Cyber Disaster Recovery Cloud

21.06

Snelgids

REVISIE:1-11-2021

Inhoudsopgave

1 Cyber Disaster Recovery Cloud instellen op uw pc met Hyper-V

U hoeft geen eigen server te hebben om de hoofdfunctionaliteit van Cyber Disaster Recovery Cloud te testen. U kunt de Cyber Disaster Recovery Cloud-service gemakkelijk instellen op uw pc en de functies ervan evalueren.

Vereisten:

- U hebt een klantbeheerdersaccount in Cyber Cloud.
- Het geïnstalleerde besturingssysteem op uw pc moet Windows 10 (PRO, Enterprise of Education Edition) zijn.

Ga als volgt te werk om de Cyber Disaster Recovery Cloud-service te implementeren op uw pc:

1. Activeer de Hyper-V op uw pc.
2. Maak een virtuele machine (VM) om te gebruiken als bronmachine voor het testen.
3. Implementeer de VPN-toepassing op uw pc.

1.0.1 Stap 1. Activeer de Hyper-V service op uw pc en bereid de OS-image voor.

1. Activeer de Hyper-V-service op uw pc. Volg de instructies op de Microsoft-website.
2. Download de OS-image voor installatie op de VM. Download bijvoorbeeld ubuntu-18.04.2-desktop-amd64.iso van de officiële Ubuntu-website.

1.0.2 Stap 2. Maak een virtuele machine die uw bronmachine wordt waarvan een back-up wordt gemaakt.

1. Open de Hyper-V Manager en maak een virtuele machine waarvan u een back-up gaat maken en die u gaat gebruiken voor het testen van de Cyber Disaster Recovery Cloud-service:
   a. Klik met de rechtermuisknop op uw host en selecteer **Nieuw** > **Virtuele machine**. Volg de stappen van de wizard. Let op: het **opstartgeheugen** moet minstens 4096 MB zijn en **Verbinding** moet zijn ingesteld **Standaardswitch**.
   b. Voer de nieuw gemaakte VM uit, maak er verbinding mee en start vervolgens de OS-installatie.
2. Installeer de beveiligingsagent op de nieuw gemaakte virtuele machine:
   a. Open een browser op uw virtuele machine.
   b. Meld u als klantbeheerder aan bij de serviceconsole.
   c. Voeg in de sectie **Apparaten** de virtuele machine toe door te klikken op **Toevoegen** en selecteer vervolgens de beveiligingsagent voor een Linux-server. Het resultaat is dat de

beveiligingsagent wordt gedownload naar uw virtuele machine.

d. Open de console en installeer de aanvullende pakketten. Gebruik de volgende opdracht:

```
sudo apt-get install rpm gcc make -y
```

a. Open de map **Downloads**, wijzig de machtigingen zodat het installatiebestand voor de beveiligingsagent een uitvoerbaar bestand wordt en voer dit bestand vervolgens uit.

```
cd Downloads
```

```
sudo chmod +x Cyber_Protection_Agent_for_Linux_x86_64.bin
```

```
sudo ./Cyber_Protection_Agent_for_Linux_x86_64.bin
```

a. Volg de stappen van de installatiewizard. Selecteer als laatste stap de optie **Registratiegegevens weergeven**. Wanneer u de machine registreert in de serviceconsole, ziet u de link die in de browser moet worden geopend en de registratiecode die moet worden opgegeven.

b. Uw virtuele machine is dan geregistreerd in de serviceconsole. Maak het beschermingsschema en de back-up van de hele machine. Deze back-up wordt later gebruikt om een herstelserver te maken.

