Cyber Disaster Recovery Cloud

25.06

Quick Start Guide

REVISION: 6/24/2025

Table of contents

How to set up Disaster Recovery on your PC with Hyper-V **3**

Step 1. Activate the Hyper-V service on your PC and prepare the OS image. 3

Step 2. Create a virtual machine that will be your source machine to be backed up. 3

Step 3. Deploy the VPN appliance on your PC. 4

How to set up Disaster Recovery on your PC with Hyper-V

You do not have to own a server to test the Disaster Recovery main functionality. You can easily set up the Disaster Recovery service on your PC and evaluate its features.

Prerequisites:

- You have a customer administrator account in Cyber Protect Cloud.
- The operating system on your PC must be Windows 10 Pro, Windows 10 Enterprise, or Windows 10 Education.

To deploy the Disaster Recovery service on your PC, do the following:

1. Activate the Hyper-V on your PC.
2. Create a virtual machine (VM) to be used as a source machine for testing.
3. Deploy the VPN appliance on your PC.

Step 1. Activate the Hyper-V service on your PC and prepare the OS image.

1. Activate the Hyper-V service on your PC. Follow the instructions on the Microsoft website.
2. Download the OS image for installation into the VM. For example, download ubuntu-18.04.2-desktop-amd64.iso from the official Ubuntu website.

Step 2. Create a virtual machine that will be your source machine to be backed up.

1. Open the Hyper-V Manager and create a virtual machine that you are going to back up and use for testing the Disaster Recovery service:
   a. Right-click on your host and select **New** > **Virtual Machine**. Follow the wizard steps, taking into account that the **Startup memory** must be at least 4096 MB and the **Connection** must be the **Default Switch**.
   b. Run the newly created VM, connect to it, and then launch the OS installation.
2. Install the protection agent in the newly created virtual machine:
   a. On your virtual machine, open a browser.
   b. Log in to the Cyber Protect console as a customer administrator.
   c. In the **Devices** section, add the virtual machine by clicking **Add**, and then select the protection agent for a Linux server. As a result, the protection agent is downloaded to your virtual machine.
   d. Open the console and first install the additional packages. Use the following command:

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

a. Open the **Downloads** folder, change the permissions for the protection agent installation file to be executable, and then run this file.

```
cd Downloads
```

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

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

a. Follow the installation wizard steps. At the last step, select **Show registration info**. You will see the link to be opened in the browser and the registration code that must be specified when registering the machine in the Cyber Protect console.
b. As a result, your virtual machine is registered in the Cyber Protect console. Create the protection plan and the backup of the entire machine. This backup will be used for creating a recovery server later.

Step 3. Deploy the VPN appliance on your PC.

To deploy the VPN appliance on your PC, do the following:

1. On your PC, log in to the Cyber Protect console as a customer administrator.
2. Go to **Disaster Recovery** > **Connectivity**, and then click **Configure**. The connectivity configuration wizard will open.
3. Select **Site-to-site connection** and click **Start**.
   The system starts deploying the connectivity gateway in the cloud, this will take some time. Meanwhile, you can proceed to the next step.
4. Click **Download and deploy**. Download the archive with the VPN appliance for Hyper-V (.vhd file), unpack the archive, and then deploy it to your local environment:
   a. Open the Hyper-V Manager, right-click on your host, and then select **New** > **Virtual Machine**.
   b. Specify the descriptive name for a VM (for example, VPN appliance VM).
   c. Follow the wizard steps, taking into account that the **Connection** must be set to **Default Switch**.
   d. On the **Connect Virtual Hard Disk** step, select the **Use an existing virtual hard disk** option. Select the downloaded VPN appliance file.
   e. Complete VM creation.
5. Connect the appliance to the production networks.
6. Run the VPN appliance VM and connect to it.
7. Once the appliance boots up and the login prompt appears, log in to the appliance with the following credentials:
   Login: admin
   Password: admin
8. You will see a start page similar to the following:

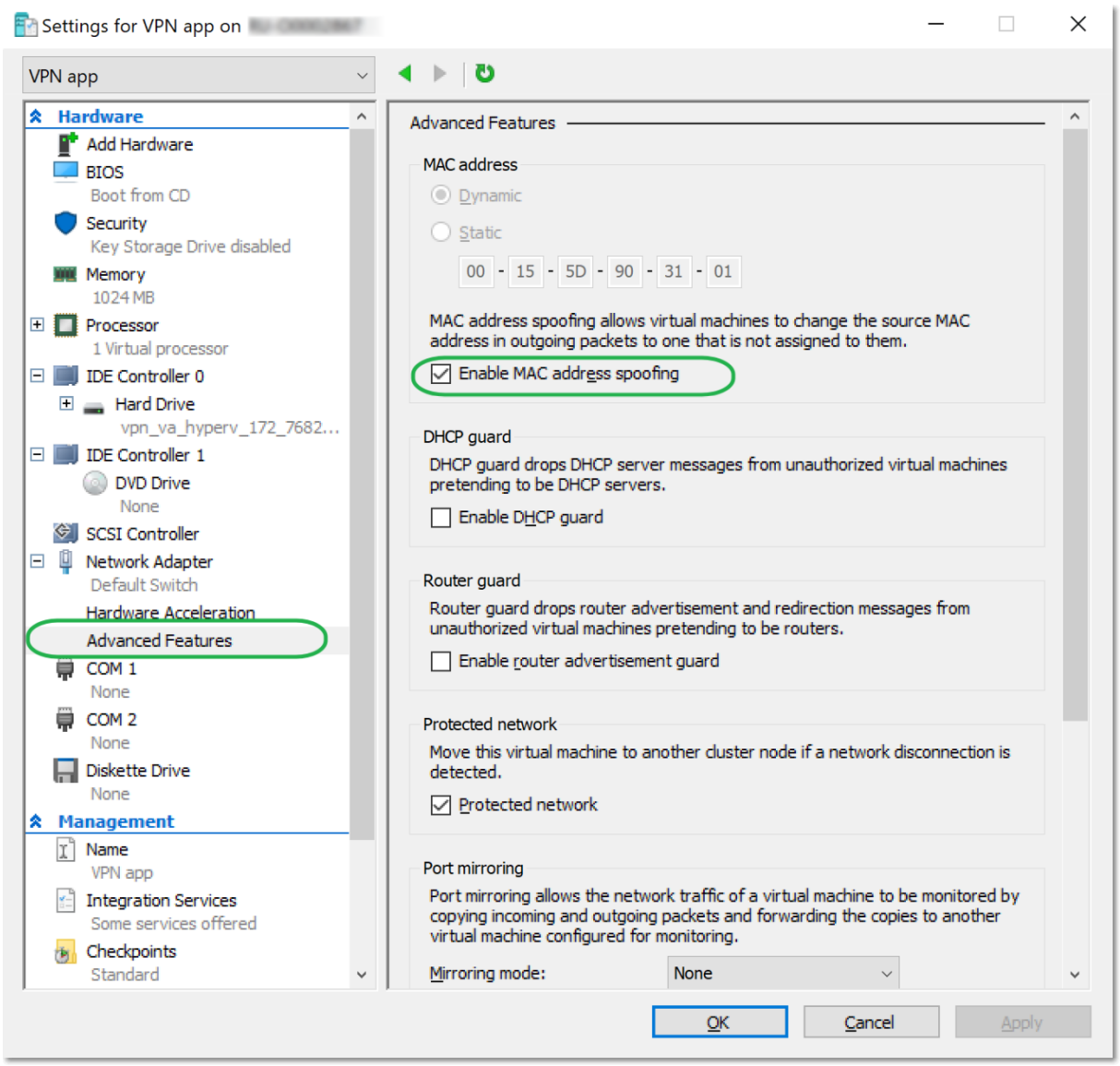
Make sure that the **IP address**, **Default gateway**, and **Preferred DNS server** settings are in place and correct. Note that the **Internet** and **Gateway** settings on the left side of the table must be **Available** for a successful appliance registration. Otherwise, please check your Default gateway and DNS availability settings before proceeding with registration or set the IP address manually.

9. Select **Register** from the menu and click **Enter**.
10. You will be prompted to enter the Cyber Protection service URL address. Enter the same URL you are using to access the Cyber Protect console.

11. Specify your customer administrator credentials for the Cyber Protect console.

Note
If two-factor authentication is configured for your account, you will also be prompted to enter the TOTP code. If two-factor authentication is enabled but not configured for your account, you cannot register the VPN appliance. First, you must go to the Cyber Protect console login page and complete the two-factor authentication configuration for your account. For more details on two-factor authentication, go to the **Customer Administrator's Guide**.

12. Press**Y**to confirm the settings and start the registration process.
13. After a successful registration process, you will see your VPN appliance in the Cyber Protect console.
14. Enable the promiscuous mode to make sure that the network replication functionality is properly enabled:
    a. Open the Hyper-V Manager.
    b. Right-click on your VPN appliance VM and select **Settings**.
    c. In the **Network Adapter** > **Advanced Features** section, select the **Enable MAC address spoofing** option.



You have configured a secure site-to-site VPN connection between your local site and the cloud recovery site. Now you can create a recovery server for your local machine and check how failover and failback work. For more details, refer to the **Disaster Recovery Administrator's Guide**.