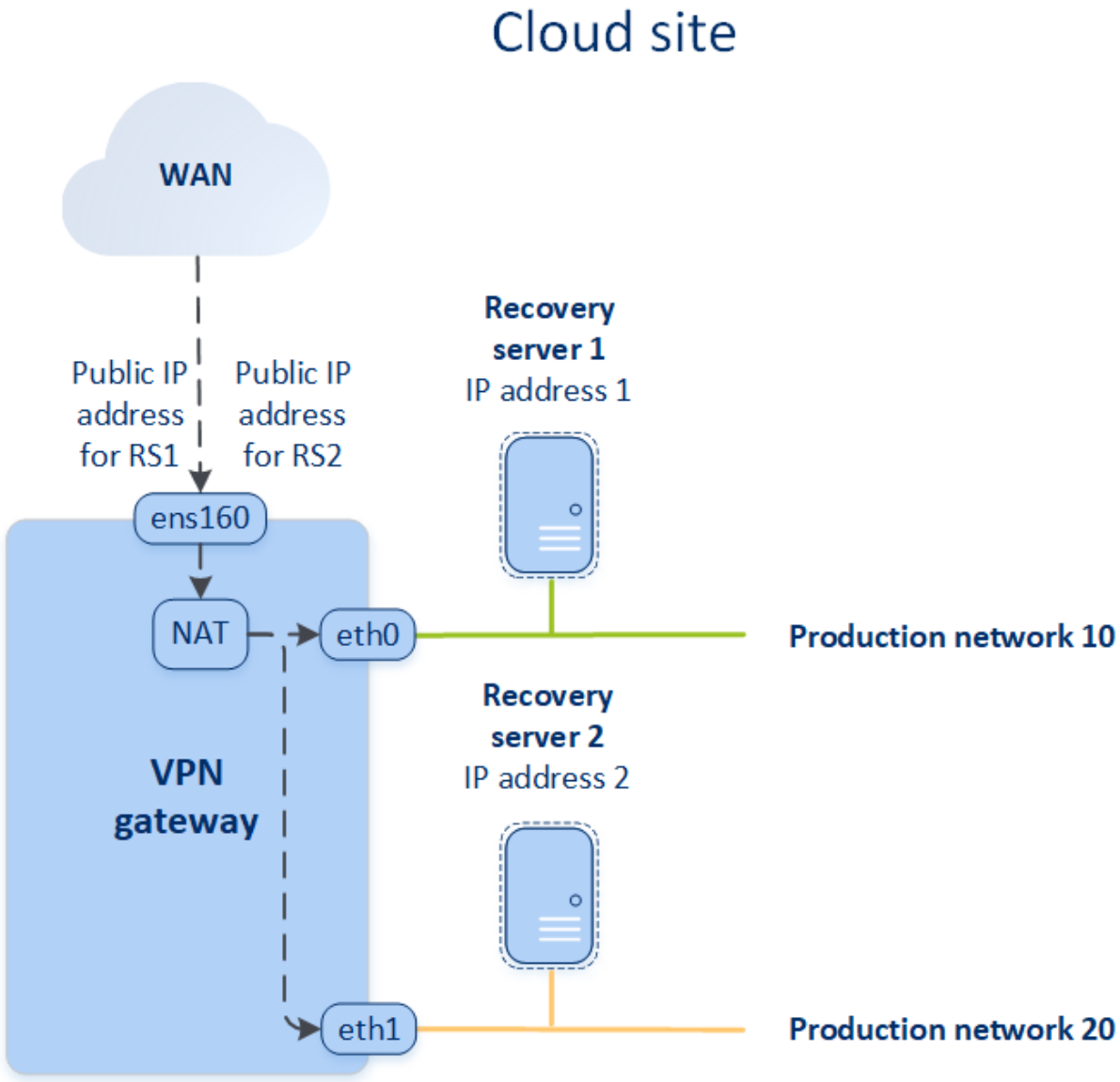
Een **herstelserver**: een replica van de oorspronkelijke machine op basis van de beveiligde serverback-ups die in de cloud zijn opgeslagen. Herstelservers worden gebruikt om workloads vanaf de oorspronkelijke servers te verplaatsen in het geval van een ramp.

Bij het maken van een herstelserver moet u de volgende netwerkparameters opgeven:

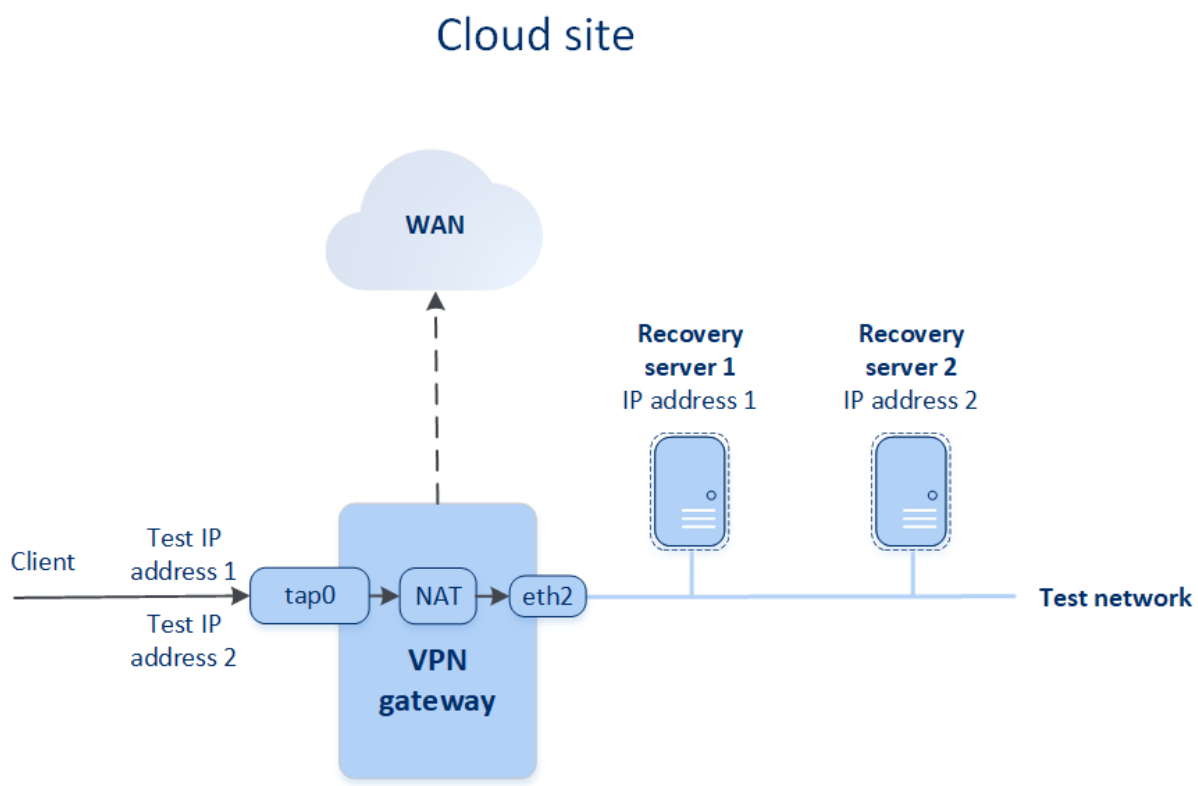
- **Cloudnetwerk** (verplicht): een cloudnetwerk gebruikt voor verbinding met een herstelserver.
- **IP-adres in productienetwerk** (verplicht): een IP-adres waarmee een virtuele machine voor een herstelserver wordt gestart. Dit adres wordt zowel in productie- als in testnetwerken gebruikt. Voor de start 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. 76) 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.

