Cyber Disaster Recovery Cloud

24.04

Instrukcja szybkiego rozpoczęcia pracy

WERSJA:09.05.2024

Spis treści

Jak skonfigurować usługę Cyber Disaster Recovery Cloud na komputerze PC z usługą Hyper-V

Nie trzeba mieć serwera, aby móc przetestować główne funkcje usługi Cyber Disaster Recovery Cloud. Usługę Cyber Disaster Recovery Cloud można łatwo skonfigurować na komputerze PC i tam wypróbować jej funkcje.

Wymagania wstępne:

- Masz konto administratora klienta na platformie Cyber Protect Cloud.
- Na komputerze musi być zainstalowany system operacyjny Windows 10 Pro, Windows 10 Enterprise lub Windows 10 Education.

Aby wdrożyć usługę Cyber Disaster Recovery Cloud na komputerze PC:

1. Aktywuj na komputerze usługę Hyper-V.
2. Utwórz maszynę wirtualną, której użyjesz do testów w charakterze komputera źródłowego.
3. Wdróż na komputerze PC urządzenie VPN.

Krok 1. Aktywuj na komputerze usługę Hyper-V i przygotuj obraz systemu operacyjnego.

1. Aktywuj na komputerze usługę Hyper-V. Postępuj zgodnie z instrukcjami podanymi w tej witrynie internetowej firmy Microsoft.
2. Pobierz obraz systemu operacyjnego do zainstalowania na maszynie wirtualnej. Na przykład pobierz obraz Ubuntu-18.04.2-desktop-amd64.iso z oficjalnej witryny internetowej systemu Ubuntu.

Krok 2. Utwórz maszynę wirtualną, która będzie komputerem źródłowym, którego kopię zapasową należy utworzyć.

1. Otwórz Menedżera funkcji Hyper-V i utwórz maszynę wirtualną, którą chcesz uwzględnić w kopii zapasowej i wykorzystać do testów usługi Cyber Disaster Recovery Cloud:
   a. Kliknij host prawym przyciskiem myszy i wybierz **Nowe** > **Maszyna wirtualna**. Postępuj zgodnie z instrukcjami kreatora, pamiętając, że **Pamięć początkowa** musi mieć co najmniej 4096 MB, a w polu **Połączenie** trzeba wybrać ustawienie **Przełącznik domyślny**.
   b. Uruchom nowo utworzoną maszynę wirtualną, nawiąż z nią połączenie, a następnie uruchom instalację systemu operacyjnego.
2. Zainstaluj agenta ochrony na nowo utworzonej maszynie wirtualnej:

a. Na maszynie wirtualnej otwórz przeglądarkę.

b. Zaloguj się do konsoli Cyber Protect jako administrator klienta.

c. W sekcji **Urządzenia** dodaj maszynę wirtualną, klikając **Dodaj**, a następnie wybierz agenta ochrony dla serwera Linux. W wyniku tych działań na maszynę wirtualną zostanie pobrany agent ochrony.

d. Otwórz konsolę i najpierw zainstaluj dodatkowe pakiety. Użyj następującego polecenia:

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

a. Otwórz folder **Pobrane**, zmień uprawnienia do pliku instalacyjnego agenta ochrony, a następnie uruchom ten plik.

```
cd Downloads
```

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

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

a. Postępuj zgodnie z instrukcjami kreatora. W ostatnim kroku wybierz **Pokaż informacje rejestracyjne**. Pojawi się łącze, które należy otworzyć w przeglądarce, i kod rejestracji, który należy podać podczas rejestracji maszyny w konsoli Cyber Protect.

b. W wyniku tych działań maszyna wirtualna zostanie zarejestrowana w konsoli Cyber Protect. Utwórz plan ochrony i zrób kopię zapasową całej maszyny. Ta kopia zapasowa zostanie później wykorzystana do utworzenia serwera odzyskiwania.

Krok 3. Wdróż na komputerze urządzenie VPN.

