Cyber Disaster Recovery Cloud

24.03

Guida di avvio rapido

REVISIONE:11/04/2024

Sommario

Come configurare Cyber Disaster Recovery Cloud su un PC con Hyper-V

Non è necessario disporre di un server per testare le funzionalità principali di Cyber Disaster Recovery Cloud. È infatti possibile configurare il servizio Cyber Disaster Recovery Cloud sulla macchina in uso e valutarne il funzionamento.

Prerequisiti:

- È necessario disporre di un account come amministratore del cliente in Cyber Protect Cloud.
- Il sistema operativo installato nel PC deve essere Windows 10 Pro, Windows 10 Enterprise o Windows 10 Education.

Per distribuire il servizio Cyber Disaster Recovery Cloud sul proprio PC, attenersi alla seguente procedura:

1. Attivare Hyper-V nel PC.
2. Creare una macchina virtuale (VM) da utilizzare come macchina di origine per il test.
3. Distribuire l'appliance VPN sul PC.

Passaggio 1. Attivare il servizio Hyper-V nel PC e preparare l'immagine del sistema operativo.

1. Attivare il servizio Hyper-V nel PC. Seguire le istruzioni disponibili nel sito web di Microsoft.
2. Scaricare l'immagine del sistema operativo per l'istallazione nella MV. Ad esempio, scaricare l'immagine ubuntu-18.04.2-desktop-amd64.iso dal sito ufficiale di Ubuntu.

Passaggio 2. Creare una macchina virtuale che sarà la macchina di origine di cui verrà eseguito il backup.

1. Aprire Hyper-V Manager e creare una macchina virtuale di cui verrà eseguito il backup e che verrà utilizzata per testare il servizio Cyber Disaster Recovery Cloud:
   a. Fare clic con il pulsante destro sull'host e selezionare **Nuova** > **Macchina virtuale**. Seguire le istruzioni della procedura guidata, considerando che la **memoria di avvio** deve essere pari almeno a 4096 MB e che **Connessione** deve essere **l'opzione predefinita**.
   b. Eseguire la macchina virtuale appena creata, connettersi ad essa e quindi avviare l'istallazione del sistema operativo.
2. Installare l'agente di protezione nella macchina virtuale appena creata:
   a. Nella macchina virtuale aprire un browser.
   b. Accedere alla console di Cyber Protect come amministratore del cliente.

c. Nella sezione **Dispositivi** aggiungere la macchina virtuale facendo clic su **Aggiungi**, quindi selezionare l'agente di protezione per un server Linux. Viene eseguito il download dell'agente di protezione nella macchina virtuale.

d. Aprire la console e installare innanzitutto i pacchetti aggiuntivi. Utilizzare il comando seguente:

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

a. Aprire la cartella **Download**, modificare le autorizzazioni affinché il file di installazione dell'agente di protezione sia eseguibile e quindi eseguire il file.

```
cd Downloads
```

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

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

a. Attenersi alle istruzioni della procedura di installazione. Nell'ultimo passaggio selezionare **Visualizza informazioni di registrazione**. Viene visualizzato il link da aprire nel browser e il codice di registrazione da specificare durante la registrazione del sistema nella console di Cyber Protect.

b. La virtual machine viene registrata nella console di Cyber Protect. Creare il piano di protezione e il backup dell'intero sistema. Tale backup verrà utilizzato per creare un server di ripristino in un secondo momento.

Passaggio 3. Distribuire l'appliance VPN sul PC.

Per distribuire l'appliance VPN sul PC, attenersi alla seguente procedura:

1. Nel PC, accedere alla console di Cyber Protect come amministratore del cliente.
2. Passare a **Disaster Recovery** > **Connessione**, quindi fare clic su **Configura**. Si apre la procedura guidata per la configurazione della connessione.
3. Selezionare **Connessione da sito a sito** quindi fare clic su **Avvio**.
   Il sistema avvia la distribuzione del gateway di connessione nel cloud. L'operazione potrebbe richiedere qualche minuto. Nel frattempo, è possibile procedere al passaggio successivo.
4. Fare clic su **Download e distribuzione**. Scaricare l'archivio con l'appliance VPN per Hyper-V (file .vhd), decomprimere l'archivio e quindi distribuirlo nell'ambiente locale:
   a. Aprire Hyper-V Manager, fare clic con il pulsante destro sull'host e selezionare **Nuova** > **Macchina virtuale**.
   b. Specificare un nome descrittivo per la MV, ad esempio MV appliance VPN.
   c. Seguire le istruzioni della procedura guidata, considerando che **Connessione** deve essere **l'opzione predefinita**.