4.1.3 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. 40) 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.

4.1.4 Externe point-to-site-VPN-toegang

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

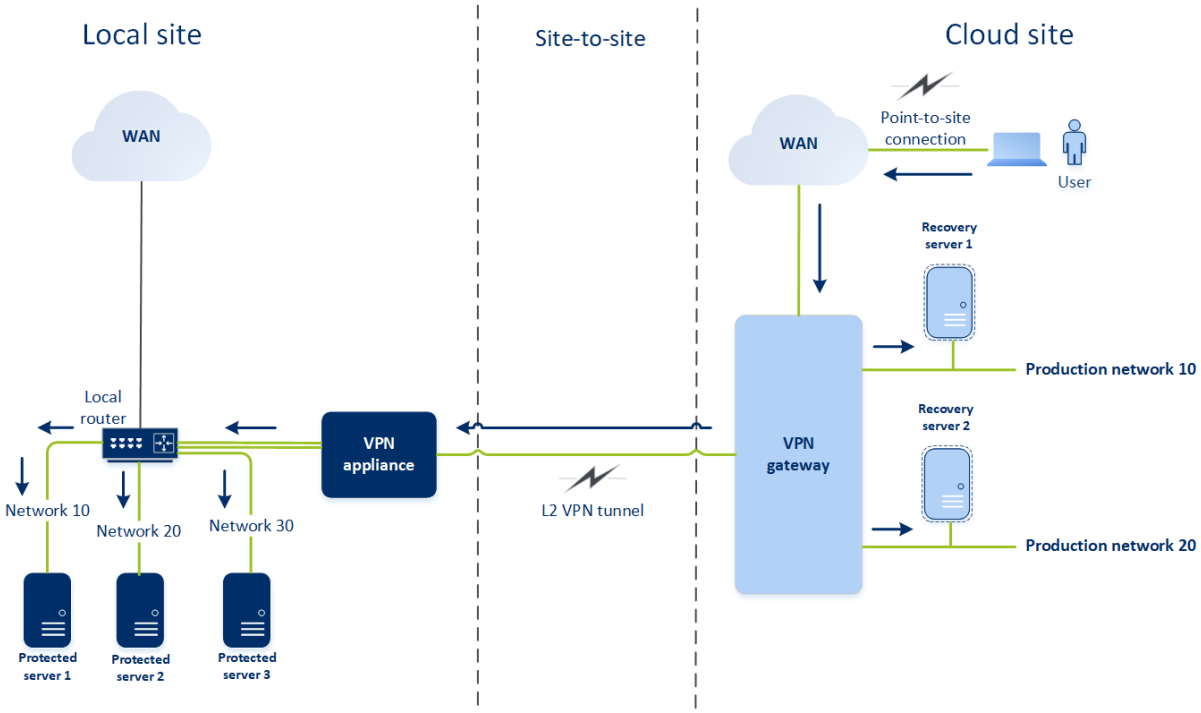
De point-to-site-verbinding is een veilige externe VPN-verbinding naar uw cloudsite en lokale site via uw eindpuntapparaten (zoals computer of laptop). Deze is beschikbaar nadat u een site-to-site OpenVPN-verbinding met de Cyber Disaster Recovery Cloud-site tot stand hebt gebracht. Dit type verbinding 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.

4.1.5 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.

4.2 Initiële connectiviteitsconfiguratie

In dit gedeelte worden de scenario's voor de connectiviteitsconfiguratie beschreven.

4.2.1 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.

4.2.2 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.

4.2.3 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**.

Vereisten

- Een geconfigureerde multi-site IPsec VPN-connectiviteit. Zie "Multi-site IPsec VPN configureren" (p. 25) 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. 27) 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. 28) 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.

4.2.4 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. 40) 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. 40) voor meer informatie.

4.2.5 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.

4.3 Netwerkbeheer

In dit gedeelte worden scenario's voor netwerkbeheer beschreven.