Aby wdrożyć urządzenie VPN na komputerze PC:

1. Na komputerze zaloguj się do konsoli Cyber Protect jako administrator klienta.
2. Wybierz **Odzyskiwanie po awarii** > **Łączność** i kliknij **Konfiguruj**. Zostanie otwarty kreator konfiguracji łączności.
3. Wybierz **Połączenie site-to-site** i kliknij **Rozpocznij**.
   System rozpocznie wdrażanie bramy łączności w chmurze. Potrwa to jakiś czas. W międzyczasie możesz przejść do następnego kroku.
4. Kliknij **Pobierz i wdróż**. Pobierz archiwum za pomocą urządzenia VPN dla usługi Hyper-V (plik .vhd), rozpakuj archiwum, a następnie wdróż je w środowisku lokalnym:
   a. Otwórz Menedżera funkcji Hyper-V, kliknij host prawym przyciskiem myszy i wybierz **Nowe** > **Maszyna wirtualna**.
   b. Nadaj maszynie wirtualnej opisową nazwę (na przykład VM z urządzeniem VPN).
   c. Postępuj zgodnie z instrukcjami kreatora, pamiętając, że w polu **Połączenie** trzeba wybrać ustawienie **Przełącznik domyślny**.

d. W kroku **Podłączanie wirtualnego dysku twardego** wybierz opcję **Użyj istniejącego wirtualnego dysku twardego**. Wskaż pobrany plik urządzenia VPN.

e. Dokończ tworzenie maszyny wirtualnej.

5. Podłącz urządzenie do sieci produkcyjnych.
6. Uruchom maszynę wirtualną urządzenia VPN i nawiąż z nią połączenie.
7. Po uruchomieniu urządzenia i pojawieniu się monitu logowania zaloguj się do urządzenia przy użyciu następujących poświadczeń:

   Nazwa logowania: admin

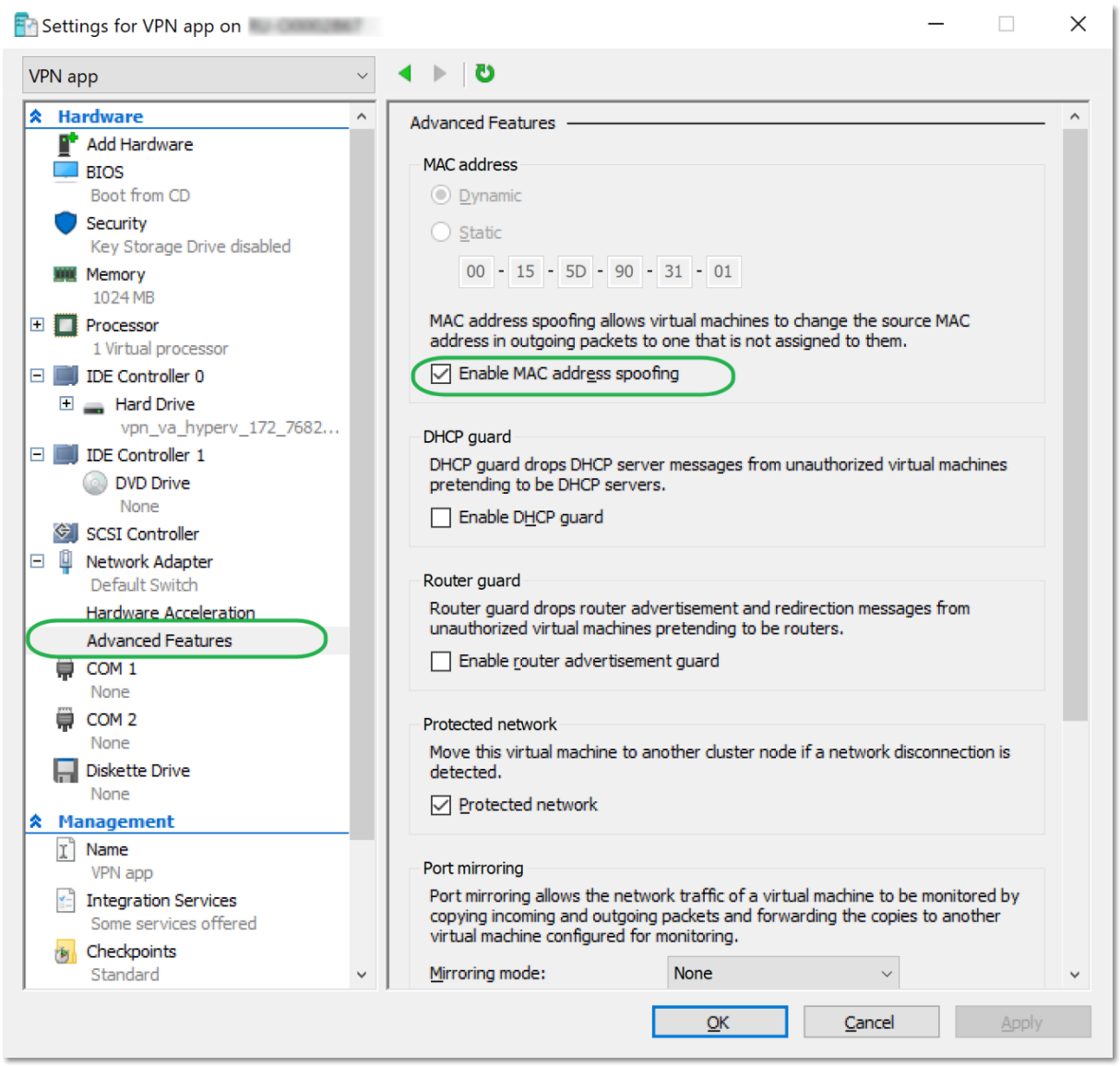
   Hasło: admin
8. Zostanie wyświetlona strona początkowa podobna do następującej:

   Upewnij się, że ustawienia **Adres IP**, **Brama domyślna** i **Preferowany serwer DNS** są poprawnie skonfigurowane. Pamiętaj, że w celu pomyślnej rejestracji urządzenia ustawienia **Internet** i **Brama** z lewej strony tabeli muszą mieć wartość **Dostępne**. Jeśli nie ma takiej konfiguracji, sprawdź ustawienia dostępności bramy domyślnej i serwera DNS, zanim będziesz kontynuować rejestrację, lub ręcznie ustaw adres IP.
9. Wybierz **Zarejestruj** z menu i naciśnij klawisz **Enter**.
10. Zostanie wyświetlony monit o wprowadzenie adresu URL usługi Cyber Protection. Wprowadź ten sam adres URL, którego używasz w celu uzyskania dostępu do konsoli Cyber Protect.

11. Podaj poświadczenia administratora klienta umożliwiające uzyskanie dostępu do konsoli Cyber Protect.

Uwaga
Jeśli na koncie jest skonfigurowane uwierzytelnianie dwuskładnikowe, pojawi się również monit o wprowadzenie kodu TOTP. Jeśli uwierzytelnianie dwuskładnikowe jest włączone, ale nie jest skonfigurowane na koncie, nie można zarejestrować urządzenia VPN. Najpierw trzeba przejść do strony logowania się do konsoli Cyber Protect i skonfigurować na koncie uwierzytelnianie dwuskładnikowe. Więcej informacji na temat uwierzytelniania dwuskładnikowego można znaleźć w **Podręczniku administratora klienta**.

12. Naciśnij **T**, aby potwierdzić ustawienia i rozpocząć proces rejestracji.
13. Po pomyślnym ukończeniu procesu rejestracji urządzenie VPN pojawi się w konsoli Cyber Protect.
14. Włącz tryb nieograniczony, aby się upewnić, że funkcja replikacji przez sieć będzie odpowiednio działać:
    a. Otwórz Menedżera funkcji Hyper-V.
    b. Kliknij prawym przyciskiem myszy urządzenie VPN i wybierz **Ustawienia**.
    c. W sekcji **Karta sieciowa** > **Funkcje zaawansowane** zaznacz opcję **Włącz fałszowanie adresów MAC**.



Teraz masz skonfigurowane bezpieczne połączenie VPN site-to-site między lokalizacją lokalną i lokalizacją odzyskiwania w chmurze. Możesz utworzyć serwer odzyskiwania dla komputera lokalnego i sprawdzić, jak działa przełączanie awaryjne i powrót po awarii. Więcej informacji można znaleźć w **Podręcznik administratora programu Cyber Disaster Recovery Cloud**.