Cyber Disaster Recovery Cloud

24.03

Schnellstartanleitung

REVISION: 11.04.2024

Inhaltsverzeichnis

So können Sie Cyber Disaster Recovery Cloud auf Ihrem PC mit Hyper-V einrichten

Sie müssen keinen Server besitzen, um die Hauptfunktionalität von Cyber Disaster Recovery Cloud testen zu können. Sie können den Cyber Disaster Recovery Cloud Service leicht auf Ihrem PC einrichten und so dessen Funktionen testen.

Voraussetzungen:

- Sie haben ein Kundenadministratorkonto in Cyber Protect Cloud.
- Bei dem Betriebssystem auf Ihrem PC muss es sich um Windows 10 Pro, Windows 10 Enterprise oder Windows 10 Education handeln.

Gehen Sie folgendermaßen vor, um den Cyber Disaster Recovery Cloud Service auf Ihrem PC bereitzustellen:

1. Aktivieren Sie den Hyper-V Service auf Ihrem PC.
2. Erstellen Sie eine virtuelle Maschine (VM), die als Quellmaschine für den Test verwendet wird.
3. Stellen Sie die VPN-Appliance auf Ihrem PC bereit.

Schritt 1. Aktivieren Sie den Hyper-V Service auf Ihrem PC und bereiten Sie das Betriebssystem-Image (OS-Image) vor.

1. Aktivieren Sie den Hyper-V Service auf Ihrem PC. Befolgen Sie die Anweisungen auf der Microsoft-Website.
2. Laden Sie das OS-Image zur Installation in die VM herunter. Laden Sie beispielsweise das Image 'ubuntu-18.04.2-desktop-amd64.iso' von der offiziellen Ubuntu-Website herunter.

Schritt 2. Erstellen Sie eine virtuelle Maschine, die als Backup-Quelle dienen sein soll.

1. Öffnen Sie den Hyper-V Manager und erstellen Sie eine virtuelle Maschine, die Sie per Backup sichern und zum Testen des Cyber Disaster Recovery Cloud Service verwenden wollen:
   a. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Neu** –> **Virtuelle Maschine**. Befolgen Sie die Anweisungen des Assistenten und berücksichtigen Sie dabei, dass der **Arbeitsspeicher beim Start** mindestens 4096 MB und die **Verbindung** der **Standardswitch** sein muss.
   b. Führen Sie die neu erstellte VM aus, erstellen Sie eine Verbindung mit dieser und starten Sie dann die Betriebssysteminstallation.
2. Installieren Sie den Protection Agenten in der neu erstellten virtuellen Maschine:
   a. Öffnen Sie auf Ihrer virtuellen Maschine einen Browser.
   b. Melden Sie sich als Kunden-Administrator an der Cyber Protect-Konsole an.

c. Fügen Sie im Bereich **Geräte** die virtuelle Maschine hinzu, indem Sie auf **Hinzufügen** klicken. Wählen Sie anschließend den Protection Agenten für einen Linux-Server aus. Dadurch wird der Protection Agent auf Ihre virtuelle Maschine heruntergeladen.

d. Öffnen Sie die Konsole und installieren Sie zuerst die zusätzlichen Pakete. Verwenden Sie folgenden Befehl:

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

a. Öffnen Sie den Ordner **Downloads**, ändern Sie die Berechtigungen für die Installationsdatei des Protection Agenten, sodass diese ausführbar ist, und starten Sie die Datei dann.

```
cd Downloads
```

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

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

a. Befolgen Sie die Anweisungen des Assistenten. Wählen Sie im letzten Schritt den Befehl **Registrierungsinfo anzeigen** aus. Sie sehen den Link, der im Browser geöffnet werden soll, sowie den Registrierungscode, der zur Registrierung der Maschine in der Cyber Protect-Konsole spezifiziert werden muss.

b. Dadurch wird Ihre virtuelle Maschine in der Cyber Protect-Konsole registriert. Erstellen Sie den Schutzplan und das Backup der kompletten Maschine. Das Backup wird verwendet, um später einen Recovery-Server zu erstellen.

Schritt 3. Stellen Sie die VPN-Appliance auf Ihrem PC bereit.

Gehen Sie folgendermaßen vor, um die VPN-Appliance auf Ihrem PC bereitzustellen:

1. Melden Sie sich auf Ihrem PC als Kunden-Administrator an der Cyber Protect-Konsole an.
2. Gehen Sie zu **Disaster Recovery** –> **Verbindung** und klicken Sie dann auf **Konfigurieren**. Der Assistent für die Verbindungskonfiguration wird geöffnet.
3. Wählen Sie **Site-to-Site-Verbindung** aus und klicken Sie dann auf **Start**.
   Das System beginnt damit, das Verbindungsgateway in der Cloud bereitzustellen. Dies kann einige Zeit benötigen. Währenddessen können Sie zum nächsten Schritt weitergehen.
4. Klicken Sie auf **Herunterladen und bereitstellen**. Laden Sie das Archiv mit der VPN-Appliance für Hyper-V (.vhd-Datei) herunter, entpacken Sie das Archiv und stellen Sie es dann in Ihrer lokalen Umgebung bereit:
   a. Öffnen Sie den Hyper-V Manager, klicken Sie mit der rechten Maustaste auf Ihren Host und wählen Sie dann **Neu** –> **Virtuelle Maschine**.
   b. Spezifizieren Sie den beschreibenden Namen für eine VM (z.B. VPN-Appliance-VM).
   c. Befolgen Sie die Anweisungen des Assistenten und berücksichtigen Sie dabei, dass die **Verbindung** als **Standardswitch** festgelegt sein muss.