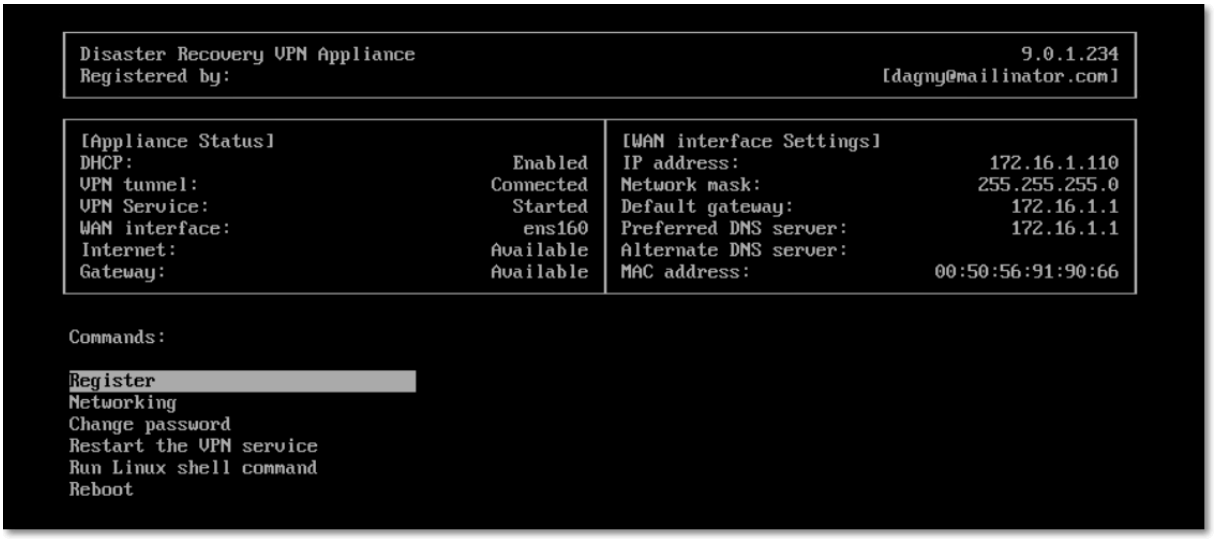
4.3.1 Netwerken beheren

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

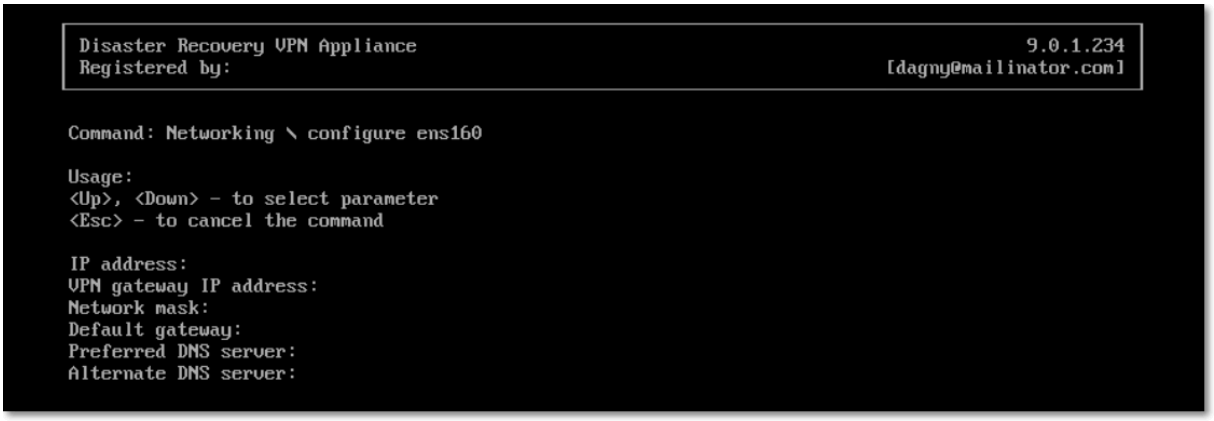
1. Meld u aan bij de VPN-toepassingsconsole.
2. Selecteer in het gedeelte **Netwerken** de interface die u wilt verwijderen en klik vervolgens op **Netwerkinstellingen wissen**.
3. Bevestig de bewerking.

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**.

4.3.2 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).

4.3.3 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.

4.3.4 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.

4.3.5 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**.

4.3.6 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**.

4.3.7 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**.

4.3.8 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

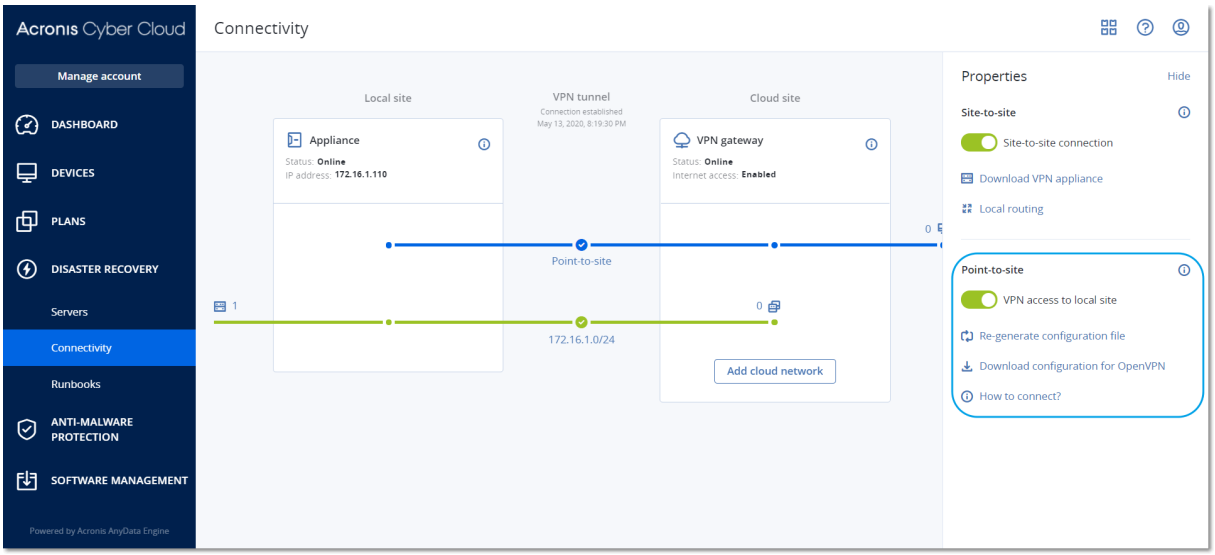
1. Ga naar **Noodherstel** > **Connectiviteit**.
2. Klik op **Eigenschappen weergeven** en klik vervolgens op **Lokale routering**.
3. Geef de lokale netwerken op in de CIDR-indeling.
4. Klik op **Opslaan**.

De servers van de opgegeven lokale netwerken kunnen dan communiceren met de cloudservers.

4.3.9 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:

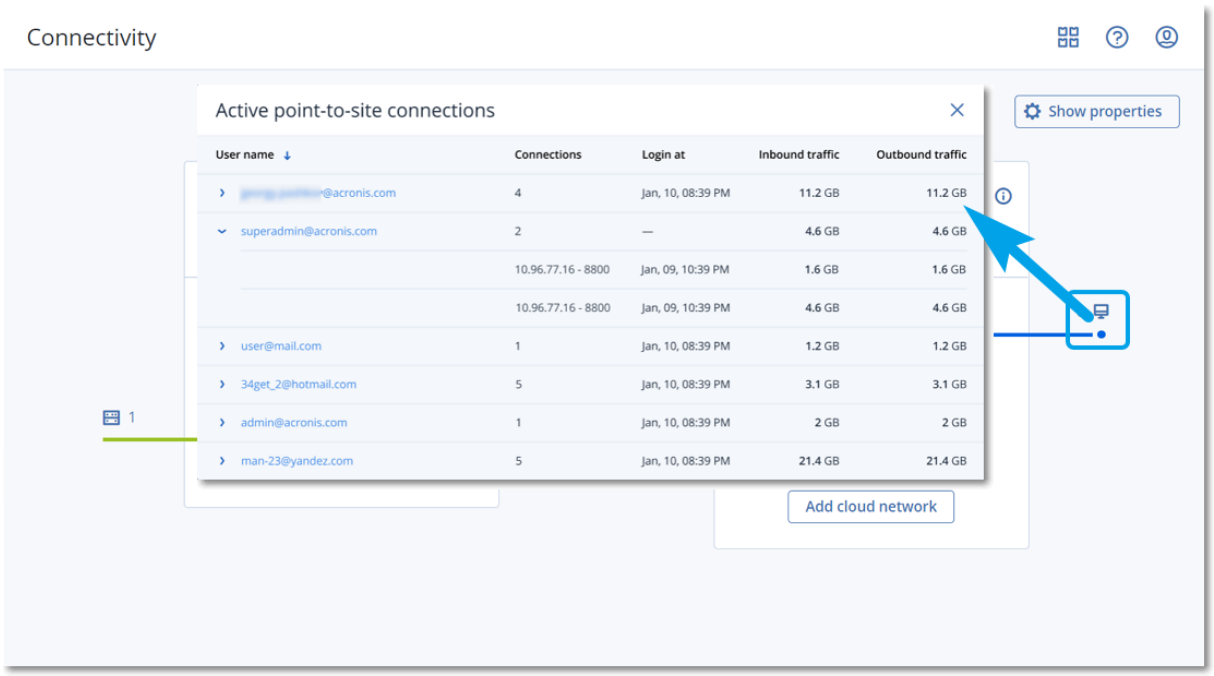
- Als u vermoedt dat het configuratiebestand is beschadigd.
- Als tweeledige verificatie is ingeschakeld voor uw account.

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.

4.3.10 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.



4.3.11 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.

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.

5 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.

5.1 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.

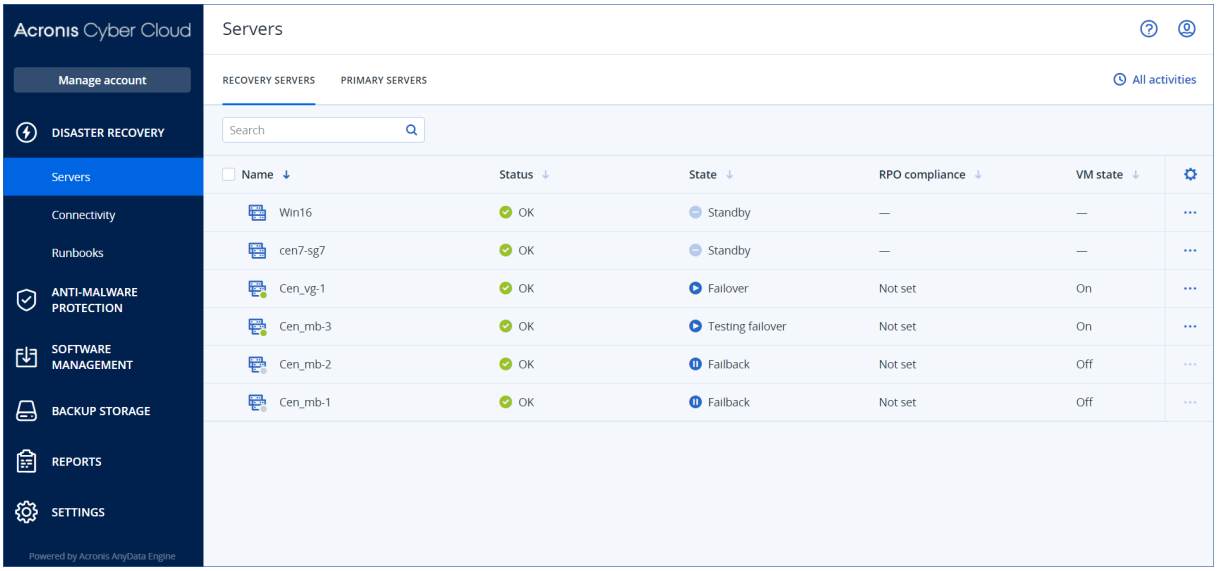
   De RPO-drempel bepaalt het maximaal toegestane tijdsinterval tussen het laatste geschikte herstelpunt voor een failover en de huidige tijd. De waarde kan worden ingesteld op 15 - 60 minuten, 1 - 24 uur, 1 - 14 dagen.
9. [Optioneel] Schakel het selectievakje **Openbaar IP-adres gebruiken** in.

   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. 66) 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.



5.2 Hoe failover werkt

5.2.1 Productiefailover

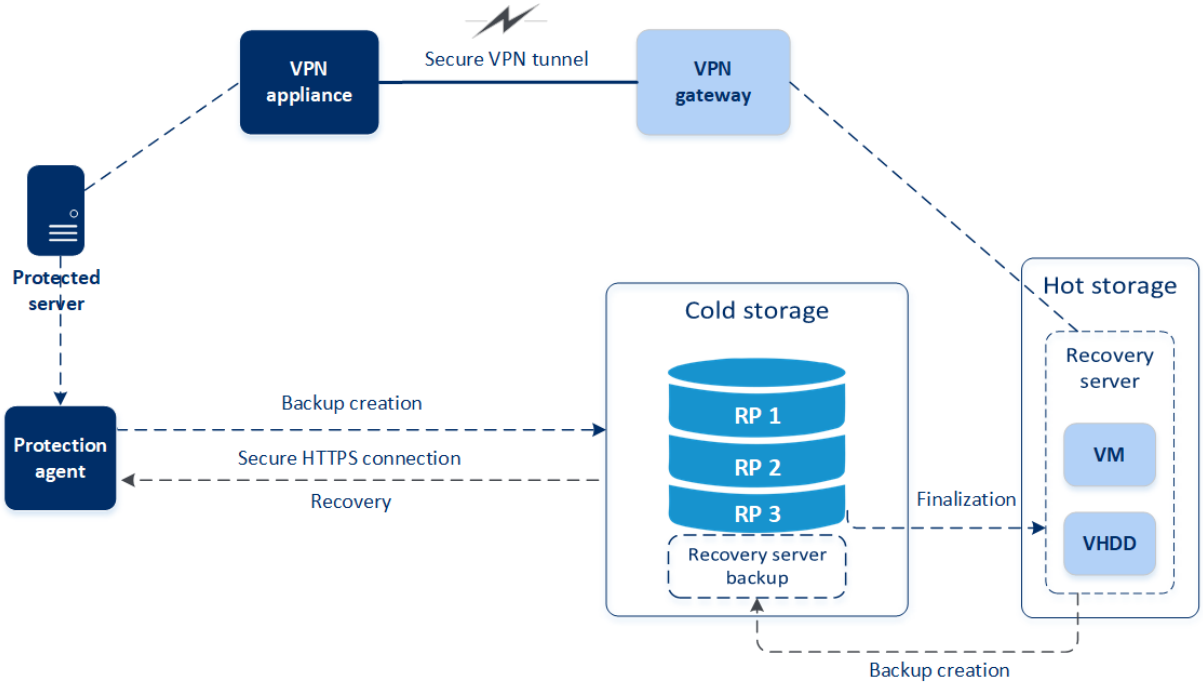
Opmerking
De beschikbaarheid van deze functie hangt af van de servicequota's die zijn ingeschakeld voor uw account.

