

Cyber Disaster Recovery Cloud

24.03



目录

如何在 PC 上使用 Hyper-V 设置 Cyber Disaster Recovery Cloud	3
第 1 步,在 PC 上激活 Hyper-V 服务 , 然后准备操作系统映像。	3
第 2 步,创建将作为要备份的源计算机的虚拟机。	3
第 3 步,在 PC 上部署 VPN 设备。	4

如何在 PC 上使用 Hyper-V 设置 Cyber Disaster Recovery Cloud

无需拥有服务器即可测试 Cyber Disaster Recovery Cloud 的主要功能。可以在 PC 上轻松设置 Cyber Disaster Recovery Cloud 服务并评估其功能。

先决条件：

- 您在 Cyber Protect Cloud 中拥有一个客户管理员帐户。
- PC 上的操作系统必须是 Windows 10 Pro、Windows 10 Enterprise 或 Windows 10 Education。

要在 PC 上部署 Cyber Disaster Recovery Cloud 服务，请执行以下操作：

1. 在 PC 上激活 Hyper-V。
2. 创建要用作测试的源计算机的虚拟机 (VM)。
3. 在 PC 上部署 VPN 设备。

第 1 步.在 PC 上激活 Hyper-V 服务，然后准备操作系统映像。

1. 在 PC 上激活 Hyper-V 服务。按照 [Microsoft 网站](#) 上的说明进行操作。
2. 下载用于安装到 VM 的操作系统映像。例如，从官方 Ubuntu 网站下载 ubuntu-18.04.2-desktop-amd64.iso。

第 2 步.创建将作为要备份的源计算机的虚拟机。

1. 打开 Hyper-V Manager，然后创建要备份并用于测试 Cyber Disaster Recovery Cloud 服务的虚拟机：
 - a. 右键单击主机，并依次选择**新建 > 虚拟机**。按照向导步骤操作，同时考虑到**启动内存**必须至少为 4096 MB，并且**连接**必须是**默认交换机**。
 - b. 运行新创建的 VM，连接到该 VM，然后启动操作系统安装。
2. 在新创建的虚拟机中安装保护代理程序：
 - a. 在虚拟机上，打开浏览器。
 - b. 以客户管理员身份登录到 Cyber Protect 中控台。
 - c. 在“**设备**”部分，单击“**添加**”以添加虚拟机，然后为 Linux 服务器选择保护代理程序。结果，系统会将保护代理程序下载到虚拟机。
 - d. 打开中控台，然后先安装其他程序包。使用以下命令：

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

- a. 打开**下载**文件夹、将保护代理程序安装文件的权限更改为“可执行”，然后运行该文件。

```
cd Downloads
```

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

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

- a. 按照安装向导步骤操作。在最后一步, 选择**显示注册信息**。您将看到要在浏览器中打开的链接, 以及在 Cyber Protect 中控台中注册计算机时必须指定的注册码。
- b. 结果, 虚拟机注册在 Cyber Protect 中控台中。创建保护计划和整个计算机的备份。此备份稍后将用于创建恢复服务器。

第 3 步.在 PC 上部署 VPN 设备。

要在 PC 上部署 VPN 设备, 请执行以下操作:

1. 在 PC 上, 以客户管理员身份登录到 Cyber Protect 中控台。
2. 转到**灾难恢复 > 连接**, 然后单击**配置**。连接配置向导将打开。
3. 选择**站点到站点连接**, 然后单击**开始**。
系统开始在云中部署连接网关, 这需要一些时间。与此同时, 您可以继续进行下一步。
4. 单击**下载和部署**。使用适用于 Hyper-V 的 VPN 设备下载存档 (.vhd file), 解压缩该存档, 然后将它部署到本地环境中:
 - a. 打开 Hyper-V Manager, 右键单击主机, 然后依次选择**新建 > 虚拟机**。
 - b. 为 VM 指定描述性名称(例如, VPN 设备 VM)。
 - c. 按照向导步骤操作, 同时考虑到**连接**必须设置为**默认交换机**。
 - d. 在**连接虚拟硬盘**步骤中, 选择**使用现有虚拟硬盘**选项。选择已下载的 VPN 设备文件。
 - e. 完成创建 VM。
5. 将设备连接到生产网络。
6. 运行 VPN 设备 VM, 并与它连接。
7. 在设备启动并显示登录提示后, 使用以下凭据登录设备:
登录名:admin
密码:admin
8. 您会看到类似于以下屏幕的起始页:

```
Disaster Recovery VPN Appliance                                     9.0.189
Registered by:                                                     [Unregistered]

[Appliance Status]
DHCP: Enabled
VPN tunnel: Disconnected
VPN Service: Started
WAN interface: eth0
Internet: Available
Gateway: Available

[WAN interface Settings]
IP address: 172.18.39.8
Network mask: 255.255.255.240
Default gateway: 172.18.39.1
Preferred DNS server: 172.18.39.1
Alternate DNS server:
MAC address: 00:15:5d:47:51:0d

Commands:
Register
Networking
Change password
Restart the VPN service
Run Linux shell command
Reboot
```

请确保 **IP 地址**、**默认网关**和**首选 DNS 服务器**设置已准备就绪并准确无误。请注意, 表格左侧的 **Internet** 和**网关**设置必须为**可用**, 才能成功注册设备。否则, 请在继续注册之前检查默认网关和 DNS 可用性设置, 或者手动设置 IP 地址。