1.0.3 Stap 3. Implementeer de VPN-toepassing op uw pc.

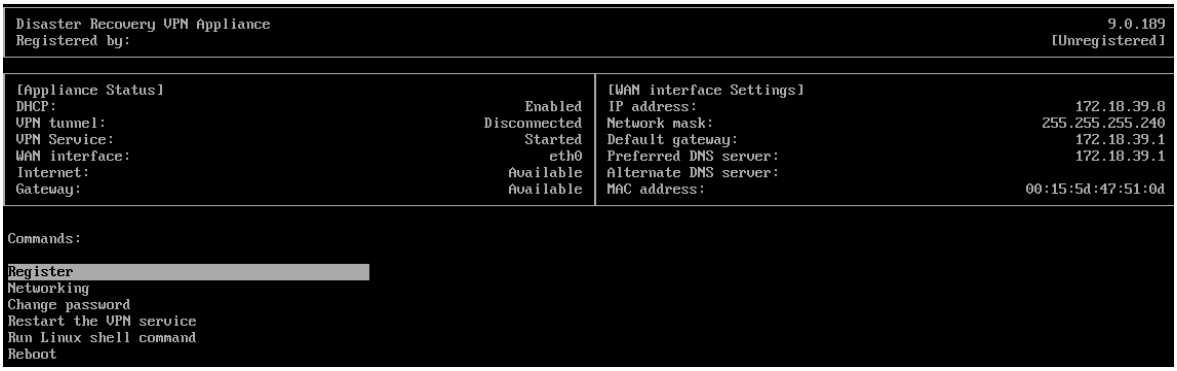
Ga als volgt te werk om de VPN-toepassing te implementeren op uw pc:

1. Meld u op uw pc als klantbeheerder aan bij de serviceconsole.
2. Ga naar **Noodherstel** > **Connectiviteit** en klik vervolgens op **Configureren**. De connectiviteitsconfiguratiewizard wordt geopend.
3. Selecteer **Site-to-site-verbinding** en klik op **Starten**.
   Het systeem begint met de implementatie van de VPN-server in de cloud. Dit kan enige tijd duren. Ondertussen kunt u doorgaan naar de volgende stap.
4. Klik op **Downloaden en implementeren**. Download het archief met de VPN-toepassing voor Hyper-V (.vhd-bestand), pak het archief uit en implementeer het vervolgens in uw lokale omgeving:
   a. Open Hyper-V Manager, klik met de rechtermuisknop op uw host en selecteer **Nieuw** > **Virtuele machine**.
   b. Geef de beschrijvende naam op voor een VM (bijvoorbeeld VM VPN-toepassing).
   c. Volg de stappen van de wizard. Let op: **Verbinding** moet zijn ingesteld op **Standaardswitch**.
   d. Bij de stap **Virtuele harde schijf verbinden** selecteert u de optie **Bestaande virtuele harde schijf gebruiken**. Selecteer het gedownloade VPN-toepassingsbestand.
   e. Voltooi het maken van de VM.

5. Verbind de toepassing met de productienetwerken.
6. Voer de VM van de VPN-toepassing uit en maak er verbinding mee.
7. Wanneer de toepassing is opgestart en de aanmeldingsprompt wordt weergegeven, meldt u zich bij de toepassing aan met de volgende gegevens:

   Gebruikersnaam: admin

   Wachtwoord: admin
8. U ziet een startpagina zoals de volgende:



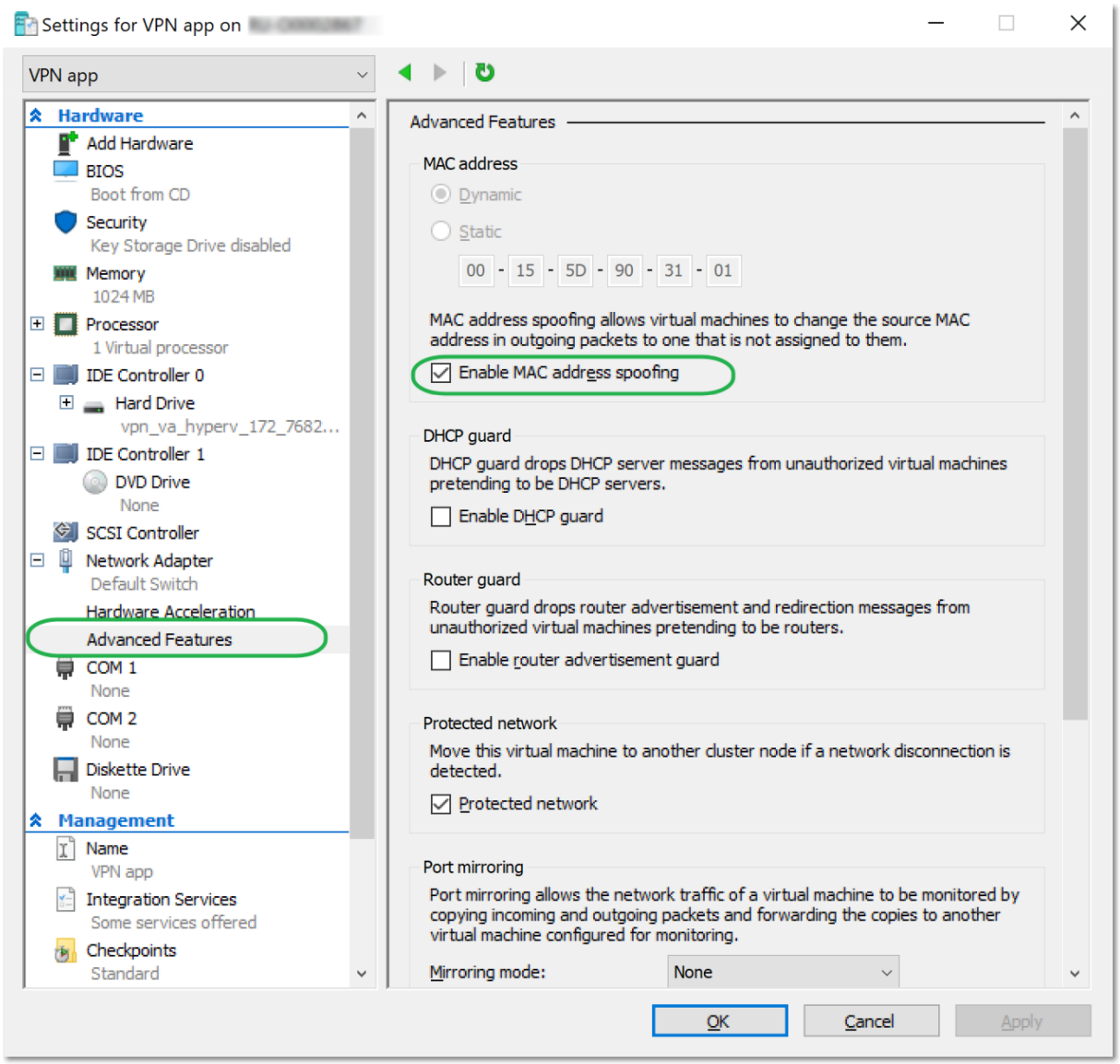
   Controleer of de instellingen voor **IP-adres**, **Standaardgateway** en **Voorkeurs-DNS-server** juist zijn geconfigureerd. Let op: De instellingen voor **Internet** en **Gateway** aan de linkerkant van de tabel moeten zijn gedefinieerd als **Beschikbaar** als u de toepassing wilt kunnen registreren. Controleer anders de instellingen voor uw standaardgateway en DNS-beschikbaarheid voordat u verdergaat met de registratie of stel het IP-adres handmatig in.
9. Selecteer **Registreren** in het menu en klik op **Enter**.
10. U wordt gevraagd om het URL-adres van de Cyberbescherming-service in te voeren. Voer de URL in die u ook gebruikt om toegang te krijgen tot de serviceconsole.

11. Geef uw referenties als klantbeheerder voor de serviceconsole op.

> **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 klanten** voor meer informatie over tweeledige verificatie.

12. Druk op **Y** om de instellingen te bevestigen en start het registratieproces.

13. Na de registratie ziet u uw VPN-toepassing in de serviceconsole.
14. Schakel de Promiscuous mode in om er zeker van te zijn dat de netwerkreplicatiefunctionaliteit correct is ingeschakeld:
    a. Open de Hyper-V Manager.
    b. Klik met de rechtermuisknop op de VM van uw VPN-toepassing en selecteer **Instellingen**.
    c. Selecteer in het gedeelte **Netwerkadapter** > **Geavanceerde functies** de optie **MAC-adresvervalsing (spoofing) inschakelen**.



U hebt nu een veilige site-to-site VPN-verbinding geconfigureerd tussen uw lokale site en de herstelsite in de cloud. U kunt nu een herstelserver voor uw lokale machine maken en controleren hoe failover en failback werken. Zie de **Beheerdershandleiding voor Cyber Disaster Recovery Cloud** voor meer informatie.

Index