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.



5.2.2 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. 50) voor meer informatie over het proces van een testfailover.

5.2.3 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.

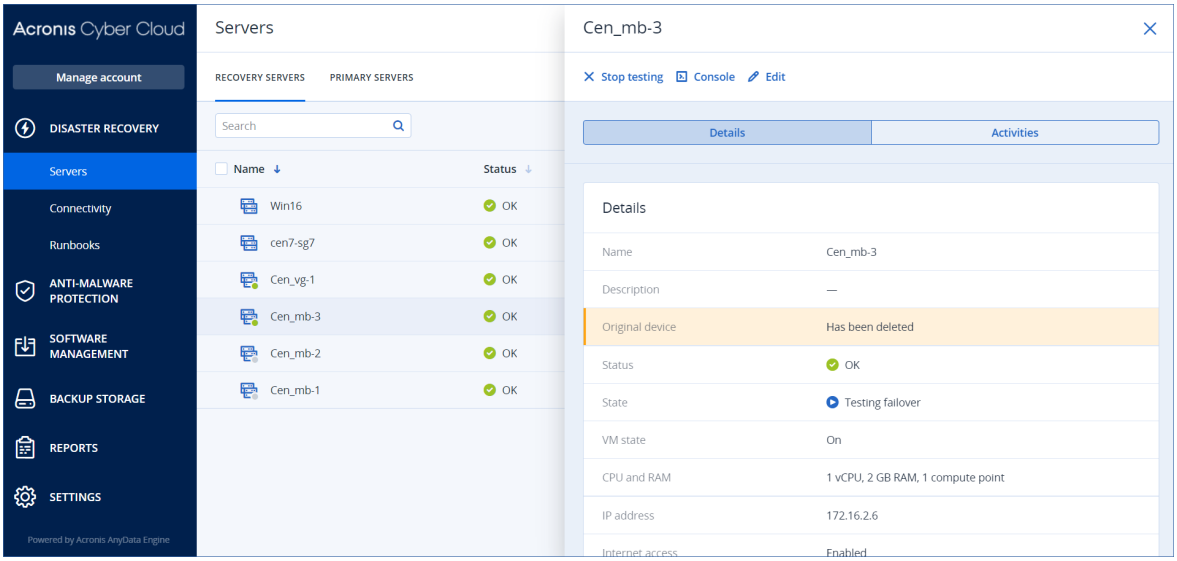
Een test-failover uitvoeren

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.

5.2.4 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.

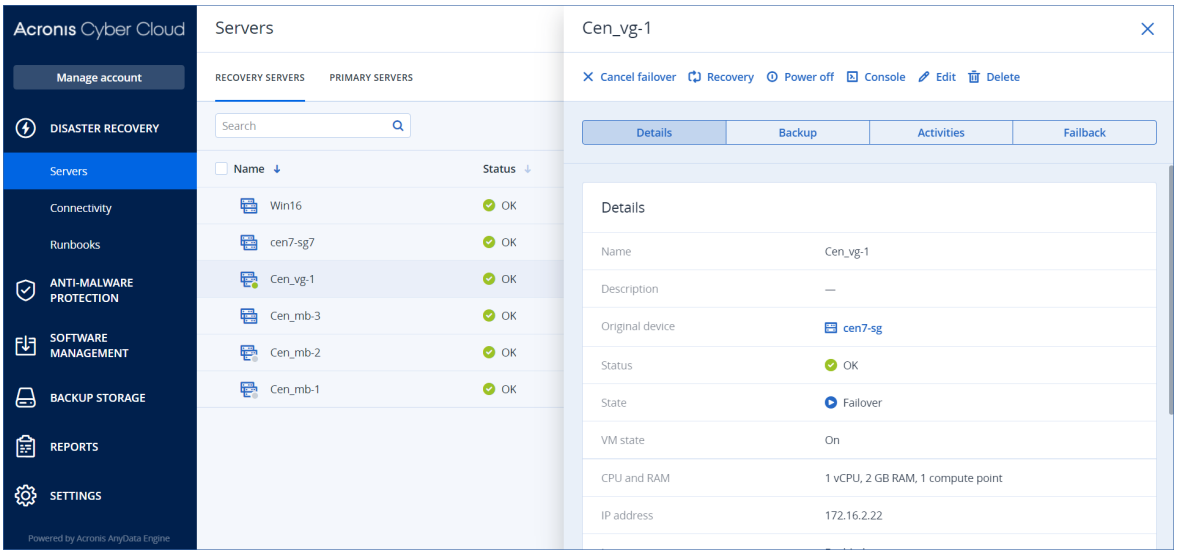
Er moet ten minste één herstelpunt worden gemaakt voordat er wordt overgeschakeld naar een herstelserver.

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. 49) 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.

5.3 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.