9. 从菜单中选择**注册**, 然后单击 **Enter** 键。

- 系统将提示您输入 Cyber Protection 服务的 URL 地址。输入要用于访问 Cyber Protect 中控台的相同 URL。

```
Disaster Recovery VPN Appliance                                     9.0.189
Registered by:                                                     [Unregistered]

Command: Register

Usage:
<Up>, <Down> - to select parameter
<Esc> - to cancel the command

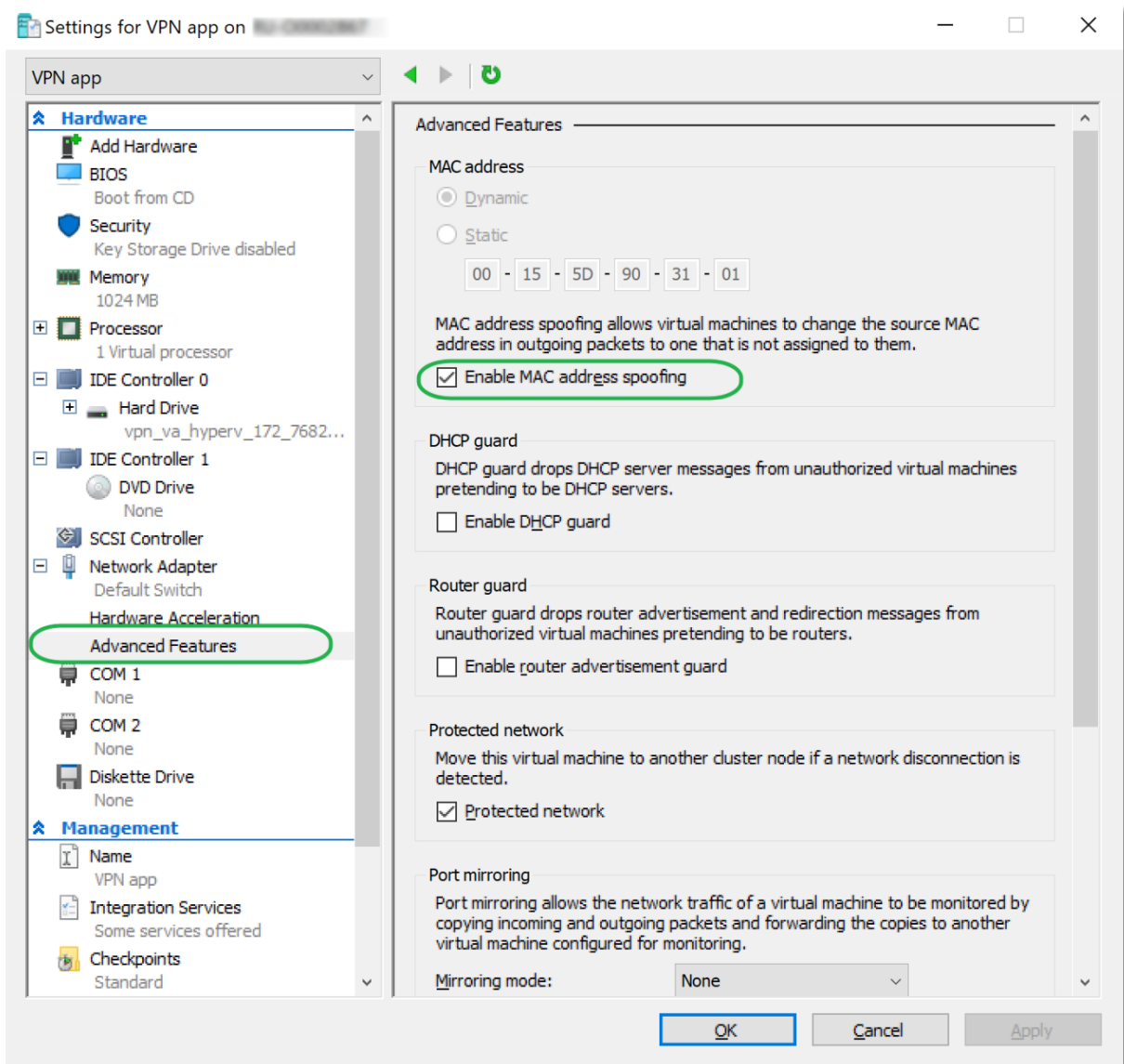
Backup service address: https://beta-cloud.acronis.com_
Login:
Password:
```

- 指定 Cyber Protect 中控台的客户管理员凭据。

注意

如果您的帐户配置了双重身份验证, 则系统还会提示您输入 TOTP 代码。如果启用了双重身份验证, 但未为您的帐户进行配置, 则无法注册 VPN 设备。首先, 必须转到 Cyber Protect 中控台登录页面并完成您帐户的双重身份验证配置。有关双重身份验证的更多详细信息, 请转到“**客户管理员指南**”。

- 按 **Y** 键以确认设置, 然后开始注册过程。
- 在成功注册后, 您会在 Cyber Protect 中控台看到您的 VPN 设备。
- 启用“混杂”模式, 以确保网络复制功能得以正确启用:
 - 打开 Hyper-V Manager。
 - 右键单击 VPN 设备 VM, 并选择**设置**。
 - 在**网络适配器** > **高级功能**部分中, 选择启用 **MAC 地址欺骗**选项。



您已在本地站点和云恢复站点之间配置了安全的站点到站点 VPN 连接。现在, 可以为本地计算机创建恢复服务器, 以及检查故障转移和故障恢复的工作方式。有关更多详细信息, 请参阅 **Cyber Disaster Recovery Cloud 管理员指南**。