Cyber Disaster Recovery Cloud

24.03



快速入門指南

版本:2024/4/10



如何使用 Hyper-V 在 PC 上設定 Cyber Disaster Recovery Cloud	3
步驟 1。在 PC 上啟用 Hyper-V 服務,並準備作業系統映像。	3
步驟 2。建立將當做要備份之來源電腦的虛擬機器。	3
步驟 3。在 PC 上部署 VPN 設備。	4

如何使用 Hyper-V 在 PC 上設定 Cyber Disaster Recovery Cloud

您不需要擁有伺服器,就可以測試 Cyber Disaster Recovery Cloud 主要功能。您可以在 PC 上輕鬆設 定 Cyber Disaster Recovery Cloud 服務,並評估其功能。

必要條件:

- 您在 Cyber Protect Cloud 有一個客戶系統管理員帳戶。
- PC上的作業系統必須是 Windows 10 專業版、Windows 10 企業版或 Windows 10 教育版。

若要在 PC 上部署 Cyber Disaster Recovery Cloud 服務, 請執行下列操作:

- 1. 在 PC 上啟用 Hyper-V。
- 2. 建立要當做來源電腦使用的虛擬機器 (VM) 以供測試之用。
- 3. 在 PC 上部署 VPN 設備。

步驟1。在PC上啟用 Hyper-V 服務, 並準備作業系統映像。

- 1. 在 PC 上啟用 Hyper-V 服務。請依照 Microsoft 網站上的指示進行。
- 2. 下載作業系統映像以安裝到 VM 中。例如, 從 Ubuntu 官方網站下載 ubuntu-18.04.2-desktopamd64.iso。

步驟2。建立將當做要備份之來源電腦的虛擬機器。

- 開啟 Hyper-V Manager, 並建立您將備份並用於測試 Cyber Disaster Recovery Cloud 服務的虛擬 機器:
 - a. 以滑鼠右鍵按一下您的主機,然後選取[新增]>[虛擬機器]。依照精靈的步驟進行,並將啟動 記憶體必須至少 4096 MB 且 [Connection] (連線)必須是 [Default Switch] (預設交換器) 納 入考量。
 - b. 執行新建立的 VM、連線到該 VM, 然後啟動作業系統安裝。
- 2. 在新建立的虛擬機器中安裝保護代理程式:
 - a. 在您的虛擬機器上,開啟瀏覽器。
 - b. 以客戶系統管理員的身分, 登入 Cyber Protect 主控台。
 - c. 在 [裝置] 區段中, 按一下 [新增] 來新增虛擬機器, 然後選取適用於 Linux 伺服器的保護代理 程式。因此, 保護代理程式會下載到您的虛擬機器。
 - d. 開啟主控台, 然後先安裝其他套件。使用下列命令:

sudo apt-get install rpm gcc make -y

a. 開啟 [下載] 資料夾、將保護代理程式安裝檔案的權限變更為可執行, 然後執行此檔案。

cd Downloads

sudo chmod +x Cyber_Protection_Agent_for_Linux_x86_64.bin

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

- a. 依照安裝精靈的步驟進行。在最後一個步驟,選取[顯示註冊資訊]。您將會看到要在瀏覽器 中開啟的連結,以及必須在 Cyber Protect 主控台中註冊電腦時指定的註冊碼。
- b. 因此, Cyber Protect 主控台中會註冊您的虛擬機器。建立保護計劃及整部電腦的備份。此備 份將用於之後建立復原伺服器。

步驟3。在PC上部署VPN設備。

若要在 PC 上部署 VPN 設備, 請執行下列操作:

- 1. 在 PC上,以客戶系統管理員的身分,登入 Cyber Protect 主控台。
- 2. 移至 [災難復原] > [連線], 然後按一下 [設定]。連線設定精靈將會開啟。
- 3. 選取[站台對站台連線],然後按一下[啟動]。

系統會開始在雲端部署連線閘道,這將需要一些時間。此時,您可以繼續進行下一個步驟。

- 4. 按一下 [下載並部署]。使用 Hyper-V 的 VPN 設備下載存檔 (.vhd 檔案)、解壓縮存檔, 然後將其部 署到本機環境中:
 - a. 開啟 Hyper-V Manager、以滑鼠右鍵按一下您的主機, 然後選取 [新增] > [虛擬機器]。
 - b. 指定 VM 的描述性名稱 (例如, VPN 設備 VM)。
 - c. 依照精靈的步驟進行,並將 [Connection] (連線) 必須設為 [Default Switch] (預設交換器) 納入考量。
 - d. 在 [Connect Virtual Hard Disk] (連線虛擬硬碟)步驟中, 選取 [Use an existing virtual hard disk] (使用現有的虛擬硬碟) 選項。選取已下載的 VPN 設備檔案。
 - e. 完成 VM 的建立。
- 5. 將設備連線至實際執行網路。
- 6. 執行 VPN 設備 VM, 並連線到該 VM。
- 7. 一旦設備啟動且登入提示出現之後,使用下列認證登入設備:

登入:admin

密碼:admin

8. 您將會看到一個類似如下的起始頁面:

		9.0.189 [Unregistered]
	[WAN interface Settings]	
Enabled	IP address:	172.18.39.8
Disconnected	Network mask:	255.255.255.240
Started	Default gateway:	172.18.39.1
eth0	Preferred DNS server:	172.18.39.1
Available	Alternate DNS server:	
Available	MAC address:	00:15:5d:47:51:0d
	Enabled Disconnected Started eth0 Available Available	Enabled Disconnected Started eth0 Available Available

請確認已填入[IP 位址]、[預設閘道],以及[慣用的 DNS 伺服器] 設定且正確無誤。請注意,表格 左側的[網際網路] 和[閘道] 設定必須適用於成功設備登錄。否則,請檢查您的[預設閘道] 和 [DNS 可用性] 設定,然後再繼續登錄,或手動設定 IP 位址。

- 9. 從功能表中選取[登錄],然後按一下[進入]。
- 10. 系統將提示您輸入 Cyber Protection 服務 URL 位址。輸入您用來存取 Cyber Protect 主控台的相同 URL。

Disaster Recovery VPN Appliance Registered by:	9.0.189 [Unregistered]
Command: Register	
Usage: <up>, <down> - to select parameter <esc> - to cancel the command</esc></down></up>	
Backup service address: https://beta-cloud.acronis.com_ Login: Password:	

11. 指定 Cyber Protect 主控台的客戶系統管理員認證。

注意事項

如果為您的帳戶設定雙重驗證機制,系統也將提示您輸入 TOTP 代碼。如左已啟用雙重驗證機制,但尚未為您的帳戶是定,則您無法登錄 VPN 設備。首先,您必須移至 Cyber Protect 主控台 登入頁面,並為您的帳戶完成雙重驗證機制設定。如需有關雙重驗證機制的更多詳細資訊,請 參閱客戶系統管理員指南。

- 12. 按下Y可確認設定並開始登錄程序。
- 13. 註冊程序成功之後,您將會在 Cyber Protect 主控台中看到您的 VPN 裝置。
- 14. 啟用混合模式以確保正確啟用網路複寫功能:
 - a. 開啟 Hyper-V Manager。
 - b. 以滑鼠右鍵按一下您的 VPN 設備 VM, 然後選取 [設定]。
 - c. 在 [網路卡] > [進階功能] 區段, 選取 [啟用 MAC 位址詐騙] 選項。

2	Settings for VPN app on	67	— —	×
VP	N арр	~	∢ ▶ ບັ	
*	Hardware	^	Advanced Features	^
	Add Hardware			
	BIOS		MAC address	
	Boot from CD		Dynamic	
	Security		○ <u>S</u> tatic	
	Memory		00 - 15 - 5D - 90 - 31 - 01	
	1024 MB			
+	Processor		MAC address spoofing allows virtual machines to change the source MAC	
	1 Virtual processor		address in outgoing packets to one that is not assigned to them.	
-	IDE Controller 0		✓ Enable MAC address spoofing	
	Hard Drive			
_	vpn_va_hyperv_1/2_/682		DHCP guard	
	IDE Controller 1		DHCP guard drops DHCP server messages from unauthorized virtual machines	
	None		pretending to be DHCP servers.	
			Enable D <u>H</u> CP guard	
	Network Adapter			
_	Default Switch		Router guard	
	Hardware Acceleration		Router guard drops router advertisement and redirection messages from	
C	Advanced Features		unauthorized virtual machines pretending to be routers.	
	🛱 COM 1		Enable router advertisement guard	
	None			
	COM 2		Protected network	
	None		Move this virtual machine to another cluster node if a network disconnection is	
	Diskette Drive		detected.	
	Management		Protected network	
^	T Name	-		
	VPN app		Port mirroring	
	Integration Services		Port mirroring allows the network traffic of a virtual machine to be monitored by	
	Some services offered		copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring	
	ᡖ Checkpoints		vir dar machine configured for monitorility.	
	Standard	~	Mirroring mode: None ~	~
			OK Cancel And	

您已經在本機站台和雲端復原站台之間設定一個安全的站台對站台 VPN 連線。現在您可以為您的本機電腦建立復原伺服器,並檢查容錯移轉和容錯回復的運作方式。如需詳細資訊,請參閱 Cyber Disaster Recovery Cloud 系統管理員指南。