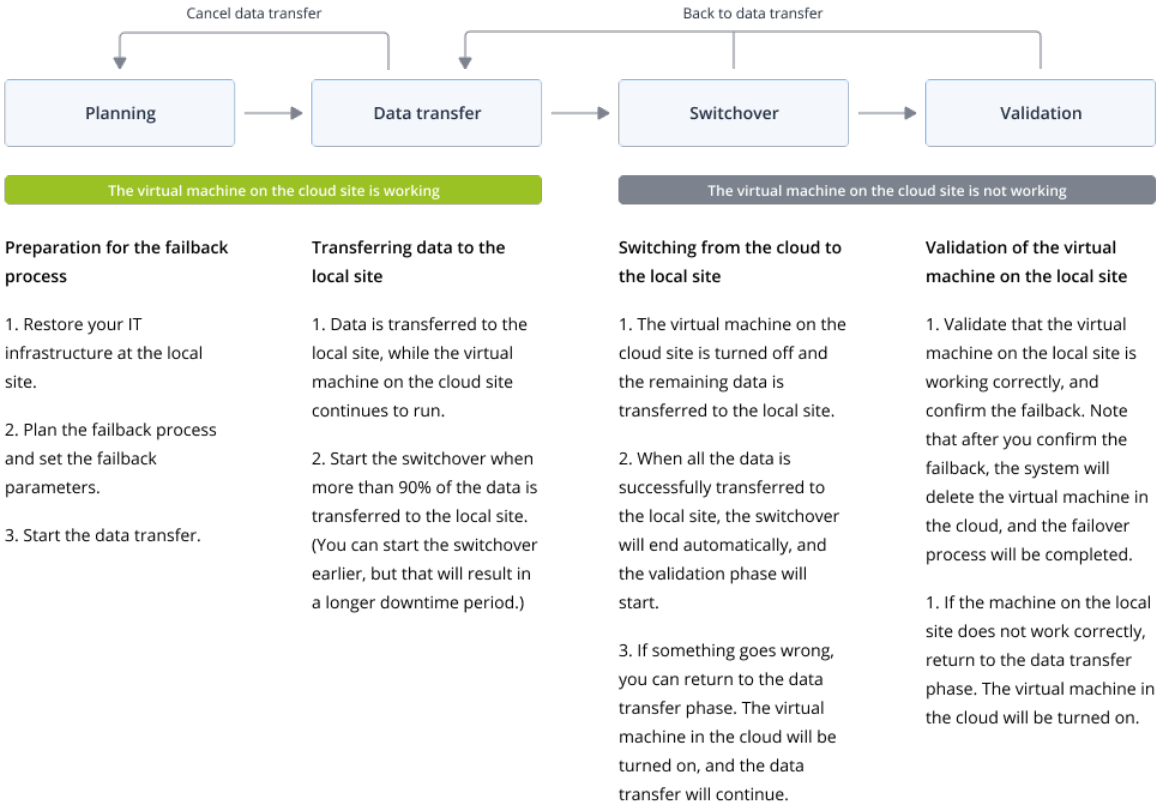
Er is een verschil tussen het failbackproces naar virtuele doelmachines en het failbackproces naar fysieke doelmachines. Zie "Failback naar een virtuele doelmachine" (p. 54) en "Failback naar een fysieke doelmachine" (p. 59) voor meer informatie over de fasen van het failbackproces.

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**.

5.3.1 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**.

5.3.2 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**.

5.3.3 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**.

5.3.4 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.

5.4 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.

6 Primaire servers instellen

In dit gedeelte wordt beschreven hoe u uw primaire servers kunt maken en beheren.

6.1 Primaire server maken

Vereisten

- Een van de typen connectiviteit met de cloudsite moet worden ingesteld.

Een primaire server maken

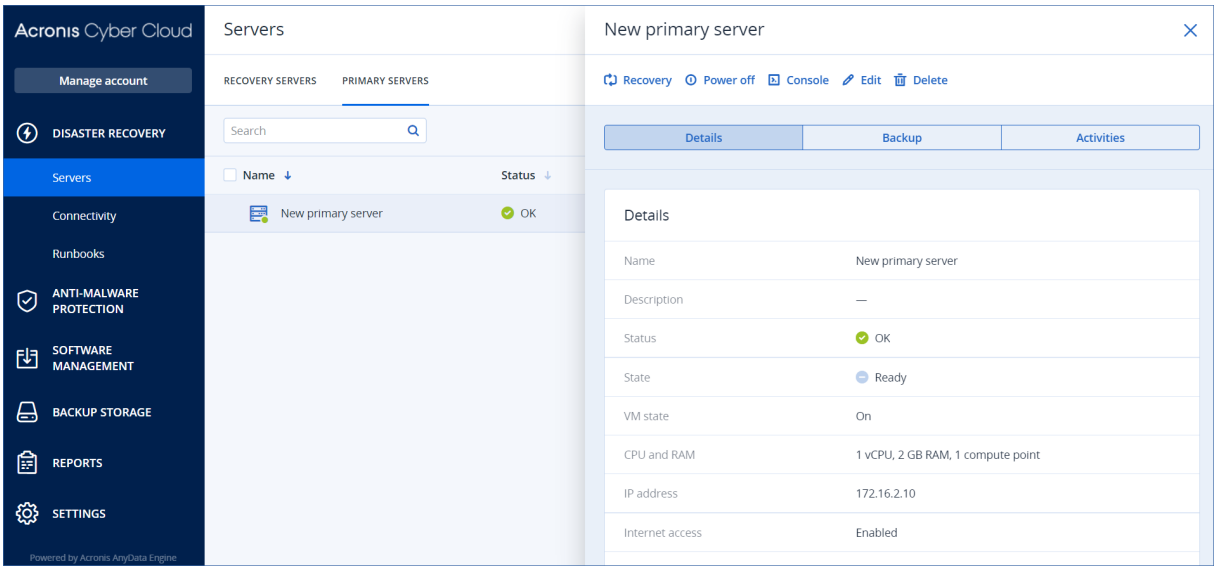
1. Ga naar **Noodherstel** > **Servers** > tabblad **Primaire servers**.
2. Klik op **Maken**.
3. Selecteer een sjabloon voor de nieuwe virtuele machine.
4. Selecteer het aantal virtuele kernen en de grootte van het RAM.
   Let op de compute-punten naast elke optie. Het aantal compute-punten geeft de 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. 66) 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.



6.2 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.

7 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

8 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

8.1 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**.

8.2 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.

9 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.

10 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**.