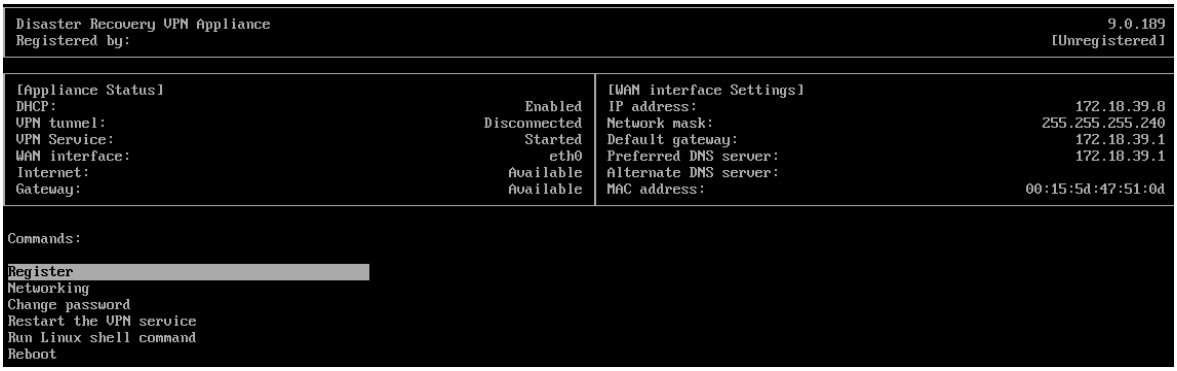
d. Nel passaggio per la **connessione del disco rigido virtuale**, selezionare l'opzione **Use an existing virtual hard disk (Utilizza un disco rigido virtuale esistente)**. Selezionare il file dell'appliance VPN scaricato.

e. Completare la creazione della MV.

5. Connettere l'appliance alle reti di produzione.
6. Eseguire la MV appliance VPN e connettersi ad essa.
7. Una volta completato l'avvio dell'appliance, viene visualizzato il prompt di accesso. Accedere all'appliance con le credenziali seguenti:

   Login: admin

   Password: admin
8. Viene visualizzata una pagina d'avvio simile alla seguente:

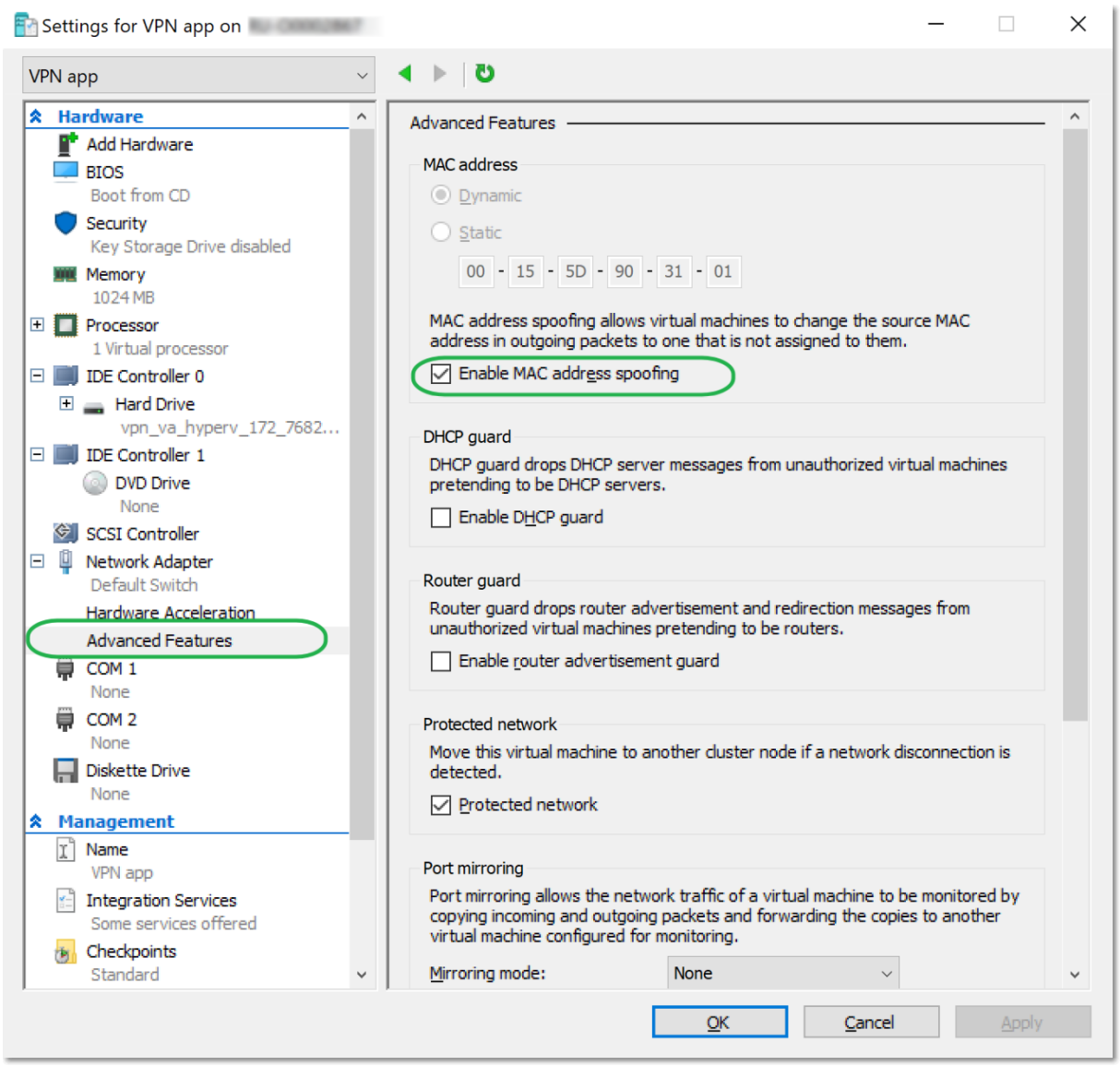


   Verificare che le impostazioni **Indirizzo IP**, **Gateway predefinito** e **Server DNS preferito** siano complete e corrette. Tenere presente che le impostazioni **Internet** e **Gateway** sul lato sinistro della tabella devono essere impostate su **Disponibile** affinché la registrazione dell'appliance abbia esito positivo. In caso contrario, consultare le impostazioni del Gateway predefinito e della disponibilità del DNS prima di procedere con la registrazione o di impostare manualmente l'indirizzo IP.
9. Nel menu selezionare **Registra** e fare clic su **Invio**.
10. Verrà richiesto di fornire l'indirizzo URL del servizio Cyber Protection. Immettere lo stesso URL utilizzato per accedere alla console di Cyber Protect.

11. Specificare le credenziali di amministratore del cliente per la console di Cyber Protect.

Nota
Se per l'account è stata configurata l'autenticazione a due fattori, verrà chiesto di inserire il codice TOTP. Se l'autenticazione a due fattori è abilitata ma non configurata per l'account, non è possibile registrare l'appliance VPN. È necessario innanzitutto aprire la pagina di login della console di Cyber Protect e completare la configurazione dell'autenticazione a due fattori per l'account. Per ulteriori dettagli sull'autenticazione a due fattori, consultare la **Guida dell'amministratore del cliente**.

12. Fare clic su **S** per confermare le impostazioni e avviare la procedura di registrazione.
13. Dopo aver completato la procedura di registrazione, l'appliance VPN viene visualizzata nella console di Cyber Protect.
14. Abilitare la modalità promiscua per verificare che la funzionalità di replica della rete sia attivata:
    a. Aprire Hyper-V Manager.
    b. Fare clic con il pulsante destro del mouse sulla MV appliance VPN e selezionare **Impostazioni**.
    c. Nella sezione **Adattatore di rete** > **Funzionalità avanzate**, selezionare l'opzione **Abilita lo spoofing degli indirizzi MAC**.



È stata configurata una connessione VPN sicura da sito a sito tra il sito locale e il sito di ripristino nel cloud. Ora è possibile creare un server di ripristino per il sistema locale e verificare il funzionamento del failover e del failback. Per ulteriori informazioni, fare riferimento alla **Guida dell'amministratore di Cyber Disaster Recovery Cloud**.