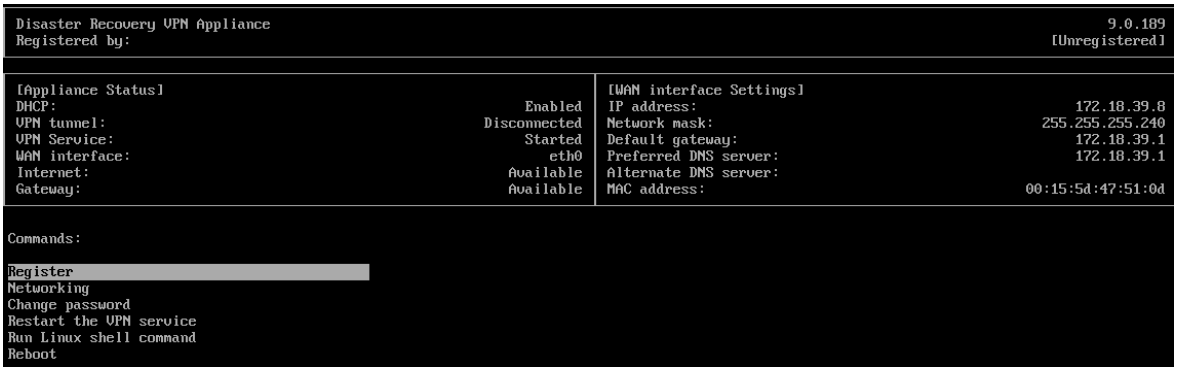
d. Wählen Sie im Schritt **Virtuelle Festplatte verbinden** die Option **Eine vorhandene virtuelle Festplatte verwenden** aus. Wählen Sie die heruntergeladene VPN-Appliance-Datei aus.

e. Schließen Sie die VM-Erstellung ab.

5. Verbinden Sie die Appliance mit den Produktionsnetzwerken.
6. Starten Sie die VPN-Appliance-VM und verbinden Sie sich mit dieser.
7. Melden Sie sich, sobald die Appliance hochgefahren ist und die Anmeldeaufforderung erscheint, mit folgenden Anmeldedaten an der Appliance an:

   Anmeldename: admin

   Kennwort: admin
8. Sie sehen eine Startseite, die ungefähr so aussieht:

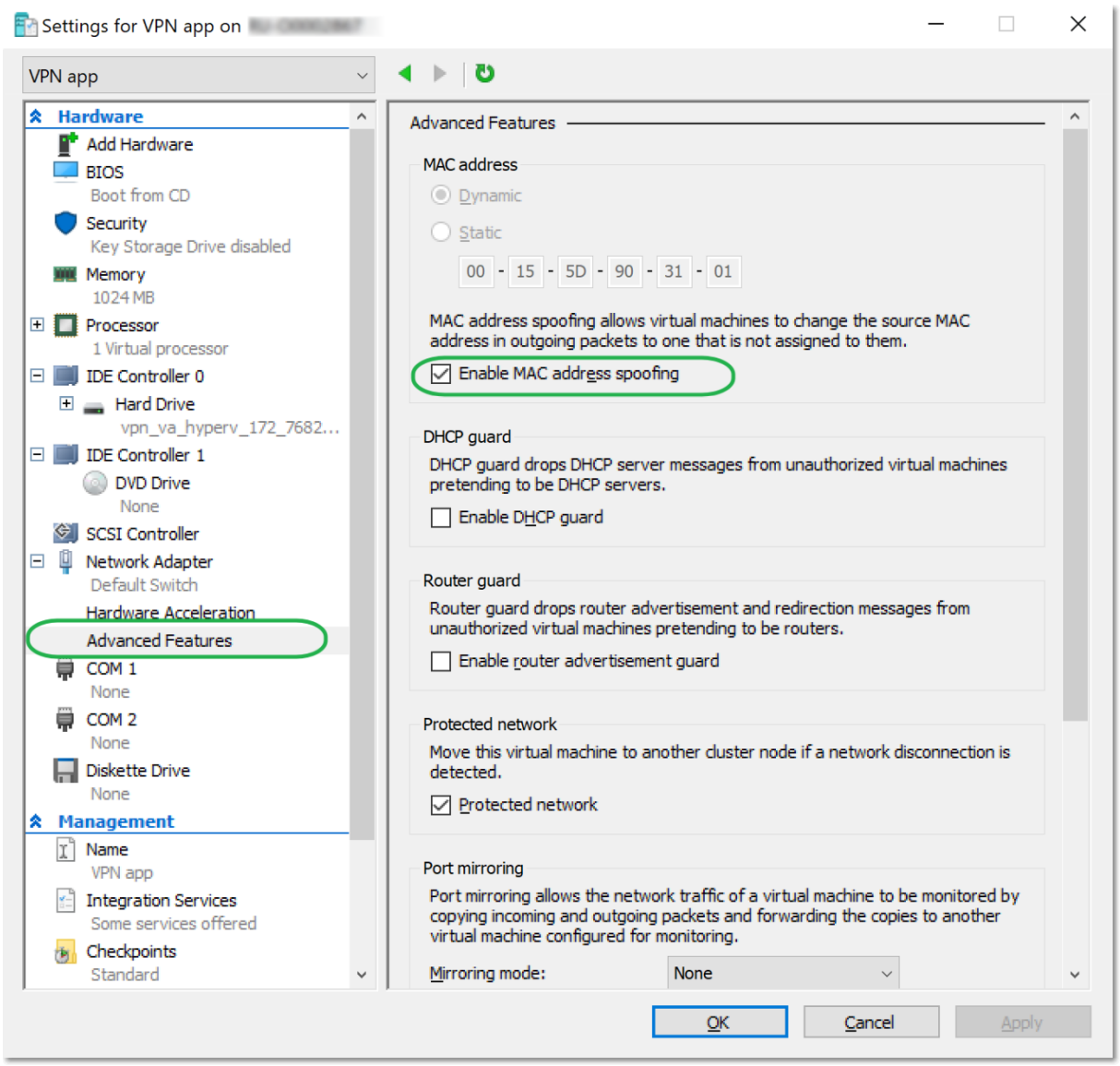


   Stellen Sie sicher, dass die Einstellungen für**IP-Adresse**,**Standard-Gateway**, und **Bevorzugter DNS-Server** vorhanden und korrekt sind. Beachten Sie, dass die **Internet**- und **Gateway**-Einstellungen auf der linken Seite der Tabelle für eine erfolgreiche Appliance-Registrierung auf **Verfügbar** stehen müssen. Überprüfen Sie anderenfalls Ihre Standard-Gateway- und DNS-Verfügbarkeitseinstellungen, bevor Sie mit der Registrierung fortfahren – oder legen Sie die IP-Adresse manuell fest.
9. Wählen Sie den Befehl **Registrieren** aus dem Menü aus und klicken Sie dann auf **Eingeben**.
10. Sie werden aufgefordert, die URL-Adresse des Cyber Protection Service anzugeben. Geben Sie dieselbe URL ein, die Sie für den Zugriff auf die Cyber Protect-Konsole verwenden.

11. Spezifizieren Sie Ihre Kunden-Administrator-Anmeldedaten für die Cyber Protect-Konsole.

Hinweis
Wenn für Ihr Konto eine Zwei-Faktor-Authentifizierung konfiguriert ist, werden Sie auch aufgefordert, den TOTP-Code einzugeben. Wenn die Zwei-Faktor-Authentifizierung aktiviert, aber für Ihr Konto nicht konfiguriert ist, können Sie die VPN-Appliance nicht registrieren. Zuerst müssen Sie zur Anmeldeseite der Cyber Protect-Konsole gehen und die Konfiguration der Zwei-Faktor-Authentifizierung für Ihr Konto abschließen. Weitere Informationen zur Zwei-Faktor-Authentifizierung finden Sie in der **Anleitung für Kunden-Administratoren**.

12. Drücken Sie auf**J**, um die Einstellungen zu bestätigen und den Registrierungsprozess zu starten.
13. Nach einem erfolgreichen Registrierungsprozess wird Ihnen die VPN-Appliance in der Cyber Protect-Konsole angezeigt.
14. Aktivieren Sie den 'Promiscuous-Modus', um sicherzustellen, dass die Netzwerkreplikationsfunktionalität ordnungsgemäß aktiviert ist:
    a. Öffnen Sie den Hyper-V Manager.
    b. Klicken Sie mit der rechten Maustaste auf Ihre VPN-Appliance-VM und wählen Sie **Einstellungen**.
    c. Wählen Sie im Bereich **Netzwerkadapter** –> **Erweiterte Funktionen** die Option **Spoofing von MAC-Adressen aktivieren**.



Sie haben eine sichere Site-to-Site-VPN-Verbindung zwischen Ihrem lokalen Standort und der Cloud-Recovery-Site konfiguriert. Jetzt können Sie einen Recovery-Server für Ihre lokale Maschine erstellen und überprüfen, ob und wie Failover und Failback funktionieren. Weitere Informationen dazu finden Sie in der **Anleitung für Cyber Disaster Recovery Cloud-Administratoren**.