10.1 Waarom runbooks gebruiken?

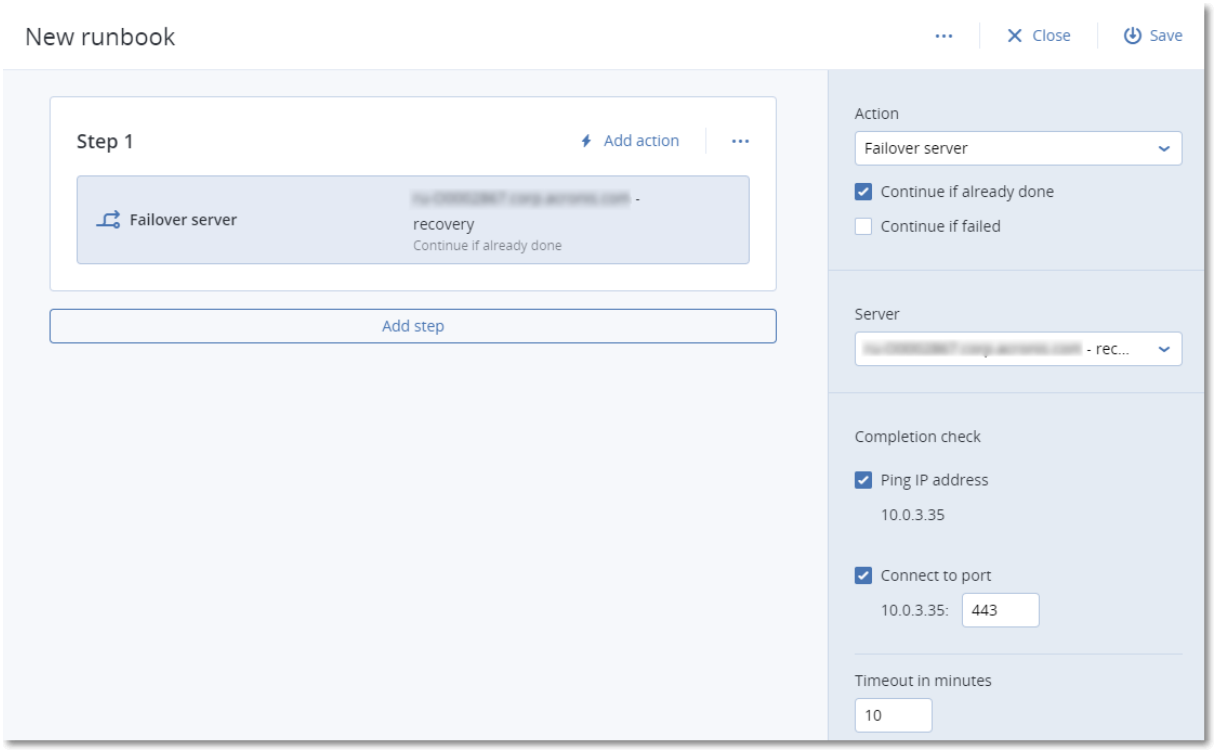
Met runbooks kunt u het volgende doen:

- 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.

10.2 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**.



10.2.1 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.

10.2.2 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.

10.2.3 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.

10.3 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**

10.3.1 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**

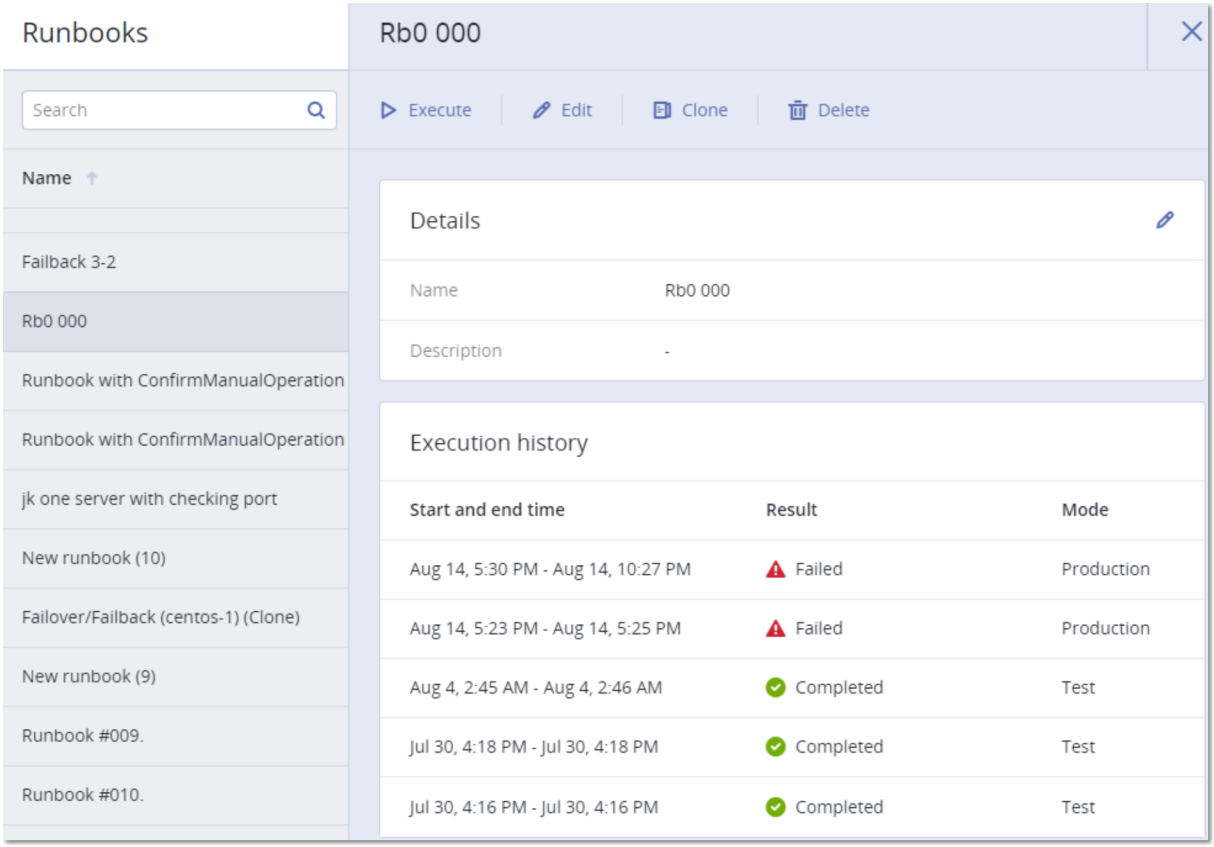
  Kies het meest recente herstelpunt (standaard) of selecteer een tijdstip in het verleden. In dit laatste geval worden de herstelpunten die zich het dichtst bij de opgegeven datum en tijd bevinden, voor elke server geselecteerd.

10.3.2 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.

10.3.3 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

11 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.

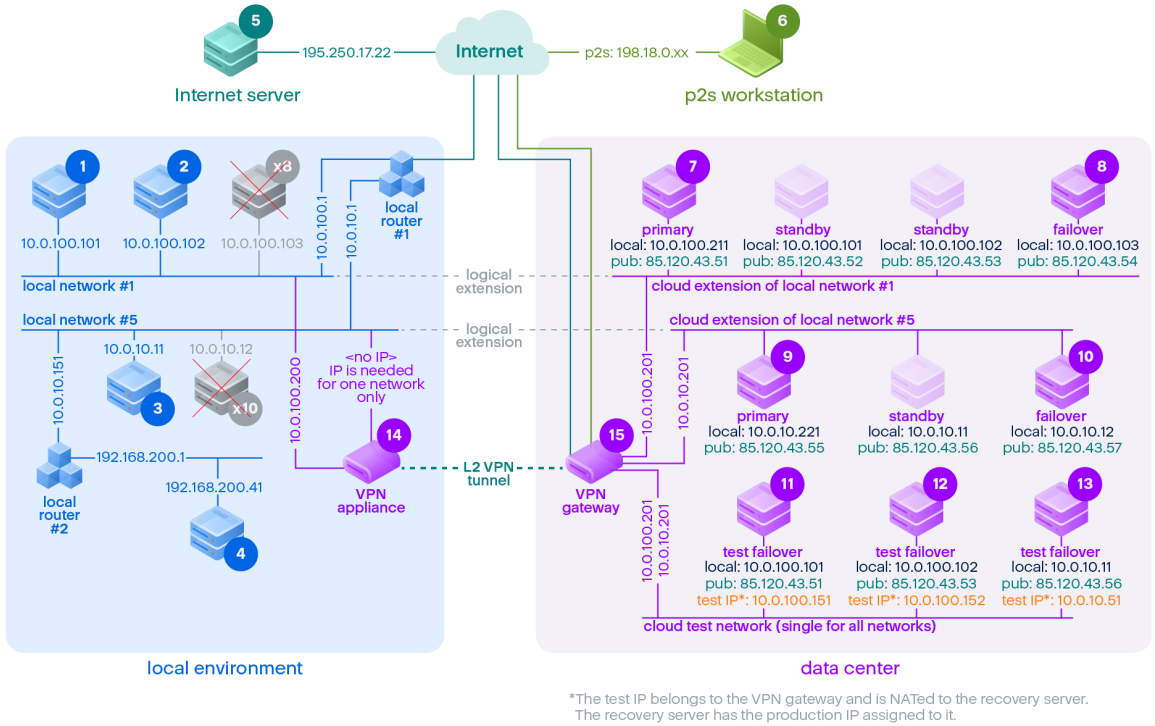
Als u een testserver wilt bereiken vanaf uw lokale site, moet u het **Test-IP-adres** gebruiken.

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)



*The test IP belongs to the VPN gateway and is NATed to the recovery server.
The recovery server has the production IP assigned to it.

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	intern	p2s	primair	failover	primair	failover	testfailov	testfailov	testfailov	VPN-	VPN-

	Tot:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						et						er	er	er	toepassing	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 router 1 en internet: pub	direct	nee
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

	Tot:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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 en internet: pub	via lokale router	nee
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 interne	via lokale router 2 en tunnel: lokaal via lokale router 2 en lokale router 1 en interne	via lokale router 2 en tunnel: lokaal via lokale router 2 en lokale router 1 en interne	via lokale router 2 en tunnel: lokaal via lokale router 2 en lokale router 1 en interne	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

	Tot:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								t: pub	t: pub	t: pub	t: pub					
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-server): lokaal via internet: pub	via p2s VPN (VPN-server): lokaal via internet: pub	via p2s VPN (VPN-server): lokaal via internet: pub	via p2s VPN (VPN-server): lokaal via internet: pub	via p2s VPN - NAT (VPN-server) via internet: pub	via p2s VPN - NAT (VPN-server) via internet: pub	via p2s VPN - NAT (VPN-server) via internet: pub	nee	nee
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	alleen DHCP- en DNS-protocol
8	failover	via tunnel	via tunnel	via tunnel en lokale router 1	via tunnel en lokale router 1 en	via internet (via VPN-server)	nee	direct in de cloud: lokaal		via tunnel en lokale router 1:	via tunnel en lokale router 1:	via VPN-server: NAT	via VPN-server: NAT	via tunnel en lokale router 1: NAT	nee	alleen DHCP- en DNS-protocol

	Tot:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
					2					lokaal	lokaal					
9	primair	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	alleen DHCP- en DNS-protocol
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	alleen 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	alleen DHCP- en DNS-protocol
12	testfailover	nee	nee	nee	nee	via internet (via VPN-	nee	nee	nee	nee	nee	direct in de cloud: lokaal		via VPN-server: lokaal (routerin	nee	alleen DHCP- en DNS-

	Tot:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						server)								g)		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	alleen DHCP- en DNS-protocol
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

B

Beveiligde server

Een fysieke of virtuele machine die eigendom is van een klant en die wordt beveiligd met de service.

C

Cloudserver

Algemene verwijzing naar een herstelserver of primaire server.

Cloudsite (of DR-site)

Externe site gehost in de cloud en gebruikt voor het uitvoeren van herstelinfrastructuur, in het geval van een ramp.

F

Failback

Het proces waarbij de servers worden hersteld naar de lokale site nadat ze tijdens de failover naar de cloudsite zijn verplaatst.

Failover

Het verplaatsen van de workload of toepassing naar de cloudsite in geval zich een door de natuur of door mensen veroorzaakte ramp voordoet op de lokale site.

H

Herstelserver

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

IP-adres testen

Een IP-adres dat nodig is in geval van een testfailover, om duplicatie van het productie-IP-adres te voorkomen.

L

Lokale site

De lokale infrastructuur die is geïmplementeerd op de locatie van uw bedrijf.

O

Openbaar IP-adres

Een IP-adres dat nodig is om cloudservers beschikbaar te maken vanaf internet.

P

Point-to-site-verbinding (P2S)

Een veilige externe VPN-verbinding naar de cloudsite en lokale site via uw eindpuntapparaten (zoals een computer of laptop).

Primaire server

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

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)

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

Gepland scenario bestaande uit configureerbare stappen waarmee de acties voor noodherstel worden geautomatiseerd.

S

Site-to-site-verbinding (S2S)

Verbinding waarmee uw lokale netwerk wordt uitgebreid naar de cloud via een veilige VPN-tunnel.

T

Testnetwerk

Geïsoleerd virtueel netwerk dat wordt gebruikt om het failoverproces te testen.

V

Voltooien

De tussenliggende status voor de productiefailover of het herstelproces van de cloudserver. 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.

VPN-gateway (voorheen VPN-server of connectiviteitsgateway)

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

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.

Index

S

U

V

W